POLYNOMIALS IN FINITE GEOMETRY

Peter Sziklai

20 February, 2008
-1 Special foreword

Before the real Foreword, let me say some words about this book. It is ready in the sense that this is the topic that I wanted to write about and this is how I wanted to write about it. Naturally, this book is not finished in the sense that (i) it is about an active field of mathematics, which changes rapidly; (ii) if you have worked on a book for years then it is hard to stop it: every day you can have a new idea how to slightly improve it; (iii) no editor/referees have seen it yet, hence there may (must!) be typos, inaccuracies, missing citations, line overflow errors... left. It would be nice to increase the number of figures as well.

However, I think that in the current state of this volume it is possible to decide about its values and shortcomings. Although I understand that it can be evaluated by this current version, in the spirit of (i) and (ii) above I will keep an updated version on the secret, unlinked webpage http://www.cs.elte.hu/~sziklai/poly.html, (where I will enlist all the changes performed, too), just for pleasure. When a decision of publication is reached, the editors of the publisher can decide between this and a possibly updated version.

0 Foreword

A most efficient way of investigating combinatorially defined pointsets of projective spaces over finite fields is associating polynomials to them. This technique was first used by Jamison and Bruen, then, followed by several people, became a standard method; nowadays, the contours of a growing theory can be seen already.

The polynomials we use should reflect the combinatorial properties of the pointset, then we have to be equipped with enough means to handle our polynomials and get an algebraic description about them; finally, we have to translate the information gained back to the original, geometric language.

The first investigations in this field examined the coefficients of the polynomials, and this idea proved to be very efficient. Then the derivatives of the polynomials came into the play and solving (differential) equations over finite fields; a third branch of results considered the polynomials as algebraic curves. The idea of associating algebraic curves to pointsets goes back to Segre, recently a bunch of new applications have shown the strength of this method. Finally, due to Gács’s recent results, dimension arguments on polynomial spaces have become fruitful.

This book is an attempt to collect and classify the most interesting ways of applying polynomials in finite geometry.

We focus on combinatorially defined (point)sets of projective geometries. They are defined by their intersection numbers with lines (or other subspaces) typically, like arcs, blocking sets, nuclei, caps, ovoids, etc. Here we do not want to give a
complete account on them, however some of the best results will be presented.
In order to show a wider scope of different applications, some other fields are
gently touched like group theory, graph theory, etc.

This book is divided into chapters. The first one (Background) contains selected
tools for a finite geometer, from the basic facts to some theory of polynomials over
finite fields; proofs are only provided when they are short or interesting for us. We
provide slightly more information than the essential background for the second
chapter. After the basic facts (Section 5) the most useful representations of affine
and projective spaces are presented (6), then we introduce our main tool, the Rédei
polynomial associated to pointsets (7,8). The coefficients of Rédei polynomials are
elementary symmetric polynomials themselves, what we need to know about them
and other invariants of subsets of fields or spaces is collected in Section 9. The
multivariate polynomials associated to pointsets can be considered as algebraic
varieties, so we can use some basic parts of algebraic geometry (10). Finally, in
Section 11 some background needed for stability results is presented.

The second (and main) chapter contains several results of finite Galois geometry,
where polynomials play a main role. We start with general results on intersection
terms of planar pointsets (12,13). Then we turn to special cases as arcs, max-
imal arcs, unitals, semi ovals, untouchable sets. (14-17). The next highlight is the
topic of directions (18,19) and blocking sets (20-22). Section 23 shows the new
resultant method for stability results. Affine blocking sets and nuclei are consid-
ered in sections 24,25. Section 26 introduces an interesting mixed representation.
Stability theorems for flocks, some basic facts for spreads and a nice result on
ovoids is proved in Sections 27,28. Finally some non-geometrical applications are
collected in Section 29.

The last chapter contains hints and solutions for the exercises.
# Contents

-1 Special foreword ........................................ iii  
0 Foreword ..................................................... iii  
1 Introduction ............................................... 1  
2 Acknowledgements ......................................... 2  
3 Definitions, basic notation ............................... 3  

## 1 Background ............................................ 5  
5 Finite fields and polynomials ............................. 5  
  5.1 Some basic facts ........................................ 5  
  5.2 Self-dual normal bases ................................. 6  
  5.3 Polynomials ........................................... 6  
  5.4 Differentiating polynomials ........................... 8  
  5.5 Polynomials vanishing at many points, Alon’s Combinatorial Nullstellensatz and the Ball-Serra refinement .... 9  
  5.6 Additive, linearized polynomials ..................... 16  
  5.7 The random-like behaviour ........................... 17  
  5.8 Lacunary polynomials ................................ 19  
6 Representations of affine and projective geometries ... 22  
  6.1 Subspaces, subgeometries ............................ 24  
  6.2 Transformations ....................................... 25  
7 The Rédei polynomial and its derivatives ............... 26  
  7.1 The Rédei polynomial ................................. 26  
  7.2 Differentiation in general ............................ 30  
  7.3 Hasse derivatives of the Rédei polynomial .......... 32  
  7.4 Examples ............................................ 33  
8 Univariate representations ................................ 35
### Contents

8.1 The affine polynomial and its derivatives .................................................. 36
8.2 The projective polynomial .............................................................................. 37
8.3 Examples ........................................................................................................... 38
9 Symmetric polynomials and invariants of subsets .............................................. 39
  9.1 The Newton formulae ....................................................................................... 39
  9.2 The invariants $u_f, v_f$ and $w_f$ ................................................................. 43
  9.3 Arbitrary subsets ............................................................................................ 47
  9.4 The generalized formulae ................................................................................. 51
  9.5 Resultants ....................................................................................................... 54
10 Elements of algebraic geometry ......................................................................... 61
  10.1 Conditions implying linear (or low-degree) components .............................. 65
11 Finding the missing factors, removing the surplus factors ................................. 68

2 Polynomials in geometry .................................................................................... 71
  12 Lines meeting a pointset .................................................................................. 71
    12.1 Prescribing the intersection numbers ....................................................... 71
    12.2 A general result .......................................................................................... 72
    12.3 Another immediate corollary ...................................................................... 73
  13 Sets with constant intersection numbers mod $p$ .......................................... 74
    13.1 Sets with intersection numbers $0$ mod $r$ ............................................... 76
    13.2 Small and large super-Vandermonde sets ............................................... 80
  14 Arcs, Segre ....................................................................................................... 85
  15 Maximal arcs ................................................................................................... 89
    15.1 Existence: hyperovals ............................................................................... 89
    15.2 Non-existence ............................................................................................ 93
    15.3 Embeddability ............................................................................................ 96
  16 Unitals, semiovals ............................................................................................ 98
  17 Sets without tangents: where Segre meets Rédei ............................................ 102
    17.1 The proof using Segre’s method ............................................................... 103
    17.2 Untouchable sets in Galois planes of even order ...................................... 109
  18 Directions ........................................................................................................ 110
    18.1 When $D$ is (contained in) a subgroup of $GF(q)^*$ ................................ 112
    18.2 When $D$ is (contained in) a subgroup of $\sqrt[q^2-1]{\mathbb{F}} \subset GF(q^2)^*$ . 115
    18.3 Sets determining $\leq \frac{q^2+1}{q+1}$ directions: affine linear pointsets ......... 115
    18.4 Small blocking sets of Rédei type are linear ............................................ 116
Contents

19 Over prime fields: the Gács method ......................................................... 122
   19.1 Permutation polynomials ................................................................. 124
   19.2 Directions in the plane ................................................................. 125
   19.3 Linear combinations of three permutation polynomials ................. 131

20 Projective linear pointsets ................................................................. 134

21 Blocking sets ......................................................................................... 136
   21.1 One curve ....................................................................................... 140
   21.2 Three new curves ........................................................................... 144
   21.3 Three old curves ........................................................................... 147
   21.4 Small blocking sets ......................................................................... 149

22 Multiple blocking sets ............................................................................ 154
   22.1 A \( t \mod p \) result ......................................................................... 155

23 Stability ................................................................................................. 162
   23.1 Stability theorems for small blocking sets and the Szönyi-Weiner method ................................................................. 164
   23.2 Stability theorems for blocking sets: the prime case ...................... 167
   23.3 Stability theorems for blocking sets: the non-prime case ............... 170
   23.4 Stability theorem for sets of even type ........................................... 176
   23.5 Number of lines meeting a \((q + 2)\)-set ......................................... 179

24 Jamison, Brouwer-Schrijver, affine blocking sets .................................. 180
   24.1 Applications of the punctured Nullstellensatz ............................... 184
   24.2 Rédei polynomials in three indeterminates ..................................... 189
   24.3 Rédei polynomials in many indeterminates ................................... 191
   24.4 Affine blocking sets ....................................................................... 195

25 Nuclei and affine blocking sets .............................................................. 198
   25.1 Lower nuclei ................................................................................... 201
   25.2 Internal nuclei ................................................................................ 203
   25.3 Higher dimensions ......................................................................... 203

26 Mixed representations ............................................................................. 205

27 Flocks ...................................................................................................... 207
   27.1 Partial flocks of the quadratic cone in \( PG(3, q) \) ......................... 208
   27.2 Partial flocks of cones of higher degree ....................................... 211

28 Spreads and ovoids .................................................................................. 214
   28.1 Spreads ......................................................................................... 214
   28.2 Ovoids ......................................................................................... 215
29 Non-geometrical applications

29.1 Normal factorizations of Abelian groups

29.2 The Paley graph

29.3 Representing systems

29.4 Wielandt’s visibility theorem

29.5 Burnside’s theorem

29.6 Jaeger’s conjecture

29.7 Graphs containing $p$-regular subgraphs

29.8 Blokhuis’ proof of Bollobás’ theorem

29.9 Alon-Füredi

29.10 Chevalley-Warning

29.11 Cauchy-Davenport

29.12 Another application

3 Hints and short solutions to the exercises

1 Of Chapter I

2 Of Chapter II

4 Glossary of concepts

5 Notation

Index

References
1 Introduction

This one is not intended to be an introductory textbook about finite geometries, finite fields nor polynomials. There are very good books of these kinds available, e.g. Ball-Weiner [23] for a smooth and fascinating introduction to the concepts of finite geometries, the three volumes of Hirschfeld and Hirshfeld-Thas [77, 78, 79] as handbooks and Lidl-Niederreiter [90] for finite fields. Still, the interested reader, even with a little background, may find all the definitions and basic information here (the Glossary of concepts at the end of the volume can help) to enjoy this interdisciplinary field in the overlap of geometry, combinatorics and algebra.

We would like to use a common terminology. Parts and reformulations of results of some interest for non-geometers will be emphasized.

Bruen and Fisher called the polynomial technique as “the Jamison method” and summarized it in performing three steps: (1) Rephrase the theorem to be proved as a relationship involving sets of points in an affine space. (2) Formulate the theorem in terms of polynomials over a finite field. (3) Calculate. (Obviously, step 3 carries most of the difficulties in general.) In some sense it is still “the method”, we will show several ways how to perform steps 1-3.

We have to mention the book of László Rédei [103] from 1970, which inspired a new series of results on blocking sets and directions in the nineties.

There are a few survey papers on polynomial methods, by Blokhuis [35, 36], Szőnyi [122], Ball [7], I included here some of their material. The form of a book allows to show the algebraic background in more details; also to insert the most recent results.

The typical theories in this book have the following character. Define a class of (point)sets (of a geometry) in a combinatorial way (which, in general, means restrictions on the intersections with subspaces); examine its numerical parameters (usually the spectrum of sizes in the class); find the minimal/maximal values of the spectrum; characterize the extremal entities of the class; show that the extremal (or other interesting) ones are “stable” in the sense that there are no entities of the class being “close” to the extremal ones.

There are some fundamental concepts and ideas that we feel worth to put into light all along this treatise:

- an algebraic curve (or envelope) containing all the “interesting” lines of a pointset;
- the Lemma of tangents with its generalizations and analogues;
- resultants as sophisticated tools improving the simple use of Bézout’s theorem;
- examination of (lacunary) coefficients of polynomials;
Introduction

• considering (sub)spaces generated by polynomials.

Apology. There are some theorems being proved more than once in this book, these multiple proofs were included in order to show how the different ideas and techniques can lead to the same result; sometimes they even serve as touchstones of a new method.

Also, this book contains a few proofs being longer than the usual ones. They were included to show some elaborate series of ideas that lead to practical use of polynomial techniques.

There are exercises, like a hundred and twenty. One type of them is for the necessary technicalities where no further idea is needed (so boring but useful), another type is where an argument analogous to the preceding ones can solve the question (so good to practice), and a third type which needs minor new ideas (so the interesting ones). We provide short solutions for a great part of them at the end of the volume.

There are side comments on the margins. They might help reading, the editors/referees are kindly asked to decide whether they should be (i) left as they are, or (ii) included into the normal text, or (iii) the number of them can be increased (I would be happy to add more).

2 Acknowledgements

Most of this book is about the work of Simeon Ball, Aart Blokhuis, András Gács, Tamás Szőnyi and Zsuzsa Weiner. They, together with the author, contributed in roughly one half of the references; also their results (and sometimes even their texts with minor modifications: thanks to them for letting me do so) form an important part of this volume. Not least, I always enjoyed their warm, joyful, inspiring and supporting company in various situations in the last some years. I hope that the selection and the choice of the topics covered in this book makes them happy as well, and that being the “topic” of a book is at least as funny as writing it. Most of them have seen a preliminary version of it, I am grateful for all the suggestions they made.

Above all I am deeply indebted to Tamás Szőnyi, from whom most of my knowledge and most of my enthusiasm for finite geometries I have learned.

It was Gábor Korchmáros who suggested (and not only to me) some seven years ago to write a book like this. Probably any of us, or maybe someone else, could have done it. Of course this one is about the way how I can see the topic.

Last but not least I am grateful to all the colleagues and friends who helped me in any sense in the last some years: researchers of Ghent (and among them my multiple coauthor Leo Storme), Potenza, Naples, Barcelona, Eindhoven and, of course, Budapest.
3. Definitions, basic notation

We will not be very strict and consistent in the notation (but at least we’ll try to be). However, here we give a short description of the typical notation we are going to use.

If not specified differently, \( q = p^h \) is a prime power, \( p \) is a prime, and we work in the Desarguesian projective (or affine) space \( \mathbb{P}G(n, q) \) (\( \mathbb{A}G(n, q) \), resp.), each space coordinatized by the finite (Galois) field \( \mathbb{F}G(q) \). The \( n \)-dimensional vectorspace over \( \mathbb{F}G(q) \) will be denoted by \( \mathbb{V}G(n, q) \) or simply by \( \mathbb{F}G^n \). When discussing \( \mathbb{P}G(n, q) \) and the related \( \mathbb{V}G(n+1, q) \) together then for a subspace dimension \( rank=dim+1 \) will be meant projectively while vector space dimension will be called \( rank \). A field, which is not necessarily finite will be denoted by \( \mathbb{F} \).

In general capital letters \( X, Y, Z, T, ... \) will denote independent variables, while \( x, y, z, t, ... \) will be elements of \( \mathbb{F}G(q) \). A pair or triple of variables or elements in any pair of brackets can be meant homogeneously, hopefully it will be always clear from the context and the actual setting.

We write \( \mathbb{X} \) or \( \mathbb{V} = (X, Y, Z, ..., T) \) meaning as many variables as needed; \( \mathbb{V}^q = (X^q, Y^q, Z^q, ...) \). As over a finite field of order \( q \) for each \( x \in \mathbb{F}G(q) \) \( x^q = x \) holds, two different polynomials, \( f \) and \( g \), in one or more variables, can have coinciding values “everywhere” over \( \mathbb{F}G(q) \). In this case we ought to write \( f \equiv g \), as for univariate polynomials \( f(X), g(X) \) it means that \( f \equiv g \mod X^q - X \) in the ring \( \mathbb{F}G(q)[X] \). However, as in the literature \( f \equiv g \) is used in the sense ‘\( f \) and \( g \) are equal as polynomials’, we will use it in the same sense; though simply \( f = g \) and \( f(X) = g(X) \) may denote the same.

Throughout this book we mostly use the usual representation of \( \mathbb{P}G(n, q) \). This means that the points have homogeneous coordinates \( (x, y, z, ..., t) \) where \( x, y, z, ..., t \) are elements of \( \mathbb{F}G(q) \). The hyperplane \( [a, b, c, ..., d] \) of the space have equation \( aX + bY + cZ + ... + dT = 0 \).

When \( \mathbb{P}G(n, q) \) is considered as \( \mathbb{A}G(n, q) \) plus the hyperplane at infinity, then we will use the notation \( H_\infty \) for that (‘ideal’) hyperplane. If \( n = 2 \) then \( H_\infty \) is called the line at infinity \( \ell_\infty \).

According to the standard terminology, a line meeting a pointset in one point will be called a tangent and a line intersecting it in \( r \) points is an \( r \)-secant (or a line of length \( r \)).

This book is about combinatorially defined (point)sets of (mainly projective or affine) finite geometries. They are defined by their intersection numbers with lines (or other subspaces) typically. The most important definitions and basic information are collected in the Glossary of concepts at the end of this book. These are: blocking sets, arcs, nuclei, spreads, sets of even type, etc.

Warning. In this book a curve is allowed to have multiple components, so in fact the curves considered here are called cycles in a different terminology.
Introduction
Chapter 1

Background

5 Finite fields and polynomials

5.1 Some basic facts

Here the basic facts about finite fields are collected. For more see [90].

For any prime \( p \) and any positive integer \( h \) there exists a unique finite field (or Galois field) \( \text{GF}(q) \) of size \( q = p^h \). The prime \( p \) is the characteristic of it, meaning
\[
a + a + ... + a = 0 \quad \text{for any } a \in \text{GF}(q) \quad \text{whenever the number of } a \text{‘} s \text{ in the sum is (divisible by) } p.
\]
The additive group of \( \text{GF}(q) \) is elementary abelian, i.e. \((\mathbb{Z}_p, +)^h\) while the non-zero elements form a cyclic multiplicative group \( \text{GF}(q)^* \simeq \mathbb{Z}_{q-1} \), any generating element (often denoted by \( \omega \)) of it is called a primitive element of the field.

For any \( a \in \text{GF}(q) \) \( a^q = a \) holds, so the field elements are precisely the roots of \( X^q - X \). (Lucas’ theorem implies, see below, that) we have \( (a + b)^p = a^p + b^p \) for any \( a, b \in \text{GF}(q) \), so \( x \mapsto x^p \) is a field automorphism. \( \text{GF}(q) \) has a (unique) subfield \( \text{GF}(p^t) \) for each \( t \mid h \); \( \text{GF}(q) \) is an \( h/t \)-dimensional vectorspace over its subfield \( \text{GF}(p^t) \).

The (Frobenius-) automorphisms of \( \text{GF}(q) \) are \( x \mapsto x^{p^t} \) for \( i = 0, 1, ..., h - 1 \), forming the complete, cyclic automorphism group of order \( h \). Hence \( x \mapsto x^{p^t} \) fixes the subfield \( \text{GF}(p^{	ext{gcd}(t,h)}) \) pointwise (and all the subfields setwise!); equivalently, \( (X^{p^t} - X)(X^q - X) \text{ iff } t|h.\)

One can see that for any \( k \) not divisible by \( (q - 1) \), \( \sum_{a \in \text{GF}(q)} a^k = 0. \) From this, if \( f : \text{GF}(q) \to \text{GF}(q) \) is a bijective function then \( \sum_{x \in \text{GF}(q)} f(x)^k = 0 \) for all \( k = 1, ..., q - 2 \). See also Dickson’s theorem.

We will frequently use Lucas’ theorem when calculating binomial coefficients \( \binom{n}{k} \) in finite characteristic, so “modulo \( p^r \)”:
\[
l = n_0 + n_1 p + n_2 p^2 + ... + n_r p^r, \quad k =\]

so if \( a \neq 0 \) then \( a^{q^e-1} = 1 \) and \( X^{q^e-1} - 1 \) is the root polynomial of \( \text{GF}(q)^* \)

write \( \text{GF}(q)^* = \{ \omega^0, \omega^1, ..., \omega^{q-2} \} \) and consider
\[
\sum_{i=0}^{q-2} \omega^i = \sum_{i=0}^{q-2} \omega^i = \omega^{q-1} - 1 = \frac{\omega^k(q-1) - 1}{\omega^k - 1}.
\]
Prove Lucas’ theorem!

Exercise 5.1. Prove Lucas’ theorem!

Exercise 5.2. Show that for and also Section 5.27

Exercise 5.1. We define the trace and norm functions on \( GF(q^{n}) \) as \( \text{Tr}_{q^{n} \to q}(X) = X + X^{q} + X^{q^{2}} + \cdots + X^{q^{n-1}} \) and \( \text{Norm}_{q^{n} \to q}(X) = X \cdot X^{q} \cdot X^{q^{2}} \cdots X^{q^{n-1}} \), so the sum and the product of all conjugates of the argument. Both maps \( GF(q^{n}) \) onto \( GF(q) \), the trace function is \( GF(q) \)-linear while the norm function is multiplicative.

Exercise 5.2. Show that \( \text{Tr} \) and \( \text{Norm} \) are in some sense unique, i.e. any \( GF(q) \)-linear function mapping \( GF(q^{n}) \) onto \( GF(q) \) can be written in the form \( \text{Tr}_{q^{n} \to q}(aX) \) with a suitable \( a \in GF(q^{n}) \) and any multiplicative function mapping \( GF(q^{n}) \) onto \( GF(q) \) can be written in the form \( \text{Norm}_{q^{n} \to q}(X^{a}) \) with a suitable integer \( a \). (See Exercise 5.27 and also Section 8.1 for \( \text{Tr} \)).

5.2 Self-dual normal bases

\( GF(q^{n}) \) is a vector-space over its subfield \( GF(q) \), so several bases can be chosen. There are some “natural choices” like normal bases of form \( \{ \omega, \omega^{q}, \omega^{q^{2}}, \ldots, \omega^{q^{n-1}} \} \), the conjugates of a certain primitive element. Another “nice requirement” is self-duality (with respect to the inner product \( \langle a, b \rangle = \text{Tr}_{q^{n} \to q}(ab) \)), i.e. the inner product of two basis elements \( b_{i} \) and \( b_{j} \) is \( \text{Tr}_{q^{n} \to q}(b_{i}b_{j}) = 0 \) if \( i \neq j \) and 1 if \( i = j \).

The following theorem answers the question whether self-dual normal bases exist.

Result 5.3. [89] For a prime power \( q \) and \( n > 1 \) a self-dual normal basis of \( GF(q^{n}) \) over \( GF(q) \) exists if and only if either \( n \) is odd, or \( n \equiv 2 \pmod{4} \) and \( q \) is even.

5.3 Polynomials

Here we summarize some properties of polynomials over finite fields. Given a field \( \mathbb{F} \), a polynomial \( f(X_{1}, X_{2}, \ldots, X_{k}) \) is a finite sum of monomial terms \( a_{i_{1}i_{2} \cdots i_{k}} X_{1}^{i_{1}} X_{2}^{i_{2}} \cdots X_{k}^{i_{k}} \), where each \( X_{i} \) is a free variable, \( a_{i_{1}i_{2} \cdots i_{k}} \), the coefficient of the term, is an element of \( \mathbb{F} \). The (total) degree of a monomial is \( i_{1} + i_{2} + \cdots + i_{k} \) if the coefficient is nonzero and \( -\infty \) otherwise. The (total) degree of \( f \), denoted by \( \deg f \) or \( f^{\circ} \), is the maximum of the degrees of its terms. These polynomials form the ring \( \mathbb{F}[X_{1}, X_{2}, \ldots, X_{k}] \). A polynomial is homogeneous if all terms have the same total degree. If \( f \) is not homogeneous then one can homogenize it, i.e. transform it to the following homogeneous form: \( Z^{\deg f} \cdot f(\frac{X_{1}}{Z}, \frac{X_{2}}{Z}, \ldots, \frac{X_{k}}{Z}) \), which is a polynomial again (\( Z \) is an additional free variable).
Given $f(X_1, ..., X_n) = \sum a_{i_1,...,i_n} X_1^{i_1} \cdots X_n^{i_n} \in F[X_1, ..., X_n]$, and the elements $x_1, ..., x_n \in F$ then one may substitute them into $f$: $f(x_1, ..., x_n) = \sum a_{i_1,...,i_n} x_1^{i_1} \cdots x_n^{i_n} \in F$; $(x_1, ..., x_n)$ is a root of $f$ if $f(x_1, ..., x_n) = 0$.

A polynomial $f$ may be written as a product of other polynomials, if not (except in a trivial way) then $f$ is irreducible. If we consider $f$ over $\overline{F}$, the algebraic closure of $F$, and it still cannot be written as a product of polynomials over $\overline{F}$ then $f$ is absolutely irreducible. E.g. $X^2 + 1 \in GF(3)[X]$ is irreducible but not absolutely irreducible, it splits to $(X + i)(X - i)$ over $GF(3)$ where $i^2 = -1$. $X^2 + Y^2 + 1 \in GF(3)[X, Y]$ is absolutely irreducible. Over the algebraic closure every univariate polynomial splits into linear factors.

In particular, $x$ is a root of $f(X)$ (of multiplicity $m$, see below) if $f(X)$ can be written as $f(X) = (X - x)^m \cdot g(X)$ for some polynomial $g(X)$, $m \geq 1$.

Over a field any polynomial can be written as a product of irreducible polynomials (factors) in an essentially unique way (so apart from constants and rearrangement).

Let $f : GF(q) \to GF(q)$ be a function. Then it can be represented by the linear combination

$$\forall x \in GF(q) \quad f(x) = \sum_{a \in GF(q)} f(a) \mu_a(x),$$

where

$$\mu_a(X) = 1 - (X - a)^{q-1}$$

is the characteristic function of the set $\{a\}$. In other terms it means that any function can be given as a polynomial of degree $\leq q - 1$. As both the number of functions $GF(q) \to GF(q)$ and polynomials in $GF(q)[X]$ of degree $\leq q - 1$ is $q^q$, this representation is unique.

Let now $f \in GF(q)[X]$. Then $f$, as a function, can be represented by a polynomial $\overline{f}$ of degree at most $q - 1$, this is called the reduced form of $f$. The degree of $\overline{f}$ will be called the reduced degree of $f$.

**Proposition 5.4.** For any (reduced) polynomial $f(X) = c_{q-1} X^{q-1} + \ldots + c_0$,

$$\sum_{x \in GF(q)} x^k f(x) = -c_{q-1} k_0,$$

where $k = t(q - 1) + k_0$, $0 \leq k_0 \leq q - 2$. In particular, $\sum_{x \in GF(q)} f(x) = -c_{q-1}$.

**Proof:** $\sum_{x} x^k f(x) = \sum_{x} \sum_{i=0}^{q-1} c_i x^{i+k} = \sum_{i=0}^{q-1} c_i \sum_{x} x^{i+k} = -c_{q-1} k_0$. \hfill \blacksquare

**Exercise 5.5.** If $f$ is bijective (permutation polynomial) then the reduced degree of $f^k$ is at most $q - 2$ for $k = 1, \ldots, q - 2$.

We note that (i) if $p \nmid |\{t : f(t) = 0\}|$ then the converse is true; see also Exercise 9.13, which is Dickson's...
If \( q = 2^h \) then the quadratic equation \( aX^2 + bX + c = 0 \) has no solution iff \( \text{Tr}_{2^h \rightarrow 2} \left( \frac{a}{b} \right) = 1 \).

Let’s examine \( \text{GF}(q)[X] \) as a vector space over \( \text{GF}(q) \).

Exercise 5.7. Gács [67] For any subspace \( V \) of \( \text{GF}(q)[X] \), \( \dim(V) = \left| \{ \deg(f) : f \in V \} \right| \).

Exercise 5.8. [56] Consider the space \( S_\lambda \) spanned as \( S_\lambda = \langle (X - a)^\lambda : a \in \text{GF}(q) \rangle \). Write \( \lambda = \sum_{i=0}^{h-1} \alpha_i p^i \), where \( 0 \leq \alpha_i < p \) and let \( M_\lambda = \{ \sum_{i=0}^{h-1} \beta_i p^i : 0 \leq \beta_i \leq \alpha_i \} \). Then \( S_\lambda \) has a basis \( \{ X^r : r \in M_\lambda \} \).

In several situations we will be interested in the zeros of (uni- or multivariate) polynomials. Let \( \mathbf{a} = (a_1, a_2, ..., a_n) \) be in \( \text{GF}(q)^n \). We shall refer to \( \mathbf{a} \) as a point in the \( n \)-dimensional vector space \( V(n, q) \) or affine space \( \text{AG}(n, q) \). Consider an \( f \) in \( \text{GF}(q)[X_1, ..., X_n] \), \( f = \sum \alpha_{i_1, i_2, ..., i_n} X_1^{i_1} \cdots X_n^{i_n} \).

We want to define the multiplicity of \( f \) at \( \mathbf{a} \). It is easy if \( \mathbf{a} = \mathbf{0} = (0, 0, ..., 0) \). Let \( m \) be the largest integer such that for every \( 0 \leq i_1, ..., i_n, i_1 + ... + i_n < m \) we have \( \alpha_{i_1, i_2, ..., i_n} = 0 \). Then we say that \( f \) has a zero at \( \mathbf{0} \) with multiplicity \( m \).

For general \( \mathbf{a} \) one can consider the suitable “translate” of \( f \), i.e. \( f_{\mathbf{a}}(Y_1, ..., Y_n) = f(Y_1 + a_1, Y_2 + a_2, ..., Y_n + a_n) \), and we say that \( f \) has a zero at \( \mathbf{a} \) with multiplicity \( m \) if and only if \( f_{\mathbf{a}} \) has a zero at \( \mathbf{0} \) with multiplicity \( m \).

5.4 Differentiating polynomials

Given a polynomial \( f(X) = \sum_{i=0}^{n} a_i X^i \), one can define its derivative \( \partial_X f = f_{X} = f’ \) in the following way: \( f’(X) = \sum_{i=0}^{n} i a_i X^{i-1} \). Note that if the characteristic \( p \) divides \( i \) then the term \( ia_i X^{i-1} \) vanishes. In particular \( \deg f’ < \deg f - 1 \) may occur. Multiple differentiation is denoted by \( \partial_X^m f = f^{(m)} \) or \( f^{(m)}, f’’ \), etc. If \( a \) is a root of \( f \) with multiplicity \( m \) then \( a \) will be a root of \( f’ \) with multiplicity at least \( m - 1 \), and of multiplicity at least \( m \) iff \( p \mid m \). Also if \( k \leq p \) then \( a \) is root of \( f \) with multiplicity at least \( k \) iff \( f^{(k)}(a) = 0 \) for \( i = 0, 1, ..., k - 1 \).

We will use the differential operator \( \nabla = (\partial_X, \partial_Y, \partial_Z) \) (when we have three variables) and maybe \( \nabla^i = (\partial_X^i, \partial_Y^i, \partial_Z^i) \) and probably \( \nabla_{i}^k = (\mathcal{H}_{X}^k, \mathcal{H}_{Y}^k, \mathcal{H}_{Z}^k) \), where \( \mathcal{H} \) stands for the \( i \)-th Hasse-derivation operator (see 7.3). The only properties we need are that \( \mathcal{H}^i X^k = \binom{i}{j} X^{k-j} \) if \( k \geq j \) (otherwise 0); \( \mathcal{H}^i \) is a linear operator; \( \mathcal{H}^i(fg) = \sum_{j=0}^{i} \mathcal{H}^j f \mathcal{H}^{i-j} g; a \) is root of \( f \) with multiplicity at least \( k \) iff \( \mathcal{H}^k f(a) = 0 \) for \( i = 0, 1, ..., k - 1 \); and finally \( \mathcal{H}^i \mathcal{H}^j = \binom{i+j}{i} \mathcal{H}^{i+j} \).
5. Finite fields and polynomials

We might use the following differential equation:

$$\mathbf{V} \cdot \nabla F = X \partial_X F + Y \partial_Y F + Z \partial_Z F = 0,$$

where $F = F(X,Y,Z)$ is a homogeneous polynomial in three variables, of total degree $n$. Let $F(X,Y,Z,\lambda) = F(\lambda X, \lambda Y, \lambda Z) = \lambda^n F(X,Y,Z)$, then

$$n \lambda^{n-1} F(X,Y,Z) = (\partial_\lambda \hat{F})(X,Y,Z,\lambda) = (X \partial_X F + Y \partial_Y F + Z \partial_Z F)(\lambda X, \lambda Y, \lambda Z).$$

It means that if we consider $\mathbf{V} \cdot \nabla F = 0$ as a polynomial equation then $(\partial_\lambda \hat{F})(X,Y,Z,\lambda) = 0$ identically, which holds if and only if $p$ divides $n = \deg(F)$. If we consider our equation as $(\mathbf{V} \cdot \nabla F)(x,y,z) = 0$ for all $(x,y,z) \in \mathbb{F}_p^3$, and $\deg(F)$ is not divisible by $p$, then the condition is that $F(x,y,z) = 0$ for every choice of $(x,y,z)$, i.e. $F \in \langle Y^q Z - Y Z^q, Z^q X - Z X^q, X^q Y - X Y^q \rangle$, see later.

5.5 Polynomials vanishing at many points, Alon’s Combinatorial Nullstellensatz and the Ball-Serra refinement

We will quite often get into a situation when our polynomials have many roots, sometimes they vanish almost everywhere in their domain. It was Bruns and later Alon who started to explore this situation; here we show some results of this kind. An incredible number of wonderful applications were found later, we will see some of the geometrical ones and in the last section some more non-geometrical ones as well. Recently Ball and Serra achieved a new improvement on Alon’s Nullstellensatz, (which promises new applications, in fact they found some already), we show that as well. Therefore this Section is essentially based on [1] and [22].

Exercise 5.9. Let $S$ be a subset of $\mathbb{F}_p^2$ and $f \in \mathbb{F}_p[X,Y]$, such that $f(aY + bY) = 0$, for all $(a,b) \in S$. If $|S| > \deg(f)$ then $f(X,Y) \equiv 0$.

Exercise 5.10.

- **Show that** $G(x_1, ..., x_n) = 0$ for all $(x_1, ..., x_n) \in \mathbb{F}_p^n$ if and only if $G$ is of form $g_1(X_1, ..., X_n) \cdot (X_1^n - 1) + ... + g_n(X_1, ..., X_n) \cdot (X_n^n - 1)$.

- **Similarly show that** $G(x_1, ..., x_n) = 0$ for all $(x_1, ..., x_n) \in \mathbb{F}_p^n$ if and only if $G \in \langle (X_1^{q-1} - 1), ..., (X_n^{q-1} - 1) \rangle$.

- **Show that all** $(x_1, ..., x_n) \in \mathbb{F}_p^n$ are $t$-fold zeros of $G(X_1, ..., X_n)$ if and only if $G$ is an element of the ideal

$$J_t = J_t(X_1, ..., X_n) = \langle (X_1^n - X_1)^{i_1} (X_2^n - X_2)^{i_2} ... (X_n^n - X_n)^{i_n} : i_1 + i_2 + ... + i_n = t \rangle.$$

- **Similarly show that** all $(x_1, ..., x_n) \in \mathbb{F}_p^n$ are $t$-fold zeros of $G(X_1, ..., X_n)$ iff $G \in \langle (X_1^{q-1} - 1)^{i_1} (X_2^{q-1} - 1)^{i_2} ... (X_n^{q-1} - 1)^{i_n} : i_1 + i_2 + ... + i_n = t \rangle$.

Theorem 5.11. Let $f \in \mathbb{F}_p[X_1, ..., X_n]$ satisfy $f(0,0,...,0) \neq 0$ and $f(a) = 0$ for all $a \neq 0$. Then $\deg(f) \geq n(q-1)$. 

Proof Let \( f(0) = c \neq 0 \) and \( g(x_1, \ldots, x_n) = \prod_{i=1}^n (1 - x_i^{q-1}) \). Then \( \frac{1}{c} f - g \) vanishes everywhere hence it is in \( J_1 \).

Exercise 5.12. Let \( t \) be a positive integer, and let the polynomial \( f \in \mathbb{GF}(q)[X_1, \ldots, X_n] \) satisfy \( f(0,0,\ldots,0) \neq 0 \) and \( \text{mult}_a f \geq t \) for all \( a \neq 0 \). Then \( \deg(f) \geq (n + t - 1)(q - 1) \).

Exercise 5.13. Give an example when in Exercise 5.12 \( \deg(f) = (n + t - 1)(q - 1) \) holds, for \( n + t - 1 \leq q + 1 \).

Exercise 5.14. Suppose that the curves \( C_1, \ldots, C_m \) cover \( AG(2,q) \setminus \{(0,0)\} \) but neither of them contains the origin. Then \( \sum_i \deg(C_i) \geq 2(q - 1) \).

Theorem 5.15. Let \( A, B \subseteq \mathbb{GF}(q)^* \). Let \( f(X,Y) \in \mathbb{GF}(q)[X,Y] \) satisfy (i) \( f(0,0) \neq 0 \) and (ii) \( f(a,b) = 0 \) whenever \( a \in A \) or \( b \in B \). Then \( f \) can be written as \( f = g + h \), where \( h \in J_1(X,Y) \), \( \deg(g) \leq \deg(f) \) and \( \deg(f) \geq |A| + |B| \).

Proof: Let’s reduce \( f \) modulo \( X^q - X \) and modulo \( Y^q - Y \), this gives \( f = g + h \) with \( \deg_X(g) \leq q-1 \), \( \deg_Y(g) \leq q-1 \), \( h \in J_1(X,Y) \), \( \deg(h) \leq \deg(f) \) and clearly \( \deg(f) \geq \deg(g) \). Write \( g(X,Y) = \sum c_i(Y)X^i \).

As \( g(x,b) = 0 \) for any \( x \in \mathbb{GF}(q), b \in B \) and \( \deg_X(g), \deg_Y(g) \leq q-1 \), it follows that \( h(X,b) = 0 \), so each \( c_i(b) = 0 \). Hence \( \prod_{b \in B} (Y-b) \) divides \( g \), and similarly \( \prod_{a \in A} (X-a) \) divides \( g \).

Note that it gives another proof of Theorem 5.11 for \( n = 2 \), with \( A = B = \mathbb{GF}(q)^* \).

In applications we often need the “homogeneous version” of Exercise 5.10. Note that e.g. \( X^qY - XY^q = Y(X^q - X) - X(Y^q - Y) \). If \( f(X,Y) \), a homogeneous polynomial in \( X \) and \( Y \), of total degree \( d \), vanishes everywhere on \( \mathbb{GF}(q)^2 \) then \( f \in (X^q - X), (Y^q - Y) \), so \( f(X,Y) = f_1(X,Y)(X^q - X) + f_2(X,Y)(Y^q - Y) \), where \( f_1 \) and \( f_2 \) can be chosen to be homogeneous polynomials of total degree \( d - q \). Now the terms of low degree must disappear, so \( Xf_1 + Yf_2 = 0 \). Hence \( Y \) divides \( f_1 \); let \( f_1(X,Y) = Y g(X,Y) \), then
\[
\frac{f(X,Y) - f_1(X,Y)(X^q Y - XY^q)}{Y}.
\]

Alon’s Nullstellensatz

Hilbert’s Nullstellensatz is the fundamental theorem stating that if \( \mathbb{F} \) is an algebraically closed field, and \( f_1, \ldots, f_m \) are polynomials in \( \mathbb{F}[X_1, \ldots, X_n] \), where \( f \) vanishes over all common zeros of \( g_1, \ldots, g_m \), then there is an integer \( k \) and polynomials \( h_1, \ldots, h_m \) in \( \mathbb{F}[X_1, \ldots, X_n] \) so that \( f^k = \sum_{i=1}^m h_i g_i \). In the special case \( m = n \), where each \( g_i \) is a univariate polynomial of the form \( \prod_{s \in S_i} (X_i - s) \), a stronger conclusion holds, by Alon’s result [2].
5. Finite fields and polynomials

**Theorem 5.16.** Let $\mathbb{F}$ be an arbitrary field, and let $f = f(X_1, \ldots, X_n)$ be a polynomial in $\mathbb{F}[X_1, \ldots, X_n]$. Let $S_1, \ldots, S_n$ be nonempty subsets of $\mathbb{F}$ and define $g_t(X_i) = \prod_{s \in S_i} (X_i - s)$. If $f$ vanishes over all the common zeros of $g_1, \ldots, g_n$ (that is, if $f(s_1, \ldots, s_n) = 0$ for all $s_i \in S_i$), then $f \in \langle g_1, \ldots, g_n \rangle$ and there are polynomials $h_1, \ldots, h_n \in \mathbb{F}[X_1, \ldots, X_n]$ satisfying $\deg(h_i) \leq \deg(f) - \deg(g_i)$ so that

$$f = \sum_{i=1}^{n} h_i g_i.$$

Moreover, if $f; g_1, \ldots, g_n$ lie in $R[X_1, \ldots, X_n]$ for some subring $R$ of $\mathbb{F}$ then there are polynomials $h_i \in R[X_1, \ldots, X_n]$ as above.

As a consequence of the above one can prove the following:

**Theorem 5.17.** Let $\mathbb{F}$ be an arbitrary field, and let $f = f(X_1, \ldots, X_n)$ be a polynomial in $\mathbb{F}[X_1, \ldots, X_n]$. Suppose that $\deg(f) = \sum_{i=1}^{n} t_i$, where each $t_i$ is a non-negative integer, and suppose the coefficient of $\prod_{i=1}^{n} X_i^{t_i}$ in $f$ is nonzero. Then, if $S_1, \ldots, S_n$ are subsets of $\mathbb{F}$ with $|S_i| > t_i$, there are $s_1 \in S_1, s_2 \in S_2, \ldots, s_n \in S_n$ so that $f(s_1, \ldots, s_n) \neq 0$.

To prove Theorem 5.16 we need the following lemma.

**Lemma 5.18.** Let $P = P(X_1, \ldots, X_n)$ be a polynomial in $n$ variables over an arbitrary field $\mathbb{F}$. Suppose that the degree of $P$ as a polynomial in $X_i$ is at most $t_i$ for $1 \leq i \leq n$, and let $S_i \subset \mathbb{F}$ be a set of at least $t_i + 1$ distinct members of $\mathbb{F}$. If $P(X_1, \ldots, X_n) = 0$ for all $n$-tuples $(x_1, \ldots, x_n) \in S_1 \times \ldots \times S_n$ then $P \equiv 0$.

**Proof:** We apply induction on $n$. For $n = 1$, the lemma is simply the assertion that a non-zero polynomial of degree $t_1$ in one variable can have at most $t_1$ distinct zeros. Assuming that the lemma holds for $n - 1$, we prove it for $n$ ($n \geq 2$). Given a polynomial $P = P(X_1, \ldots, X_n)$ and sets $S_i$ satisfying the hypotheses of the lemma, let us write $P$ as a polynomial in $X_n$; that is,

$$P = \sum_{i=0}^{t_n} P_i(X_1, \ldots, X_{n-1})X_n^i,$$

where each $P_i$ is a polynomial with $X_j$-degree bounded by $t_j$. For each fixed $(n-1)$-tuple $(x_1, \ldots, x_{n-1}) \in S_1 \times \ldots \times S_{n-1}$, the univariate polynomial $P(x_1, \ldots, x_{n-1}, X_n)$ vanishes for all $x_n \in S_n$, and is thus identically 0. Thus $P_i(x_1, \ldots, x_{n-1}) \equiv 0$ for all $(x_1, \ldots, x_{n-1}) \in S_1 \times \ldots \times S_{n-1}$. Hence, by the induction hypothesis, $P_i \equiv 0$ for all $i$, implying that $P \equiv 0$. 

**Proof of Theorem 5.16** Define $t_i = |S_i| - 1$ for all $i$. By assumption,

$$f(x_1, \ldots, x_n) = 0 \quad \forall (x_1, \ldots, x_n) \in S_1 \times \ldots \times S_n$$

(1)
For each $i$, $1 \leq i \leq n$, let

$$g_i(X_i) = \prod_{s \in S_i} (X_i - s) = X_i^{t_i + 1} - \sum_{j=0}^{t_i} g_{ij} X_i^j.$$ 

Observe that, if $x_i \in S_i$ then $g_i(x_i) = 0$; that is, $x_i^{t_i + 1} = \sum_{j=0}^{t_i} g_{ij} x_i^j$. \hfill (2)

Let $\bar{f}$ be the polynomial obtained by writing $f$ as a linear combination of monomials and replacing, repeatedly, each occurrence of $X_i^{m_i}$ ($1 \leq i \leq n$), where $u_i > t_i$, by a linear combination of smaller powers of $X_i$, using the relations (2). The resulting polynomial $\bar{f}$ is of degree at most $t_i$ in $X_i$, for each $1 \leq i \leq n$, and is obtained from $f$ by subtracting from it products of the form $h_i g_i$, where the degree of each polynomial $h_i \in \mathbb{F}[X_1, \ldots, X_n]$ does not exceed $\deg(f) - \deg(g_i)$ (and where the coefficients of each $h_i$ are in the smallest ring containing all coefficients of $f$ and $g_1, \ldots, g_n$). Moreover, $\bar{f}(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$, for all $(x_1, \ldots, x_n) \in S_1 \times \ldots \times S_n$, since the relations (2) hold for these values of $x_1, \ldots, x_n$. Therefore, by (1), $\bar{f}(x_1, \ldots, x_n) = 0$ for every $n$-tuple $(x_1, \ldots, x_n) \in S_1 \times \ldots \times S_n$ and hence, by the Lemma, $\bar{f} \equiv 0$. This implies that $f = \sum_{i=1}^n h_i g_i$, and completes the proof. \hfill \Box

**Proof of Theorem 5.17** We may assume that $|S_i| = t_i + 1$ for all $i$. Suppose the statement is false, and define $g_i(X_i) = \prod_{s \in S_i} (X_i - s)$. By Theorem 5.16 there are polynomials $h_1, \ldots, h_n \in \mathbb{F}[X_1, \ldots, X_n]$ satisfying $\deg(h_i) \leq \sum_{i=1}^n t_i - \deg(g_i)$ so that $f = \sum_{i=1}^n h_i g_i$. By assumption, the coefficient of $\prod_{i=1}^n X_i^{t_i}$ on the left hand side is nonzero, and hence so is the coefficient of this monomial on the right hand side. However, the degree of $h_i g_i = h_i \prod_{s \in S_i} (X_i - s)$ is at most $\deg(f)$, and if there are any monomials of degree $\deg(f)$ in it they are divisible by $X_i^{t_i + 1}$. It follows that the coefficient of $\prod_{i=1}^n X_i^{t_i}$ on the right hand side is zero, and this contradiction completes the proof. \hfill \Box

For nice applications see Section 29.

Now we present the punctured version of Alon’s Nullstellensatz by Ball and Serra [22], which states that if $f$ vanishes at nearly all, but not all, of the common zeros of some polynomials $g_1(X_1), \ldots, g_n(X_n)$ then every $I$-residue of $f$, where the ideal $I = \langle g_1, \ldots, g_n \rangle$, has a large degree. As a consequence we prove a converse of the corollary to Alon’s Nullstellensatz. The corollary to Alon’s Nullstellensatz states that if $f$ has a term of maximum degree $X_1^{r_1} \cdots X_n^{r_n}$, where $r_i = |S_i| - t_i$ and $t_i > 0$ for all $i$, then a grid $D_1 \times \cdots \times D_n$ containing the points of the grid $S_1 \times \cdots \times S_n$ where $f$ does not vanish, satisfies $|D_i| \geq t_i$. The converse, which will follow as a corollary to the punctured version of Alon’s Nullstellensatz, states that if $D_1 \times \cdots \times D_n$ is a grid containing the points of the grid $S_1 \times \cdots \times S_n$ where $f$ does not vanish, then $f$ has a term $X_1^{r_1} \cdots X_n^{r_n}$, where $r_i$ satisfies $|S_i| - 1 \geq r_i \geq |S_i| - |D_i|$ for all $i$. Furthermore, Ball and Serra extend Alon’s Nullstellensatz to functions which
have multiple zeros at the common zeros of $g_1, g_2, \ldots, g_n$ and prove a punctured version of this generalised version.

The following corollary is slightly more general than Theorem 5.17. Note that under the hypothesis there is always at least one point of the grid where $f$ does not vanish.

**Corollary 5.19.** If $f \in \mathbb{F}[X_1, X_2, \ldots, X_n]$ has a term of maximum degree $X_1^{r_1} \cdots X_n^{r_n}$, where $r_i = |S_i| - t_i$ and $t_i \geq 1$ for all $i$, then a grid which contains the points of $S_1 \times \ldots \times S_n$ where $f$ does not vanish, has size at least $t_1 \times \ldots \times t_n$.

**Proof:** Suppose that there is a grid $M_1 \times \ldots \times M_n$, where $|M_j| < t_j$ for some $j$, containing all the points $S_1 \times \ldots \times S_n$ where $f$ does not vanish. Let

$$e_j(X_j) = \prod_{m_j \in M_j} (X_j - m_j).$$

The polynomial $fe_j$ is zero at all points of $S_1 \times \ldots \times S_n$ and has a term of maximum degree $X_1^{r_1} \cdots X_n^{r_n} X_j^{|M_j|}$. Note that $r_j + |M_j| < |S_j|$ and $r_i < |S_i|$ for $i \neq j$. By Theorem 5.16 the polynomial $fe_j = \sum_{i=1}^n g_i h_i$ for some polynomials $h_i$. The terms of maximum degree in $fe_j$ have degree in $X_i$ at least $|S_i|$ for some $i$, which is a contradiction.

**Punctured Combinatorial Nullstellensatz**

In Alon’s Combinatorial Nullstellensatz, Theorem 5.16, the function $f$ was assumed to have zeros at all points of the grid $S_1 \times S_2 \times \ldots \times S_n$. In the case that there is a point in $S_1 \times S_2 \times \ldots \times S_n$ where $f$ does not vanish a slightly different conclusion holds. The following can be thought of as a punctured version of Alon’s Combinatorial Nullstellensatz.

Let $\mathbb{F}$ be a field and let $f$ be a polynomial in $\mathbb{F}[X_1, X_2, \ldots, X_n]$. For $i = 1, \ldots, n$, let $D_i$ and $S_i$ be finite non-empty subsets of $\mathbb{F}$, where $D_i \subseteq S_i$, and define

$$g_i(X_i) = \prod_{s_i \in S_i} (X_i - s_i), \quad \text{and} \quad l_i(X_i) = \prod_{d_i \in D_i} (X_i - d_i).$$

**Theorem 5.20.** If $f$ vanishes over all the common zeros of $g_1, g_2, \ldots, g_n$ except at least one element of $D_1 \times D_2 \times \ldots \times D_n$, where it is not zero, then there are polynomials $h_1, h_2, \ldots, h_n \in \mathbb{F}[X_1, X_2, \ldots, X_n]$ satisfying $\deg(h_i) \leq \deg(f) - \deg(g_i)$ and a non-zero polynomial $w$, whose degree in $X_i$ is less than $|S_i|$ and whose total degree is at most $\deg f$, with the property that

$$f = \sum_{i=1}^n h_i g_i + w.$$
and

\[ w = u \prod_{i=1}^{n} \frac{g_i}{l_i}, \]

for some non-zero polynomial \( u \).

Note that the theorem gives the lower bound \( \deg f \geq \sum_{i=1}^{n} (|S_i| - |D_i|) \).

**Proof:** We can write

\[ f = \sum_{i=1}^{n} g_i h_i + w, \]

for some polynomials \( h_i \) of degree at most the degree of \( f \) minus the degree of \( g_i \), and a polynomial \( w \), where the degree of \( w \) in \( X_i \) is less than the degree of \( g_i \) and the overall degree of \( w \) is at most the degree of \( f \). For each \( i \) the polynomial \( f l_i \) has zeros on all common zeros of \( g_i \), by assumption, and hence so does \( w l_i \). By Alon’s Nullstellensatz there are polynomials \( v_i \) with the property that

\[ w l_i = \sum_{i=1}^{n} g_i v_i. \]

However the degree of \( X_j \) in \( w l_i \), for \( j \neq i \), is less than the degree of \( g_j(X_j) \) and so \( w l_i = g_i v_i \). Thus \( g_i \) divides \( w l_i \). Note that \( l_i \) divides \( g_i \), so this divisibility implies \( g_i/l_i \) divides \( w \). Hence

\[ w = u \prod_{i=1}^{n} \frac{g_i}{l_i}, \]

for some polynomial \( u \) and \( u \) is not zero since \( 0 \neq f(d_1, d_2, ..., d_n) = w(d_1, d_2, ..., d_n) \) for some \( d_i \in D_i \).

The following corollary is a converse of the corollary to Alon’s Nullstellensatz, Corollary 5.19.

**Exercise 5.21.** If \( D_1 \times ... \times D_n \) is a grid containing all the points of the grid \( S_1 \times ... \times S_n \) where \( f \) does not vanish, then \( f \) has a term \( X_1^{r_1} \cdots X_n^{r_n} \), where \( |S_i| - 1 \geq r_i \geq |S_i| - |D_i| \).

**Combinatorial Nullstellensatzen with multiplicity**

In this section we shall consider polynomials that have zeros of multiplicity, see the end of Section 5.3. The following proof of Theorem 5.22 is based on the proof of Theorem 1.3 in [53].

Let \( T \) be the set of all non-decreasing sequences of length \( t \) on the set \( \{1, 2, ..., n\} \). For any \( \tau \in T \), let \( \tau(i) \) denote the \( i \)-th element in the sequence \( \tau \).
Let $F$ be a field and let $f$ be a polynomial in $F[X_1, X_2, \ldots, X_n]$. Suppose that $S_1, S_2, \ldots, S_n$ are arbitrary non-empty finite subsets of $F$ and define

$$g_i(X_i) = \prod_{s_i \in S_i} (X_i - s_i).$$

**Theorem 5.22.** If $f$ has a zero of multiplicity $t$ at all the common zeros of $g_1, g_2, \ldots, g_n$ then there are polynomials $h_\tau$ in $F[X_1, X_2, \ldots, X_n]$, satisfying $\deg(h_\tau) \leq \deg(f) - \sum_{\tau \in T} \deg(g_i)$, such that

$$f = \sum_{\tau \in T} g_{\tau(1)} \cdots g_{\tau(t)} h_\tau.$$

**Proof:** This can be proved by double induction on $n$ and $t$. If $n = 1$ and $f$ has a zero of degree $t$ for all $s_i \in S_i$ then $f = g(X_1)^{h(X_1)}$ for some polynomial $h$. If $t = 1$ then the theorem is Alon’s Nullstellensatz, Theorem 5.16. For the details see [22].

Theorem 5.22 has the following corollary.

**Exercise 5.23.** Let $F$ be a field and let $f$ be a polynomial in $F[X_1, X_2, \ldots, X_n]$ and suppose that $f$ has a term $X_1^{r_1}X_2^{r_2}\ldots X_n^{r_n}$ of maximal degree. If $S_1, S_2, \ldots, S_n$ are nonempty subsets of $F$ with the property that for all $\tau \in T$, the set of non-decreasing sequences of length $t$ on $\{1, 2, \ldots, n\}$, there exists an $i$ such that

$$\sum_{i \in \tau} |S_i| > r_i,$$

then there is a point $a = (a_1, a_2, \ldots, a_n)$, with $a_i \in S_i$, where $f$ has a zero of multiplicity at most $t - 1$.

Note that this statement with $t = 1$ is the original corollary to Alon’s Nullstellensatz that has proven so useful. Specifically, if $r_i < |S_i|$ for all $i$ then there is a point $(a_1, a_2, \ldots, a_n)$, with $a_i \in S_i$, where $f$ does not vanish. When $t = 2$ the hypothesis is that $r_i < |S_i|$ for all $i$ except possibly one, when $i = 1$ say, for which $r_1 < 2|S_1|$. The conclusion is that there is a point $(a_1, a_2, \ldots, a_n)$, with $a_i \in S_i$, where $f$ has a simple zero (of multiplicity one) or does not vanish. When $t = 3$ the hypothesis is that $r_i < |S_i|$ for all $i$ except possibly two values, 1 and 2 say, for which $r_1 < 3|S_1|$ and $r_2 < 2|S_2|$.

The following is a version of Theorem 5.20 for functions that have many zeros with multiplicity.

Let $F$ be a field and let $f$ be a polynomial in $F[X_1, X_2, \ldots, X_n]$. For $i = 1, \ldots, n$, let $D_i$ and $S_i$ be finite non-empty subsets of $F$, where $D_i \subseteq S_i$, and define

$$g_i(X_i) = \prod_{s_i \in S_i} (X_i - s_i), \text{ and } l_i(X_i) = \prod_{d_i \in D_i} (X_i - d_i).$$
Theorem 5.24. If \( f \) has a zero of multiplicity at least \( t \) at all the common zeros of \( g_1, g_2, \ldots, g_n \), except at at least one point of \( D_1 \times D_2 \times \ldots \times D_n \) where it has a zero of multiplicity less than \( t \), then there are polynomials \( h_i \) in \( \mathbb{F}[X_1, X_2, \ldots, X_n] \), satisfying \( \deg(h_i) \leq \deg(f) - \sum_{i \in \tau} \deg(g_i) \), and a non-zero polynomial \( u \) satisfying \( \deg(u) \leq \deg(f) - \sum_{i=1}^n (\deg(g_i) - \deg(l_i)) \), such that

\[
    f = \sum_{\tau \in \mathcal{T}} g_{\tau(1)} \cdots g_{\tau(t)} h_\tau + u \prod_{i=1}^n \frac{g_i}{l_i}.
\]

Moreover, if there is a point of \( D_1 \times D_2 \times \ldots \times D_n \) where \( f \) is non-zero, then for any \( j \),

\[
    \deg(f) \geq (t-1)(|S_j| - |D_j|) + \sum_{i=1}^n (|S_i| - |D_i|).
\]

5.6 Additive, linearized polynomials

A polynomial \( f \in \mathbb{GF}(q)[X] \) is additive if \( f(U+V) = f(U) + f(V) \) or, alternatively, \( f(x+y) = f(x) + f(y) \) for all \( x, y \in \mathbb{GF}(q) \). It is \( \mathbb{GF}(p^e) \)-linear if it is additive and for all \( \lambda \in \mathbb{GF}(p^e) \subseteq \mathbb{GF}(q) \), \( f(\lambda X) = \lambda f(X) \) or \( f(\lambda x) = \lambda f(x) \) for each \( x \in \mathbb{GF}(q) \). If all the exponents in \( f \) are powers of \( p^e \) then \( f \) is obviously \( \mathbb{GF}(p^e) \)-linear.

We remark that \( \mathbb{GF}(p) \)-linearity and additivity are equivalent.

Note that the polynomial \( X^0 + X^4 + X^2 + X \in \mathbb{GF}(3)[X] \) is additive (\( \mathbb{GF}(3) \)-linear) but the exponents are not powers of 3. This cannot occur if the degree is at most \( q-1 \).

Theorem 5.25. A polynomial \( f \in \mathbb{GF}(q)[X] \) of degree at most \( q-1 \) is \( \mathbb{GF}(p^e) \)-linear if and only if all of its exponents are powers of \( p^e \).

Proof: The “if” part is obvious. Consider \( \mathbb{GF}(q) \) as an \( \frac{q}{p^e} \)-dimensional vectorspace over \( \mathbb{GF}(p^e) \), then \( f \) is a \( \mathbb{GF}(p^e) \)-linear transformation of it. The number of such transformations is \( (p^e)^{\left(\frac{q}{p^e}\right)^2} \). The polynomials of degree at most \( q-1 \) and with all exponents being powers of \( p^e \) are among these transformations, the number of these polynomials is \( q^\frac{q}{p^e} = (p^e)^{\left(\frac{q}{p^e}\right)^2} \).

Exercise 5.26. (Segre-Bartocci) A linear map \( f : \mathbb{GF}(q) \to \mathbb{GF}(q) \) is nonsingular if and only if for the coefficients of its unique polynomial form \( f(X) = \sum_{i=0}^{h-1} a_i X^{p^i} \), the matrix

\[
    A = \begin{pmatrix}
    a_0 & a_1 & \ldots & a_{h-1} \\
    a_1 & a_0 & \ldots & a_{h-2} \\
    a_2 & a_1 & \ldots & a_{h-3} \\
    \vdots & \vdots & \ddots & \vdots \\
    a_{h-1} & a_{h-2} & \ldots & a_0
    \end{pmatrix}
\]

is nonsingular.
Note that the determinant of the Segre-Bartocci matrix is always an element of \( \text{GF}(p) \).

**Exercise 5.27.** A polynomial \( f \in \text{GF}(q)[X] \) of degree \( q - 1 \) maps to the subfield \( \text{GF}(p^e) \) and is \( \text{GF}(p^e) \)-linear if and only if it is of the form \( f(X) = \text{Tr}_{q \rightarrow p^e}(aX) \) with some \( a \in \text{GF}(q) \).

**Theorem 5.28.** Fundamental Theorem of Additive Polynomials. Let \( f(X) \in \mathbb{F}[X] \) be a separable polynomial with roots \( \{x_1, \ldots, x_m\} \). Then \( f(X) \) is additive if and only if \( S = \{x_1, \ldots, x_m\} \) is a (n additive) subgroup of \( (\mathbb{F}, +) \).

**Proof:** The “additive \( \Rightarrow \) subgroup” direction is obvious. To show the other, consider

\[
f(X) = \prod_{i=1}^{m} (X - x_i).
\]

If \( y \in S \) then \( f(X + s) = f(X) \). Now for any \( y \) put \( g(X) = f(X + y) - f(X) - f(y) \). Here \( \deg g < \deg f = m \) and \( g(x_i) = 0 \) for \( i = 1, \ldots, m \), hence \( g(X) = 0 \) and \( f \) is additive.

### 5.7 The random-like behaviour

In this section we prove a lemma, which is a generalization of a result of Szönyi. It is interesting in itself, and it is used in several applications as well. In fact this lemma is a consequence of the character sum version of Weil’s estimate. In order to formulate it, we need

**Definition 5.29.** Let \( f_1(X), \ldots, f_m(X) \in \text{GF}(q)[X] \) be given polynomials. We say that their system is \( d \)-power independent, if no partial product \( f_{i_1}^{s_1} f_{i_2}^{s_2} \cdots f_{i_j}^{s_j} \) (\( 1 \leq j \leq m; \quad 1 \leq i_1 < i_2 < \ldots < i_j \leq m; \quad 1 \leq s_1, s_2, \ldots, s_j \leq d - 1 \)) can be written as a constant multiple of a \( d \)-th power of a polynomial.

Equivalently, one may say that if any product \( f_{i_1}^{s_1} f_{i_2}^{s_2} \cdots f_{i_j}^{s_j} \) is a constant multiple of a \( d \)-th power of a polynomial, then this product is ‘trivial’, i.e. for all the exponents \( d | s_i, i = 1, \ldots, j \). Now

**Lemma 5.30.** Let \( f_1, \ldots, f_m \in \text{GF}(q)[X] \) be a set of \( d \)-power independent polynomials, where \( d|(q - 1) \), \( d, m \geq 2 \). Denote by \( N \) the number of solutions \( \{x \in \text{GF}(q) : f_i(x) \text{ is a } d \text{-th power in } \text{GF}(q) \text{ for all } i = 1, \ldots, m\} \). Then \( |N - \frac{q}{d^m}| \leq \sqrt{q \sum_{i=1}^{m} \deg f_i} \).

Note that this lemma implies that, under some natural conditions, one can solve a system of equations

\[
\chi_d(f_i(X)) = \delta_i \quad (i = 1, \ldots, m),
\]
where the \(\delta_i\)-s are \(d\)-th complex roots of unity, and \(\chi_d\) is a multiplicative character of order \(d\). So ‘the \(d\)-th power behaviour’ can be prescribed if the polynomials are ‘independent’.

It can be interpreted as ‘being a \(d\)-th power’ is like a random event of probability \(\frac{1}{d}\).

Some words about the condition \(d|(q-1):\) if \(d\) and \(q-1\) are co-primes, then every element is a \(d\)-th power in \(\mathbb{G}F(q)\). If \(\text{g.c.d.}(d,q-1)=d_1\) and we write \(d=d_1d_2\) and \(\text{g.c.d.}(d_2,q-1)=\text{g.c.d.}(d_1,d_2)=1\), then the lemma can be applied with \(d_1\), as \(d\)-th and \(d_1\)-th powers are the same in this case.

We remark that Szönyi [126] proved this lemma for \(d=2\). [114] contains a general bound; the proof below is a modified version of a lemma for linear polynomials in Babai, Gál and Wigderson [5].

We need the character sum version of Weil’s estimate:

**Result 5.31.** ([90], Thm. 5.41) Let \(f(X)\) be a polynomial over \(\mathbb{G}F(q)\) and \(r\) the number of distinct roots of \(f\) in its splitting field. If \(\chi_e\) is a multiplicative character (of order \(e\)) of \(\mathbb{G}F(q)\) and \(f(X) \neq cg(X)^e\), then

\[
| \sum_{x \in \mathbb{G}F(q)} \chi_e(f(x)) | \leq (r-1)\sqrt{q}.
\]

**Proof of Lemma 5.30:** First note that we use the definition \(\chi(x) = \chi_d(x) = x^{\frac{q-1}{d}}\).

Let \(\{\varepsilon_0 = 1, \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{d-1}\}\) be the set of \(d\)-th complex roots of unity. Let \(h(Z) = \frac{Z^d-1}{Z-1} = 1 + Z + \ldots + Z^{d-1}\); then \(h(1) = d\), \(h(\varepsilon_j) = 0\) for \(j = 1, \ldots, d-1\) and \(h(0) = 1\). Define \(H(x) = \prod_{i=1}^{m} h(\chi(f_i(x)))\).

If \(x\) is a solution then \(H(x) = d^m\), if \(x\) is a root of some \(f_i\) then \(H(x) = 0\) or \(H(x) = d^{m-1}\). In the remaining cases \(H(x) = 0\). Hence, if \(N\) denotes the number of solutions and \(D := \sum_{i=1}^{m} \deg f_i\) then the sum \(S = \sum_{x \in \mathbb{G}F(q)} H(x)\) satisfies

\[
Nd^m \leq S \leq Nd^m + Dd^{m-1}. \tag{*}
\]

\(H(x)\) is a product of sums of \(d\) terms each. Let’s expand the product to the sum of \(d^m\) terms. Let \(\Psi\) denote the set of the \(d^m\) functions \(\psi : \{1, \ldots, m\} \rightarrow \{0, \ldots, d-1\}\), which will serve to index this sum. Now

\[
S = \sum_{x \in \mathbb{G}F(q)} \sum_{\psi \in \Psi} \prod_{i=1}^{m} (\chi(f_i(x)))^{\psi(i)} = \sum_{x \in \mathbb{G}F(q)} \sum_{\psi \in \Psi} \chi(f_\psi(x)),
\]

where \(\chi(f_\psi(x)) = \prod_{i=1}^{m} f_i(x)^{\psi(i)}\). Let \(\psi_0(i) \coloneqq 0\) for all \(i\) and \(\Psi^* = \Psi \setminus \{\psi_0\}\). After switching the order of summation and separating the term corresponding to \(\psi_0\), this (“main”) term will be \(q\). For the “error term” \(R = S - q\) we have

\[
|R| \leq \sum_{\psi \in \Psi^*} \left| \sum_{x \in \mathbb{G}F(q)} \chi(f_\psi(x)) \right|.
\]
By our assumption for the $d$-th power independence of $\{f_1, ..., f_m\}$ and as each $\psi(i)$ is at most $d-1$, we can use Theorem 5.31 (note that $f_\psi$ have at most $D$ distinct roots in the splitting field), so the inner sum has absolute value $\leq (D-1)\sqrt{q}$. Hence $|R| \leq d^m(D-1)\sqrt{q}$ and from (*) we get $|N - \frac{D}{d}| \leq (D-1)\sqrt{q} + D/d \leq D\sqrt{q}$ (as if $D/d > \sqrt{q}$ then Lemma 5.30 clearly holds).

The bounds in Result 5.31 can be strengthened when $f(X)$ and $\chi$ are quadratic.

**Exercise 5.32.** Let $q$ be an odd prime power, $f(X) = aX^2 + bX + c \in \mathbb{GF}(q)[X]$ with $a \neq 0$, and let $\chi$ denote the quadratic character $\mathbb{GF}(q) \to \{1, -1, 0\}$. Then

$$\sum_{x \in \mathbb{GF}(q)} \chi(ax^2 + bx + c) = \begin{cases} -\chi(a), & \text{if } b^2 - 4ac \neq 0; \\ (q-1)\chi(a), & \text{if } b^2 - 4ac = 0. \end{cases}$$

## 5.8 Lacunary polynomials

A polynomial is called **lacunary** if an interval is missing from its terms, i.e. some consecutive coefficients happen to be zero. A polynomial of $\mathbb{GF}(q)[X]$ is **fully reducible** if it splits to linear factors over $\mathbb{GF}(q)$. These two requirements proved to be hard to satisfy simultaneously, there are a few results stating that fully reducible lacunary polynomials (the extent of lacunarity must be specified) should have some particular feature.

The theory of lacunary polynomials is treated in R´edei’s book [103], where the following two problems are considered:

**Problem 5.33. Problem 1 of R´edei** Let $d|q-1$, $d > 1$. Determine the fully reducible polynomials $f(X) = X^{q-1} + g(X)$ for which $\deg g \leq \frac{q-1}{d}$, $X \not| g$, and $f$ has no multiple factors.

**Problem 5.34. Problem 2 of R´edei** Determine the fully reducible polynomials $f(X) = X^q + g(X)$, $f(X) \in \mathbb{GF}(q)[X] \setminus \mathbb{GF}(q)[X^p]$, for which $\deg g \leq \frac{q+1}{2}$. In geometric applications a modified version of Problem 2 will be crucial, where $f$ is allowed to be a polynomial of $X^p$:

**Problem 5.35. Problem 2’** Determine the fully reducible polynomials $f(X) = X^q + g(X)$, $f(X) \in \mathbb{GF}(q)[X]$, for which $\deg g \leq \frac{q+1}{2}$.

Problem 1 is rather easy:

**Theorem 5.36.** (R´edei, [103]) If $d > 2$ then the only solutions of Problem 1 are the Euler-binoms $X^{\frac{q-1}{d}} - \alpha$, where $\alpha = u^{\frac{q-1}{d}}$ for a $u \in \mathbb{GF}(q)^*$. If $d = 2$ and $q \equiv 1 \pmod{4}$ then there are other solutions as well, namely the four polynomials
\[
\left(X^{q-1} \pm 1\right)\left(X^{q-1} \pm \gamma\right),
\]

where \(\gamma^2 = -1\).

Let’s consider Problem 2. The conditions in it do not seem natural. The following lemma ([103], Satz 18) shows that the degree of \(g\) is always at least \(\frac{q+1}{2}\) unless \(f(X) = X^q - X\). The degree of a polynomial \(h\) is denoted by \(h^o\).

**Lemma 5.37.** Let \(s\) be a power of \(p\) with \(1 \leq s < q\) and suppose that\( X^{q/s} + g(X) \in GF(q)[X] \setminus GF(q)[X^p]\)
is fully reducible over \(GF(q)\). Then either \(s = 1\) and \(g(X) = -X\) or
\[
g^o \geq \frac{q + s}{s(s + 1)}.
\]

**Proof:** A zero of \(X^{q/s} + g\) of multiplicity \(k\) is a zero of \((X^{q/s} + g)^t = g^t\) of multiplicity at least \(k - 1\) and a zero of \(X^q - X\) with multiplicity 1. Hence
\[
X^{q/s} + g \mid ((X^{q/s} + g)^s - (X^q - X))g' = (g^s + X)g'.
\]

By assumption \(g' \neq 0\) so either \(g^s = -X\) and hence \(s = 1\) or the right hand side is non-zero and \(q/s \leq sg^o + g^o - 1\).

At this stage one can solve Problem 2 in the \(q = p\) prime case.

**Theorem 5.38.** [103] If \(q = p \neq 2\) is a prime then the solutions of Problem 2 are precisely the four polynomials
\[
f(X) = (X + a)\left((X + a)^{\frac{p+1}{2} - \sigma} - \sigma\right)\left((X + a)^{\frac{p+1}{2}} - \sigma\tau\right), \quad \sigma = \pm 1, \tau = 0, 1.
\]

It means that either \(f\) has one single and \(\frac{p+1}{2}\) double roots, or it has one root of multiplicity \(\frac{p+1}{2}\) and \(\frac{p-1}{2}\) other single roots.

**Proof:** As the translation \(x \mapsto x + a\) does not change the problem, we can assume that in \(g(X) = a_0X^{\frac{p+1}{2}} + a_1X^{\frac{p+1}{2}} + \ldots + a_{\frac{p+1}{2}}\) the coefficient \(a_1\) is zero. From the proof of Lemma 5.37 \((s = 1)\) one can see that \(f(X)|(g(X) + X)g'(X)\); as their degrees are equal, one is constant times the other.Comparing the leading coefficients we get
\[
\frac{a_0^2}{2}f(X) = \frac{a_0^2}{2}(X^p + g(X)) = (g(X) + X)g'(X).
\]

In particular
5. Finite fields and polynomials

(i) \(g(X) + X\) and \(g'(X)\) are fully reducible;
(ii) \(g(X) + X\) divides \(X^p - X\) hence its roots are all single.

In (*) one can observe that the coefficients of \(X^{p-1}, \ldots, X^{p^2-3}\) are all zero. From this, comparing coefficients we get that \(a_2 = a_3 = \ldots = a_{p+1} = 0\), so \(g(X) = a_0X^{p+1} + a_{p-1}X + a_{p+1}\). Now \(g'(X) = a_0X^{p+1} + a_{2p+1}\) will be reducible only if \(a_{2p+1} = \pm \frac{a_0}{2}, 0\). Now using full reducibility and comparing the coefficients the statement of the theorem follows.

The following generalization of Lemma 5.37 is easy:

**Exercise 5.39.** [32] Suppose that \(f(X) = X^q g(X) + h(X) \in GF(q)[X] \) \((q = p^n, p\) prime) is fully reducible over \(GF(q)\), \((g, h) = 1\). Then either \(f(X) = a(X^q - X)\); \(f(X) = aX^q + b = (aX + b)^q\); or \(q = p\) and \(\max(g^a, h^c) \geq \frac{p+1}{2}\); or \(n \geq 2\) and \(\max(g^a, h^c) \geq p^{\frac{n+1}{2}}\).

The best (currently available) result of this kind is the following (up to my knowledge):

**Theorem 5.40.** [39] Suppose that \(f(X) = X^q g(X) + h(X) \in GF(q)[X] \) \((q = p^n, p\) prime) is fully reducible over \(GF(q)\), \((g, h) = 1\). Let \(k = \max(g^a, h^c) < q\). Let \(e\) be maximal such that \(f\) is a \(p^e\)-th power. Then we have exactly one of the following cases:

1. \(e = n\) and \(k = 0\);
2. \(e \geq 2n/3\) and \(k \geq p^e\);
3. \(2n/3 > e > n/2\) and \(k \geq p^{n-e/2} - \frac{3}{2}p^{n-e}\);
4. \(e = n/2\) and \(k = p^e\) and \(f(X) = a\text{Tr}_{q^{-1}}(bX + c) + d\) or \(f(X) = a\text{Norm}_{q^{-1}}(bX + c) + d\) for suitable constants \(a, b, c, d, e\);
5. \(e = n/2\) and \(k \geq p^e\left[\frac{1}{4} + \sqrt{(p^e+1)/2}\right]\);
6. \(n/2 > e > n/3\) and \(k \geq p^{n/2+e/2} - p^{n-e} - p^e/2\), or, if \(3e = n+1\) and \(p \leq 3\) then \(k \geq p^e(p^e+1)/2\);
7. \(n/3 \geq e > 0\) and \(k \geq p^e[(p^{n-e} + 1)/(p^e + 1)]\);
8. \(e = 0\) and \(k \geq (q+1)/2\);
9. \(e = 0\), \(k = 1\) and \(f(X) = a(X^q - X)\).
I. Background

The following lemma will be required, for example to prove Theorem 18.14.

**Lemma 5.41.** Let $s$ be a power of $p$ with $1 \leq s < q$ and suppose that

$$f = X^{q/s} + g \in \text{GF}(q)[X] \setminus \text{GF}(q)[X^p]$$

is fully reducible over $\text{GF}(q)$. If $3(g')^o < 2q/s - sg^o$ then

$$f \in \langle 1, X, X^s, X^{s^2}, ..., X^{q/s} \rangle_{\text{GF}(q)}.$$

**Proof:** We have the same divisibility as in Lemma 5.37. Let $m(X)$ be defined by

$$(X^{q/s} + g)m = (X + g^o)g'.$$  

Now $m^o = sg^o - q/s + (g')^o$. Differentiating $(*)$, we get another equation: combining them we conclude to

$$(X^{q/s} + g)(g''m - g'm') = (m - 1)(g')^2.$$  

The degree of the right hand side is at most $m^o + 2g'^o \leq sg^o - q/s + 3(g')^o < q/s$, so $g''m - g'm' = 0$, implying $(m - 1)g' = 0$ and hence $m = 1$. It follows that $g'$ is constant and from the differential equation $(*)$ it is an easy task to deduce that $f$ is in the required span.  

6 Representations of affine and projective geometries

In order to profit from the Desarguesian structure of an affine or projective geometry, a few ways of representation or coordinatization is used. In each of them the following questions should be answered:

- How can the subspaces be seen or handled?
- How can one calculate the intersection or span of two subspaces?
- How can the subgeometries and other “nice subsets”, like quadrics, Hermitean surfaces, etc. be seen or handled?
- How can transformations (collineations, polarities) be represented?
- How can general pointsets be handled?

The standard representation of $\text{AG}(n, q)$ is just $\text{GF}(q)^n = V(n, q)$, the $n$-dimensional vectorspace over $\text{GF}(q)$, where the $k$-subspaces of $\text{AG}(n, q)$ are represented by the $k$-dimensional affine subspaces (i.e. translates of linear subspaces) of $\text{GF}(q)^n$, for $k = 0, 1, ..., n$, and incidence is the natural one.
In the standard homogeneous representation of $\text{PG}(n, q)$ the $k$-subspaces of $\text{PG}(n, q)$ are represented by the $(k+1)$-dimensional linear subspaces of $\text{GF}(q)^{n+1} = V(n+1, q)$, for $k = 0, 1, \ldots, n$, and incidence is the natural one. In particular, points can be represented by nonzero vectors $(v_1, \ldots, v_{n+1})$ and another vector $(w_1, \ldots, w_{n+1})$ represents the same point if $(v) = (w)$, i.e. there is a $\lambda \in \text{GF}(q)$ for which $w_i = \lambda v_i$ for $i = 1, \ldots, n+1$.

When coordinatizing, an inner product should be chosen and used, in these two representations the easiest is the standard inner product.

Hence a hyperplane, i.e. a 1-codimensional subspace can be represented by any (nonzero) vector $[v_1, \ldots, v_{n+1}]$ being orthogonal to it(s points), i.e. for any point $u$ of the hyperplane $\sum u_i v_i = 0$; and another vector $[w_1, \ldots, w_{n+1}]$ represents the same hyperplane if $(v) = (w)$.

**Exercise 6.1.** Calculate the number of $k$-dimensional subspaces of $V(n, q)$, $\text{AG}(n, q)$ and $\text{PG}(n, q)$. You may want to use the notation $\binom{a}{b}_q = \frac{(q^n-1)(q^{n-1}-1)\ldots(q^{b+1}-1)}{(q^b-1)(q^{b-1}-1)\ldots(q-1)}$ $q$-binomials and $b_i = \binom{i+1}{1}_q$.

As $\text{AG}(n, q)$ can be imagined as an $n$-dimensional vectorspace over $\text{GF}(q^n)$, it is quite natural to identify them. The incidence structure of $\text{AG}(n, q)$ will be recognised in the following way: three points $A, B, C$ are collinear if for the corresponding elements $a, b, c$ of $\text{GF}(q^n)$ there exists a $\lambda \in \text{GF}(q)$ such that $c = (1 - \lambda)a + \lambda b$ or equivalently $\lambda(a - b) = a - c$. Taking $(q-1)$th powers kills the coefficient $\lambda \in \text{GF}(q)$ and we get $(a - b)^{q-1} = (a - c)^{q-1}$. That is why we can identify the directions with the $\theta_{n-1}$-th roots of unity in $\text{GF}(q^n)$, which are the $(q - 1)$-st powers, and then one can say that $A$ and $B$ determine the direction $(a - b)^{q-1}$.

In this and in the next representation, when an inner product is needed, the usual one is $(x, y) = \text{Tr}_{q^n \rightarrow q}(xy)$ (or $\text{Tr}_{q^{n+1} \rightarrow q}(xy)$); we will see that this is the most natural one.

As $\text{PG}(n, q)$ can be imagined as an $(n+1)$-dimensional vectorspace over $\text{GF}(q)$ ‘modulo’ multiplication by non-zero scalars, it is quite natural to identify it with $\text{GF}(q^{n+1})^*/\text{GF}(q)^*$, i.e. the elements $x$ and $y$ of $\text{GF}(q^{n+1})^*$ represent the same point of $\text{PG}(n, q)$ if and only if $x = \lambda y$ for some $\lambda \in \text{GF}(q)$. Note that in this case $x^{q-1} = y^{q-1}$ as $\lambda^{q-1} = 1$ for all $\lambda \in \text{GF}(q)^*$; this is again the common trick to eliminate factors from a subfield. As usually the hyperplanes are represented by the same set as the points (referring to the geometrically self-dual structure), we will make it so. The incidence structure of $\text{PG}(n, q)$ will be recognized in the following way: the point $A$ will be incident with the hyperplane $H$ iff for the corresponding elements $a$ and $h$ of $\text{GF}(q^{n+1})$ we have $\text{Tr}_{q^{n+1} \rightarrow q}(ah) = 0$. For this the most convenient way is the use of a trace-orthogonal normal base (if exists, as for example in the planar case), see Section 5.2.
Suppose that \( \omega \) is a primitive element of \( \text{GF}(q^{n+1}) \), i.e.

\[
\text{GF}(q^{n+1})^* = \{1 = \omega^0, \omega^1, \omega^2, \ldots, \omega^{q^{n+1}-2}\}.
\]

Then for the subfield \( \text{GF}(q)^* \equiv \{1 = \omega^0, \omega^{\theta_n}, \omega^{2\theta_n}, \ldots, \omega^{(q-1)\theta_n}\} \). Now one can see what ‘modulo \( \text{GF}(q)^* \)’ means: \( \text{PG}(n, q) \) is represented as the factor group of these two cyclic groups; for calculations the convenient representation is either \( \{\omega^0, \omega^1, \omega^2, \ldots, \omega^{\theta_n-1}\} \) or \( \{\omega^0, \omega^{q-1}, \omega^{2(q-1)}, \ldots, \omega^{(\theta_n-1)(q-1)}\} \), so points (and the hyperplanes) are represented by the \( \theta_n \)-th roots of unity in \( \text{GF}(q^{n+1}) \), which are the \( (q-1) \)-st powers. In the first one the map \( \omega^i \mapsto \omega^{i+1} \) (mod \( \theta_n \)), in the second one the map \( \omega^{i(q-1)} \mapsto \omega^{(i+1)(q-1)} \) (mod \( q^{n+1} - 1 \)) gives a cyclic (“Singer-”) automorphism, being regular on both the points and the hyperplanes. This representation is very useful if the cyclic structure, or some very regular substructure of the space is examined.

### 6.1 Subspaces, subgeometries

It is vital to be able to describe subspaces and subgeometries in affine and projective spaces. In the standard representations they are quite obvious however.

In the affine big field representation the points \( x \) of a hyperplane are \( \text{Tr}_{q^n}^{-q}(ax) + b = 0, \) where \( a \in \text{GF}(q^n)^* \) and \( b \in \text{GF}(q) \). A suitable linear combination of \( k \) hyperplane polynomials gives an equation \( \sum_{j=0}^{n-k+1} \alpha_j X^q^j + \beta = 0 \) whose zeros correspond to an \( (n-k+1) \)-dimensional subspace, the intersection of the \( k \) hyperplanes. In particular, lines are given by \( X^q = \alpha X + \beta = 0, \) and for a line joining \( x_1 \) and \( x_2 \) we have \( \alpha = (x_1 - x_2)^{q-1} \). The non-zero \( (q-1) \)-th powers are \( \theta_{n-1} \)-th roots of unity in \( \text{GF}(q^n) \), so we see the one-to-one correspondence between the \( \theta_{n-1} \)-th roots of unity in \( \text{GF}(q^n) \) and the \( \theta_{n-1} \) direction of lines in \( \text{AG}(n, q) \).

In the projective representation we have a slightly more complicated situation.

Given a set of indeterminates \( \{X_i : i = 0, \ldots, n\} \) the hyperplanes of \( \text{PG}(n, q) \) (i.e. subspaces of \( \text{V}(n+1, q) \) of rank \( n \)) are given by linear homogeneous equations of the form

\[
\sum_{i=0}^{n} c_i X_i = 0, \quad (\star)
\]

where \( (c_0, c_1, \ldots, c_n) \) is a point of \( \text{PG}(n, q) \). The points of \( \text{PG}(n, q) \) are subspaces of rank 1 in \( \text{V}(n+1, q) \) which in \( \text{GF}(q^{n+1}) \) are given by the sets of zeros of equations of the form \( X^u = uX \) where \( u^{q^n+q^{n-1}+\ldots+q+1} = 1 \). This is a necessary and sufficient condition on \( u \) for the polynomial \( X^u - uX \) to divide \( X^{q^{n+1}} - X \) and hence be a polynomial that splits completely into distinct linear factors over \( \text{GF}(q^{n+1}) \). Hence we got again that it makes sense to refer to the points of \( \text{PG}(n, q) \) as \( (q^n + q^{n-1} + \ldots + q + 1) \)-st roots of unity in \( \text{GF}(q^{n+1}) \). In \( \text{GF}(q^{n+1}) \) the polynomial

\[
\text{Tr}_{q^{n+1}}(\gamma^q X) = \gamma^q X + \gamma^{q+1} X^q + \ldots + \gamma^{q+n-1} X^{q^n-1} + \gamma^{q+n} X^n
\]
Any automorphism as is known, the automorphism group of $\text{GF}(q^{n+1})$, has degree $q^n$ and is linear over $\text{GF}(q)$. Hence we choose $\gamma = \omega$ to be a fixed primitive element of $\text{GF}(q^{n+1})$ and consider the hyperplane $X_i = 0$ of $\text{PG}(n,q)$ as the equation $\text{Tr}_{q^{n+1} \rightarrow q}(\omega^q X) = 0$, over $\text{GF}(q^{n+1})$, and in general the hyperplane $(*)$ as the equation

$$\text{Tr}_{q^{n+1} \rightarrow q}\left( \sum_{i=0}^{n} c_i \omega^{q^i} X \right) = 0.$$ 

In other words, the points $x$ of a hyperplane are $\text{Tr}_{q^{n+1} \rightarrow q}(cx) = 0 = c\sum_{i=0}^{n} x^{q^i}q^{q^i}$. Writing $z = x^{q^i}$ and $a = e^{q^i}$ we get

$$\sum_{i=0}^{n} a_i = 0.$$ 

A suitable linear combination of $k$ hyperplane polynomials gives an equation $\sum_{i=0}^{n} a_i Z^{q^i} + \beta = 0$ whose zeros correspond to an $(n-k+1)$-dimensional subspace, the intersection of the $k$ hyperplanes. In particular lines are given by $Z^{q^i} + \alpha Z + \beta = 0$ (where there exist relations between $\alpha$ and $\beta$ depending on the direction), and for a line joining $z_1$ and $z_2$ (viewed as $(q-1)$-th powers) we have $\alpha = (z_1^{q^i} - z_2^{q^i})/(z_1 - z_2)$.

For example, the lines of $\text{PG}(3,q)$ represented in $\text{GF}(q^4)$ are obtained by looking at the set of zeros of polynomials whose zeros are zeros of two such hyperplane polynomials and we conclude that these have the form $L(Z) := Z^{q^2} + cZ^q + eZ$ for some $c$ and $e$ in $\text{GF}(q^4)$. These polynomials must have $q^2$ distinct zeros in $\text{GF}(q^4)$ and hence divide $Z^{q^2} - Z$. The polynomial $L^{q^2} - c^{q^2} L^q - (e^{q^2} - c^{q^2+q}) L$ (mod $Z^{q^2} - Z$) has degree $q$ and $q^2$ zeros and is therefore identically zero. Equating coefficients gives the following necessary and sufficient conditions that

$$e^{q^i+1} = e^q - e^{q^2+q^i} \text{ and } e^{q^i+q^i+q} = 1. \quad (***)$$

### 6.2 Transformations

As is known, the automorphism group of $\text{PG}(n,q)$ and $\text{AG}(n,q)$ are $\text{PGL}(n+1,q)$ and $\text{AGL}(n,q)$, respectively. Here we describe them in the non-standard representations as well.

**Theorem 6.2.** Any automorphism $\varphi : \text{AG}(n,q) \rightarrow \text{AG}(n,q)$, $\varphi : \mathbf{x} \mapsto \varphi(\mathbf{x})$, where the point $\mathbf{x}$ is represented in the standard way, can be written in the form $\varphi(\mathbf{x}) = M\mathbf{x} + \mathbf{v}$, where $M$ is a non-singular linear map, $\mathbf{v} \in \mathcal{V}(n,q)$ gives a translation and $\sigma : \text{GF}(q) \rightarrow \text{GF}(q)$ is a field automorphism.

**Theorem 6.3.** Any automorphism $\varphi : \text{PG}(n,q) \rightarrow \text{PG}(n,q)$, $\varphi : \mathbf{x} \mapsto \varphi(\mathbf{x})$, where the point $\mathbf{x}$ is represented with homogeneous coordinates, can be written in the form $\varphi(\mathbf{x}) = M\mathbf{x}$, where $M$ is a non-singular linear map and $\sigma : \text{GF}(q) \rightarrow \text{GF}(q)$ is a field automorphism.
So we have to understand what a linear transformation, a translation and a field automorphism means in the big field representation \( r : \mathcal{V}(n, q) \rightarrow \mathbf{GF}(q^n) \).

Translation is easy: adding the vector \( \mathbf{v} \) to each point of \( \mathcal{V}(n, q) \) is the very same as adding its representative \( r(\mathbf{v}) \) to each element of \( \mathbf{GF}(q^n) \).

Field automorphism is also easy: the automorphism \( \sigma \) of \( \mathbf{GF}(q) \) is just among the automorphisms of \( \mathbf{GF}(q^n) \), and it “commutes with \( r \), i.e. it is the same to use it in the big field representation.

The interesting one is the linear map. Let its matrix be \( M = (m_{ij}) \), so \( M \mathbf{x} = \mathbf{y} \), \( y_i = \sum_{j=0}^{n-1} m_{ij} x_j \). On the other hand, a polynomial \( f(X) = c_0 X + c_1 X^q + c_2 X^{q^2} + ... + c_{n-1} X^{q^{n-1}} \), with \( c_0, ..., c_{q-1} \in \mathbf{GF}(q^n) \) defines a map \( \mathbf{GF}(q^n) \rightarrow \mathbf{GF}(q^n) \), which is linear over \( \mathbf{GF}(q) \). One can check that the number of matrices is equal to the number of these \( \mathbf{GF}(q) \)-linear polynomials (i.e. \( q^{n^2} \)). See Section 5.6 about polynomials being linear over a subfield.

Given \( M \), the corresponding \( f(X) \) depends on the base chosen in \( \mathbf{GF}(q^n) \). If a base of the form \( \{\omega, \omega^q, \omega^{q^2}, ..., \omega^{q^{n-1}}\} \) was chosen, then to find \( f_M \) we have

\[
\begin{align*}
M(X) &= \sum_{k=0}^{n-1} y_k \omega^{q^k} = \sum_{k=0}^{n-1} m_{kj} x_j \omega^{q^k} = \sum_{j=0}^{n-1} x_j \sum_{k=0}^{n-1} m_{kj} \omega^{q^k} \quad \text{and} \\
M(r(\mathbf{x})) &= \sum_{i=0}^{n-1} c_i \sum_{j=0}^{n-1} x_j \omega^{q^{j+i}} = \sum_{j=0}^{n-1} x_j \sum_{i=0}^{n-1} c_i \omega^{q^{j+i}} 
\end{align*}
\]

so to find the coefficients \( c_0, ..., c_{n-1} \) we have to solve the linear equation

\[
\begin{pmatrix}
\omega^0 & \omega^q & \omega^{q^2} & \cdots & \omega^{q^{n-1}} \\
\omega^q & \omega^q & \omega^{q^2} & \cdots & \omega^{q^{n-2}} \\
\omega^{q^2} & \omega^{q^3} & \omega^q & \cdots & \omega^{q^{n-3}} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\omega^{q^{n-1}} & \omega^{q^{n-2}} & \omega^{q^{n-3}} & \cdots & \omega^0
\end{pmatrix}
\begin{pmatrix}
c_0 \\
c_1 \\
c_2 \\
\vdots \\
c_{n-1}
\end{pmatrix}
= 
\begin{pmatrix}
\sum_{k=0} m_{k0} \omega^{q^k} \\
\sum_{k=0} m_{k1} \omega^{q^k} \\
\sum_{k=0} m_{k2} \omega^{q^k} \\
\vdots \\
\sum_{k=0} m_{k,n-1} \omega^{q^k}
\end{pmatrix}
= M^\top
\begin{pmatrix}
\omega^0 \\
\omega^q \\
\omega^{q^2} \\
\vdots \\
\omega^{q^{n-1}}
\end{pmatrix}
\]

The assumption that \( M \) is a non-singular linear map is equivalent to the following: \( f_M(X) \) has no root in \( \mathbf{GF}(q^n)^* \).

7 The Rédei polynomial and its derivatives

7.1 The Rédei polynomial

Generally speaking, a Rédei polynomial is just a (usually multivariate) polynomial which splits into linear factors. We use the name Rédei polynomial to emphasize that these are not only fully reducible polynomials, but each linear factor corresponds to a geometric object, usually a point or a hyperplane of an affine or projective space.

Let \( S \) be a pointset of \( \mathbf{PG}(n, q) \), \( S = \{ \mathbf{P}_i = (a_i, b_i, ..., d_i) : i = 1, ..., |S| \} \).

The (Rédei-)factor corresponding to a point \( \mathbf{P}_i = (a_i, b_i, ..., d_i) \) is \( \mathbf{P}_i \mathbf{V} = a_i X + b_i Y + ... + d_i T \). This is simply the equation of hyperplanes passing through \( \mathbf{P}_i \).

When we decide to examine our pointset with polynomials, and if there is no
7. The Rédei polynomial and its derivatives

special, distinguished point in \( S \), it is quite natural to use symmetric polynomials of the Rédei-factors. The most popular one of these symmetric polynomials is the Rédei-polynomial, which is the product of the Rédei-factors, and the \(*\)-polynomial, which is the \((q - 1)\)-th power sum of them.

**Definition 7.1.** The Rédei-polynomial of the pointset \( S \) is defined as follows:

\[
R^S(X, Y, ..., T) = R(X, Y, ..., T) := \prod_{i=1}^{|S|} (a_iX + b_iY + ... + d_iT) = \prod_{i=1}^{|S|} P_i \cdot V.
\]

The points \((x, y, ..., t)\) of \( R \), i.e. the roots \( R(x, y, ..., t) = 0 \), correspond to hyperplanes (with the same \((n+1)\)-tuple of coordinates) of the space. The multiplicity of a point \((x, y, ..., t)\) on \( R \) is \( m \) if and only if the corresponding hyperplane \([x, y, ..., t]\) intersects \( S \) in \( m \) points exactly.

Given two pointsets \( S_1 \) and \( S_2 \), for their intersection

\[
R^{S_1 \cap S_2}(X, Y, ..., T) = \gcd \left( R^{S_1}(X, Y, ..., T) \right), \quad R^{S_2}(X, Y, ..., T)
\]

holds, while for their union, if we allow multiple points or if \( S_1 \cap S_2 = \emptyset \), we have

\[
R^{S_1 \cup S_2}(X, Y, ..., T) = R^{S_1}(X, Y, ..., T) \cdot R^{S_2}(X, Y, ..., T).
\]

**Definition 7.2.** The \(*\)-polynomial of \( S \) is

\[
G^S(X, Y, ..., T) = G(X, Y, ..., T) := \sum_{i=1}^{|S|} (a_iX + b_iY + ... + d_iT)^{q-1}.
\]

If a hyperplane \([x, y, ..., t]\) intersects \( S \) in \( m \) points then the corresponding \( m \) terms will vanish, hence \( G(x, y, ..., t) = |S| - m \) (in other words, all \( m \)-secant hyperplanes will be solutions of \( G(X, Y, ..., T) - |S| + m = 0 \)).

The advantage of the \(*\)-polynomial (compared to the Rédei-polynomial) is that it is of lower degree if \(|S| \geq q\). The disadvantage is that while the Rédei-polynomial contains the complete information of the pointset (\( S \) can be reconstructed from it), the \(*\)-polynomial of two different pointsets may coincide. This is a hard task in general to classify all the pointsets belonging to one given \(*\)-polynomial.

The \(*\)-polynomial of the intersection of two pointsets does not seem to be easy to calculate; the \(*\)-polynomial of the union of two pointsets is the sum of their \(*\)-polynomials.

The next question is what happens if we transform \( S \). Let \( M \in \text{GL}(n + 1, q) \) be a linear transformation. Then

\[
R^{M(S)}(V) = \prod_{i=1}^{|S|} (MP_i) \cdot V = \prod_{i=1}^{|S|} P_i \cdot (M^T V) = R^S(M^T V).
\]

The points \((x, y, ..., t)\) of \( R \), i.e. the roots \( R(x, y, ..., t) = 0 \), correspond to hyperplanes (with the same \((n+1)\)-tuple of coordinates) of the space. The multiplicity of a point \((x, y, ..., t)\) on \( R \) is \( m \) if and only if the corresponding hyperplane \([x, y, ..., t]\) intersects \( S \) in \( m \) points exactly.
For a field automorphism $\sigma$, $R^\sigma(S)(V) = (R^S)^\sigma(V)$, which is the polynomial $R^S$ but all coefficients are changed for their image under $\sigma$.

Similarly $G^{M(S)}(V) = G^S(M^T V)$ and $G^{\sigma(S)}(V) = (G^S)^\sigma(V)$.

The following statement establishes a further connection between the Rédei polynomial and the *-polynomial.

**Lemma 7.3.** (Gács) For any set $S$,

$$R^S \cdot (G^S - |S|) = (X^q - X)\partial_X R^S + (Y^q - Y)\partial_Y R^S + \ldots + (T^q - T)\partial_T R^S.$$ 

In particular, $R^S(G^S - |S|)$ is zero for every substitution $[x, y, \ldots, t]$.

**Proof:** Trivial induction on $|S|$.

We remark that

$$\partial_X G(X, Y, \ldots, T) = -\sum_{i=1}^{[S]} a_i (a_i X + b_i Y + \ldots + d_i T)^{q-2}.$$ 

Note that $\alpha^{q-2} = \frac{1}{\alpha}$ for all $0 \neq \alpha \in \text{GF}(q)$. Compare this to the derivative of the Rédei polynomial, see below.

Next we shall deal with Rédei-polynomials in the planar case $n = 2$. This case is already complicated enough, it has some historical reason, and there are many strong results based on algebraic curves coming from this planar case. Most of the properties of “Rédei-surfaces” in higher dimensions can be proved in a very similar way, but it is much more difficult to gain useful information from them.

Let $S$ be a pointset of $\text{PG}(2, q)$. Let $L_X = [1, 0, 0]$ be the line $\{(0, y, z) : y, z \in \text{GF}(q), (y, z) \neq (0, 0)\}$; $L_Y = [0, 1, 0]$ and $L_Z = [0, 0, 1]$. Let $N_X = |S \cap L_X|$ and $N_Y, N_Z$ are defined similarly. Let $S = \{P_i = (a_i, b_i, c_i) : i = 1, \ldots, |S|\}$.

**Definition 7.4.** The Rédei-polynomial of $S$ is defined as follows:

$$R(X, Y, Z) = \prod_{i=1}^{[S]} (a_i X + b_i Y + c_i Z) = \prod_{i=1}^{[S]} P_i \cdot V = r_0(Y, Z)X^{[S]} + r_1(Y, Z)X^{[S]-1} + \ldots + r_{[S]}(Y, Z).$$

For each $j = 0, \ldots, |S|$, $r_j(Y, Z)$ is a homogeneous polynomial in two variables, either of total degree $j$ precisely, or (for example when $0 \leq j \leq N_X - 1$) $r_j$ is identically zero. If $R(X, Y, Z)$ is considered for a fixed $(Y, Z) = (y, z)$ as a polynomial of $X$, then we write $R_{y,z}(X)$ (or just $R(X, y, z)$). We will say that $R$ is a curve in the dual plane, the points of which correspond to lines (with the same triple of coordinates) of the original plane. The multiplicity of a point $(x, y, z)$ on $R$ is $m$ if and only if the corresponding line $[x, y, z]$ intersects $S$ in $m$ points exactly.
Remark 7.5. Note that if \( r = 1 \), i.e. \([x, y, z]\) is a tangent line at some \((a_i, b_i, c_i) \in S\), then \( R \) is smooth at \((x, y, z)\) and its tangent at \((x, y, z)\) coincides with the only linear factor containing \((x, y, z)\), which is \(a_iX + b_iY + c_iZ\).

Exercise 7.6. Let \( S \) be the pointset of the parabola \( X^2 - YZ \) in \( \text{PG}(2, q) \). Prove that \( G^S(X, Y, Z) = X^{q-1} \) if \( q \) is even and \( G^S(X, Y, Z) = (X^2 - 4YZ)^{\frac{q-1}{2}} \) if \( q \) is odd. What is the geometrical meaning of it?

Exercise 7.7. Let \( S \) be the pointset of the parabola \( X^2 - YZ \) in \( \text{PG}(2, q) \). Prove that

\[
R^S(X, Y, Z) = Y \prod_{t \in \text{GF}(q)} (tX + t^2Y + Z) = Y(Z^q + Y^{q-1}Z - C_{q-1}Y^\frac{q+1}{2}Z^\frac{q-1}{2} - C_{q-3}X^2Y^\frac{q-5}{2}Z^\frac{q-3}{2} - \ldots - C_1X^{q-3}YZ^2 - C_0X^{q-1}Z),
\]

where \( C_k = \frac{1}{k+1} \binom{2k}{k} \) are the famous Catalan numbers.

Remark. If there exists a line skew to \( S \) then w.l.o.g. we can suppose that \( L_X \cap S = \emptyset \) and all \( a_i = 1 \). If now the lines through \((0, 0, 1)\) are not interesting for some reason, we can substitute \( Z = 1 \) and now \( R \) is of form

\[
R(X, Y) = \prod_{i=1}^{[S]} (X + b_iY + c_i) = X^{[S]} + r_1(Y)X^{[S]-1} + \ldots + r_{[S]}(Y).
\]

This is the affine Rédei polynomial. Its coefficient-polynomials are \( r_j(Y) = \sigma_j(\{b_iY + c_i : i = 1, \ldots, [S]\}) \), elementary symmetric polynomials of the linear terms \( b_iY + c_i \), each belonging to an ‘affine’ point \((b_i, c_i)\). In fact, substituting \( y \in \text{GF}(q) \), \( b_iY + c_i \) just defines the point \((1, 0, b_iY + c_i)\), which is the projection of \((1, b_i, c_i) \in S\) from the center ‘at infinity’ \((0, -1, y)\) to the line (axis) \([0, 1, 0]\).

One may ask what happens with the affine Rédei polynomial if the pointset \( \{(b_i, c_i)\} \) is translated by the vector \((u, v)\) or enlarged by \( \lambda \). Then \( R^{S+(u,v)}(X, Y) = R^S(X + uY + v, Y) \) and \( R^{\lambda S}(X, Y) = \lambda^{[S]}R^S(\frac{1}{\lambda}X, Y) \).

Exercise 7.8. Suppose that \( S = \{(x, f(x)) : x \in \text{GF}(q)\} \subset \text{AG}(2, q) \), i.e. the graph of a function \( Y = f(X) \), where \( f(X) = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_0 \). Express the Rédei polynomial of \( S \), or some coefficient if it, from the \( a_i\)-s.

How can one “see” the points of \( S \) from its Rédei polynomial?

1. They can be seen from the factors of \( R(X, Y, Z) \);

2. Let \( \{1, \omega, \omega^2\} \) be a base of \( \text{GF}(q^3) \) over \( \text{GF}(q) \). Then if \( b\omega + c\omega^2 \) is a root of \( R(X, \omega, \omega^2) \) then \((-1, b, c)\) is a point of \( S \). (You can’t see the points \((0, b, c)\) this way.)
3. If $S$ is an affine pointset then, using the affine Rédei polynomial $R(X,Y)$ and the $\overline{\text{GF}}(q^2)$-representation of $\text{AG}(2,q)$, with $\omega \in \overline{\text{GF}}(q^2) \setminus \text{GF}(q)$, now $R(X,\omega)$ has roots exactly $a+b\omega$ where $(-a,b)$ are the points of $S$.

7.2 Differentiation in general

Here we want to introduce some general way of “differentiation”. Give each point $P_i$ the weight $\mu(P_i) = \mu_i$ for $i = 1, \ldots, |S|$. Define the curve

$$R'_\mu(X,Y,Z) = \sum_{i=1}^{|S|} \mu_i \frac{R(X,Y,Z)}{a_i X + b_i Y + c_i Z}. \quad (*)$$

If $\forall \mu_i = a_i$ then $R'_\mu(X,Y,Z) = \partial_X R(X,Y,Z)$, and similarly, $\forall \mu_i = b_i$ means $\partial_Y R$ and $\forall \mu_i = c_i$ means $\partial_Z R$.

**Theorem 7.9.** Suppose that $[x,y,z]$ is an $m$-secant with $S \cap [x,y,z] = (P_{t_i}(a_{t_i}, b_{t_i}, c_{t_i}) : i = 1, \ldots, m)$. 

(a) If $m \geq 2$ then $R'_\mu(x,y,z) = 0$. Moreover, $(x,y,z)$ is a point of the curve $R'_\mu$ of multiplicity at least $m-1$.

(b) $(x,y,z)$ is a point of the curve $R'_\mu$ of multiplicity at least $m$ if and only if for all the $P_{t_j} \in S \cap [x,y,z]$ we have $\mu_{t_j} = 0$.

(c) Let $[x,y,z]$ be an $m$-secant with $[x,y,z] \cap [1,0,0] \not\in S$. Consider the line $[0,-z,y]$ of the dual plane. If it intersects $R'_\mu(X,Y,Z)$ at $(x,y,z)$ with intersection multiplicity $\geq m$ then $\sum_{j=1}^m \frac{\mu_{t_j}}{a_{t_j}} = 0$.

**Proof:** (a) Suppose w.l.o.g. that $(x,y,z) = (0,0,1)$ (so every $c_{t_j} = 0$). Substituting $Z = 1$ we have $R'_\mu(X,Y,1)$. In the sum (*) each term of $\sum_{\not\in \{t_1, \ldots, t_m\}} \mu_i \frac{R(X,Y,1)}{a_i X + b_i Y + c_i}$ will contain $m$ linear factors through $(0,0,1)$, so, after expanding it, there is no term with (total) degree less than $m$ (in $X$ and $Y$).

Consider the other terms contained in

$$\sum_{i \in \{t_1, \ldots, t_m\}} \mu_i \frac{R(X,Y,1)}{a_i X + b_i Y} = \frac{R(X,Y,1)}{R_{[0,0,1]}(X,Y,1)} \sum_{j=1}^m \mu_{t_j} \frac{R_{[0,0,1]}(X,Y,1)}{a_{t_j} X + b_{t_j} Y}.$$  

Here $\frac{R(X,Y,1)}{R_{[0,0,1]}(X,Y,1)}$ is non-zero in $(0,0,1)$. Each term $\frac{R_{[0,0,1]}(X,Y,1)}{a_{t_j} X + b_{t_j} Y}$ contains at least $m-1$ linear factors through $(0,0,1)$, so, after expanding it, there is no term with (total) degree less than $(m-1)$ (in $X$ and $Y$). So $R'_\mu(X,Y,1)$ cannot have such a term either.
Consider the polynomials \( R_{\mu}^{S_{[0,0,1]}}(X,Y,Z) \). They are \( m \) homogeneous polynomials in \( X, Y, Z \), of total degree \((m-1)\). Form an \( m \times m \) matrix \( M \) from the coefficients. If we suppose that \( \mu_j = 1 \) for all \( P_j \in S \cap [0,0,1] \) then the coefficient of \( X^{m-1-i}Y^k \) in \( R_{\mu}^{S_{[0,0,1]}}(X,Y,Z) \) is \( m_{jk} \) is \( \sigma_k(\{b_{t_1}, \ldots, b_{t_m}\} \setminus \{b_j\}) \) for \( j = 1, \ldots, m \) and \( k = 0, \ldots, m-1 \). So \( M \) is the elementary symmetric matrix (see in Section 9 on symmetric polynomials) and \( \det M = \prod_{i<j}(b_{t_i} - b_{t_j}) \), so if the points are all distinct then \( \det M \neq 0 \). Hence the only way of \( R_{\mu}^{S_{[0,0,1]}}(X,Y,Z) = 0 \) is when \( \forall j \mu_{t_j} = 0 \).

In order to prove (c), consider the line \([0,-z,y]\) in the dual plane. To calculate its intersection multiplicity with \( R_{\mu}^{S_{[0,0,1]}}(X,Y,Z) \) at \((x,y,z)\) we have to look at \( R_{\mu}^{S_{[0,0,1]}}(X,y,z) \) and find out the multiplicity of the root \( X = x \). As before, for each term of \( \sum_{i \in \{t_1, \ldots, t_m\}} \mu_{t_j} \frac{R(X,y,z)}{a_{t_j}X + b_{t_j}y + c_{t_j}z} \) this multiplicity is \( m \), while for the other terms we have
\[
\sum_{i \in \{t_1, \ldots, t_m\}} \mu_{t_j} \frac{R(X,y,z)}{a_{t_j}X + b_{t_j}y + c_{t_j}z} = \frac{R(X,y,z)}{R_{S[X,y,z]}(X,y,z)} \sum_{j=1}^m \mu_{t_j} \frac{R_{S[X,y,z]}(X,y,z)}{a_{t_j}X + b_{t_j}y + c_{t_j}z}.
\]
Here \( \frac{R(X,y,z)}{R_{S[X,y,z]}(X,y,z)} \) is non-zero at \( X = x \). Now \( R_{S[X,y,z]}(X,y,z) = \prod_{j=1}^m a_{t_j}X + b_{t_j}y + c_{t_j}z \).

Each term \( \frac{R_{S[X,y,z]}(X,y,z)}{a_{t_j}X + b_{t_j}y + c_{t_j}z} \) is of \((X-)\)degree at most \( m-1 \). We do know that the degree of \( \sum_{j=1}^m \mu_{t_j} \frac{R_{S[X,y,z]}(X,y,z)}{a_{t_j}X + b_{t_j}y + c_{t_j}z} \) is at least \((m-1)\) (or it is identically zero), as the intersection multiplicity is at least \( m-1 \). So if we want intersection multiplicity \( \geq m \) then it must vanish, in particular its leading coefficient
\[
(\prod_{j=1}^m a_{t_j}) \sum_{j=1}^m \frac{\mu_{t_j}}{a_{t_j}} = 0.
\]

Remark. If \( \forall \mu_i = a_i \), i.e. we have the partial derivative w.r.t \( X \), then each \( \frac{\mu_i}{a_{t_j}} \) are equal to 1. The multiplicity in question remains (at least) \( m \) if and only if on the corresponding \( m \)-secant \([x,y,z]\) the number of “affine” points (i.e. points different from \((0,-z,y)\)) is divisible by the characteristic \( p \).

In particular, we may consider the case when all \( \mu(\mathbf{P}) = 1 \). Consider
\[
R_1 = \sum_{\mathbf{b} \in B} \frac{R(X,Y,Z)}{a_{b_1}X + b_{b_2}Y + b_{b_3}Z} = \sigma_{|B|-1}(\{b_1X + b_2Y + b_3Z : \mathbf{b} \in B\}).
\]
For any \( \geq 2 \)-secant \([x, y, z]\) we have \( R_1(x, y, z) = 0 \). It does not have a linear component if \(|B| < 2q\) and \( B\) is minimal, as it would mean that all the lines through a point are \( \geq 2\)-secants. Somehow this is the “prototype” of “all the derivatives” of \( R \). E.g. if we coordinatize s.t. each \( b_1 \) is either 1 or 0, then 
\[
\frac{\partial^1 X}{\partial b_1} R = \sum_{b \in B \setminus L_X} \frac{R(X, Y, Z)}{b_1 X + b Y + b_2 Z},
\]
which is a bit weaker in the sense that it contains the linear factors corresponding to pencils centered at points in \( B \cap L_X \).

Substituting a tangent line \([x, y, z]\), with \( B \cap [x, y, z] = \{a\} \), into \( R_1 \) we get 
\[
R_1(x, y, z) = \prod_{b \in B \setminus \{a\}} (b_1 x + b_2 y + b_3 z),
\]
which is non-zero. It means that \( R_1 \) contains precisely the \( \geq 2 \)-secants of \( B \). In fact an \( m \)-secant will be a singular point of \( R_1 \), with multiplicity at least \( m - 1 \).

A similar argument shows, that in general, if 
\[
R_t = \sigma_{|B| - 1}(\{b_1 X + b_2 Y + b_3 Z : b \in B\}),
\]
then for any \( t + 1 \)-secant \([x, y, z]\) we have \( R_t(x, y, z) = 0 \). It does not have a linear component if \(|B| < (t + 1)q\) and \( B\) is minimal, as it would mean that all the lines through a point are \( \geq t + 1 \)-secants. Somehow this is the “prototype” of “all the \( t \)-th derivatives” of \( R \). E.g. if we coordinatize s.t. each \( b_1 \) is either 1 or 0, then 
\[
\frac{\partial^1 X}{\partial b_1} R = \sigma_{|B| - 1}(\{b_1 X + b_2 Y + b_3 Z : b \in B \setminus L_X\}),
\]
which is a bit weaker in the sense that it contains the linear factors corresponding to pencils centered at the points in \( B \cap L_X \).

Substituting a \( t \)-secant line \([x, y, z]\) into \( R_t \) we get 
\[
R_t(x, y, z) = \prod_{b \in B \setminus \{a\}} (b_1 x + b_2 y + b_3 z),
\]
which is non-zero. It means that \( R_0 \) contains all the \( \geq t + 1 \)-secants but none of the \( t \)-secants of \( B \). In fact \( R_t \) contains all the \( m \)-secants with multiplicity at least \( m - t \).

### 7.3 Hasse derivatives of the Rédei polynomial

The next theorem is about Hasse derivatives of \( R(X, Y, Z) \). (For its properties see Section 5.4.)

**Theorem 7.10.** (1) Suppose \([x, y, z]\) is an \( r \)-secant line of \( S \) with \([x, y, z] \cap S = \{(a_s, b_s, c_s) : l = 1, \ldots, r\}\). Then 
\[
(\mathcal{H}_X \mathcal{H}_Y \mathcal{H}_Z)^{r-i-j} R(x, y, z) = \sum_{m_1+\ldots+m_r \leq r \atop m_1 \leq \ldots \leq m_r} a_{s_{m_1}} \ldots a_{s_{m_r}} b_{s_{m_{1}+\ldots+m_r}} c_{s_{m_{1}+\ldots+m_r}}
\]
where 
\[
\bar{R}(x, y, z) = \prod_{i \notin \{s_1, \ldots, s_r\}} (a_i x + b_i y + c_i z),
\]
a non-zero element, independent from \( i \) and \( j \).

(2) From this we also have 
\[
\sum_{0 \leq t+j \leq r} (\mathcal{H}_X \mathcal{H}_Y \mathcal{H}_Z^{r-i-j} R)(x, y, z) X^t Y^j Z^{r-i-j} = \bar{R}(x, y, z) \prod_{l=1}^r (a_{s_l} X + b_{s_l} Y + c_{s_l} Z),
\]
constant times the Rédei polynomial belonging to \([x, y, z] \cap S\).
7. The Rédei polynomial and its derivatives

(3) If \( [x, y, z] \) is a \((\geq r+1)\)-secant, then \((\mathcal{H}_X^i\mathcal{H}_Y^j\mathcal{H}_Z^{r-i-j} R)(x, y, z) = 0\).

(4) If for all the derivatives \((\mathcal{H}_X^i\mathcal{H}_Y^j\mathcal{H}_Z^{r-i-j} R)(x, y, z) = 0\) then \([x, y, z]\) is not an \(r\)-secant.

(5) Moreover, \([x, y, z] \) is a \((\geq r+1)\)-secant iff for all \(i_1, i_2, i_3, 0 \leq i_1 + i_2 + i_3 \leq r\) the derivatives \((\mathcal{H}_X^{i_1}\mathcal{H}_Y^{i_2}\mathcal{H}_Z^{i_3} R)(x, y, z) = 0\).

(6) The polynomial

\[
\sum_{0 \leq i+j \leq r} (\mathcal{H}_X^i\mathcal{H}_Y^j\mathcal{H}_Z^{r-i-j} R)(X, Y, Z)X^iY^jZ^{r-i-j}
\]

vanishes for each \([x, y, z] \ (\geq r)\)-secant lines.

(7) In particular, when \([x, y, z] \) is a tangent line to \(S\) with \([x, y, z] \cap S = \{(a_t, b_t, c_t)\}\), then

\[
(\nabla R)(x, y, z) = (\ (\partial_X R)(x, y, z), \ (\partial_Y R)(x, y, z), \ (\partial_Z R)(x, y, z) \ ) = (a_t, b_t, c_t).
\]

If \([x, y, z] \) is a \((\geq 2)\)-secant, then \((\nabla R)(x, y, z) = 0\). Moreover, \([x, y, z] \) is a \((\geq 2)\)-secant iff \((\nabla R)(x, y, z) = 0\).

Proof: (1) comes from the definition of Hasse derivation and from \(a_{s_i}x + b_{s_i}y + c_{s_i}z = 0; i = 1, ..., r\). In general \((\mathcal{H}_X^i\mathcal{H}_Y^j\mathcal{H}_Z^{r-i-j} R)(X, Y, Z) = \)

\[
\sum_{m_1 + m_2 + ... + m_{l+1} \leq m_{l+2} \leq m_{l+3} \leq \cdots \leq m_{l+2+i} \leq \cdots \leq m_{l+2+i+j} \leq \cdots \leq m_{l+2+i+j} \leq \cdots \leq r} (a_{s_1}X + b_{s_1}Y + c_{s_1}Z).
\]

(2) follows from (1). For (3) observe that after the “\(r\)-th derivation” of \(R\) still remains a term \(a_{s_r}x + b_{s_r}y + c_{s_r}z = 0\) in each of the products. Suppose that for some \(r\)-secant line \([x, y, z]\) all the \(r\)-th derivatives are zero, then from (2) we get that \(\prod_{i=1}^{r}(a_{s_i}X + b_{s_i}Y + c_{s_i}Z)\) is the zero polynomial, a nonsense, so (4) holds. Now (5) and (7) are proved as well. For (6) one has to realise that if \([x, y, z] \) is an \(r\)-secant, still \(\prod_{i=1}^{r}(a_{s_i}x + b_{s_i}y + c_{s_i}z) = 0\).

Or: in the case of a tangent line

\[
\nabla R = \sum_{j=1}^{S} \nabla(P_j \cdot V) \prod_{i \neq j} P_i \cdot V = \sum_{j=1}^{S} P_j \prod_{i \neq j} (P_i \cdot V).
\]

7.4 Examples

In this section we compute the polynomials (curves) for some well-known pointsets. The computations are also used to illustrate several results and ideas of this book. In the cases
when the pointset is a blocking set, we use the notation \( f = (f_1, f_2, f_3) \) and \( g = (g_1, g_2, g_3) \) for certain curves (see Section 21.2) satisfying \( R = f \cdot (X, Y, Z) = g \cdot (Y^q Z - Y Z^q, Z^q X - Z X^q, X^q Y - X Y^q) \).

**Example 7.11.**

The line \([a, b, c] \). Its Rédéi polynomial is \( a(Y^q Z - Y Z^q) + b(Z^q X - Z X^q) + c(X^q Y - X Y^q) \).

**Example 7.12.**

A conic. For the Rédéi polynomial of the parabola \( X^2 - Y Z \) see Exercise 7.7.

**Example 7.13.**

The **projective triangle**. Let \( q \) be odd, \( B = \{(1, 0, 0); (0, 1, 0); (0, 0, 1)\} \cup \{(a^2, 0, 1); (1, -a^2, 0); (0, 1, a^2) : a \in \mathbb{GF}(q)^* \}. Then

\[
R(X, Y, Z) = X Y Z (-Z^{q-1} - X^{-1} Z^{-1}) (X^{-1} - Y^{-1} Z^{-1}) (-Z^{q-1} - Y^{q-1} Z^{-1}) =
\]

\[
(X^q - X) Y Z [Z^{q-1} - (-Y)^{q-1} + (Y^q - Y) X Z (-X)^{q-1} - Z^{q-1}] +
\]

\[
(Z^q - Z) X Y [(-Y)^{q-1} - (-X)^{q-1}] =
\]

\[
(X^q Y - Y^q Z) Z [Z^{q-1} - (-Y)^{q-1} - (-X)^{q-1}] + (Y^q Z - Y Z^q) X [(-X)^{q-1} - Z^{q-1} - (Y)^{q-1} +
\]

\[
(Z^q X - Z X^q) Y [(-Y)^{q-1} - Z^{q-1} - (-X)^{q-1}].
\]

Note that \( g = 0 \) iff \([x, y, z] = [a^2, 1, 0] \) or \([1, 0, -a^2] \) or \([0, -a^2, 1] \), so for the 2-secants.

**Example 7.14.**

The **sporadic almost-Rédéi blocking set**. The affine plane of order 3 can be embedded into \( \mathbb{PG}(2, 7) \) as the points of inflexion of a non-singular cubic. The 12 lines of this plane cover each point of \( \mathbb{PG}(2, 7) \), so in the dual plane they form a blocking set of size 12 = 3(7+1)/2, but its maximal line-intersection is only 4 = (12 - 7) - 1. A characterization of it can be found in [69].

A representation of this blocking set is the following: its affine part is \( U = \{(x, -x^3 + 3x^3 + 1, 1) : x \in \mathbb{GF}(7)\} \cup \{(0, -1, 1)\}, \) the infinite part is \( D = \{(1, 0, 0), (1, 1, 0), (1, 2, 0), (1, 4, 0)\}. Now

\[
R(X, Y, Z) = X^{10} Y^2 - X^{10} Z^2 - X^{7} Y^5 - 2 X^{7} Y^3 Z^2 + 3 X^{7} Y Z^4 - X^{4} Y^8 + X^{4} Z^8 + X Y^{11} +
\]

\[
X Y^3 Z^2 + 4 X Y^7 Z^4 + X Y^3 Z^8
\]

from which we get \( f = (X^{3} Y^2 - X^{3} Z^2 - Y^5 - 2 Y^3 Z^2 + 3 Y Z^4, -X^4 Y + X Y^4 + X Y^2 Z^2 + 4 X Z^4, X^4 Z + X Y^3 Z) \)

and \( g = (X Y^2 Z, X^3 Z + 2 Y^3 Z, X^3 Y - Y^4 + 3 Z^4) \).

Note that \( g(x, y, z) = (0, 0, 0) \) iff \((x, y, z) \in \{(0, 0, 0); (1, 2, 0); (1, 4, 0)\} \) and all three are 2-secants.

**Example 7.15.**
8. Univariate representations

The Baer-subplane.

In $\text{PG}(2, q^3)$ the standard embedding of a Baer subplane is $\{(a, b, 1) : a, b \in \text{GF}(\sqrt{q})\} \cup \{(m, 1, 0) : m \in \text{GF}(\sqrt{q})\} \cup \{(1, 0, 0)\}$. Now its Rédei polynomial is

$$R(X, Y, Z) = \prod_{a,b \in \text{GF}(\sqrt{q})} (aX + bY + Z) \prod_{a \in \text{GF}(\sqrt{q})} (aX + Y)X =$$

$$(X^q - X)[YZ - Y\sqrt{q}Z] + (Y^q - Y)[XZ - X\sqrt{q}Z] + (Z^q - Z)[XY - X\sqrt{q}Y] =$$

$$(Y^qZ - YZ^q)X\sqrt{q} + (Z^qX - ZX^q)Y\sqrt{q} + (X^qY - XY^q)Z\sqrt{q}.$$  

Here the equation of the blocking set is

$$X\sqrt{q}(c\sqrt{q}b - cb\sqrt{q}) + Y\sqrt{q}(a\sqrt{q}b - ab\sqrt{q}) + Z\sqrt{q}(a\sqrt{q}c - ac\sqrt{q}) = 0.$$  

Example 7.16.

In $\text{PG}(2, q^3)$ let $U = \{(x, x + x^q + x^{q^2}, 1) : x \in \text{GF}(q^3)\}$, and $D$ the directions determined by them, $|D| = q^2 + 1$.

Now for $B = U \cup D$ we get

$$f = ( X^{q^2}Z + X^{q^2-q}yZ - X^{q^2-q}Y Z^q + Y^{q^2}Z - Y Z^{q^2}, X^{q^2}Z + X^{q^2-q+1}Z^q + XZ^{q^2}, -X^{q^2+1} - X^{q^2}Y - X^{q^2-q+1}Y q - X Y q^2 )$$

and  

$$g = ( -X^{q^2}, X^{q^2} + X^{q^2-q}Y q + Y^{q^2}, X^{q^2-q}Z q + Z^{q^2} ).$$  

Example 7.17.

In $\text{PG}(2, q^3)$ let $U = \{(x, x^q, 1) : x \in \text{GF}(q^3)\}$, and $D$ the directions determined by them, $D = \{(1, a^{q-1}, 0) : a \in \text{GF}(q^3)\}$, $|D| = q^2 + q + 1$.

Then, after the linear transformation $(1, a^{q-1}, 0) \mapsto (1 - a^{q-1}, a^{q-1} - \beta, 0)$, where $\beta$ is a $(q - 1)$-st power, we have

$$r_{N_Z} = (X - \beta Y)^{q^2+q+1} - (X - Y)^{q^2+q+1}.$$  

Example 7.18.

The Hermitian curve. In $\text{PG}(2, q)$, the Hermitian curve, which is a unital, $\{(x, y, z) : x^{q+1} + y^{q+1} + z^{q+1} = 0\}$ in $\text{PG}(2, q)$ has the following Rédei polynomial:

$$R(X, Y, Z) = (X^{q+1} + Y^{q+1} + Z^{q+1})y^{q+1} - X^{q+1} - Y^{q+1} - Z^{q+1}.$$  

8 Univariate representations

Here we describe the analogue of the Rédei polynomial for the big field representations.
8.1 The affine polynomial and its derivatives

After the identification $\text{AG}(n, q) \leftrightarrow \text{GF}(q^n)$, described in Section 6, for a subset $S \subset \text{AG}(n, q)$ one can define the root polynomial

$$B_S(X) = B(X) = \prod_{s \in S} (X - s) = \sum_k (-1)^k \sigma_k X^{|S| - k};$$

and the direction polynomial

$$F(T, X) = \prod_{s \in S} (T - (X - s)^q) = \sum_k (-1)^k \hat{\sigma}_k T^{|S| - k}.$$

Here $\sigma_k$ and $\hat{\sigma}_k$ denote the $k$-th elementary symmetric polynomial of the set $S$ and $\{(X - s)^q : s \in S\}$, respectively. The roots of $B$ are just the points of $S$ while $F(x, t) = 0$ iff the direction $t$ is determined by $x$ and a point of $S$, or if $x \in S$ and $t = 0$.

If $F(T, x)$ is viewed as a polynomial in $T$, its zeros are the $\theta_{n-1}$-th roots of unity, moreover, $(x - s_1)^q = (x - s_2)^q$ if and only if $x, s_1$ and $s_2$ are collinear.

In the special case when $S = L_k$ is a $k$-dimensional affine subspace, one may think that $B_{L_k}$ will have a special shape.

We know that all the field automorphisms of $\text{GF}(q^n)$ are Frobenius-automorphisms $x \mapsto x^q$ for $i = 0, 1, \ldots, n - 1$, and each of them induces a linear transformation of $\text{AG}(n, q)$. Any linear combination of them, with coefficients from $\text{GF}(q^n)$, can be written as a polynomial over $\text{GF}(q^n)$, of degree at most $q^{n-1}$. These are called linearized polynomials. Each linearized polynomial $f(X)$ induces a linear transformation $x \mapsto f(x)$ of $\text{AG}(n, q)$. What’s more, the converse is also true: all linear transformations of $\text{AG}(n, q)$ arise this way. Namely, distinct linearized polynomials yield distinct transformations as their difference has degree $\leq q^{n-1}$ so cannot vanish everywhere unless they were equal. Finally, both the number of $n \times n$ matrices over $\text{GF}(q)$ and linearized polynomials of form $c_0 X + c_1 X^q + c_2 X^{q^2} + \ldots + c_{n-1} X^{q^{n-1}}, c_i \in \text{GF}(q^n)$ is $(q^n)^n$. This is the same argument as in Section 5.6.

Here we show (what we did already in 6.1) that

**Proposition 8.1.** (i) The root polynomial of a $k$-dimensional subspace of $\text{AG}(n, q)$ containing the origin, is a linearized polynomial of degree $q^k$;

(ii) the root polynomial of a $k$-dimensional subspace of $\text{AG}(n, q)$ is a linearized polynomial of degree $q^k$ plus a constant term.

**Proof:** (i) For $k = 0$ the statement is obvious, $B_0 = X$. Any one-dimensional linear subspace is of form $\{a \lambda : \lambda \in \text{GF}(q)\} = a\text{GF}(q)$ for some $a \in \text{GF}(q^n)^*$. The root polynomial of the one-dimensional subspace corresponding to $\text{GF}(q)$ is $B_{\text{GF}(q)} = X^q - X$, so the root polynomial of $a\text{GF}(q)$ is $B_{\text{GF}(q)}(a^{-1} X)$, which is a linearized polynomial of degree $q$. 
8. Univariate representations

Now if \(L\) is a subspace of dimension \(k > 1\) then let \(K\) be a subspace of \(L\) of dimension \(k - 1\). By induction, the root polynomial \(B_K\) is a linearized polynomial inducing a linear map with kernel \(K\). The image of \(L\) is one-dimensional, \(B_K(L) = M\). It is easy to check that \(B_L(X) = B_M(B_K(X))\).

(ii) Any subspace is a translate of a linear subspace; consider any subspace \(v + L\) with \(v \in \GF(q^n)\), its root polynomial is \(B_L(X - v)\). As \(B_L\) is a linear map, we have \(B_L(X - v) = B_L(X) - B_L(v)\).

A more compact form of the equation of a hyperplane is \(\Tr_{q^n \to q}(aX) + b = 0\), where \(a, b \in \GF(q^n), a \neq 0\). Indeed, for the root polynomial

\[
B_H(X) = \sum_{i=0}^{n-1} c_i X^{q^i} + b
\]

of the hyperplane \(H\), the polynomial \(c_{n-1}B_H^q - q^{q+1}(X^{q^n} - X) - c_q B_H\) has degree at most \(q^{n-2}\) and vanishes in all the \(q^n - 1\) points of \(H\), hence it is identically zero. Equating the coefficients of \(X^{q^i}\) for \(0 \leq i \leq n - 2\) implies the trace function form above.

Now we examine the derivative(s) of the affine root polynomial (written up with a slight modification). Let \(S \subseteq \GF(q^n)\) and consider the root and direction polynomials of \(S^{-1} = \{1/s : s \in S\}:

\[
B(X) = \prod_{s \in S} (1 - sX) = \sum_k (-1)^k \sigma_k X^k;
\]

\[
F(T, X) = \prod_{s \in S} (1 - (1 - sX)^{q-1}T) = \sum_k (-1)^k \tilde{\sigma}_k T^k.
\]

For the characteristic function \(\chi\) of \(S^{-1}\) we have \(|S| - \chi(X) = \sum_{s \in S} (1 - sX)^{q^n-1}\). Then, as \(B'(X) = B(X) \sum_{s \in S} \frac{1}{1 - sX}\), we have \((X - X^{q^n})B' = B(|S| - \sum_{s \in S} (1 - sX)^{q^n-1}) = B\chi\), after derivation \(B' + (X - X^{q^n})B'' = B\chi + B\chi',\) so \(B' \equiv (B\chi)'\) and (as \(B\chi \equiv 0\)) we have \(BB' \equiv B^2\chi'\).

8.2 The projective polynomial

After the identification \(\PG(n, q) \leftrightarrow \GF(q^{n+1})/\GF(q)^*\), described in Section 6, for a subset \(S \subseteq \PG(n, q)\) one can define \(C_0(X) = \prod_{s \in S} \Tr(sX) =

\[
= X^{\sum_{s \in S} (1)} \prod_{s \in S} (X^{q^{n-1} \theta_{n-1} (s^{q-1})^\theta_{n-1} + \ldots + (X^{q-1} \theta_1 (s^{q-1})^\theta_1 + X^{q-1} s^{q-1} + 1)).
\]
So it is enough to consider
\[ C(X) = \prod_{s \in S} \left( \sum_{i=0}^{n-1} (X^{q-1})^\theta_i (s^{q-1})^\theta_i + 1 \right) = \prod_{\beta \in S^{[n-1]}} \left( \sum_{i=0}^{q-1} Y^{\theta_i} \beta^{\theta_i} + 1 \right) = \prod_{\beta^{-1} \in S^{[n-1]}} \left( \sum_{i=0}^{q-1} Y^{\theta_i} \beta^{\theta_i - \theta_i} + \beta^{\theta_i - 1} \right), \]
where \( Y = X^{q-1} \).

Here the *direction polynomial* is
\[ F(U, X) = \prod_{s \in S} (1 - sX(1 - sX)^{q-1}U). \]

For a value \( x \), the linear factors of \( F(U, x) \) have zeros of the form \( u^{-1} = sx(1 - sx)^{q-1} \) which satisfies \( 1 + v + v^{q+1} + v^{q^2+q+1} + \ldots + v^{\theta_n - 1} = 0 \) for \( v = u^{-1} \). Moreover, \( s_1x(1 - s_1x)^{q-1} = s_2x(1 - s_2x)^{q-1} \) if and only if \( 1/x, s_1 \) and \( s_2 \) are collinear, so there is a one-to-one correspondence between the zeros \( v \) and the \( \theta_n - 1 \) direction of lines through \( 1/x \).

### 8.3 Examples

This section is about the polynomials for some well-known pointsets, like in a former part. We leave them as exercises.

**Affine sets**

For an affine line we have the equation \( X^q - c_0X + b = 0 \) as we have seen already.

**Exercise 8.2.** Calculate the polynomials of the following affine pointsets.
For an ellipse, i.e. the \( q + 1 \) points of a conic contained in \( \text{AG}(2, q) \).

An affine Baer-subplane: \( A = \text{AG}(2, \sqrt{q}) = \{(a, b) : a, b \in \text{GF}(\sqrt{q})\} \leftrightarrow \{a + b\omega : a, b \in \text{GF}(\sqrt{q})\} \subset \text{GF}(q^2) \).

**Projective sets**

**Exercise 8.3.** Calculate the polynomials of the following projective pointsets.
A conic.

The projective triangle, see Section 7.4.

A Baer-subplane \( \text{PG}(2, \sqrt{q}) \) of \( \text{PG}(2, q) \) in “standard position”.

The cyclic embedding of the Baer-subplane: \( \text{GF}(q^3) = \langle w \rangle, B = \langle w^{q-\sqrt{q}+1} \rangle \).

The cyclic \((q - \sqrt{q} + 1)\)-arc

The Hermitian curve.
9 Symmetric polynomials and invariants of subsets

9.1 The Newton formulae

In this section we recall some classical results on symmetric polynomials. For more information and the proofs of the results mentioned here, we refer to [135].

The multivariate polynomial \( f(X_1, \ldots, X_t) \) is symmetric, if \( f(X_1, \ldots, X_t) = f(X_{\pi(1)}, \ldots, X_{\pi(t)}) \) for any permutation \( \pi \) of the indices \( 1, \ldots, t \). Symmetric polynomials form a (sub)ring (or submodule over \( F \)). The most famous particular types of symmetric polynomials are the following two:

**Definition 9.1.** The \( k \)-th elementary symmetric polynomial of the variables \( X_1, \ldots, X_t \) is defined as

\[
\sigma_k(X_1, \ldots, X_t) = \sum_{\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, t\}} X_{i_1}X_{i_2} \cdots X_{i_k}.
\]

\( \sigma_0 \) is defined to be 1 and for \( j > t \) \( \sigma_j = 0 \), identically.

Given a (multi)set \( A = \{a_1, a_2, \ldots, a_t\} \) from any field, it is uniquely determined by its elementary symmetric polynomials, as

\[
\sum_{i=0}^{t} \sigma_i(A)X^{t-i} = \prod_{j=1}^{t}(X + a_j).
\]

**Definition 9.2.** The \( k \)-th power sum of the variables \( X_1, \ldots, X_t \) is defined as

\[
\pi_k(X_1, \ldots, X_t) := \sum_{i=1}^{t} X_i^k.
\]

The power sums determine the (multi)set a “bit less” than the elementary symmetric polynomials. For any fixed \( s \) we have

\[
\sum_{i=0}^{s} \binom{s}{i} \pi_i(A)X^{s-i} = \sum_{j=1}^{t} (X + a_j)^s
\]

but in general it is not enough to gain back the set \( \{a_1, \ldots, a_t\} \). Note also that in the previous formula the binomial coefficient may vanish, and in this case it “hides” \( \pi_i \) as well.

One may feel that if a (multi)set of field elements is interesting in some sense then its elementary symmetric polynomials or its power sums can be interesting as well.

E.g.

\( A = \text{GF}(q) \): \( \sigma_j(A) = \pi_j(A) = \begin{cases} 
0, & \text{if } j = 1, 2, \ldots, q - 2, q; \\
-1, & \text{if } j = q - 1.
\end{cases} \)

\( \prod_{a \in \text{GF}(q)^*} a = -1 \) in Wilson’s theorem
If $A$ is an additive subgroup of $\text{GF}(q)$ of size $p^k$: $\sigma_j(A) = 0$ whenever $p \nmid j < q - 1$ holds. Also $\pi_j(A) = 0$ for $j = 1, \ldots, p^k - 2, p^k$.

If $A$ is a multiplicative subgroup of $\text{GF}(q)$ of size $d|q - 1)$: $\sigma_j(A) = \pi_j(A) = 0$ for $j = 1, \ldots, d - 1$.

The fundamental theorem of symmetric polynomials: Every symmetric polynomial can be expressed as a polynomial in the elementary symmetric polynomials.

There are several proofs for this theorem, the most well-known one uses induction for the exponent-series of the terms after ordering the terms in a lexicographic way; one may formulate the proof in the language of initial ideals (see [72]), or there is another one using Galois-theory, etc.

According to the fundamental theorem, also the power sums can be expressed in terms of the elementary symmetric polynomials. The Newton formulae are equations with which one can find successively the relations in question. Essentially there are two types of them:

$$k\sigma_k = \pi_1\sigma_{k-1} - \pi_2\sigma_{k-2} + \ldots + (-1)^{i-1}\pi_i\sigma_{k-i} + \ldots + (-1)^{k-1}\pi_k\sigma_0$$

(N1)

and

$$\pi_{t+k} - \pi_{t+k-1}\sigma_1 + \ldots + (-1)^{t}\pi_{t+k-i}\sigma_i + \ldots + (-1)^{t}\pi_k\sigma_t = 0.$$  

(N2)

In the former case $1 \leq k \leq t$, in the latter $k \geq 0$ arbitrary. Note that if we define $\sigma_i = 0$ for any $i < 0$ or $i > t$, and, for a fixed $k \geq 0$, $\pi_0 = k$, then the following equation generalizes the previous two:

$$\sum_{i=0}^{k} (-1)^{i}\pi_i\sigma_{k-i} = 0.$$  

(N3)

Exercise 9.3. Prove the Newton identities by differentiating

$$B(X) = \prod_{s \in S} (1 + sX) = \sum_{i=0}^{|S|} \sigma_i X^i.$$  

Symmetric polynomials play an important role when we use Rédei polynomials, as e.g. expanding the affine Rédei polynomial $\prod_{a \in \text{GF}(q)} (X + aY + b_i)$ by $X$, the coefficient polynomials will be of the form $\sigma_k(\{a_iY + b_i : i\})$.

Magic. (Gács) Let $f(X) = \sum_{i=0}^{q-1} c_iX^i$ be a polynomial from $\text{GF}(q)[X]$. Consider the following (affine Rédei-) polynomial of its graph:

$$\prod_{a \in \text{GF}(q)} (X - aY - f(a));$$  

I. Background
then its homogeneous part of degree \( q - 1 \) is precisely the homogenized form of \( f \), i.e. \( \sum_{i=0}^{q-1} c_i X^i Y^{q-1-i} \).

**Proof:** Let \( \gamma_k \) be the coefficient of \( X^{q-1-k} Y^k \) in the Rédei-polynomial, we prove by induction that \( \gamma_k = c_{q-1-k} \). Let \( \text{GF}(q) = \{a_1, \ldots, a_q\} \) and \( b_i = f(a_i) \).

We know that \( \gamma_0 = -\sum b_i = c_{q-1} \) and

\[
\gamma_k = (-1)^{k+1} \sum_{i_1 < \ldots < i_k} a_{i_1} \cdots a_{i_k} \sum_{i \notin \{i_1, \ldots, i_k\}} b_i
\]

if \( 1 \leq k \leq q - 1 \). Hence \( \gamma_k = (-1)^{k+1} \sigma_k(a_1, \ldots, a_q) \sum_{i=1}^{q} b_i + \hat{\gamma}_{k-1} \), where \( \hat{\gamma}_{k-1} \) is defined as \( \gamma_{k-1} \), with \( b_i \) replaced by \( a_i b_i \).

Let \( \hat{f}(X) = (c_0 + c_{q-1}) X + \sum_{i=2}^{q-1} c_{i-1} X^i \); then \( \hat{f}(a_i) = a_i b_i \). By induction we may assume that \( \hat{\gamma}_{k-1} \) is the coefficient of \( X^{q-k} \) in \( \hat{f}(X) \). Hence we obtain

\[
\gamma_k = \hat{\gamma}_{k-1} = c_{q-k-1}
\]

for \( k < q - 1 \); finally \( \gamma_{q-1} = -c_{q-1} + \hat{\gamma}_{q-2} = c_0 \).

**Corollary 9.4.** Expanding the Rédei-polynomial

\[
\prod_{a \in \text{GF}(q)} (X - a Y - f(a)) = \sum_{k=0}^{q} r_k(Y) X^{q-k},
\]

for \( k = 1, \ldots, q - 2 \) we get \( \deg_Y(r_k) \leq k - 1 \); equality holds iff \( c_{q-k} \neq 0 \).

**Proof:** The first part is easy: \( r_k(Y) = (-1)^k \sigma_k(\{(aY + f(a)) : a \in \text{GF}(q)\}) \) so the leading coefficient is just \( \sigma_k(\text{GF}(q)) = 0 \). The second part, the case of equality follows from the previous statement.

Given \( S = \{x_1, x_2, \ldots, x_n\} \), the following determinant is called the Vandermonde-determinant of \( S \):

\[
VdM(x_1, x_2, \ldots, x_n) = \begin{vmatrix}
1 & 1 & \cdots & 1 \\
x_1 & x_2 & \cdots & x_n \\
x_1^2 & x_2^2 & \cdots & x_n^2 \\
\vdots & \vdots & \ddots & \vdots \\
x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1}
\end{vmatrix} = \prod_{i<j} (x_i - x_j)
\]

The \( P \)-adic (\( P = p^e \), \( p \) prime) Moore-determinant of \( S \) is

\[
MRD_P(x_1, \ldots, x_n) = \begin{vmatrix}
x_1^1 & x_2^1 & \cdots & x_n^1 \\
x_1^2 & x_2^2 & \cdots & x_n^2 \\
\vdots & \vdots & \ddots & \vdots \\
x_1^{p^{n-1}} & x_2^{p^{n-1}} & \cdots & x_n^{p^{n-1}}
\end{vmatrix} = \prod_{(\lambda_1, \ldots, \lambda_n) \in \text{PG}(n-1, P)} \sum_{i=1}^{n} \lambda_i x_i
\]
Note that this formula gives the value of the determinant up to a non-zero constant only, one way to find the exact value is choosing each homogeneous vector $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ in such a way that its first non-zero coordinate is 1.

The **elementary symmetric determinant** of $S$ is

$$
\begin{vmatrix}
1 & 1 & \cdots & 1 \\
\sigma_1(S \setminus \{x_1\}) & \sigma_1(S \setminus \{x_2\}) & \cdots & \sigma_1(S \setminus \{x_n\}) \\
\sigma_2(S \setminus \{x_1\}) & \sigma_2(S \setminus \{x_2\}) & \cdots & \sigma_2(S \setminus \{x_n\}) \\
\vdots & \vdots & \ddots & \vdots \\
\sigma_{n-1}(S \setminus \{x_1\}) & \sigma_{n-1}(S \setminus \{x_2\}) & \cdots & \sigma_{n-1}(S \setminus \{x_n\})
\end{vmatrix} = \prod_{i<j} (x_i - x_j)
$$

**Exercise 9.5.** Give a unified proof for the determinant formulae! (Hint: consider $x_1, \ldots, x_n$ as free variables.)

**Exercise 9.6.**

(a) Prove that $V d M(x_1, x_2, \ldots, x_n) \neq 0$ iff $\{x_1, \ldots, x_n\}$ are pairwise distinct.

(b) Prove that $MRD_{p^e}(x_1, x_2, \ldots, x_n) \neq 0$ iff $\{x_1, \ldots, x_n\}$ are independent over $GF(p^e)$.

(c) Prove the following version of Wilson’s theorem:

$$
\prod_{y \in \{x_1, \ldots, x_n\} \setminus GF(p^e)} y = (-1)^n MRD_{p^e}(x_1, \ldots, x_n)^{p^e-1}.
$$

**Exercise 9.7.** Prove the following general form of the elementary symmetric determinant: Given $S = \{x_1, x_2, \ldots, x_{n+1}, \ldots, x_m\}$,

$$
\begin{vmatrix}
1 & 1 & \cdots & 1 \\
\sigma_1(S \setminus \{x_1\}) & \sigma_1(S \setminus \{x_2\}) & \cdots & \sigma_1(S \setminus \{x_m\}) \\
\sigma_2(S \setminus \{x_1\}) & \sigma_2(S \setminus \{x_2\}) & \cdots & \sigma_2(S \setminus \{x_m\}) \\
\vdots & \vdots & \ddots & \vdots \\
\sigma_{n-1}(S \setminus \{x_1\}) & \sigma_{n-1}(S \setminus \{x_2\}) & \cdots & \sigma_{n-1}(S \setminus \{x_m\})
\end{vmatrix} = \prod_{1 \leq i < j \leq n} (x_i - x_j),
$$

so somehow the elements $x_{n+1}, \ldots, x_m$ “do not count”.

**Exercise 9.8.** Prove that

$$
\prod_{\Delta \in GF(q)^n} (T + \lambda_1 X_1 + \lambda_2 X_2 + \ldots + \lambda_{n-1} X_{n-1} + \lambda_n) =
$$

$$
\begin{vmatrix}
T & X_1 & X_2 & \cdots & X_{n-1} & 1 \\
T^q & X_1^q & X_2^q & \cdots & X_{n-1}^q & 1 \\
T^{q^2} & X_1^{q^2} & X_2^{q^2} & \cdots & X_{n-1}^{q^2} & 1 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
T^{q^n} & X_1^{q^n} & X_2^{q^n} & \cdots & X_{n-1}^{q^n} & 1
\end{vmatrix}
\begin{vmatrix}
X_1 & X_2 & \cdots & X_{n-1} & 1 \\
X_1^q & X_2^q & \cdots & X_{n-1}^q & 1 \\
X_1^{q^2} & X_2^{q^2} & \cdots & X_{n-1}^{q^2} & 1 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
X_1^{q^n-1} & X_2^{q^n-1} & \cdots & X_{n-1}^{q^n-1} & 1
\end{vmatrix}.
$$
9. Symmetric polynomials and invariants of subsets

9.2 The invariants $u_f, v_f$ and $w_f$

In this section, which is extracted from [135] mostly, we consider a fixed polynomial $f(X) = \sum_{i=0}^n c_i X^i \in \text{GF}(q)[X]$ of degree $n$. Put $s_k = \sigma_k(\{f(x) : x \in \text{GF}(q)\})$, so $\prod_{x \in \text{GF}(q)}(X + f(x)) = \sum_{k=0}^q s_k X^{q-k}$.

- Let $u = u_f$ be the smallest positive integer $k$ with $s_k \neq 0$ if such $k$ exist, otherwise set $u = \infty$.
- Let $v = v_f$ denote the number of distinct values of $f$ (so $v \geq 2$ if we assume that $f$ is not a constant function). If $v = q$ then $f$ is called a permutation polynomial (PP).
- Let $w = w_f$ be the smallest positive integer with $p_k = \pi_k(\{f(x) : x \in \text{GF}(q)\}) = \sum_{x \in \text{GF}(q)} f(x)^k \neq 0$ if such $k$ exists, otherwise set $w = \infty$.

One can find another description of $u$ and $w$ in Proposition 9.9.

Firstly we study the relations among $u, v, w, n, q$. Then we shall investigate the number $M_f$ of $c \in \text{GF}(q)$ such that $f(X) - cX$ is a PP. With any family $S$ of $q$ elements of $\text{GF}(q)$, counted possibly with multiplicity, we may associate the same invariants $u = u_S, v = v_S, w = w_S$ as above; obviously the order of the values is irrelevant. However, $n$ measures the “complexity” of this set (ordered in a certain sense) somehow. If $g(X)$ is a permutation polynomial then $f(g(X))$ has the same invariants $u, v$ and $w$ as $f$; and the same is true if $f$ is replaced by $af(X) + b$ with $a, b \in \text{GF}(q), a \neq 0$ (and $b = 0$ if $v = 1$).

The similar invariants can be defined for a (multi)set $S$ of cardinality $S \neq q$. Note that if $|S| < q$ then the multiset $S' = (q - |S|)\{0\} = S$ of size $q$ has the same invariants $u$ and $w$ as $S$, while $v$, the number of distinct elements of $S$, increases by one iff $0 \not\in S$.

If $|S| > q$ and $v = q$ then for $S' = S \setminus \text{GF}(q)$ we have $u_{S'} = u_S$ and $w_{S'} = w_S$ if any of these values is less than $q - 1$.

Proposition 9.9. (a) $q - u$ is the degree of $X^q - \prod_{a \in \text{GF}(q)} (X - f(a))$. This polynomial is equal to $c \in \text{GF}(q)$ iff $f(X) = c$ is a constant polynomial. Hence $v \geq 2$ implies $1 \leq u < q$ and $v = 1$ implies $u = q$ or $u = \infty$ according to $f = 0$ or $f = c \neq 0$.

(b) $q - 1 - w = \deg \left( \sum_{a \in \text{GF}(q)} (X - f(a))^{q-1} \right) = \deg \left( \prod_{a \in \text{GF}(q)} (X - f(a)) \right)$.

(c) $\sum_{a \in \text{GF}(q)} a^k f(a) = -c_{q-1-k}$ for $0 \leq k < q - 1$ and $\sum_{a \in \text{GF}(q)} a^{q-1} f(a) = -(c_q + c_{q-1})$. Hence $n = q - 1$ iff $u = 1$ iff $w = 1$. For arbitrary $f$ we have that $f$ has reduced degree $\leq q - l - 2$ iff $\sum_{a \in \text{GF}(q)} a^k f(a) = 0$ for $0 \leq k \leq l$. (We will see it later again.)
I. Background

(d) From (c) it is clear that \( w \) is the smallest positive integer \( k \) such that the reduction of \( f(X)^k \mod X^q - X \) has degree \( q - 1 \), if such \( k \) exists, and otherwise \( w = \infty \).

Note that if \( v \geq 2 \) then (c) implies that one can change the order of the values such that the polynomial will have degree \( q - 1 \) or \( q - 2 \) (in fact one transposition is enough); while the invariants \( u, v, w \) remain the same.

Lemma 9.10. (a) If \( 1 \leq k \leq q \) and \( k < u + w \) then \( p_k = (-1)^{k-1}ks_k \).
(b) If \( ks_k \neq 0 \) for some \( 1 \leq k \leq q - 1 \) then \( w \) is the smallest \( k \) with this property, otherwise \( w = \infty \).

For (a) use the Newton identity, for (b) see (d) below.

Here we simply enlist some of the relations known for \( u, v, w, n, q \), most of them are easy to prove (an asterisk denotes some of the non-obvious ones):

Proposition 9.11.

(a) \( v = 1 \iff n = 0 \) or \( n = -\infty \), \( u = q \) in the first and \( u = \infty \) in the latter case;
(b) if \( n \geq 1 \) then \( v \geq q/n \) and hence \( v \geq \left\lfloor \frac{q-1}{n} \right\rfloor + 1 \). \( v = q/n \Rightarrow w = \infty \) or \( n = 1 \). \( v = \left\lfloor \frac{q-1}{n} \right\rfloor + 1 \) implies \( n|q - 1 \) or \( w = \infty \). If \( \gcd(n, p) = 1 \) then the case \( n|q - 1 \) can occur only. If \( n < p \) then \( f \) is of form \( a(X - b)^n + c \) with \( a \neq 0 \).
(c) \( n = q - 1 \iff u = 1 \iff w = 1 \);
(d) If \( w < \infty \) then \( w < q \) (since \( f(a)^n = f(a) \)); and \( p \not| w \) (since \( p_{kp} = (pk)^p \)). Compare to the section on Vandermonde sets, 9.3;
(e) \( w < \infty \Rightarrow w < v \);
(f) \( w \geq \frac{q-1}{n} \), with equality iff \( n|q - 1 \);
(g) \( w = \infty \iff \) for each \( a \in \text{GF}(q) \) the number \( n_a \) of preimages of \( a \) is divisible by \( p \), see Exercise 9.17.
(h) \( w = \infty \Rightarrow n \geq p, \ v \leq q/p \) (if \( n \geq 1 \));
(i) if \( f(X) = X^p - X \) then \( w = \infty, \ n = p, \ v = q/p \);
(j) if \( f(X) = X^n \) then \( w = v - 1 \);
(k) \( n|q - 1 \Rightarrow v \leq q - 1 \);
(l) \( w < \infty \Rightarrow u \leq w, \) with equality iff \( p \not| u \);
(m) \( w = \infty \Rightarrow p|u \) or \( u = \infty \);
(n) \( * \) \( w < \infty \Rightarrow w < 2(q - v) \) or \( v = q \);
9. Symmetric polynomials and invariants of subsets

(o) \( u \geq \frac{q-1}{n} \), with equality if \( n|q-1 \);

(p) \( 2 \leq v < q \Rightarrow u + v \leq q \);

(q) \( v < q \Rightarrow v < q - \frac{q-1}{n} \) (if \( n \geq 1 \));

(r) \( v < q \Rightarrow w \leq \frac{2q}{3} - 1 \) if \( w < \infty \), (this bound is probably not optimal);

(s) \( v < q \Rightarrow v + w \leq \frac{4q}{3} - 1 \) if \( w < \infty \), (this bound is probably not optimal);

(t) \( v < q \Rightarrow v + w \leq q \) if \( v > q - p, v > 1 \).

The proof of (e) is obvious from the first equality of Proposition 9.9 (b): if \( g(X) = \sum_{a \in \text{GF}(q)} (X - f(a))^{q-1} \) then for every \( b \), which is not in the range of \( f(X) \), we have \( f(b) = 0 \). For another proof (and a generalization) see Exercise 9.14.

Proposition 9.12. The following properties are equivalent if \( 1 \leq n < q \):

(a) \( v = q \), i.e. \( f \) is a permutation polynomial;

(b) \( u = q - 1 \);

(c) \( u > q - q/n \);

(d) \( u > q - v \);

(e) \( v > q - \frac{q-1}{n} \);

(f) \( w = q - 1 \);

(g) \( 2q/3 - 1 < w < \infty \);

(h) \( q - \frac{q+1}{n} < w < \infty \);

(i) \( q - u \leq w < \infty \);

(j) \( u > \frac{q-1}{2} \) and \( w < \infty \).

Exercise 9.13. Prove that if \( w_f \geq q-1 \) then either (i) \( f \) is a permutation polynomial and \( \sum_x f(x)^{q-1} = -1 \); or (ii) \( \sum_x f(x)^{q-1} = 0 \) and \( f \) assumes every value \( 0 \mod p \) times.

A general form of Proposition 9.11 (e) is the following:

Exercise 9.14. (P. Das) Let \( f(X_1, \ldots, X_n) \) be a polynomial, its value set (range) is \( V(f) = \{ f(\alpha_1, \ldots, \alpha_n) : (\alpha_1, \ldots, \alpha_n) \in \text{GF}(q)^n \} \). Define \( w_f \) as the smallest positive integer \( k \) such that \( \sum_{(\alpha_1, \ldots, \alpha_n) \in \text{GF}(q)^n} f(\alpha_1, \ldots, \alpha_n)^k \neq 0 \). Prove (using a Vandermonde determinant) that \( |V(f)| \geq w_f + 1 \).

We defined \( M_f \) as the number of elements in \( C = \{ c \in \text{GF}(q) : f(X) - cX \text{ is a permutation polynomial} \} \). An alternative definition can be given with the help of the following
Proposition 9.15. Let \( D = D_f = \{ \frac{f(a) - f(b)}{a - b} : a \neq b \in \text{GF}(q) \} \), the set of difference quotients (or directions), determined by (the graph of) \( f \). Then \(-C = \text{GF}(q) \setminus D\).

Later we will use the notation \( N = N_f = |D| \) for the number of directions determined by \( f \). The obvious connection is

\[
M_f + N_f = q.
\]

For more on directions we refer to Section 18. Note that \( M_f \) is “a bit less invariant” than \( u, v, w \) are; in general, if \( f \) is changed for \( a \cdot f(g(X)) + b \cdot X + c, \) \( M_f \) remains the same only if \( g(X) \) is a linear polynomial (and not an arbitrary permutation, as in the earlier cases, but there the term \( bX \) was not allowed).

Let \( n_k \) denote the reduced degree of \( f(X)^k \). Here we summarize some properties of \( M_f \):

1. If \( f(X) + cX \) is a permutation polynomial then for \( 1 \leq k < q - 1 \), in the notation \( \prod_{a \in \text{GF}(q)}(X - aY - f(a)) = \sum_{k=0}^{q} r_k(Y)X^{q-k} \) (see Magic), we have \( r_k(c) = 0 \). So if \( r_k(Y) \neq 0 \) then \( \deg_Y(r_k) \geq M_f \).

2. \( n_1 < q - M_f \).

3. If \( M_f < p \) then \( n_k < q - M_f + k - 1 \) for all \( k \geq 1 \).

4. If \( M_f + 1 < p \) and \( n_1 < q - M_f - 1 \) then \( n_k < q - M_f + k - 2 \) for all \( k \geq 1 \).

5. If \( f(X) = X^n \) and \( n \mid q \) then \( X^n - cX \) is a PP iff \( a^n - ca \neq 0 \) if \( a \neq 0 \).

Hence (if \( n > 1 \)) \( q - M_f \) is the number of \( (n-1)\)-st powers in \( \text{GF}(q)^* \), so \( q - M_f = \frac{q-1}{\gcd(n-1,q-1)} \). In particular, for \( n = q/p \) we have \( M_f = q - \frac{q-1}{p-1} \), while \( n = \sqrt{q} \) yields \( M_f = q - \sqrt{q} - 1 \).

6. \( M_f \leq 1 \) if \( 1 < n^4 < p = q \).

7. \( M_f \leq n - 1 \) if \( n \not\mid q \) and \( n^4 \leq q \).

8. \( M_f \leq q - 1 \) with equality iff \( f \) has reduced degree \( \leq 1 \).

9. \( M_f \leq q - \frac{q-1}{n-1} \) if \( 1 < n < q \).

10. If \( M_f < q - 1 \) then \( M_f \leq q - \sqrt{q} - 1 \). See Section 21.

11. (Lovász-Schrijver) If \( q = p \) then \( M_f \leq \frac{p-3}{2} \). If \( M_f = \frac{p-3}{2} \) then \( f(X) = X^{\frac{p+1}{2}} \), up to a linear transform; see Theorem 19.1 as well.
12. (Rédei) If $M_f > \frac{q^3}{2}$ then

(i) if $f(X) - cX$ is not a PP then the number of preimages of each value $f(a) - ca$ is divisible by $p$;

(ii) $M_f \geq q - \frac{2}{p+1}$ and $p|(M_f + 1)$;

(iii) if $n < q$ then $f'(X) = f'(0)$.

(iv) in fact much more is known: in this case, after assuming $f(0) = 0$, $f$ is “linear over $\mathbb{GF}(p^e)$” for some $e|h$ (so $\mathbb{GF}(p^e)$ is a subfield of $\mathbb{GF}(q = p^h)$); for details see [43] and Theorem 18.14.

In Section 9.4 we shall see that $M_f$ is somewhat related to double symmetric polynomials and double power sums as well.

9.3 Arbitrary subsets

Now we consider the more general case when the number of elements is not necessarily $q$.

Definition 9.16. Let $1 < t < q$. We say that $T = \{y_1, \ldots, y_t\} \subseteq \mathbb{GF}(q)$ is a Vandermonde-set, if $\pi_k = \sum_i y_i^k = 0$ for all $1 \leq k \leq t - 2$.

Vandermonde-sets were first defined and studied in [70]. This part is a generalization from [120].

Here we do not allow multiple elements in $T$. Observe that the power sums do not change if the zero element is added to (or removed from) $T$. Note that in general the Vandermonde property is invariant under the transformations $y \to ay + b$ ($a \neq 0$) if and only if $p|t$: if $p \nmid t$ then a “constant term” $tb^k$ occurs in the power sums. (It may help in some situations: we can “translate” $T$ to a set with $\pi_1 = 0$ if needed.)

If $p|t$ then a $t$-set cannot have more than $t - 2$ zero power sums (so in this case Vandermondeness means $w = w_T = t - 1$). This is an easy consequence of the fact that a Vandermonde-determinant of distinct elements cannot be zero: consider the product

$$
\begin{pmatrix}
1 & 1 & \cdots & 1 \\
1 & 1 & \cdots & 1 \\
\vdots & \vdots & \ddots & \vdots \\
1 & 1 & \cdots & 1
\end{pmatrix}
\begin{pmatrix}
1 \\
1 \\
\vdots \\
1
\end{pmatrix},
$$

it cannot result in the zero vector.

Note that we have already seen that for a set of $q$ elements the value $w$ can be $\infty$. Recall that in that case the set has to contain multiple elements, in fact we had $w = \infty \iff$ all the multiplicities are divisible by the characteristic $p$. 
Exercise 9.17. Prove that if \( 1 < t \leq q \), \(|T| = t\) and multiplicities are allowed then \( w_T = \infty \iff \) all the multiplicities of the elements of \( T \) are divisible by the characteristic \( p \).

The proof above, with slight modifications, shows that in general a \( t \)-set cannot have more than \( t - 1 \) zero power sums (so for a Vandermonde-set \( w_T \) is either \( t - 1 \) or \( t \)). If the zero element does not occur in \( T \) then consider the product

\[
\begin{pmatrix}
y_1^t & y_2^t & \cdots & y_t^t \\
\vdots & \vdots & \ddots & \vdots \\
y_1^{t-1} & y_2^{t-1} & \cdots & y_t^{t-1}
\end{pmatrix}
\begin{pmatrix}
y_1^t \\
\vdots \\
y_1^{t-1}
\end{pmatrix},
\]

it cannot result in the zero vector as the determinant is still non-zero. If \( 0 \in T \) then remove it and we are again in the zero-free situation.

If for a set \( T \) of cardinality \( t \) we have that \( \pi_k(T) = 0 \) for \( k = 1, \ldots, t - 1 \), so \( w_T = t \) then such a set can be called a super-Vandermonde set. Note that the zero element is never contained in a super-Vandermonde set (removing it, for the other \( t - 1 \) elements all the first \( t - 1 \) power sums would be zero, which is impossible). The same argument gives the first examples of super-Vandermonde sets:

Example 9.18. If \( T \) is a Vandermonde set, containing the zero element, then \( T \setminus \{0\} \) is a super-Vandermonde set. In particular, if \( T \) is a Vandermonde set and \(|T| = t\) is divisible by the characteristic \( p \), then for any \( a \in T \), the translate \( T - a \) is a Vandermonde set, containing the zero element.

In the next proposition we characterize the Vandermonde-property.

Proposition 9.19. Let \( T = \{y_1, \ldots, y_t\} \subseteq \text{GF}(q) \). The following are equivalent

(i) \( T \) is a Vandermonde set, i.e. \( w_T = t - 1 \);

(ii) the polynomial \( f(Y) = \prod_{i=1}^{t} (Y - y_i) \) is of the form \( Y^{t'} g(Y)^p + aY + b \) (where \( 0 \leq t' \leq p - 1 \), \( t' \equiv t \mod p \));

(iii) for the polynomial \( \chi(Y) = -\sum_{i=1}^{t} (Y - y_i)^{q-1} \), \( ty^{q-1} + \chi(Y) \) has degree \( q - t \); moreover

(iv) for some \( Q = p^s \), \( t < Q \), the polynomial \( ty^{Q-1} - \sum_{i=1}^{t} (Y - y_i)^{Q-1} \) has degree \( Q - t \).

Proof: The coefficients of \( \chi \) are the power sums of the set \( T \), so (i) and (iii) are clearly equivalent. (i) \( \iff \) (iv) is similar. The equivalence of (i) and (ii) is an easy consequence of the Newton formulae relating power sums and elementary symmetric polynomials. \( \blacksquare \)
Note that for the function \( \chi \) in (iii), \( t + \chi(Y) \) is the characteristic function of \( T \), that is it is 1 on \( T \) and 0 everywhere else. (i) means that a Vandermonde set is equivalent to a fully reducible polynomial of form \( g^p(Y) + Y^t + cY \). (In the important case when \( p\mid t \) we have \( g^p(Y) + Y \).)

And now we characterize the super-Vandermonde-property.

**Proposition 9.20.** Let \( T = \{y_1, \ldots, y_t\} \subseteq \text{GF}(q) \). The following are equivalent

(i) \( T \) is a super-Vandermonde set, i.e. \( w_T = t \); 
(ii) the polynomial \( f(Y) = \prod_{i=1}^t (Y - y_i) \) is of the form \( Y^t g(Y)^p + c \) (where \( 0 \leq t' \leq p - 1, t' \equiv t \mod p \));
(iii) for the polynomial \( \chi(Y) = -\sum_{i=1}^t (Y - y_i)^{q-1}, tY^{q-1} + \chi(Y) \) has degree \( q - t - 1 \); moreover
(iv) for some \( Q = p^s \), \( t < Q \), the polynomial \( tY^{Q-1} - \sum_{i=1}^t (Y - y_i)^{Q-1} \) has degree \( Q - t - 1 \).

**Proof:** Very similar to the Vandermonde one above.

Here come some really motivating examples for Vandermonde sets.

**Example 9.21.** Let \( q \) be a prime power.

(i) Any additive subgroup of \( \text{GF}(q) \) is a Vandermonde set.

(ii) Any multiplicative subgroup of \( \text{GF}(q) \) is a (super-)Vandermonde set.

(iii) For \( q \) even, consider the points of \( \text{AG}(2, q) \) as elements of \( \text{GF}(q^2) \). Any \( q \)-set corresponding to the affine part of a hyperoval with two infinite points is a Vandermonde set in \( \text{GF}(q^2) \).

(iv) Let \( q \) be odd and consider the points of \( \text{AG}(2, q) \) as elements of \( \text{GF}(q^2) \) and a \( q+1 \)-set \( A = \{a_1, \ldots, a_{q+1}\} \) in it, intersecting every line in at most two points (i.e. an oval or \((q+1)\)-arc). Suppose that it is in a normalized position, i.e. \( \sum a_i = 0 \). Then \( A \) is a super-Vandermonde set in \( \text{GF}(q^2) \).

**Proof:** (i) Suppose \( T \) is an additive subgroup of size \( t \) in \( \text{GF}(q) \). We want to prove that Proposition 9.19 (ii) is satisfied, that is \( f(Y) = \prod_{y \in T} (Y - y) \) has only terms of degree divisible by \( p \), except for the term \( Y \). By Theorem 5.25 if we prove that \( f \) is additive, hence \( \text{GF}(p) \)-linear, then this implies that \( f \) has only terms of degree a power of \( p \).

Consider the polynomial in two variables \( F(X, Y) = f(X) + f(Y) - f(X + Y) \). First of all note that it has full degree at most \( t \) and that the coefficient of \( X^t \) and \( Y^t \) is zero. Considering \( F \) as a polynomial in \( X \), we have

\[
F(X, Y) = r_1(Y)X^{t-1} + r_2(Y)X^{t-2} + \cdots + r_t(Y),
\]
where \( r_i(Y) \) \((i = 1, \ldots, t)\) is a polynomial in \( Y \) of degree at most \( i \) (and \( \deg(r_i) \leq t - 1 \)). Now \( F(X, y) \equiv 0 \) for any \( y \in T \) (as a polynomial of \( X \)), so all \( r_i \)-s have at least \( t \) roots. Since their degree is smaller than this number, they are zero identically, so we have \( F(X, Y) \equiv 0 \), hence \( f \) is additive.

(ii) Suppose \( T \) is a multiplicative subgroup of size \( t \) in \( GF(q) \). Then the polynomial \( f(Y) = \prod_{i=1}^{t}(Y - y_i) \) is of the form \( Y^t - 1 \) so Proposition 9.20 (ii) is satisfied, we are done.

(iii) Let \( \{x_1, \ldots, x_q\} \subseteq GF(q^2) \) correspond to the affine part of the hyperoval \( \mathcal{H} \) and \( \varepsilon_1 \) and \( \varepsilon_2 \) be \((q+1)\)-st roots of unity corresponding to the two infinite points. Consider the polynomial \( \chi(X) = \sum_{i=1}^{q}(X - x_i)^{q-1} \). For any point \( x \) out of the hyperoval every line through \( x \) meets \( \mathcal{H} \) in an even number of points, and since \((x - x_i)^{q-1}\) represents the slope of the line joining the affine points \( x \) and \( x_i \), we have that \( \chi(x) = \varepsilon_1 + \varepsilon_2 \) for any \( x \notin \{x_1, \ldots, x_q\} \). There are \( q^2 - q \) different choices for such an \( x \), while the degree of \( \chi \) is at most \( q - 2 \), so \( \chi(X) \equiv \varepsilon_1 + \varepsilon_2 \) identically (that is, all coefficients of \( \chi \) are zero except for the constant term), so by Proposition 9.19 (iv), we are done.

(iv) A short proof is that by Segre’s theorem 14.9 such a pointset is a conic if \( q \) is odd, so affine equivalent to the “unit circle” \( \{\alpha \in GF(q^2) : a^{q+1} = 1\} \), which is a multiplicative subgroup.

**Exercise 9.22.** Given an additive subgroup \( G \leq (GF(q), +) \), with base \( G = \langle g_1, \ldots, g_t \rangle_{GF(P)} \), write up its root polynomial \( \prod_{g \in G}(Y - g) \) as in Proposition 9.19 (ii).

For a multiplicative subgroup \( H = \langle \alpha \rangle \leq (GF(q)^*, \cdot) \), \( |H| = t \), its root polynomial is \( \prod_{h \in H}(Y - h) = Y^t - 1 \).

Note that Proposition 9.19 (iv) implies that if \( T \subseteq GF(q_1) \leq GF(q_2) \) then \( T \) is a Vandermonde-set in \( GF(q_1) \) if and only if it is a Vandermonde-set in \( GF(q_2) \).

There are other interesting examples as well.

**Example 9.23.** Let \( q = q_0^{t-1} \), then in \( GF(q) \) \( T = \{1\} \cup \{\omega^q i : i = 0, \ldots, t - 2\} \) for some element \( \omega \in GF(q)^* \) satisfying \( \text{Tr}_{q_0}^{q_0} (\omega^k) = -1 \) for all \( k = 1, \ldots, t - 1 \).

As:

\[
\sum_{i=0}^{t-2} (\omega^q i)^k = \sum_{i=0}^{t-2} (\omega^k)^q i = \text{Tr}_{q_0}^{q_0} (\omega^k) = -1.
\]

Note that such \( \omega \) exists for several triples \((t, q_0, q)\), here I enlist some values; “-” means that such \( \omega \) does not exist, while “x” means that the only element with the property above is \( 1 \in GF(q_0^{t-1}) \), see Exercise 9.24:
Exercise 9.24. Prove that if $g.c.d.(q_0, t) \neq 1$ then the only element with the property above is $1 \in \mathbb{GF}(q_0^{t-1})$.

Exercise 9.25. Let $T = \{y_1, \ldots, y_t\}$ be a super-Vandermonde set. Prove that

\[
\left(\frac{y_1}{y_2} - 1\right)\left(\frac{y_1}{y_3} - 1\right) \cdots \left(\frac{y_1}{y_t} - 1\right) = t.
\]

Note that it is easy to check the previous condition for a multiplicative subgroup; also that any element of $T$ can play the role of $y_1$, so in fact we have $t$ conditions.

For applications see for instance Section 13, Proposition 13.9 and its consequence, Theorem 13.12.

9.4 The generalized formulae

Following Gács in this section, we define two functions in the independent variables $a_1, \ldots, a_t$ and $b_1, \ldots, b_t$ over any field $K$, where $t$ is a positive integer. Let $k$ and $l$ be two non-negative integers, $(k, l) \neq (0, 0)$, $k, l \leq t$.

Definition 9.26. The elementary symmetric polynomial of order $(k, l)$ is defined as

\[
\sigma_{k, l}(a_1, \ldots, a_t; b_1, \ldots, b_t) = \sum_{\substack{(i_1, \ldots, i_k) \subseteq \{1, \ldots, t\} \setminus \{j_1, \ldots, j_l\} = \emptyset}} a_{i_1}a_{i_2}\cdots a_{i_k} \cdot b_{j_1}b_{j_2}\cdots b_{j_l}.
\]

In other words, $\sigma_{k, l}$ is the coefficient of $X^{t-l-k}Y^k$ in the Rédei polynomial $\prod_{i=1}^{t}(X + a_iY + b_i)$; or the coefficient of $X^kY^l$ in $\prod_{i=1}^{t}(a_iX + b_iY + 1)$. It shows again that $\sigma_{k, l}$’s determine the set $\{a_1, \ldots, a_t; b_1, \ldots, b_t\}$.

For $k = l = 0$, we define $\sigma_{0, 0}(a_1, \ldots, a_t; b_1, \ldots, b_t) := 1$ identically.

Definition 9.27. The power sum of order $(k, l)$ is defined to be

\[
\pi_{k, l}(a_1, \ldots, a_t; b_1, \ldots, b_t) := \sum_{i=1}^{t} a_i^kb_i^l.
\]

Evaluating $\pi_{0, l}$ or $\pi_{k, 0}$, $0^0$ may occur, which is defined to be 1.
Note that for \( k = 0 \), \( \sigma_{0,i}(a_1, \ldots, a_i; b_1, \ldots, b_l) = \sigma_i(b_1, \ldots, b_l) \), the \( l \)-th elementary symmetric polynomial of the \( b \)-s, and \( \sigma_{k,0}(a_1, \ldots, a_i; b_1, \ldots, b_l) = \sigma_k(a_1, \ldots, a_i) \) similarly.

Taking \( l = 0 \) or \( k = 0 \) in the second definition, we get the corresponding power sum of the \( a \)-s or \( b \)-s, respectively.

The functions in the previous two definitions are somewhat ‘parallelly symmetric’; they do not change value if we take the same permutation of the first \( t \) and second \( t \) variables simultaneously. A direct analogue of the fundamental theorem mentioned in the previous section does not seem to be true for such functions, but the Newton formulae can be generalized:

**Theorem 9.28.** For fixed \( k \) and \( l \), define \( \pi_{0,0} := k + l \) and \( \sigma_{a,b} = 0 \) for any \( a > t \), \( b > t \) or \( a + b > t \). The following holds:

\[
\sum_{r=0}^{k} \sum_{s=0}^{l} (-1)^{r+s} \binom{r+s}{r} \pi_{r,s} \sigma_{k-r,l-s} = 0. \tag{NG}
\]

**Proof:** It is easy to see that on the left hand side we have a homogeneous polynomial of degree \( k + l \) with monomials \( a_i^t b_j^t a_1 \cdots a_{k-r} \cdot b_{j_1} \cdots b_{j_{l-s}} \), where all indices are different and \( 0 \leq r \leq k \), \( 0 \leq s \leq l \).

If \( r \) and \( s \) are both positive, then we can get such a term from three summands:

\[
\pi_{r,s} \sigma_{k-r,l-s}, \pi_{r-1,s} \sigma_{k+1-r,l-s} \text{ and } \sigma_{r,s-1} \sigma_{k-r,l+1-s}. \]

Hence the coefficient of such a monomial is \((-1)^{r+s}(r+s)_r + (-1)^{r+s-1}(r+s-1)_r + (r+s-1)_r\) = 0. (Note that if the monomial in question exists, then necessarily \( k + 1 - r \leq t \), \( l + 1 - s \leq t \) and \( k + l + 1 - r - s \leq t \), hence \( \sigma_{r,s-1} \) and \( \sigma_{r-1,s} \) are not zero by definition. Similar remarks will hold for the next two cases.)

If \( r = 0 \), \( s > 1 \), then there are two summands giving the monomial in question:

\[
\pi_{0,s} \sigma_{k-l-s} \text{ and } \pi_{0,s-1} \sigma_{k,l+1-s}, \]

so the coefficient is \((-1)^s (s)_0 + (-1)^{s-1} (s-1)_0\) = 0 again. The \( s = 0 \), \( r > 1 \) case is similar.

The \( \{r, s\} = \{0\} \) and \( \{r, s\} = \{0, 1\} \) cases are the same, so what is left is to show that the coefficient of a monomial of type \( a_i \cdots a_{i_k} \cdot b_{j_1} \cdots b_{j_{l}} \) is also zero. We get this term \( k + l \) times from \( \pi_{0,0} \sigma_{k,l} \), \(-k \) times from \( \pi_{1,0} \sigma_{k-1,l} \) and \(-l \) times from \( \pi_{0,1} \sigma_{k,l-1} \), so its coefficient is certainly zero (here the binomial coefficients are all 1).

\[\blacksquare\]

**Remark 9.29.** Taking \( l = 0 \), the theorem coincides with (N3).

**Remark 9.30.** There is a slightly more general formula:

\[
\sum_{r=0}^{k} \sum_{s=0}^{l} f(r,s) \pi_{r,s} \sigma_{k-r,l-s} = 0, \tag{NG*}
\]
were \( \pi_{0,0} \) is defined to be 1 and the function \( f(r, s) \) is defined as follows. Let \( a \) and \( b \) be two fixed field elements, \( f(0, 0) = ak + bl \), and for \( (r, s) \neq (0, 0) \),

\[
f(r, s) = (-1)^{r+s} \left( \binom{r+s-1}{s} a + \binom{r+s-1}{r} b \right). \tag{NG**}
\]

**Proof:** Looking through the proof of 9.28, it is easy to see that the function \( f(r, s) \) has to satisfy the following equations:

- \( f(0, 0) + kf(1, 0) + lf(0, 1) = 0; \)
- \( f(r, 0) + f(r+1, 0) = 0 \) for all \( r \geq 1; \)
- \( f(0, s) + f(0, s+1) = 0 \) for all \( s \geq 1; \)
- \( f(r, s) + f(r-1, s) + f(r, s-1) = 0 \) for all \( r \geq 1, s \geq 1. \)

Now defining \( f(1, 0) = -a, \)

\( f(0, 1) = -b, \)

it can be seen by induction on \( k + l \) that the general solution for such a function is (NG**).

(NG*) seems to be much stronger, but (NG) has turned out to be sufficient for all applications found so far. In many applications, the set \( U = \{(a_i, b_i) : i = 1, ..., t\} \) will be the graph (or almost a graph) of a polynomial. For the graph of a polynomial, the double power sum \( \pi_{k,l} \) becomes \( \sum x^k f(x)^l \), the meaning of which can be understood through Proposition 5.4.

For a demonstration of the strength of using Rédei polynomials together with these formulæ see 15.10.

**The invariant \( W_f \)**

For any polynomial \( f \), let

\[
W_f = \min \{ k + l : \sum_{x \in \mathbb{GF}(q)} x^k f(x)^l \neq 0 \} = \min \{ k + l : \pi_{k,l}(a_1, ..., a_q; f(a_1), ..., f(a_q)) \neq 0 \}
\]

(where \( \{ a_i : i \} = \mathbb{GF}(q) \)). Here \( k \) and \( l \) are non-negative integers; for \( k = 0 \) or \( l = 0, x^0 \) or \( f(x)^0 \) is defined to be the polynomial 1. By the remarks at the end of the previous section, \( W_f \) is the smallest \( k + l \), for which \( x^k f(x)^l \) has reduced degree \( p - 1. \) \( W_f \) is very similar to \( w_f \) above. The second and third statements of the next lemma can be implicitly found in [91].

**Lemma 9.31.** (Gács [66]) (i) For any of the transformations mentioned after Proposition 9.15 for \( M_f \), the value of \( W_f \) remains unchanged;

(ii) For any polynomial \( f \), \( W_f + N_f \geq p + 1; \)

(iii) For any non-linear polynomial, \( W_f \leq \frac{p+1}{2} \) with equality if and only if \( f(x) \) is affinely equivalent to \( x^2 \) or \( x^{\frac{p+1}{2}}; \)

(iv) For any polynomial of degree between 2 and \( \frac{p+1}{2} \), \( W_f \leq \frac{p-1}{3} \), unless it is affinely equivalent to \( x^2 \) or \( x^{\frac{p+1}{2}}. \)
A polynomial of the form \(x^k f(x)^l\) will be called a double power of \(f\), the degree of \(x^k f(x)^l\) is defined to be \(k + l\).

We will need the following result of A. Biró:

**Theorem 9.32.** (A. Biró [28]) Suppose the graph of \(f \in \text{GF}(p)[X]\) is contained in the union of two intersecting lines. Then \(W_f = \frac{p-1}{2}\) or \(W_f = \frac{p-1}{3}\) or \(W_f \leq \frac{p-1}{4}\). There is an example with \(\frac{p-1}{4} > W_f > \frac{p-1}{5}\).

**Exercise 9.33.** Prove the equalities or compute the value of the symmetric functions of the interesting sets below:

\[\sigma_k(\text{GF}(q)) = 0 \text{ if } k = 1, \ldots, q - 2 \text{ or } q \text{ and } = -1 \text{ if } k = q - 1;\]

\[\pi_k = \sum_{t \in \text{GF}(q)} t^k = 0 \text{ if } (q - 1) \nmid k \text{ and } = -1 \text{ if } (q - 1)|k;\]

\[\sum_{(t_1, \ldots, t_k, t_{k+1}, \ldots, t_{k+l}) \subseteq \text{GF}(q) \text{ all distinct}} t_1 t_2 \ldots t_k t_{k+1}^2 t_{k+2}^2 \ldots t_{k+l}^2 = ?;\]

\[\sum_{S \subseteq \text{GF}(q) \atop |S| = k} \sigma_j(S) = ?\]

### 9.5 Resultants

In this section the classical notion of resultant is reconsidered. The author does not know who found the generalization considered below. It appears in a theorem and its corollary by Green and Eisenbud [72], and probably already in Coolidge [58]; also in Szönyi [125] where it was first applied in finite geometry. The method was refined later in Weiner [137].

As is known from classical algebra, given two polynomials \(f(X) = a_0 X^k + a_1 X^{k-1} + \ldots + a_{k-1} X + a_k\) and \(g(X) = b_0 X^l + b_1 X^{l-1} + \ldots + b_{l-1} X + b_l\), not both \(a_0\) and \(b_0\) being zero, then their greatest common divisor has degree at least one iff the determinant of the following matrix of size \((l + k) \times (l + k)\)

\[
R_0(f, g) = R_0 = \begin{pmatrix}
0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 \\
0 & a_0 & 0 & \cdots & 0 & b_0 & b_1 & \cdots & 0 \\
0 & a_1 & a_0 & \cdots & 0 & b_1 & b_2 & \cdots & 0 \\
\vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots \\
0 & a_k & a_{k-1} & a_{k-2} & \cdots & b_k & b_{k-1} & \cdots & 0 \\
0 & a_k & a_{k-1} & \cdots & \vdots & b_{k-1} & \vdots & \ddots & \ddots \\
\cdots & \cdots & \cdots & a_0 & \cdots & b_{l-1} & b_l & \cdots & \cdots \\
0 & \cdots & \cdots & \cdots & a_k & b_l & \cdots & \ddots & \ddots \\
0 & \cdots & \cdots & \cdots & \cdots & b_l & b_{l-1} & \cdots & \ddots \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots
\end{pmatrix}
\]
is zero. This matrix is sometimes called the Sylvester matrix $\text{Syl}(f, g)$ of $f$ and $g$; the determinant of it is the resultant of $f$ and $g$ and is equal to $a_0^l b_0^k \prod_{i,j} (\alpha_i - \beta_j) = b_0^k \prod_j f(\beta_j) = a_0^l \prod_i g(\alpha_i)$, where $\{\alpha_i : i = 1, \ldots, k\}$ and $\{\beta_j : j = 1, \ldots, l\}$ are the roots of $f$ and $g$, resp., in the algebraic closure. Note also that the resultant is a homogeneous polynomial of degree $l$ in the variables $a_0, \ldots, a_k$ and of degree $k$ in $b_0, \ldots, b_l$.

We will frequently need the following

**Theorem 9.34.** Let $f(X) = a_0 X^k + a_1 X^{k-1} + \ldots + a_{k-1} X + a_k$ and $g(X) = b_0 X^l + b_1 X^{l-1} + \ldots + b_{l-1} X + b_l$, not both $a_0$ and $b_0$ being zero. If their greatest common divisor has degree $m$ then the next matrix is non-singular, moreover, their greatest common divisor has degree at least $m + 1$ iff the determinant of the following matrix of size $(k + l - 2m) \times (k + l - 2m)$

$$
R_m(f, g) = R_m = 
\begin{pmatrix}
 a_0 & 0 & 0 & \ldots & 0 & b_0 & 0 & \ldots & 0 \\
 a_1 & a_0 & 0 & \ldots & 0 & b_1 & b_0 & \ldots & 0 \\
 a_2 & a_1 & a_0 & \ldots & 0 & b_2 & b_1 & \ldots & 0 \\
 \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
 a_{l-m-1} & a_{l-m-2} & a_{l-m-3} & \ldots & a_0 & b_{l-m} & b_{l-m-1} & \ldots & b_0 \\
 a_{l-m} & a_{l-m-1} & a_{l-m-2} & \ldots & a_1 & b_{l-m} & b_{l-m-1} & \ldots & b_0 \\
 \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
 a_{k+l-2m-1} & \ldots & \ldots & a_{k-m} & b_{k+l-2m-1} & b_{k+l-2m-2} & \ldots & b_{l-m}
\end{pmatrix}
$$

is zero. ($a_i$ and $b_j$ are considered to be zero if they are out of the range $0 \leq i \leq k, 0 \leq j \leq l$.)

Note that when the greatest common divisor of the two polynomials is supposed to be large then the matrix $R_m$ is small.

**Proof:** Let $r(X)$ be the greatest common divisor of $f$ and $g$. Denote by $\bar{c}$ the quotient $f/r$ and let $\bar{d} = g/r$. We can suppose that $r$ is monic (of degree $m$), so

$$
\bar{c}(X) = a_0 X^{k-m} + \bar{c}_1 X^{k-m-1} + \bar{c}_2 X^{k-m-2} + \ldots + \bar{c}_{k-m}
$$

and

$$
\bar{d}(X) = b_0 X^{l-m} + \bar{d}_1 X^{l-m-1} + \bar{d}_2 X^{l-m-2} + \ldots + \bar{d}_{l-m}.
$$

For these polynomials we have $r = f/\bar{c} = g/\bar{d}$. In other words, this means that $f \bar{d} - g \bar{c} = 0$ or equivalently

$$
f(\bar{d} - b_0 X^{l-m}) - g(\bar{c} - a_0 X^{k-m}) = a_0 X^{k-m} g - b_0 X^{l-m} f, \quad (*)
$$
and this polynomial equation can be interpreted as a system of linear equations for the coefficients \( \tilde{d}_1, \ldots, \tilde{d}_{l-m}, \tilde{c}_1, \ldots, \tilde{c}_{k-m} \).

More precisely, compute the coefficient of \( X^{k+l-m-1}, X^{k+l-m-2}, \ldots, X^m \) in (\( * \)), it yields the system of linear equations

\[
R_m(\tilde{d}_1, \ldots, \tilde{d}_{l-m}, -\tilde{c}_1, \ldots, -\tilde{c}_{k-m})^T = (a_0b_1 - b_0a_1, a_0b_2 - b_0a_2, \ldots, a_0b_{k+l-2m} - b_0a_{k+l-2m})^T.
\]

It is important to note that the solutions of the system of linear equations correspond to solutions of the polynomial equation, if we know in advance that the greatest common divisor \( r \) has degree at least \( m \). Indeed, if \( (\tilde{d}_1, \ldots, \tilde{d}_{l-m}, \tilde{c}_1, \ldots, \tilde{c}_{k-m}) \) is a solution of our system of linear equations, then the polynomials \( \tilde{c}(X) = a_0X^{k-m} + \tilde{c}_1X^{k-m-1} + \ldots + \tilde{c}_{k-m} \) and \( \tilde{d}(X) = b_0X^{l-m} + \tilde{d}_1X^{l-m-1} + \ldots + \tilde{d}_{l-m} \) will have the property that \( f\tilde{d} - g\tilde{c} \) has degree less than \( m \). Since this polynomial is divisible by \( r \), it must be identically zero.

Now the polynomial equation (and hence the system of linear equations) has a unique solution if \( r \) has degree exactly \( m \). To see this, first observe that \( f/r = \tilde{c}, g/r = \tilde{d} \) is a solution of the polynomial equation of degree exactly \( k - m \), this means that there is at least one solution. (Remember that \( r \) was supposed to be monic.) Suppose that there are two solutions of the equations, yielding \( \tilde{d}', \tilde{d}'' \) and \( \tilde{c}', \tilde{c}'' \). Then from \( f\tilde{d}' - g\tilde{c}' = 0 \) and \( f\tilde{d}'' - g\tilde{c}'' = 0 \) we get \( f(\tilde{d}' - \tilde{d}'') - g(\tilde{c}' - \tilde{c}'') = 0 \). Now the degree of \( \tilde{c}' - \tilde{c}'' \) is less than \( k - m \); so we get a contradiction after dividing by \( r \); in \( \tilde{c}(\tilde{d}' - \tilde{d}'') = \tilde{d}(\tilde{c}' - \tilde{c}'') \) we have that \( \tilde{c} \) and \( \tilde{d} \) are relatively primes, so e.g. \( \tilde{d} \) divides \( (\tilde{d}' - \tilde{d}'') \), but the latter has smaller degree so \( \tilde{d}' = \tilde{d}'' \), and similarly \( \tilde{c}' = \tilde{c}'' \). Therefore the solution is unique if \( \deg(r) = m \), \( \det R_m \neq 0 \), and the solution can be obtained by Cramer’s rule.

If the degree of \( r \) is strictly bigger, say \( m' > m \), then \( \det R_m \) is zero, since the polynomial equation \( f\tilde{d} - g\tilde{c} = 0 \) cannot have a unique solution. Indeed, we can determine \( \tilde{d}, \tilde{c} \) of degree \( l - m' \) and \( k - m' \) resp., and then multiply both by the same arbitrary monic polynomial of degree \( m' - m \).}

\[
\text{Cramer’s rule}
\]

Note that if \( a_0 = b_0 = 0 \) then both \( \det R_m \) and the right hand side of the equation (\( * \)) is zero.

In the applications the coefficients \( a_j \) and \( b_j \) are polynomials in \( Y \) (or homogeneous polynomials in \( Y, Z \) say), which satisfy \( \deg(a_j), \deg(b_j) \leq j \). Then, by the remark on Cramer’s rule above, the coefficients of \( \tilde{d} \) and \( \tilde{c} \) will be quotients of two polynomials, where the denominator is \( \det R_m(Y) \). Multiply each coefficient of \( \tilde{d} \) and \( \tilde{c} \) by \( \det R_m(Y) \) to obtain the polynomials \( d^m(X, Y) \) and \( c^m(X, Y) \). Then the following holds.

**Result 9.35.** (Szönyi [125]) Suppose that \( f(X) = \sum a_i(Y)X^{n-i} \) and \( g(X) = \sum b_i(Y)X^{n-1-i} \) satisfy \( \deg(a_i), \deg(b_i) \leq i \) and not both \( a_0 \) and \( b_0 \) are zero. Then
the determinant of \( R_m(Y) \) in Theorem 9.34 has degree at most \( (l-m)(k-m) \) as a polynomial in \( Y \). The total degree of the polynomial \( c^m(X,Y) \) is at most \( (l-m+1)(k-m) \), and the total degree of \( d^m(X,Y) \) is at most \( (l-m)(k-m+1) \).

**Proof:** To estimate the degree of the determinant \( R_m(Y) \), observe that the degree of the \((i,j)\)-th entry \((i,j = 1,\ldots,k+l-2m)\) is at most \( i-j \) if we are on the left-hand side, and it is at most \( i-j+l-m \) if we are on the right-hand side of \( R_m(Y) \). So each term in the expression of the determinant has \( Y \)-degree at most \((l-m)(k-m)\).

The solutions \( \bar{a}_1,\ldots,\bar{a}_{k-m},-\bar{c}_1,\ldots,-\bar{c}_{k-m} \) can be obtained using Cramer’s rule; \( \bar{a}_0 = b_0, \bar{c}_0 = c_0 \). If we put the right hand side of the equation in place of the \( j \)-th column, then the degree will be bigger than that of \( R_m \) by \( j \) or \( j-l+m \) according as \( j \) is in the left or right part of the matrix, from which the second part of the result follows.

Note that the elements of \( R_m(Y) \) depend on \( a_i(Y) \), \( i \leq k-m \), and on \( b_j(Y) \), \( j \leq l-m \). This is also true for the polynomials \( a^m(X,Y) \) and \( c^m(X,Y) \). Hence in Result 9.35 it is enough to assume that \( \deg(a_i) \leq i \), when \( i \leq k-m \), and \( \deg(b_j) \leq j \), when \( j \leq l-m \).

How can these observations be applied? Consider two homogeneous polynomials \( f(X,Y,Z) \) and \( g(X,Y,Z) \), \( f(a,b,c) = 0 \) iff the line \([a,b,c] \) has some (good) property \( P_f \), and \( g(a,b,c) = 0 \) iff the line \([a,b,c] \) has some (good) property \( P_g \). We want to find/count the infinite points \((0,-c,b) \) through which there pass \( > m \) affine lines being good in both sense, i.e. for which \( \deg(\gcd(f(X,b,c), g(X,b,c))) > m \) for a certain value \( m \). From Theorem 9.34 it follows that these are all roots of \( R_m(Y,Z) = R_m(f(X,Y,Z), g(X,Y,Z)) \). See Theorem 12.1 for a nice illustration.

The polynomials \( \bar{c}, \bar{d}, c^m(X,Y) \), \( d^m(X,Y) \) seem to appear in the reasonings above as by-products; however at some point, e.g. in stability results, they play a crucial role. The idea will be the following. Like before, we are given \( f(X,Y,Z) \) and \( g(X,Y,Z) \), where \( g \) is responsible for some “had” property of lines (and \( f \) for some good property). So we are interested in \( \frac{f(X,b,c)}{\gcd(f(X,b,c), g(X,b,c))} \) but this is somewhat meaningless.

Well, then we can calculate \( \frac{f(X,b,c)}{\gcd(f(X,b,c), g(X,b,c))} \), but it does not say anything about the change of the situation when we alter \((b,c)\). Suppose that there is a so-called “typical index” \( m \) on the line \([1,0,0] \), meaning that for “most of” the points \((0,b,c) \), the degree of \( \gcd(f(X,b,c), g(X,b,c)) \) is exactly \( m \). Then, like in Theorem 9.34, construct \( R_m(Y,Z) = R_m(f(X,Y,Z), g(X,Y,Z)) \) and the other polynomials \( \bar{c}(X,Y,Z), c^m(X,Y,Z) \). We have estimates on their degree, and we do know that for all typical points (so for most of the points of \([1,0,0] \)) \( \frac{f(X,b,c)}{\gcd(f(X,b,c), g(X,b,c))} = \bar{c}(X,b,c) \). So \( \bar{c}(X,Y,Z) \) is zero for most of the \((a,b,c)\)-s we are interested in. The only problem is that we gained \( \bar{c}(X,Y,Z) \) from Cramer’s rule, so it is a fraction with denominator \( R(Y,Z) \). Hence if we prefer polynomials / algebraic curves (as we usually do), we have to consider \( \bar{c}(X,Y,Z)R_m(Y,Z) = c^m(X,Y,Z) \) instead. Note
that in principle we know it precisely, it can be calculated from the coefficient polynomials \(a_i(Y, Z)\) and \(b_j(Y, Z)\) as above.
For illustrations see the proof of Theorem 15.17 in [137].

We want to refine the statement that if the greatest common divisor has degree bigger than \(m\) then \(\det R_m\) is zero; we will show that as the degree gets bigger, the determinant becomes “more and more zero”.

More precisely, we know that if for the fix value \(Y = y\) the degree of the greatest common divisor of \(f(X, y)\) and \(g(X, y)\) is bigger than \(m\), then the determinant of \(R_m(y)\) is 0; hence \((Y - y)\) is a factor of \(\det R_m(Y)\). The refinement is the following

**Theorem 9.36.** For \(Y = y\), if \(\deg(\gcd(f(X, y), g(X, y))) = m\) then \(\det(R_m(f(X, y), g(X, y)))\) is non-zero. If \(\deg(\gcd(f(X, y), g(X, y))) \geq m + t\) then \((Y - y)^t \det(R_m(f(X, Y), g(X, Y)))\).

The homogeneous version is:

**Theorem 9.37.** Let \(f(X, Y, Z) = \sum a_i(Y, Z)X^k-i\) and \(g(X, Y, Z) = \sum b_i(Y, Z)X^{l-i}\) be homogeneous polynomials in three variables and assume that not both \(a_0\) and \(b_0\) are zero. For \((Y, Z) = (y, z)\), if \(\deg(\gcd(f(X, y, z), g(X, y, z))) = m \geq 0\) then
\[
\det(R_m(f(X, y, z), g(X, y, z)))
\]
is non-zero. If \(\deg(\gcd(f(X, y, z), g(X, y, z))) \geq m + t\) then
\[
(zY - yZ)^t \det(R_m(f(X, Y, Z), g(X, Y, Z))).
\]

For the proof the next lemma is needed.

**Lemma 9.38.** Let \(M(Y, Z)\) be an \(n \times n\) matrix with entries being polynomials depending on \(Y\) and \(Z\) and \(s \geq 1\). Assume that for the fix value \(y\) and \(z\), \((zY - yZ)^s\) divides all \((n - 1) \times (n - 1)\) subdeterminants of \(M(Y, Z)\), then \((zY - yZ)^{s+1}\) is a factor of \(\det M(Y, Z)\).

**Proof:** Let \(M^*(Y, Z)\) be the transpose of the matrix obtained by replacing each element \(m_{ij}\) of \(M(Y, Z)\) by \((-1)^{i+j}\) times the corresponding \((n - 1) \times (n - 1)\) subdeterminant of \(M(Y, Z)\). Note that \(M^*(Y, Z)M(Y, Z) = (\det M(Y, Z))I\), where \(I\) is the \(n \times n\) identity matrix; hence \(\det M^*(Y, Z) = (\det M(Y, Z))^{n-1}\). By assumption the elements of \(M^*(Y, Z)\) are divisible by \((zY - yZ)^s\), therefore \((zY - yZ)^{s+1}\) divides \(\det M^*(Y, Z) = (\det M(Y, Z))^{n-1}\) and so the lemma follows.

**Proof of Theorem 9.37** As before, we want to determine the coefficients of the polynomials \(d(X)\) and \(c(X)\), for that \(f(X, y, z)d(X) - g(X, y, z)c(X) = 0\) holds,
\[ \deg \tilde{c} = k - m \text{ and } \deg \tilde{d} = l - m. \] Again this equation can be interpreted as a system of linear equations with matrix \( R_m(y, z) \), for the coefficients of \( \tilde{c} \) and \( \tilde{d} \).

Since the degree of the greatest common divisor of \( f(X, y, z) \) and \( g(X, y, z) \) is \( m + t \), the polynomials \( \tilde{d} \) and \( \tilde{c} \) are the products \( \tilde{c}(X) = \frac{f(X, y, z)}{\gcd(f(X, y, z), g(X, y, z))}(X^t + u_1 X^{t-1} + \cdots + u_t) \) and \( \tilde{d}(X) = \frac{f(X, y, z)}{\gcd(f(X, y, z), g(X, y, z))}(X^t + u_1 X^{t-1} + \cdots + u_t) \), where every \( u_i \) can be chosen freely. This means that the \((k + l - 2m - t + 1) \times (k + l - 2m - t + 1)\) subdeterminants of \( \det R_m(y, z) \) are all 0. As \( \det R_m(Y, Z) \) is a homogeneous polynomial, \((zY - yZ)\) divides all \((k + l - 2m - t + 1) \times (k + l - 2m - t + 1)\) subdeterminants of \( \det R_m(Y, Z) \). The result follows by applying Lemma 9.38 \( t \) times.

Later we will see how Theorem 9.37 can be used and this is one of the observations that lead to improvement on several results.

Let’s say some words about the connections with Bézout’s theorem 10.6. Applying Theorem 9.37 with \( m = 0 \) for the homogeneous polynomials \( f(X, Y, Z) \) and \( g(X, Y, Z) \), and using the notation \( m_{y,z} = \deg \gcd(f(X, y, z), g(X, y, z)) \), i.e. the “common intersection multiplicities” with the line \([0, -z, y]\), we have that the number of common points of the two curves (even if counted with these multiplicities) is at most

\[ \sum_{(y, z)} m_{y,z} \leq \deg \det R_0(f, g) = kl. \]

In fact here the common intersection multiplicities with horizontal lines, i.e. lines through \((1, 0, 0)\) are added up.

It becomes more interesting when we fix a “typical multiplicity” \( m \) and we want to estimate the number of \((y, z)\)-s for which \( f(X, y, z) \) and \( g(X, y, z) \) has more than \( m \) common roots. If this “excess” is \( t_{y,z} \), i.e. \( m + t_{y,z} = \deg \gcd(f(X, y, z), g(X, y, z)) \), then Theorem 9.37 gives

**Theorem 9.39.**

\[ \sum_{(y, z) \in \mathbb{Z}^2} t_{y,z} \leq \deg \det R_m(f, g) = (\deg(f) - m)(\deg(g) - m). \] 

As an application let’s consider the case when we are interested in \( \gcd(X^q - X, f(X)) \), so the distinct factors of \( f \). If we look for more than \( m \) factors, we need
Example: \( R = P = \begin{pmatrix} 3, & 3 \end{pmatrix} \), i.e. 
we look for the multiple factors of \( f \). If we want more than \( m \) multiple factors, we need the determinant of

\[
\begin{vmatrix}
  a_0 & & & & \\
  a_1 & a_0 & & & \\
  \vdots & \vdots & \ddots & \vdots & \\
  a_{k-m-1} & a_{k-m-2} & \cdots & a_0 & 0 \\
  a_{k-m} & a_{k-m-1} & \cdots & a_0 & 0 \\
  a_{k-m+1} & a_{k-m+2} & \cdots & a_0 & 0 \\
  \vdots & \vdots & \ddots & \vdots & \\
  a_{k-2} & a_{k-3} & \cdots & a_0 & 0 \\
  0 & & & & a_{q+k-2m-1} a_{q+k-2m-2} \cdots a_{k-m} \\
\end{vmatrix} = 0
\]

where the -1's do not appear in the lower left corner if \( q + k - 2m - 1 < q - 1 \) i.e. \( k/2 < m \). In this case the determinant is just the determinant of the lower right submatrix. In any case, if the coefficients \( a_i \) are polynomials of \( Y \)-degree at most \( i \), then the degree of the determinant above is at most \( (q - m)(k - m) \).

The second very important example is when we work on \( \gcd(f(X), f'(X)) \), i.e. we look for the multiple factors of \( f \). If we want more than \( m \) multiple factors, we need the determinant of

\[
\begin{vmatrix}
  a_0 & & & & & & k_{a_0} & 0 & \cdots & 0 \\
  a_1 & a_0 & & & & (k-1)a_1 & k_{a_0} & 0 & \cdots & 0 \\
  \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\
  a_{k-m-2} & a_{k-m-3} & \cdots & a_0 & 0 & (m+1)a_{k-m-3} & k_{a_0} & 0 & \cdots & 0 \\
  a_{k-m-1} & a_{k-m-2} & \cdots & a_0 & 0 & (m+2)a_{k-m-2} & k_{a_0} & 0 & \cdots & 0 \\
  \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\
  a_{k-2} & a_{k-3} & \cdots & a_0 & 0 & (2m+k-a_{k-2})a_{k-3} & k_{a_0} & 0 & \cdots & 0 \\
  0 & & & & & & 0 & \cdots & \cdots & \cdots & 0 \\
\end{vmatrix} = 0
\]

to be zero. Again, if the coefficients \( a_i \) are polynomials of degree at most \( i \), then the degree of this determinant is at most \( (k - m)(k - m - 1) \).

**Additive/linearized polynomials, \( P \)-adic resultant**

Let \( f(X), g(X) \) be monic separable \( \text{GF}(p^e) \)-linear polynomials (i.e. each of them splits into distinct linear factors), and let \( S = \{x_1, \ldots, x_n\} \) and \( U = \{t_1, \ldots, t_m\} \) be bases for the \( \text{GF}(p^e) \)-vectorspaces of their roots (see Theorem 5.28), respectively.

The \( P \)-adic resultant of them is defined as 

\[
R_P(f, g) = \frac{\text{MRD}(x_1, \ldots, x_n, t_1, \ldots, t_m)}{\text{MRD}(x_1, \ldots, x_n) \text{MRD}(t_1, \ldots, t_m)}.
\]

**Theorem 9.40.** (1) \( R_P(f, g)^{p^e-1} = R(\frac{f(X)}{X}, \frac{g(X)}{X}) \);

(2) \( R_P(f, g) = \frac{\text{MRD}(f(t_1), \ldots, f(t_m))}{\text{MRD}(t_1, \ldots, t_m)} = (-1)^{nm} \frac{\text{MRD}(g(x_1), \ldots, g(x_n))}{\text{MRD}(x_1, \ldots, x_n)} \);

(3) \( R_P(f, g) = 0 \iff \text{the \( \text{GF}(p^e) \)-vectorspaces} \langle x_1, \ldots, x_n \rangle \text{ and} \langle t_1, \ldots, t_m \rangle \text{ have a non-trivial intersection.} \)
10 Elements of algebraic geometry

A typical method in Galois geometry is to associate an algebraic curve to a pointset of the plane or the space. The classical example of this method is Segre’s theory of complete arcs or the theory of Rédei polynomials.

The usual idea is that investigating a pointset in $\text{PG}(2, q)$ we are trying to collect all the interesting (“deviant”, “irregular”) lines in an envelope (so a curve in the dual plane, or a dual curve), where the meaning of “interesting” depends on the special properties of the pointset. E.g. in the case of arcs Segre introduced a dual curve containing all the tangent lines. He proved the existence of that curve using Menelaos’ theorem only; in some other cases we need the explicite form of a curve. For finding something similar to it we often write up the Rédei-polynomial of the pointset and we consider the Rédei polynomial, or another polynomial derived from it, as an algebraic curve.

For using a very little from the enormous theory of algebraic geometry we collect a few results here concerning algebraic curves. Some parts of this section are taken from Szőnyi [128]. We use a slightly simplified terminology, the interested reader can find several thousands pages of introductory books on algebraic geometry, we mention [64], [107] or the recent excellent Hirschfeld-Korchmáros-Torres [81].

An algebraic plane curve defined over a field $\mathbb{F}$ is just a polynomial $f(X, Y)$ in two variables or a homogeneous polynomial $f(X, Y, Z)$ in three variables, with coefficients from $\mathbb{F}$. For a constant $\lambda \in \mathbb{F}$, $\lambda f$ is considered to be the same curve. The irreducible components of the curve $f$ correspond to the irreducible factors of the polynomial $f$. We may quite often switch back and forth between bivariate (‘affine’) polynomials and their homogenized 3-variate (‘projective’) forms. Defined over $\mathbb{F}$, the curve can be viewed over any field $\mathbb{G}$ containing $\mathbb{F}$. The points of $f$ over $\mathbb{G}$ are just the pairs $(x, y)$ or homogeneous triples $(x, y, z)$ for which $f(x, y) = 0$ or $f(x, y, z) = 0$, resp., where $x, y, z \in \mathbb{G}$ (so $(x, y) \in \text{AG}(2, \mathbb{G})$ or $(x, y, z) \in \text{PG}(2, \mathbb{G})$). Obviously, the same $f$ can have more zeros (points) over a larger field.

Exercise 10.1. Let $\mathbb{F} = \text{GF}(q)$. How many different curves (projectively inequivalent homogeneous polynomials) of degree $n$ are there?

Exercise 10.2. Let $S$ be a set of points in $\text{AG}(2, q)$. Then there exists a two-variable polynomial of degree at most $\sqrt{2|S|} - 1$, so that it vanishes at every point of $S$.

One can write the affine curve $f(X, Y)$ in the form

$$f(X, Y) = f_0 + f_1(X, Y) + f_2(X, Y) + \ldots + f_n(X, Y),$$
where $f_i$ is a homogeneous polynomial in two variables of total degree $i$. Now the point $(0,0)$ has multiplicity $k$ on $f(X,Y)$ if $k$ is maximal such that $f$ can be written as

$$f(X,Y) = f_k(X,Y) + f_{k+1}(X,Y) + \ldots + f_n(X,Y),$$

so $f_0 = f_1 = \ldots = f_{k-1} = 0$. Multiplicity of another point $P(a,b)$ can be defined by translating it to the origin, i.e. we can examine $f(X+a,Y+b)$ instead. The tangents of $f(X,Y)$ at $(0,0)$ are the linear factors of $f_k(X,Y)$ above, they may well be defined over the algebraic closure $\overline{F}$; tangents at another point can be defined by translating it to the origin. A point is simple if it has multiplicity 1. At a simple (projective) point $(x,y,z)$ the (unique) tangent line is 

$$[\left(\partial_X f(x,y,z), \partial_Y f(x,y,z), \partial_Z f(x,y,z)\right)]$$. Equivalently, $(x,y,z)$ is a singular point if

$$([\partial_X f(x,y,z), \partial_Y f(x,y,z), \partial_Z f(x,y,z)] = (0,0,0)).$$

As the following result shows, a curve can have only a restricted number of points with multiplicity more than one.

**Result 10.3.** [64, p.118] Let $F$ be a projective plane curve of degree $n$ without multiple components. Then for the multiplicities $m_P$ of its points 

$$\sum_{P \in F} \frac{m_P(m_P-1)}{2} \leq \binom{n}{2}$$

holds.

One can define the intersection multiplicity (denoted by $I(f \cap g; P)$ or $I(P; f \cap g)$) of two curves $f$ and $g$ at a point $P(x,y,z)$ of the plane. The direct definition is rather complicated in the general case; here is a list of some easy facts which will be enough for our purposes:

(a) If at least one of $f$ and $g$ does not go through $P$ then obviously $I(f \cap g; P) = 0$.

(b) If $P$ is a simple point on both $f$ and $g$ and the tangents at $P$ are distinct then $I(f \cap g; P) = 1$. In particular, if $f \neq g$ are linear, meeting at $P$, then $I(f \cap g; P) = 1$.

(c) $P$ is not on a common component of $f$ and $g \Leftrightarrow I(f \cap g; P) < \infty$.

(d) $I(f \cap g; P) = I(g \cap f; P)$.

(e) $I(f \cap g; P) = I(f \cap g + hf; P)$.

(f) If $g$ is of degree 1 (i.e. a line) then $I(f \cap g; P)$ can be calculated easily: one can express one of the variables from $g(X,Y,Z) = 0$ and substitute it into $f$; then the resulting homogeneous polynomial in two variables will vanish at $P$, the multiplicity of this root will be the intersection multiplicity. Note that, as a univariate polynomial of degree $n$ has at most $n$ roots (and the same holds for homogeneous polynomials in two variables), this intersection multiplicity
is at most the degree of $f$, except when after the substitution $f$ vanishes identically, which means that $g$ was a factor of $f$. In this case (and generally when $f$ and $g$ have a common factor through $P$) we say $I(f \cap g; P) = \infty$.

(g) Note that if $g$ is linear and it happens to be a tangent of $f$ at $P$ then $I(f \cap g; P) \geq 2$.

(h) $I(f \cap (g_1g_2); P) = I(f \cap g_1; P) + I(f \cap g_2; P)$.

(b') A more general form of (b) is: $I(f \cap g; P) \geq m_P(f)m_P(g)$, where $m_P$ is the multiplicity of $P$ on the curve in question.

We note that there is a unique intersection multiplicity satisfying these properties (and being invariant under projective transformations), so they can be used to define intersection multiplicity. Also note that these properties can be used to actually compute the intersection multiplicity of two curves. Let us briefly recall how this works for the origin. Since any point can be transformed to the origin, this approach works for other points, too.

We wish to compute $I(P; F \cap G)$, where $P = (0, 0)$. Let $f(X) = F(X, 0)$, $g(X) = G(X, 0)$ and $d(X) = \text{g.c.d.}(f(X), g(X))$. Then we can write $d(X) = a(X)f(X) + b(X)g(X)$ by the Euclidean algorithm. Put $f_1(X) = f(X)/d(X)$, $g_1(X) = g(X)/d(X)$. Then $f_1(X)a(X) + g_1(X)b(X) = 1$, which means that

$$
\begin{pmatrix}
-f_1(X) & g_1(X) \\
 b(X) & a(X)
\end{pmatrix}
\begin{pmatrix}
G(X, Y) \\
F(X, Y)
\end{pmatrix}
= \begin{pmatrix}
R(X, Y) \\
U(X, Y)
\end{pmatrix}
$$

is an invertible linear transformation. Hence the ideals $(F, G)$ and $(H, U)$ are the same, so $I(P; F \cap G) = I(P; H \cap U)$. Since $Y$ divides $R(X, Y) = -f_1(X)G(X, Y) + g_1(X)F(X, Y)$, so we can use property (h) of the intersection multiplicity. This process can be continued and after some steps we can recognize that a certain intersection multiplicity is 0, using property (a).

As an illustration the following useful lemma can be proved, which can be found in [107], Lemma 9.2, see also p. 87 in [107].

**Lemma 10.4.** Let $P$ be the origin.

1. If $I(P; F \cap Y) = r$, $I(P; G \cap Y) = s$ and $r \geq s$, then $I(P; F \cap G) \geq s$.

2. If $r > s$ and $P$ is a simple point of $F$, then $I(P; F \cap G) = s$.

**Proof:** We only prove (1). In determining the intersection multiplicity with the approach indicated above, then we have $X^r|d(X)$. So when we compute $I(P; H \cap U)$ with $H = YH_1$, we get $I(P; YH_1 \cap U) = I(P; Y \cap U) + \ldots$, where $\ldots \geq 0$. Now put $U = U_1(X) + YU_2(X, Y)$. Then $I(P; Y \cap U) = I(P; Y \cap U_1)$. Since the terms of $U$ that do not contain $Y$ come from similar terms of $F$ and $G$, and $d(X)$ is divisible by $X^r$, $X^r$ divides $U_1(X)$. But then $I(P; Y \cap U_1(X)) \geq I(P; Y \cap X^r) = s$. (2) is
left as an exercise.

**Exercise 10.5.** Prove case (2) above!

In the applications we need bounds on the common points of two curves, and bounds on the number of points on a single curve.

**Theorem 10.6. (Bézout)** If \( f \) and \( g \) has no common component then the number of their common points, counted with intersection multiplicities, is at most \( \deg(f) \deg(g) \). Over the algebraic closure \( \overline{F} \) always equality holds.

The proof of Bézout’s theorem is based on resultants, compare to Section 9.5.

Now let \( F = GF(q) \). How many points can a curve \( f \in GF(q)[X,Y,Z] \) of degree \( n \) have over \( GF(q) \)? Denote this number by \( N_q = N_q(f) \).

**Theorem 10.7. Hasse-Weil, Serre** For an absolutely irreducible non-singular algebraic curve \( f \in GF(q)[X,Y,Z] \) of degree \( n \) we have

\[
|N_q(f) - (q + 1)| \leq g |2\sqrt{q}| \leq (n-1)(n-2)\sqrt{q}.
\]

In the theorem \( g \) denotes the genus of \( f \), we do not define it here. Note that \( N_q \) counts the points of \( f \) with multiplicities, also that for \( GF(q) \subset GF(q_1) \) we have \( N_q(f) \leq N_{q_1}(f) \).

It happens that some absolutely irreducible component of \( f \) cannot be defined over \( GF(q) \) (but it still has some \( GF(q) \)-rational points, i.e. points in \( PG(2,q) \)). Then the following bound can be used:

**Exercise 10.8.** Prove that for an absolutely irreducible algebraic curve \( f \in GF(q)[X,Y,Z] \) of degree \( n \), that cannot be defined over \( GF(q) \), we have \( N_q(f) \leq n^2 \).

In some cases the Hasse-Weil bound can be changed for a better one, for example when \( q = p \) is a prime number.

**Theorem 10.9. Stöhr-Voloch [111]** For an irreducible algebraic curve \( f \in GF(q)[X,Y,Z] \), \( q = p^k \), of degree \( n \) with \( N_q \) rational points over \( GF(q) \) we have

(i) if \( n > 1 \), not every point is an inflexion and \( p \neq 2 \) then \( N_q \leq \frac{1}{2}n(q + n - 1) \);

(ii) if \( n > 2 \), not every point is an inflexion and \( p = 2 \) then \( N_q \leq \frac{1}{2}n(q + 2n - 4) \);

(iii) if \( q = p \) and \( n > 2 \) then \( N_p \leq 2n(n-2) + \frac{1}{2}np \);

(iv) if \( q = p \), \( 3 \leq n \leq \frac{1}{2}p \) and \( f \) has \( s \) double points then \( N_p \leq \frac{3}{2}n(5(n-2) + p) - 4s \).

In (i) the condition is automatically satisfied if \( q = p \) is a prime.
Exercise 10.10. Let \( f(X) \) be a polynomial of degree at most \( \sqrt[q]{q} \), \((q \text{ odd})\), which assumes square elements of \( \text{GF}(q) \) only. Prove that \( f = g^2 \) for a suitable polynomial \( g \).

10.1 Conditions implying linear (or low-degree) components

In the applications it is typical that after associating a curve to a certain set (in principle), the possible linear components of the curve have a very special meaning for the original problem. Quite often it more or less solves the problem if one can prove that the curve splits into linear factors, or at least contains a linear factor. Here some propositions ensuring the existence of linear factors are gathered. The usual statement below considers the number of points (in \( \text{PG}(2,q) \)) of a curve.

We will use two numbers: for a curve \( C \), defined by the homogeneous polynomial \( f(X,Y,Z) \), \( M_q \) denotes the number of solutions (i.e. points \((x,y,z) \in \text{PG}(2,q) \)) for \( f(x,y,z) = 0 \), while \( N_q \) counts each solution with its multiplicity on \( C \).

Exercise 10.11. Barlotti-bound Prove that if a curve of order \( n \) has no linear factors over \( \text{GF}(q) \) then \( N_q \leq (n-1)q + n \).

Exercise 10.12. Prove that a curve of degree \( n \) defined over \( \text{GF}(q) \), without linear components, has always \( N_q \leq (n-1)q + n^2 \) points in \( \text{PG}(2,q) \). Hint: let \( k \) be maximal such that every tangent of the curve contains at least \( k \) points of the curve (counting without multiplicity, in \( \text{PG}(2,q) \)). Show that (i) \( N_q \leq (n-1)q + k \); (ii) \( N_q \leq (n-1)q + (n-k) \).

Conjecture 10.13. We conjecture that a curve of degree \( n \) defined over \( \text{GF}(q) \), without linear components, has always \( N_q \leq (n-1)q + 1 \) points in \( \text{PG}(2,q) \).

For \( n = 1, 2, \sqrt{q} + 1, q - 1 \) it would be sharp as the curves \( X^2 - YZ, X^{q+1} + Y^{q+1} + Z^{q+1} \) and \( \alpha X^{q-1} + \beta Y^{q-1} - (\alpha + \beta) Z^{q-1} \) (where \( \alpha, \beta, \alpha + \beta \neq 0 \)) show.

It can be called the Lunelli-Sce bound for curves, see Section 25.

Note that the conjecture is true

(i) if there exists a line skew to the curve and \((q,n) = 1\), see Corollary 25.6;

(ii) if \( n \leq \sqrt{2} + 1 \) then \( q + 1 + (n-1)(n-2) \sqrt{q} \leq nq - q + 1 \) proves it by Weil’s bound Theorem 10.7;

(iii) if the curve has a singular point in \( \text{PG}(2,q) \);

(iv) if \( n \geq q + 2 \).

The statement (ii) can be proved by induction: if \( C \) has more points then it cannot be irreducible, so it splits to the irreducible components \( C_1 \cup C_2 \cup \ldots \cup C_k \) with degrees \( n_1, \ldots, n_k \); if each \( C_i \) had \( \leq (n_i - 1)q + 1 \) points then in total \( C \) would have \( \leq \sum_{i=1}^k (n_i q - q + 1) = nq - k(q-1) < nq - q + 1 \) points. So at least one of them,
$C_j$ say, has more than $n_jq - q + 1$ points. By Exercise 10.8 $C_j$ can be defined over $\mathbf{GF}(q)$ and Weil does its job again.

For (iii) the Barlotti-bound, recounted looking around from a singular point, will work.

The truth of the conjecture would also mean that the counterexamples for the Lunelli-Sce conjecture are not pointsets of curves, see Section 25, Corollary 25.6.

Let $C_n$ be a curve of degree $n$ defined over $\mathbf{GF}(q)$, with at least $qn$ affine points (counted with multiplicity). (In fact it’s enough to have $qn - \delta$ points, see below).

We want to prove that it has a linear component, then repeat everything for $n - 1$ and $(n - 1)q$. The next proposition, which may be omitted in the final version, deals with curves of high degree as well.

**Proposition 10.14.** A curve of degree $n$ defined over $\mathbf{GF}(q)$, without linear components, has always $N_q \leq nq$ points in $\mathbf{AG}(2, q)$. More precisely, if $tq < n \leq (t + 1)q$ then $N_q \leq \max\{tq^2, (q + 1)(n - t - 1)\}$.

(For $t = 0$ it gives $N_q \leq (n - 1)q + n - 1$.)

The key idea is that if you find a line intersecting $C_n$ in at least $n + 1$ points then it is a (linear) component by Bézout. If not then $C_n$ is a $(k, n)$-arc and one can estimate its cardinality.

Let $tq < n \leq (t + 1)q$ and suppose that $C_n$ is a curve with

$N_q > \max\{tq^2, (q + 1)(n - t - 1)\}$

points. Then $N_q > tq^2$, so there is a point $P$ of maximal multiplicity $m \geq t + 1$. Consider a tangent line $\ell$ through $P$, then $I(C_n \cap \ell, P) \geq m + 1$, so there are at most $n - m - 1$ further points on $\ell \setminus P$. As there exist at least $m$ tangents through $P$, we have

$N_q \leq m + (q + 1)(n - m) - m = (q + 1)(n - m) \leq (q + 1)(n - t - 1),$  

which is a contradiction.

The following lemma is a generalization of a result by Szőnyi. For $d = 1$ it can be found in Sziklai [113], which is a variant of a lemma by Szőnyi [124].

**Lemma 10.15.** Let $C_n$, $1 \leq d < n$ be a curve of order $n$ defined over $\mathbf{GF}(q)$, not containing a component defined over $\mathbf{GF}(q)$ of degree $\leq d$. Denote by $N$ the number of points of $C_n$ in $\mathbf{PG}(2, q)$. Choose a constant $\frac{1}{d+1} + \frac{d(d-1)\sqrt{q}}{(d+1)(q+1)} \leq \alpha$. Assume that $n \leq \alpha \sqrt{q} - \frac{1}{\alpha} + 1$. Then $N \leq n(q + 1)\alpha$. 
It works also with \( \alpha > \frac{1}{d+1} + \frac{1+d(d-1)\sqrt{q}}{(d+1)^2 q}, \) \( n < \alpha\sqrt{q} - d + 2, \) \( N < n\alpha q. \) Here \( \alpha = \frac{1}{d+1} \) can be written (that is often needed) when \( d \leq \sqrt{q}. \)

**Proof:** Suppose first that \( C_n \) is absolutely irreducible. Then Weil’s theorem ([136], [77]) gives \( N \leq q + 1 + (n-1)(n-2)\sqrt{q} \leq n(q+1)\alpha. \) (The latter inequality, being quadratic in \( n, \) has to be checked for \( n = d+1 \) and \( n = \alpha\sqrt{q} - \frac{1}{\alpha} + 1 \) only.)

If \( C_n \) is not absolutely irreducible, then it can be written as \( C_n = D_{i_1} \cup \ldots \cup D_{i_r}, \) where \( D_{i_j} \) is an absolutely irreducible component of order \( i_j, \) so \( \sum_{j=1}^s i_j = n. \) If \( D_{i_j} \) can not be defined over \( GF(q), \) then it has at most \( N_{i_j} \leq (i_j)^2 \leq i_j(q+1)\alpha \) points in \( PG(2, q) \) (see Ex. 10.8). If \( D_{i_j} \) is defined over \( GF(q), \) then the Weil-bound implies again that \( N_{i_j} \leq i_j(q+1)\alpha. \) Hence

\[
N = \sum_{j=1}^s N_{i_j} \leq \sum_{j=1}^s i_j(q+1)\alpha = n(q+1)\alpha.
\]

For applications see Section 11, Theorem 23.1, Theorem 23.2 and Theorem 27.8.

**Exercise 10.16.** Prove that if \( q = p \) is prime and \( \alpha > \frac{3}{5} \) then in the theorem above \( n \leq (\frac{1}{2}\alpha - \frac{1}{5})p + 2 \) is enough for \( N \leq n(p+1)\alpha. \)

In the applications quite often happens that we do not know the number of points of a certain curve but we know the numbers of intersections with a pencil of lines (each intersection counted with intersection multiplicity).

**Lemma 10.17.** Let \( C, 1 \leq d < n \) be a curve defined by the homogeneous polynomial \( F \in GF(q)[X, Y, Z], \) \( \deg(F) = n. \) Suppose that \( C \) does not contain a component defined over \( GF(q) \) of degree \( \leq d. \) Assume that \( C \) does not contain (multiple components nor) components with vanishing partial derivative with respect to \( X. \) Let \( \ell_1, \ldots, \ell_{q+1} \) be the lines of the pencil centered at \( P(1, 0, 0). \) Denote by \( N_0 \) the number of intersection points of \( C \) and the lines \( \{\ell_1, \ldots, \ell_{q+1}\}, \) each point on \( \ell_j \) counted with the intersection multiplicity of \( \ell_j \) and \( C \) (but we do not count \( P \) even if it is on \( C. \) Choose a constant \( \frac{1}{d+1} + \frac{d(d-1)\sqrt{q}}{(d+1)^2 q} \leq \alpha. \) Assume that \( n \leq \alpha\sqrt{q} - \frac{1}{\alpha} + 1. \) Then \( N_0 \leq n(q+1)\alpha + n(n-1)\).

**Proof:** The only difference here, compared to the situation of Lemma 10.15, is that \( N_0 \) can be bigger than \( N, \) the number of points of \( C. \) As before we can count componentwise. The difference \( N_0 - N \) comes from points where the tangent of an irreducible component \( G_{i_j} \) of the curve is horizontal, that is the intersection points of \( G_{i_j} \) and \( \partial_X G_{i_j}. \) If \( \partial_X G_{i_j} \) is not zero and \( \deg G_{i_j} = i_j \) then by Bézout’s theorem \( i_j(i_j - 1) \) is an upper bound for the number of points in \( G_{i_j} \cap \partial_X G_{i_j}. \) So \( N_0 \leq N + \sum_{j} i_j(i_j - 1) \leq n(q+1)\alpha + n(n-1). \)

**Exercise 10.18.** (De Beule - Gács) Let \( I \) consist of all the linear combinations of the monomials \( X^{p+1}, Y^{p+1}, Z^{p+1}, X^p Y, XY^p, Y^p Z, Y Z^p, Z^p X, Z X^p. \) Suppose that \( f \) is a homogeneous quadratic polynomial for which \( f^{1+1} \) is in \( I. \) Then \( f \) is reducible.
11 Finding the missing factors, removing the surplus factors

Here we treat a very general situation, with several applications in future.
Given \( A = \{a_1, \ldots, a_{q-\varepsilon}\} \subset \text{GF}(q) \), all distinct, let \( F(X) = \prod_{i=1}^{q-\varepsilon}(X - a_i) \) be their root polynomial. We would like to find the “missing elements” \( \{a_{q-\varepsilon+1}, \ldots, a_q\} = \text{GF}(q) \setminus A \), or, equivalently, \( G^*(X) = \prod_{i=q-\varepsilon+1}^{q}(X - a_i) \). Obviously, \( G^*(X) = \frac{X^q - X}{F(X)} \), so \( F(X)G^*(X) = X^q - X \). Expanding this, and introducing the elementary symmetric polynomials

\[
\sigma_j = \sigma_j(A), \quad \sigma_k^* = \sigma_k(\text{GF}(q) \setminus A),
\]

we get

\[
X^q - X = (X^{q-\varepsilon} - \sigma_1 X^{q-\varepsilon-1} + \sigma_2 X^{q-\varepsilon-2} - \ldots \pm \sigma_{q-\varepsilon-1} X \mp \sigma_{q-\varepsilon} ) (X^{\varepsilon} - \sigma_1^* X^{\varepsilon-1} + \sigma_2^* X^{\varepsilon-2} - \ldots \pm \sigma_{\varepsilon-1}^* X \mp \sigma_{\varepsilon}^* ),
\]

from which \( \sigma_j^* \) can be calculated recursively from the \( \sigma_k \)-s, as the coefficient of \( X^{q-j}, j = 1, \ldots, q - 2 \) is 0 = \( \sigma_j^* + \sigma_j^* \sigma_1 + \ldots + \sigma_j^* \sigma_{j-1} + \sigma_j \); for example

\[
\sigma_1^* = -\sigma_1; \quad \sigma_2^* = \sigma_1^2 - \sigma_2; \quad \sigma_3^* = -\sigma_1^3 + 2\sigma_1 \sigma_2 - \sigma_3; \quad \text{etc.} \tag{1}
\]

Note that we do not need to use all the coefficients/equations, it is enough to do it for \( j = 1, \ldots, \varepsilon \). (The further equations can be used as consequences of the fact that the \( a_i \)-s are pairwise distinct, see e.g. Theorem 25.7 and Lemma 25.8.)

The moral of it is that the coefficients of \( G^*(X) \) can be determined from the coefficients of \( F(X) \) in a “nice way”.

* * *

Let now \( B = \{b_1, \ldots, b_{q+\varepsilon}\} \supset \text{GF}(q) \) be a multiset of elements of \( \text{GF}(q) \), and let

\[
F(X) = \prod_{i=1}^{q+\varepsilon}(X - b_i)
\]

be their root polynomial. We would like to find the “surplus elements” \( \{b_{q+\varepsilon}, \ldots, b_q\} = B \setminus \text{GF}(q) \), or, equivalently, \( G(X) = \prod_{i=1}^{\varepsilon}(X - b_i) \). Obviously, \( G(X) = \frac{X^{q+\varepsilon} - X}{F(X)} \), so \( F(X) = (X^q - X)G(X) \). Suppose that \( \varepsilon \leq q - 2 \). Expanding this equation and introducing the elementary symmetric polynomials

\[
\sigma_j = \sigma_j(B), \quad \bar{\sigma}_k = \sigma_k(B \setminus \text{GF}(q)),
\]

we get

\[
X^{q+\varepsilon} - \sigma_1 X^{q+\varepsilon-1} + \sigma_2 X^{q+\varepsilon-2} - \ldots \pm \sigma_{q+\varepsilon-1} X^{q+1} \mp \sigma_{q+\varepsilon} X^{q} \pm \ldots \\
\ldots \pm \sigma_{q+\varepsilon-1} X \mp \sigma_{q+\varepsilon} = (X^q - X)(X^{\varepsilon} - \bar{\sigma}_1 X^{\varepsilon-1} + \bar{\sigma}_2 X^{\varepsilon-2} - \ldots \pm \bar{\sigma}_{\varepsilon-1} X \mp \bar{\sigma}_{\varepsilon} ) = \\
=X^{q+\varepsilon} - \bar{\sigma}_1 X^{q+\varepsilon-1} + \bar{\sigma}_2 X^{q+\varepsilon-2} - \ldots \pm \bar{\sigma}_{q-\varepsilon} X^{q+1} \mp \bar{\sigma}_{\varepsilon} X^{q} \mp \varepsilon \text{ terms of lower degree.}
\]

From this \( \bar{\sigma}_j \) can be calculated even more easily then in the previous case:

\[
\bar{\sigma}_k = \sigma_k \quad \text{for all } k = 1, \ldots, \varepsilon. \tag{2}
\]
In both case suppose now that instead of the “elements” \( \{a_i\} \) or \( \{b_j\} \) we have (for example) linear polynomials \( c_iY + d_i \) and a set \( S \subseteq \mathbb{GF}(q) \) such that for each \( y \in S \) the set \( A_y = \{c_iy + d_i : i\} \) consists of pairwise distinct elements of \( \mathbb{GF}(q) \), or, similarly, the multiset \( B_y = \{c_iy + d_i : i\} \) contains \( \mathbb{GF}(q) \). Then the \( \sigma_k \)-s in the reasonings above become polynomials in \( Y \), with \( \deg_Y(\sigma_k) \leq k \). Now one cannot speak about polynomials \( \sigma_k^*(Y) \) (or \( \bar{\sigma}_k(Y) \), resp.) as there is no guarantee that the missing values (or the surplus values) for different \( Y \)-s can be found on \( \varepsilon \) lines. So first we define \( \sigma_k^*(y) \) (or \( \bar{\sigma}_k(y) \), resp.), meaning the coefficient of \( X^{\varepsilon - k} \) in \( G_y(X) \) or \( G_y^*(X) \), so the elementary symmetric function of the missing (or surplus) elements when substituting \( Y = y \in S \). However, the equations for the \( \sigma_k^*-s \) or \( \bar{\sigma}_k\)-s are still valid. So one may define the polynomials analogously to (1):

\[
\sigma_1^*(Y) \overset{\text{def}}{=} -\sigma_1(Y); \quad \sigma_2^*(Y) \overset{\text{def}}{=} \sigma_1^2(Y) - \sigma_2(Y);
\]

\[
\sigma_3^*(Y) \overset{\text{def}}{=} -\sigma_3(Y) + 2\sigma_1(Y)\sigma_2(Y) - \sigma_3(Y); \quad \text{etc.}
\]

or analogously to (2):

\[
\bar{\sigma}_k(Y) \overset{\text{def}}{=} \sigma_k(Y) \text{ for all } k = 1, \ldots, \varepsilon
\]

with the help of them. Note that from the defining equations it is obvious that

\[
\deg_Y \sigma_k^*(Y) \leq k \quad \text{and} \quad \deg_Y \bar{\sigma}_k(Y) \leq k.
\]

Now we can define the algebraic curve

\[
G^*(X, Y) \overset{\text{def}}{=} X^\varepsilon - \sigma_1^*(Y)X^{\varepsilon-1} + \sigma_2^*(Y)X^{\varepsilon-2} - \ldots \pm \sigma_{\varepsilon-1}^*(Y)X \pm \sigma_\varepsilon^*(Y)
\]

or in the other case

\[
\bar{G}(X, Y) \overset{\text{def}}{=} X^\varepsilon - \bar{\sigma}_1(Y)X^{\varepsilon-1} + \bar{\sigma}_2(Y)X^{\varepsilon-2} - \ldots \pm \bar{\sigma}_{\varepsilon-1}(Y)X \pm \bar{\sigma}_\varepsilon(Y)
\]

As before, for each \( y \in S \) we have that the roots of \( G(X, y) \) are just the missing (or the surplus) elements of \( A_y \) or \( B_y \), resp. Our aim is to factorize \( G^*(X, Y) \) or \( \bar{G}(X, Y) \) into linear factors \( X - (\alpha_iY + \beta_i) \). To do so, observe that \( G^*(X, y) \) has many points in \( \mathbb{GF}(q) \times \mathbb{GF}(q) \): for any \( y \in S \) we have \( \varepsilon \) solutions of \( G^*(X, y) = 0 \), i.e. the \( \varepsilon \) missing values after substituting \( Y = y \) in the linear polynomials \( c_iY + d_i \), so after determining the sets \( A_y \). So \( G^*(X, Y) \) has at least \( \varepsilon|S| \) points.

A similar reasoning is valid for \( \bar{G}(X, Y) \). If it splits into irreducible components \( \bar{G} = G_1G_2 \cdots G_r \), with \( \deg G_i = \deg_X G_i = \varepsilon_i \), \( \sum \varepsilon_i = \varepsilon \), then for any \( y \in S \), the line \( Y = y \) intersects \( G_i \) in \( \varepsilon_i \) points, counted with intersection multiplicity. So the number of points on \( G_i \), for each \( y \in S \), stands for the intersection points of \( G_i \) and \( \partial_X G_i \), where the intersection multiplicity with the line \( Y = y \) is higher than the multiplicity of that point on \( G_i \). So, unless some \( G_i \) has zero partial derivative w.r.t. \( X \), we have that \( \bar{G} \) has at least \( \sum \varepsilon_i|S| - \varepsilon_i(\varepsilon_i - 1) \geq \varepsilon|S| - \varepsilon(\varepsilon - 1) \) points.
Now we can use Lemma 10.15, Lemma 10.17 (or any similar result) repeatedly, with \( d = 1 \), it will factorize \( G(X, Y) \) into linear factors of the form \( X - (\alpha_j Y + \beta_j) \) if \( \deg G(X, Y) \), which is at most \( \varepsilon \) in our case, is small enough, i.e. if \( \varepsilon < \sqrt{q} \) and 
\[
|S| > \max\left\{ \frac{-1+\sqrt{8q}}{\sqrt{q}}, \frac{1}{2}\right\} \cdot (q+1) \text{ in the first and } |S| > \max\left\{ \frac{-1+\sqrt{8q}}{\sqrt{q}}, \frac{1}{2}\right\} \cdot (q+1)+\varepsilon-1 \text{ in the second case.}
\]

It means, that one can add \( \varepsilon \) linear polynomials \( \alpha_i Y + \beta_i \) in the first case such that for any \( y \in S \), the values \( \{c_i y + d_i\} \cup \{\alpha_j y + \beta_j\} = \text{GF}(q) \). In the second case we have a weaker corollary: for any \( y \in S \), the values \( \{c_i y + d_i\} \setminus \{\alpha_j y + \beta_j\} = \text{GF}(q) \), which means that adding the new lines \( \alpha_j Y + \beta_j \) “with multiplicity=−1” then \( S \times \text{GF}(q) \) is covered exactly once. (What we do not know in general, that these lines were among the given \( q+\varepsilon \) lines, so whether we could remove them.)

Finally, these lines (or similar objects), covering \( S \times \text{GF}(q) \) usually have some concrete meaning when applying this technique; this book contains several such applications, see Theorem 27.4, Exercise 27.6, etc.

The arguments above are easy to modify when we change some of the conditions, for example when \( a_i \) or \( b_i \) is allowed to be some low degree (but non-linear) polynomial of \( Y \).

**Exercise 11.1.** Use the second (“surplus”) case above to prove that a blocking set \( B \subset \text{PG}(2, q) \) with \( |B \cap \text{AG}(2, q)| = q + 1 \) affine points always contains an (affine) point that is unnecessary (i.e. it can be deleted without violating the blocking property).

**Exercise 11.2.** Let \( f_i(T), \ i = 1, \ldots, q - \varepsilon \) be polynomials of degree at most \( d \), and suppose that their graphs \( \{(t, f_i(t)) : t \in \text{GF}(q)\} \) are pairwise distinct. Prove that if \( \varepsilon < \ldots \) then one can find \( f_{q-\varepsilon+1}(T), \ldots, f_q(T) \), each of degree at most \( d \) such that the graphs of these \( q \) polynomials partition the affine plane.

**Exercise 11.3.** Let \( f_i(T), \ i = 1, \ldots, q - \varepsilon \) be polynomials, each from a subspace \( U \) of \( \text{GF}(q)[T] \) with \( 1 \in U \), and suppose that their graphs \( \{(t, f_i(t)) : t \in \text{GF}(q)\} \) are pairwise distinct. Prove that if \( \varepsilon < \ldots \) then one can find \( f_{q-\varepsilon+1}(T), \ldots, f_q(T) \), each from \( U \), such that the graphs of these \( q \) polynomials partition the affine plane.
Chapter 2

Polynomials in geometry

12 Lines meeting a pointset

12.1 Prescribing the intersection numbers

Suppose that a function $m : \mathcal{L} \rightarrow \mathbb{N}$ is given, where $\mathcal{L}$ is the set of lines of $\text{PG}(2, q)$. The problem is to find conditions, necessary and/or sufficient, under which we can find a pointset $S$ such that $|S \cap \ell| = m(\ell)$ for all $\ell \in \mathcal{L}$.

Note that one can pose the similar question for any hypergraph.

If $A$ denotes the incidence matrix of the plane, $m = (m(\ell_1), m(\ell_2), ..., m(\ell_{q^2+q+1}))$ is the weight-vector, then the problem is reduced to finding a ("characteristic vector") $v$ such that $Av = m$. As $A$ is non-singular, we have $v = A^{-1}m$. Now one can turn the question around: for which $m$ will $v$ be of the required type, for example a non-negative, integer or 0-1 vector?

It is easy to compute that

$$A^{-1} = \frac{1}{q} A^T - \frac{1}{q(q + 1)} J.$$ 

We also know that the eigenvalues of $A$ are $q+1$ (with multiplicity 1 and eigenvector $(1, 1, ..., 1)$); $\sqrt{q}$ and $-\sqrt{q}$ (their multiplicities depend on the order of points and lines we choose).

In most cases $m$ is not given, we know some of its properties only. It means that a certain set $M$ of weight-vectors is given (for example, the set of all vectors with each coordinate from a small fixed set of integers, say $\{0, 1, 2\}$); and we want to know some property (for example, the possible Hamming-weight, i.e. the number of nonzero coordinates) of (0-1) vectors $v$ satisfying $Av \in M$. 

71
12.2 A general result

Metsch conjectured [95] and Weiner [130] proved the following

**Theorem 12.1.** Let $B \subseteq PG(2, q)$ be a pointset of size $b$ on $r$ lines of a pencil centered at $P \notin B$. Then the number of lines meeting $B$ in at least one point is at most

$$b(q + 1) - (r(b - r + 1) - 1).$$

It can be reformulated as: the points of $B$ “determine” at least $r(b - r + 1) - 1$ lines, where a line containing $t \geq 2$ points of $B$ is counted with multiplicity $t - 1$.

First of all observe that there are point sets for which the given bound is sharp. Assume that $r - 1$ is the order of a subplane $\pi$ in $PG(2, q)$ and let $B$ be a proper subset of $\pi$ containing $r$ collinear points (i.e. a subline), hence it blocks all the lines of $\pi$. So the number of lines meeting $B$ is $((r-1)^2 + (r-1) + 1) + B((q+1) - r)$, where the first part is the number of lines of $\pi$, the second is the number of tangents through the points of $B$. The number of lines meeting $B$ through a point $P$ of $\pi \setminus B$ is $r$ and so for such a point the bound in the conjecture is sharp.

Note that this statement is stronger than the following well known result of Jamison [84] and Brouwer and Schrijver [49].

**Theorem 12.2.** (Jamison, Brouwer and Schrijver) A blocking set in $AG(2, q)$ contains at least $2q - 1$ points.

**Proof:** Assume to the contrary that there is a blocking set $B$ in $AG(2, q)$ so that $|B| \leq 2q - 2$. Embed $AG(2, q)$ in $PG(2, q)$ and let $P$ be an ideal point. Now the value $r$ in Theorem 12.1 above is $q$ and so the total number of lines meeting $B$ is at most $1 + q + ((|B| - q)(q + 1 - q) \leq q^2 + q - 1$; which is a contradiction, since $B$ blocks all the $q^2 + q$ affine lines.

Note that there are blocking sets of size $2q - 1$, e.g. the points of two intersecting lines.

**Exercise 12.3.** Prove Jamison’s theorem using the Combinatorial Nullstellensatz (Theorems 5.16, 5.17).

**Exercise 12.4.** [123] If the smallest blocking set of $AG(2, q)$ has size $r$ then in $PG(2, q)$ the smallest blocking set, which contains two different minimal blocking sets, is of size $r + 2$, and vice versa.

Note that it implies a kind of “stability” of blocking sets of size $\leq 2q$. There are blocking sets of size less than $2q - 1$ in some non-Desarguesian affine planes of order $q$, see [54]; which shows that a purely combinatorial proof cannot be given for neither Theorem 12.2 nor Theorem 12.1. To prove Theorem 12.1 the following lemma is essential.
Excercise 12.5. (Blokhuis and Brouwer, \[44\]) Let $B$ be a blocking set in $\mathbb{P}G(2, q)$ and let $P$ be an essential point of $B$. Then there are at least $2q + 1 - |B|$ tangents through $P$.

Lemma 12.6. Let $\ell_\infty = [1, 0, 0]$ be called now the line at infinity in $\mathbb{P}G(2, q)$ and let $S$ be a point set in $\mathbb{P}G(2, q) \setminus \ell_\infty$. Assume that through the ideal point $(0, -z, y)$ there pass $t$ (affine) lines meeting $S$. Denote by $n_{t+h}$ the number of ideal points through that there pass exactly $t + h$ lines meeting $S$. Then $\sum_{h=1}^{q-t} h n_{t+h} \leq (|S| - t)(q - t)$.

Proof: For the points of $S$ write $\{(a_i, b_i, 1)\}$ and consider the three-variable Rédéi polynomial of $S$, that is $R(X, Y, Z) = \prod_{i=1}^{|S|} (X + a_i Y - b_i Z) = \sum_{j=0}^{|S|} r_j(Y, Z)X^{|S| - j}$. Recall that $\deg r_j = j$. It follows from the fundamental property of the Rédéi polynomial, that $\deg_X \gcd(R(X, y, z), X^q - X) = t$.

For the polynomials $R$ and $X^q - X$ construct the matrix $R_k(Y, Z)$ introduced in Section 9.5. By Theorem 9.39, for the excess sum in question $\sum_{h=1}^{q-t} h n_{t+h} \leq \deg(\det R_k(Y, Z)) \leq (|S| - t)(q - t)$.

Proof of Theorem 12.1: For the line at infinity $\ell_\infty$ choose an $m$-secant of $B$, $m > 0$, passing through $P$. Note that now the line at infinity meets $B$. Again denote by $n_{(r-1)+h}$ the number of ideal points through that there pass exactly $(r-1) + h$ affine lines meeting $B$. Let us sum up the number of affine lines meeting $B$ through the ideal points, in total we get at most $qm + (q + 1 - m)(r - 1) + \sum_{h=1}^{q-(r-1)} h n_{(r-1)+h}$; where the first part corresponds to the points of $\ell_\infty \cap B$, the second to the points of $\ell_\infty \setminus B$. The result follows from Lemma 12.6 immediately as $1+qm+(q+1-m)(r-1)+(b-m-(r-1))(q-(r-1)) = b(q+1) - (r(b-r+1)-1)$.

It has a nice (combinatorial) corollary in the 3-space:

Corollary 12.7. [95] Suppose $B$ is a set of $b \geq q + 1$ points in $\mathbb{P}G(3, q)$. Then $B$ meets at most $q^2 + q + 1 + bq^2$ lines, with equality if and only if $B$ is a planar blocking set.

Exercise 12.8. Formulate and prove the analogue of the corollary in the plane (where a combinatorial proof can be given easily).

12.3 Another immediate corollary

An $m$-fold blocking set in $\mathbb{A}G(2, q)$ is a set of points intersecting each line in at least $m$ points. Blokhuis ([31]) showed that an $m$-fold blocking set $S$ in $\mathbb{A}G(2, q)$, where $(m, q) = 1$, has at least $(m+1)q - 1$ points. Later Ball ([6]) extended this
result to arbitrary \( m \), he showed that if \( e(m) \) is the maximal exponent such that \( p^{e(m)} | m \), then \( |S| \geq (m + 1)q - p^{e(m)} \), see Corollary 24.25.

In this subsection we show that Theorem 9.39 immediately implies a lower bound on the size of an \( m \)-fold blocking set in \( \mathbb{AG}(2,q) \). In general, except when \( m | q \), this result is weaker than Ball’s result.

**Corollary 12.9.** (Szönyi-Weiner [130]) The size of an \( m \)-fold blocking set in \( \mathbb{AG}(2,q) \) is at least \((m + 1)q - m\).

**Proof:** Assume to the contrary that there exists an affine \( m \)-fold (not necessarily minimal) blocking set \( B \) of size \((m + 1)q - m - 1\). Let \( \ell \) be an \((m + k)\)-secant, \( k \geq 0 \), where \(|B| - (m + k) \neq qm\). Such a line \( \ell \) can be chosen, since counting the points of \( B \) on the lines through a point of \( B \) and on the lines through an affine point not in \( B \) shows that the intersection numbers of \( B \) with lines take at least two different values. Change the coordinate system, so that \( \ell \) is the ideal line and \((\infty) \in B \). Now \( B \) contains at least \( m \) points from each line, except from the ‘old’ line at infinity that is skew to \( B \). Denote this line by \( \ell' \) and by \((y_\ell)\) the ideal point of it in this new coordinate system. Let \( U = B \setminus \ell = \{(a_i, b_i)\}_i \) and consider the Rédei polynomial of \( U \), that is \( R(X,Y) = \prod_{i=1}^{|B|-(m+k)} (X + a_iY - b_i) = \sum_{j=0}^{|B|-(m+k)} r_j(Y)X^{|B|-(m+k)-j} \). By the properties of the Rédei polynomial, \( \deg_X \gcd(R(X,y), (X^q - X)^m) = m(q - 1) \) and for any \((y) \in \ell \setminus (B \cup (y_\ell))\), \( \deg_X \gcd(R(X,y), (X^q - X)^m) = mq \). For the polynomial \( R \) and \((X^q - X)^m \) and for the value \( s = \max(\deg_X R, qm) - m(q - 1) \), construct the matrix \( R_s \) introduced in Section 9.5. By Result 9.34, the determinant of this matrix is not zero. Furthermore, similarly as it is in the proof of Lemma 12.6, one can show that \( \deg(\det R_s) \leq m(q - m - k - 1) \). This is a contradiction, since by Theorem 9.39, \( m(q - m - k) \leq \deg(\det R_s) \).

### 13 Sets with constant intersection numbers mod \( p \)

In [34, 40] the following is proved:

**Proposition 13.1.** Let \( S \) be a pointset in \( \mathbb{AG}(2,q) \), suppose that every line intersects \( S \) in \( 1 \pmod{p} \) points, or is completely disjoint from \( S \). Then \(|S| \leq q - p + 1\).

**Proof:** Counting the points of \( S \) on the lines through some fixed point \( s \in S \) we have \(|S| \equiv 1 \pmod{p} \). After the \( \mathbb{AG}(2,q) \leftrightarrow \mathbb{GF}(q^2) \) identification define

\[
f(X) = \sum_{s \in S} (X - s)^{q-1},
\]

it is not identically zero as the coefficient of \( X^{q-1} \) is 1. Note that for \( x \in \mathbb{GF}(q^2) \) the value of \((x - s)^{q-1}\) depends on the direction of the line joining \( x \) and \( s \). If
13. Sets with constant intersection numbers mod p

\[ x \in S \] then every direction will occur with multiplicity divisible by \( p \), hence all the \( x \) points of \( S \) are roots of \( f \), which is of degree \( q - 1 \). The biggest value \( \equiv 1 \mod p \) below \( q \) is \( q - p + 1 \).

There are examples of sets like in the statement above, e.g., some \( (1 \mod p) \) collinear points, or a projective subplane of order \( < \sqrt{q} \) completely contained in \( \text{AG}(2, q) \).

**Exercise 13.2.** Prove that in Proposition 13.1 it does not make any difference if \( S \) is allowed to be a multiset.

We remark that the projective case is totally different: there are very big pointsets in \( \text{PG}(2, q) \) with \( 1 \mod p \) -secants only, e.g., the plane itself, or a unital, etc.

**Exercise 13.3.** (Blokhuis) Prove the following generalization: Let \( S \) be a pointset in \( \text{AG}(n, q) \), \( n \geq 1 \), and suppose that every hyperplane intersects \( S \) in \( 1 \mod p \) points, or is completely disjoint from \( S \). Then \( |S| \leq q - p + 1 \).

**Exercise 13.4.** Let \( S \) be a pointset in \( \text{AG}(2, q) \) and suppose that for some \( 1 \leq r \leq p - 1 \), every line intersects \( S \) in \( r \mod p \) points, or is completely disjoint from \( S \). Then \( |S| \leq q - p + r \). Why does this statement become not very interesting after proving if?

The situation is different if we consider the projective plane.

**Theorem 13.5.** Given a pointset \( S = \{(a_i, b_i, c_i) : i = 1, ..., s\} = \{(a_i, b_i, 1) : i = 1, ..., s\} \cup \{(a_j, b_j, 0) : j = s_1 + 1, ..., s\} \subseteq \text{PG}(2, q) \), the following are equivalent:

(i) \( S \) intersects each line in \( r \mod p \) points for some fixed \( r \);

(ii) \( G(X, Y, Z) = \sum_{i=1}^{[S]} (a_iX + b_iY + c_iZ)^q-1 \equiv 0 \);

(iii) for all \( 0 \leq k + l \leq q - 1 \), \( \left(\begin{smallmatrix} k+l \\ k \end{smallmatrix}\right) \neq 0 \mod p \), we have \( \sum_{i=1}^{[S]} a_i^{q-1-k-l}b_i^kb_i^l = 0 \) for \( \theta^0 = 1 \).

(iv) for all \( 0 \leq k + l \leq q - 2 \), \( \left(\begin{smallmatrix} k+l \\ k \end{smallmatrix}\right) \neq 0 \mod p \), we have \( \sum_{i=1}^{s_1} a_i^k b_i^l = 0 \) and for all \( 0 \leq m \leq q - 1 \), \( \sum_{i=1}^{s'1} a_i^{q-1-m}b_i^m = 0 \).

**Proof:** Note that if each line intersects \( S \) in \( r \mod p \) points then \( |S| \equiv r \mod p \). So let \( r \) be defined by \( |S| \equiv r \mod p \). If each line \( [x, y, z] \) intersects \( S \) in \( r \mod p \) points then \( \mod p \) \( |S| - r \equiv 0 \) terms \( (a_i x + b_i y + c_i z)^q - 1 \) will be 1 in \( G(x, y, z) \) hence \( G(x, y, z) = 0 \). As \( \deg G \leq q - 1 \) we have (i) \( \Rightarrow \) (ii). One can turn it around: if \( G(x, y, z) = 0 \) then the number of terms \( (a_i x + b_i y + c_i z)^q - 1 \) with nonzero \( (i.e. =1) \) value should be zero mod \( p \), so (ii) \( \Rightarrow \) (i).
For the rest consider the coefficient of $X^{q-1-k-l}Y^kZ^l$ in $G$ (for $0 \leq k+l \leq q-1$), it is

$$\binom{q-1}{k+l} \sum_{i=1}^{\vert S \vert} a_i^{q-1-k-l} b_i^k c_i^l = 0$$

if (ii) holds and vice versa. Finally (iii)$\iff$(iv) is obvious.

Many interesting pointsets (small blocking sets, unitals, maximal arcs, even pointsets, in particular $(0, 2, t)$-arcs and hyperovals) have constant modulo $p$ intersection numbers with lines; we may give the name (generalized) Vandermonde set to such sets. (We recall here Section 9.3.)

Take the “affine” part of a Vandermonde-set, i.e. points with $c_i \neq 0$ and suppose the rest does not count in the power sum that all its points are written as $(a_i, b_i, 1)$. After the $\text{AG}(2, q) \leftrightarrow \text{GF}(q^2)$ identification this point becomes $a_i + b_i \omega$ for some generator $\omega$ of $\text{GF}(q^2)$. Substituting $(1, \omega, Z)$ into $G$ we get

$$0 = G(1, \omega, Z) = \sum_{(a_i, b_i, 1) \in S} ((a_i + b_i \omega) + Z)^{q-1} + \sum_{(a_j, b_j, 0) \in S} (a_j + b_j \omega)^{q-1} =$$

$$\sum_{k=0}^{a-2} \pm Z^{q-1-k} \sum_{(a_i, b_i, 1) \in S} (a_i + b_i \omega)^k + \sum_{(a_i, b_i, c_i) \in S} (a_i + b_i \omega)^{q-1}$$

which means that the affine part of a (generalized) Vandermonde set, considered as a set in $\text{GF}(q^2)$, has power sums equal to zero for exponents $1, ..., q - 2$. (The last, constant term is just $G(1, \omega, 0) = 0$.)

### 13.1 Sets with intersection numbers 0 mod $r$

Here we continue the examination of sets of $\text{PG}(2, q)$ intersecting every line in a constant number of points mod $p$. This section is based on [15]. For the more general $k$-dimensional case see Section 26. The proofs in both sections are similar and are streamlined and then generalised versions of the proof in [14].

**Theorem 13.6.** Let $1 < r < q = p^h$. A pointset $S \subset \text{PG}(2, q)$ which is incident with 0 mod $r$ points of every line has $\vert S \vert \geq (r - 1)q + (p - 1)r$ points and $r$ must divide $q$.

**Proof:** Let us first see that $r$ divides $q$. By counting the points of $S$ on lines through a point not in $S$ we have that $\vert S \vert = 0$ mod $r$. By counting points of $S$ on lines through a point in $S$ we have $\vert S \vert = 1 + (-1)(q + 1)$ mod $r$ and combining these two equalities we see that $q = 0$ mod $r$. 

13. Sets with constant intersection numbers mod p

Assuming \(|S| < r(q + 1)|\) (for if not the theorem is proved) there is an external line to \(S\), so we can view \(S\) as a subset of \(\text{GF}(q^2) \simeq \text{AG}(2, q)\) and consider the polynomial

\[
R(X, Y) = \prod_{b \in S} (X + (Y - b)^{q-1}) = \sum_{j=0}^{|S|} \sigma_j(Y)X^{|S| - j}.
\]

For all \(y, b\) and \(c \in \text{GF}(q^2)\) the corresponding points of \(\text{AG}(2, q)\) are collinear if and only if \((y - b)^{q-1} = (y - c)^{q-1}\) and each factor \(X + (y - b)^{q-1}\) of \(R(X, y)\) divides \(X^{q+1} - 1\) whenever \(y \neq b\).

For \(y \in S\) we have

\[
R(X, y) = X(X^{q+1} - 1)^{r-1}g_1(X)^r,
\]

and for \(y \notin S\)

\[
R(X, y) = g_2(X)^r.
\]

In both cases \(\sigma_j(y) = 0\) for \(0 < j < q\) and \(r\) does not divide \(j\). The degree of \(\sigma_j\) is at most \(j(q - 1)\) and there are \(q^2\) elements in \(\text{GF}(q^2)\), hence \(\sigma_j \equiv 0\) when \(0 < j < q\) and \(r\) does not divide \(j\). So

\[
R(X, Y) = X^{|S|} + \sigma_rX^{|S| - r} + \sigma_{2r}X^{|S| - 2r} + ... + \sigma_qX^{|S| - q} + \sigma_{q+1}X^{|S| - q - 1} + ... + \sigma_{|S|}.
\]

For all \(y \in \text{GF}(q^2)\) we have

\[
\frac{\partial R}{\partial Y}(X, y) = \left(\sum_{b \in S} \frac{-(y - b)^{q-2}}{X + (y - b)^{q-1}}\right) R(X, y).
\]

In all terms the denominator is a divisor of \(X^{q+1} - 1\) so multiplying this equality by \(X^{q+1} - 1\) we get an equality of polynomials and we see that

\[
R(X, y) \mid (X^{q+1} - 1)\frac{\partial R}{\partial Y}(X, y),
\]

or even better

\[
R(X, y)G_y(X) = (X^{q+1} - 1)\frac{\partial R}{\partial Y}(X, y) = (X^{q+1} - 1)(\sigma'_rX^{|S| - r} + \sigma'_{2r}X^{|S| - 2r} + ... + \sigma'_qX^{|S| - q} + \sigma'_{q+1}X^{|S| - q - 1} + ...). \quad (*)
\]

Here \(G = G_y\) is a polynomial in \(X\) of degree at most \(q + 1 - r\). The term of highest degree on the right-hand side of \((*)\) that has degree not \(1\) mod \(r\) is of degree \(|S|\) and has coefficient \(\sigma'_{q+1}\), where \(\acute{\cdot}\) is differentiation with respect to \(Y\).

First examine \(y \notin S\). As \(R(X, y)\) is an \(r\)-th power, any non-constant term in \(G\), with degree not \(1\) mod \(r\) would give a term on the right-hand side of degree \(|S|\) and not \(1\) mod \(r\), but such a term does not exist. Hence every term in \(G\) has degree \(1\) mod \(r\) except for the constant term which has coefficient \(\sigma'_{q+1}\).
For any natural number \( \kappa \) and \( i = 1, \ldots, r - 2 \) the coefficient of the term of degree \( |S| - i(q + 1) - \kappa r \) (which is not 0 or 1 mod \( r \)) on the right-hand side of (\( \ast \)) is

\[-\sigma_{i(q + 1) + \kappa r}^i + \sigma_{(i+1)(q + 1)+\kappa r}^i\]

and must be zero. However if \( (r - 1)(q + 1) + \kappa r > |S| \) then \( \sigma_{(r-1)(q + 1)+\kappa r} \equiv 0 \) and we have \( \sigma_{i(q + 1)+\kappa r}^i = 0 \) for all \( i = 1, \ldots, r - 2 \). Now consider the coefficient of the term of degree \( |S| - \kappa r \). On the right hand side of (\( \ast \)) this has coefficient \( -\sigma_{\kappa r} \) (since \( \sigma_{\kappa r + 1 + \kappa r} = 0 \)). The only term of degree zero mod \( \kappa r \) in \( G \) is the constant term which is \( \sigma_{\kappa r} \). The coefficient of the term of degree \( |S| - \kappa r \) in \( R(X, y) \) is \( \sigma_{\kappa r} \). Hence

\[\sigma_{\kappa r} \sigma_{\kappa r + 1} = -\sigma_{\kappa r} \text{ for all } y \notin S. \quad (**)\]

If \( y \in S \) then \( \sigma_{\kappa r + 1}(y) = 1 \) and if \( y \notin S \) then \( \sigma_{\kappa r + 1}(y) = 0 \). Let

\[f(Y) = \prod_{y \in S} (Y - y).\]

Then \( f \sigma_{\kappa r + 1} = (Y^q - Y)g(Y) \) for some \( g \in GF(q^2)[Y] \) of degree at most \( |S| - 1 \) (the degree of \( \sigma_{\kappa r + 1} \) is at most \( q^2 - 1 \)). Differentiate and substitute for a \( y \in S \) and we have \( f'(y) = -g(y) \). Since the degree of \( f' \) and \( g \) are less than \( |S| \) we have \( g \equiv -f' \). Now differentiate and substitute for a \( y \notin S \) and we get \( \sigma_{\kappa r + 1} f = f' \).

Thus for \( y \notin S \) we have \( \sigma_{\kappa r} f' / f = -\sigma_{\kappa r} \) and so \( (f \sigma_{\kappa r})'(y) = 0 \). The polynomial \( (f \sigma_{\kappa r})' \) has degree at most \( \kappa r(q - 1) + |S| - 2 \), which is less than \( q^2 - |S| \) if \( \kappa r \leq q - 2r \). So from now on let \( |S| = (r - 1)q + \kappa r \). The polynomial \( (f \sigma_{\kappa r})' \equiv 0 \) and so \( f \sigma_{\kappa r} \) is a \( p \)-th power. Hence \( f^{p-1} \) divides \( \sigma_{\kappa r} \).

If \( \kappa \leq p - 2 \) then \( (p - 1)(r - 1)q + \kappa r(p - 1) > \kappa r(q - 1) \) and so \( \sigma_{\kappa r} \equiv 0 \). However the polynomial whose terms are the terms of highest degree in \( R(X, Y) \) is \( (X + Y^r)^{|S|} \) which has a term \( X^{r-1}Y^{\kappa r(q - 1)} \) since \( \binom{|S|}{\kappa r} = 1 \). Thus \( \sigma_{\kappa r} \) has a term \( Y^{\kappa r(q - 1)} \) which is a contradiction. Therefore \( \kappa \geq p - 1 \).

**Corollary 13.7.** A code of dimension 3 whose weights and length have a common divisor \( r \) and whose dual minimum distance is at least 3 has length at least \( (r - 1)q + (p - 1)r \).

A maximal arc in a projective plane is a set of points \( S \) with the property that every line is incident with 0 or \( r \) points of \( S \), see Section 15. Apart from the trivial examples of a point, an affine plane and the whole plane, that is where \( r = 1, q \) or \( q + 1 \) respectively, there are examples known for every \( r \) dividing \( q \) for \( q \) even, see e.g. Denniston [59].

**Corollary 13.8.** There are no non-trivial maximal arcs in \( PG(2, q) \) when \( q \) is odd.
Proof: A maximal arc has \((r - 1)q + r\) points, see Exercise 14.1.

After Theorem 13.5 it is quite natural to return to Vandermonde-like properties (see also Section 9.3). To end this section and to kind of prepare for the next one, here is an application of the Vandermonde property from [70]:

**Proposition 13.9.** Let \(q\) be even and suppose that \(\mathcal{K}\) is a \((q + t, t)\)-arc of type \((0, 2, t)\) having \(t\) points on the line at infinity, \(\{(y_1), (y_2), ..., (y_t)\}\), say. If the \(y\)-axis is also a \(t\)-secant, then the set \(\{y_1, y_2, ..., y_t\}\) is a Vandermonde-set.

**Proof:** First of all note that \((\infty)\) cannot be in \(\mathcal{K}\), since it would contradict the easy observation that through any point of \(\mathcal{K}\) there is one \(t\)-secant and \(q\) 2-secants. Let \(U = \{(a_i, b_i) : i = 1, ..., q\}\) be the affine part of \(\mathcal{K}\). Suppose \(a_1 = ... = a_t = 0\) and consider the affine Rédéi polynomial \(R(X, Y) = \prod_{i=1}^{q}(X + a_iY + b_i)\). According to the fundamental property of the Rédéi polynomial and to the properties of \(\mathcal{K}\), for a fixed \(Y = y \neq y_i\), the polynomial \(R(X, y)\) is a square (each affine line through \((y)\) intersects \(\mathcal{K}\) in an even number of points, hence each root of \(R(X, y)\) has even multiplicity), while for \(Y = y_i\) \((i = 1, ..., t)\), \(R(X, y_i) = X^{q} - X\). This means that the coefficient polynomial \(r_{q-1}(Y)\) is 1 on the set \(T = \{y_1, ..., y_t\}\) and zero elsewhere (note that since the characteristic is two, we have 1 = \(-1\)). This is also true about the polynomial \(\chi(Y) = \sum_{i=1}^{t}(Y - y_i)^{q-1}\), so since these polynomials have degree at most \(q - 1\), they have to be the same. On the other hand (using that \(a_1 = ... = a_t = 0\)), the \(Y\)-degree of \(R\) and hence also of \(r_{q-1}\) is at most \(q - t\), so using Proposition 9.19 (iii), we are done.

**Exercise 13.10.** Let \(B \subset \text{PG}(2, q)\) be a pointset, \(|B| = q + k\), with every intersection number being 1 mod \(p\) and suppose that \(B \cap \ell_{\infty} = k\). Prove that \(B \setminus \ell_{\infty} \subset \text{AG}(2, q)\), considered as a subset of \(\text{GF}(q)\), is a Vandermonde-set.

We note that much more is true if \(k \leq \frac{q - 1}{2}\); such a set, which is a blocking set of Rédéi type, is always a (translate of a) subspace of \(\text{GF}(q^2)\), considered as a vector space over a suitable subfield (hence an additive subgroup of \(\text{GF}(q^2)\)); see Theorem 18.14.

**Exercise 13.11.** Let \(B \subset \text{PG}(2, q)\) be a pointset, \(|B| = q + k\), with every intersection number being 1 mod \(p\). Let \(\ell_1\) and \(\ell_2\) be two lines such that \(|\ell_1 \cap B| = |\ell_2 \cap B| = k\) and \(B \cap \ell_1 \cap \ell_2 = \emptyset\). W.l.o.g. let \(\ell_1 = [1, 0, 0]\) the \(X\)-axis and \(\ell_2 = [0, 0, 1]\) the line at infinity. Prove that \(\ell_1 \cap B\) and \(\ell_2 \cap B\) are Vandermonde sets!

**Theorem 13.12.** [70] The \(t\)-secants of a \((q + t, t)\)-arc of type \((0, 2, t)\) are concurrent.

**Proof:** Suppose to the contrary that (after transformation) the line at infinity and the two axes are \(t\)-secants.
Let $T = \{(y_1), ..., (y_t)\}$ be the intersection of the arc and the line at infinity. According to Proposition 13.9, $T$ is a Vandermonde-set. On the other hand, the affine transformation switching the two affine coordinates (that is $(u, v) \rightarrow (v, u)$) (which extends to the ideal line as $(y) \rightarrow (1/y)$) interchanges the two axes, while the set $T$ is replaced by $T' = \{1/y_1, ..., 1/y_t\}$ (note that $(0)$ and $(\infty)$ cannot be in $T$). It follows that again by Proposition 13.9, $T'$ is also a Vandermonde set. So we have that $\sum_i y_i^k = 0$ for any $1 \leq k \leq t - 2$ and for any $q - t + 1 \leq k \leq q - 2$.

Now consider the polynomial $\chi(Y) = \sum_{i=1}^t (Y - y_i)^{q-1}$. According to Propositions 13.9 and 9.19, it has degree $q - t$ and it has $q - t$ different roots (the complement of $T$). On the other hand, since $\sum_i y_i^k = 0$ for any $q - t + 1 \leq k \leq q - 2$, it is divisible by $Y^t$, which means that 0 is a root of multiplicity at least $t$. This is a contradiction.

13.2 Small and large super-Vandermonde sets

If in Proposition 9.20(ii) we write $Y^t f(Y^{1/q})$ then we get a polynomial of degree $t$ and its roots are $\{Y^{1/q} : y \in T\}$. Hence a super-Vandermonde set is equivalent to a fully reducible polynomial of form $g^p(Y) + Y^t$, $t > p \cdot \deg g$.

Let’s explore this situation. Firstly, if $q = p$ is a prime then the only possibility is $f(Y) = Y^t + c$, i.e. a transform of the multiplicative group $\{y : y^q = 1\}$, if it exists (so iff $t | q - 1$).

If $f(Y) = q^p(Y) + Y^t$ is a fully reducible polynomial without multiple roots then we can write it as $Y^q - Y = f(Y)h(Y)$. Now we may use the trick I have learnt from Gács: differentiating this equation one gets

$$-1 = tY^{t-1}h(Y) + f(Y)h'(Y).$$

Substituting a root $y_1$ of $f$ we get $h(y_1) = -\frac{1}{t}\frac{1}{y_1^{t-1}} = -\frac{1}{t}y_1^{q-t}$. Suppose that $t > \frac{q}{2}$, then $h(Y) = -\frac{1}{t}Y^{q-t}$ holds for more values than its degree hence it is a polynomial identity implying a contradiction unless $q - t = 1$. As $t = \frac{q}{2}$ is impossible (it would imply $p = 2$ and $f$ would be a power), we have that either $t = q - 1$ (and then $h(Y) = Y$ so $f(Y) = Y^{q-1} - 1$) or $t \leq \frac{q-1}{2}$.

For describing small and large super-Vandermonde sets we need to examine the coefficients of the original equation $Y^q - Y = f(Y)h(Y)$ carefully. What does small and large mean? We know that any additive subgroup of $GF(q)$ forms a Vandermonde set, so removing the zero element from it one gets a super-Vandermonde set. The smallest and largest non-trivial additive subgroups are of cardinality $p$ and $q/p$, respectively. Note that the super-Vandermonde set, derived from an additive subgroup of size $p$, is a transform of a multiplicative subgroup. This motivates that, for our purposes small and large will mean “of size $< p^2$” and “of size $> q/p^2$”, resp.
13. Sets with constant intersection numbers \( \text{mod} \ p \)

**Theorem 13.13.** [120] Suppose that \( T \subset \mathbb{GF}(q) \) is a super-Vandermonde set of size \( |T| < p \). Then \( T \) is a (transform of a) multiplicative subgroup.

**Proof:** Since \( t < p \) the polynomial \( f(Y) \) is of the form \( f(Y) = Y^t - b_0 \). As \( f(Y) \) is a fully reducible polynomial without multiple roots, it implies that \( b_0 \) has precisely \( t \) distinct \( t \)-th roots, \( t|q - 1 \) and \( T \) is a coset of a multiplicative subgroup. \( \blacksquare \)

**Theorem 13.14.** [120] Suppose that \( T \subset \mathbb{GF}(q) \) is a super-Vandermonde set of size \( |T| > q/p \). Then \( T \) is a (transform of a) multiplicative subgroup.

**Proof:** Let us write \( Y^q - Y = f(Y)h(Y) \), where \( f(Y) = Y^t + b_{mp}Y^{mp} + b_{(m-1)p}Y^{mp-1} + \cdots + b_pY^p + b_0 \) and \( h(Y) = Y^{q-t} + a_{q-t}Y^{q-t-1} + \cdots + a_2Y^2 + a_1Y \). Consider the coefficient of \( Y^1, Y^2, \ldots, Y^q \) in this equation. We get

\[
Y^1 = -1 = a_1b_0 \\
Y^j : a_j = 0 \text{ if } 2 \leq j \leq t \text{ and } j \neq 1 \pmod{p} \\
Y^j : a_j = 0 \text{ if } t + 1 \leq j \leq 2t \text{ and } j \neq 1, t + 1 \pmod{p} \\
Y^j : a_j = 0 \text{ if } 2t + 1 \leq j \leq 3t \text{ and } j \neq 1, t + 1, 2t + 1 \pmod{p} \text{ and so on, generally} \\
Y^j : a_j = 0 \text{ if } kt + 1 \leq j \leq (k+1)t \text{ and } j \neq 1, t + 1, \ldots, kt + 1 \pmod{p}.
\]

\[
Y^{p+1} = a_{p+1}b_0 + a_1b_p = 0 \\
Y^{2p+1} = a_{2p+1}b_0 + a_{p+1}b_p + a_1b_{2p} = 0 \\
\text{generally} \\
Y^{kp+1} = a_{kp+1}b_0 + a_{(k-1)p+1}b_p + \cdots + a_{p+1}b_{(k-1)p} + a_1b_{kp} = 0, \text{ for } k = 1, 2, \ldots, m. \\
Y^{t+1} = a_1 + b_0a_{t+1} + b_1a_{t-p+1} + b_2a_{t-2p+1} + \cdots + b_{mp}a_{t-mp+1} = 0
\]

The indices of coefficients \( a \) are of the form \( t - kp + 1 \). Since \( t - kp + 1 < t \) and \( t - kp + 1 \neq 1 \pmod{p} \) (because \( t \neq 0 \pmod{p} \) is true) these coefficients are 0.

So the equation is of the form

\[
Y^{t+1} = a_1 + b_0a_{t+1} = 0. \\
Y^{2t+1} = a_{t+1} + b_0a_{2t+1} + b_1a_{2t-p+1} + \cdots + b_{mp}a_{2t-mp+1} = 0
\]

The indices \( j \) of coefficients \( a_j \) are \( t < j < 2t \). These coefficients are 0 if \( j \neq 1, t + 1 \pmod{p} \). It means \( 2t + 1 \neq 1 \pmod{p} \) so \( 2t \neq 0 \pmod{p} \) which means \( p \neq 2 \). The other condition \( 2t + 1 \neq t + 1 \pmod{p} \) is satisfied by any \( t \). Hence

\[
Y^{2t+1} = a_{t+1} + b_0a_{2t+1} = 0 \text{ if } p \neq 2.
\]

Similarly

\[
Y^{3t+1} = a_{2t+1} + b_0a_{3t+1} + b_1a_{3t-p+1} + \cdots + b_{mp}a_{3t-mp+1} = 0
\]

The indices are between \( 2t \) and \( 3t \) here. The coefficients are 0 if \( 3t + 1 \neq 1, t + 1, 2t + 1 \pmod{p} \). It gives only one new condition: \( 3t + 1 \neq 1 \pmod{p} \) so \( 3t \neq 0 \pmod{p} \) which means \( p \neq 3 \). The two other conditions has occurred earlier: \( p \neq 2 \) and \( t \neq 0 \pmod{p} \).
II. Polynomials in geometry

\[ Y^{3t+1} : a_{2t+1} + b_0a_{3t+1} = 0 \] if \( p \neq 2, 3 \).

Generally
\[ Y^{lt+1} : a_{(l-1)t+1} + b_0a_{lt+1} + b_p a_{lt-p+1} + \ldots + b_{mp} a_{lt-mp+1} = 0, \text{ for } l = 1, 2, \ldots, n-1. \]

The indices are of the form \( t - kp + 1 \) and they are between \((l-1)t\) and \(lt\). Hence the coefficients \( a \) are 0 if \( lt + 1 \neq 1, t + 1, \ldots, (l-1)t+1 \) (mod \( p \)). It gives \((l-1)t\) conditions:
- \( lt + 1 \neq (\text{mod } p) \) so \( p \neq l; \)
- \( lt + 1 \neq t + 1 \) (mod \( p \)) so \( p \neq (l-1); \)
- \( lt + 1 \neq 2t + 1 \) (mod \( p \)) so \( p \neq (l-2); \)

and so on

\[ lt + 1 \neq (l-2)t + 1 \] (mod \( p \)) so \( p \neq 2; \) finally
\[ lt + 1 \neq (l-1)t + 1 \] (mod \( p \)) so \( t \neq 0, \) which is true.

Hence generally we get
\[ Y^{lt+1} : a_{(l-1)t+1} + b_0a_{lt+1} = 0 \] if \( p \neq 1, 2, \ldots, l. \)

In particular, substituting \( l = n - 1 \) into this equation we get
\[ Y^{(n-1)t+1} : a_{(n-2)t+1} + b_0a_{(n-1)t+1} = 0 \] if \( p \neq 1, 2, \ldots, n-1. \)

The greatest index of a coefficient \( a \) can be \( q - t - 1. \)

\((n-1)t < q - 1\) and \( nt \geq q - 1\) because of the definition of \( n. \)

It means that \((n-1)t \geq q - t - 1\) so \((n-1)t + 1 \geq q - t.\)

It implies that \( a_{(n-1)t+1} \) (which occurred in the previous equation) does not exist.

So we have two possibilities:

**Case 1.** \((n-1)t + 1 = q - t, \) so \( t = \frac{q-1}{n} \) and the equation is of the form
\[ Y^{(n-1)t+1} : a_{(n-2)t+1} + b_0 = 0. \] (Hence we can write 1 instead of \( a_{(n-1)t+1}. \))

**Case 2.** \((n-1)t + 1 > q - t, \) so the equation is of the form
\[ Y^{(n-1)t+1} : a_{(n-2)t+1} = 0 \] if \( p \neq 1, 2, \ldots, n-1. \) We will now prove that it leads to a contradiction.

Substituting \( a_{(n-2)t+1} = 0 \) into the equation
\[ Y^{(n-2)t+1} : a_{(n-3)t+1} + b_0a_{(n-2)t+1} = 0, \] we get \( a_{(n-3)t+1} = 0. \)

We can substitute this again into the equation
\[ Y^{(n-3)t+1} : a_{(n-4)t+1} + b_0a_{(n-3)t+1} = 0, \] and we get \( a_{(n-4)t+1} = 0. \)

Substituting this in a decreasing order we get
\[ Y^{t+1} : a_1 + b_0a_{t+1} = 0 \] so \( a_1 = 0. \)

Hence \(-1 = a_1b_0, \) so \( a_1 \neq 0, \) **Case 2** implied a contradiction. It means that **Case 1** will occur, so \( t = \frac{q-1}{n} \) if \( p \neq 1, 2, \ldots, n-1. \) In other words \( t|q - 1 \) if \( p \neq 1, 2, \ldots, n-1. \)

Hereafter, we can write 1 instead of \( a_j \) if \( j = (n-1)t + 1, \) and 0 if \( j > (n-1)t + 1. \)

\[ Y^{(n-1)t+1} : a_{(n-2)t+1} + b_0 = 0 \] so \( a_{(n-2)t+1} = -b_0. \)
13. Sets with constant intersection numbers mod $p$

Substituting this into the equation

$Y^{(n-2)t+1} : a_{(n-3)t+1} + b_0a_{(n-2)t+1} = 0$, we get

$Y^{(n-2)t+1} : a_{(n-3)t+1} + b_0b_0 = 0$ so $a_{(n-3)t+1} = b_0^{-2}$.

Substituting this in a decreasing order we get

$Y^{lt+1} : a_{(l-1)t+1} = (-b_0)^{n-l}$ for $l = n-1, n-2, \ldots, 1$. Finally

$Y^{t+1} : a_1 = (-b_0)^{n-1}$.

Substituting this into $-1 = a_1b_0$, we get $-1 = (-b_0)^{n-1}b_0$ so $1 = (-b_0)^n$.

We are going to examine the equation that belongs to $Y^{lt+kp+1}$. First we write up

$Y^{(n-1)t+p+1} : a_{(n-2)t+p+1} + b_p + b_{2p}a_{(n-1)t+p+1} + \ldots = 0$

We have already seen that the coefficients $a$ occurring in this equation are 0, because these are the same as in the equation of $Y^{(n-1)t+1}$. So

$Y^{(n-1)t+p+1} : a_{(n-2)t+p+1} + b_p = 0$.

Similarly

$Y^{(n-1)t+2p+1} : a_{(n-2)t+2p+1} + b_{2p} = 0$, generally

$Y^{(n-1)t+kp+1} : a_{(n-2)t+kp+1} + b_{kp} = 0$ for $k = 1, 2, \ldots, m$.

On the other hand

$Y^{lt+p+1} : a_{(l-1)t+p+1} + b_0a_{lt+p+1} + b_p a_{lt+1} = 0$, for $l = 1, 2, \ldots, n-1$.

Generally we get

$Y^{lt+kp+1} : a_{(l-1)t+kp+1} + b_0a_{lt+kp+1} + b_p a_{lt+(k-1)p+1} + \ldots + b_{kp} a_{lt+1} = 0$ for $l = 1, 2, \ldots, n-1$ and $k = 1, 2, \ldots, m$.

In particular, if $l = 1$ the equation is of the form

$Y^{t+kp+1} : a_{kp+1} + b_0a_{t+kp+1} + b_p a_{t+(k-1)p+1} + \ldots + b_{kp} a_{t+1} = 0$.

Lemma 13.15. $b_p = b_{2p} = \ldots = b_{mp} = 0$.

Proof: We prove it by mathematical induction.

Step 1. First we prove that $b_p = 0$. Consider the equation

$Y^{(n-2)t+p+1} : a_{(n-3)t+p+1} + b_0a_{(n-2)t+p+1} + b_p a_{(n-2)t+1} = 0$. (1)

We have seen that

$Y^{(n-1)t+p+1} : a_{(n-2)t+p+1} + b_p = 0$ so $a_{(n-2)t+p+1} = -b_p$ and

$Y^{(n-1)t+1} : a_{(n-2)t+1} = -b_0$.

Substituting these into the equation (1), we get

$Y^{(n-2)t+p+1} : a_{(n-3)t+p+1} - b_0b_p - b_0b_p - b_0 = 0$ so $a_{(n-3)t+p+1} = 2b_0b_p$. Generally

we can write

$Y^{lt+p+1} : a_{(l-1)t+p+1} + b_0a_{lt+p+1} + b_p a_{lt+1} = 0$ for $l = n-1, n-2, \ldots, 1$. (2)

Substituting

$Y^{(l+1)t+p+1} : a_{lt+p+1} = (-1)^{n-l-1}(n-l-1)b_0^{n-l-2}b_p$ and
\[ Y^{(l+1)l+1} : a_{l+1} = (-b_0)^{n-l} \text{ into the equation (**)}, \text{ we get} \]
\[ Y^{l+1} : a_{l+1} = (-b_0)^{n-l}(-l)b_0^{n-l}b_p \text{ for } l = n - 1, n - 2, ..., 1. \]
If \( l = 0 \) it means
\[ Y^{p+1} : a_{p+1}b_0 + a_1b_p = 0. \] (***)

Substituting
\[ Y^{l+p+1} : a_{p+1} = (-1)^{n-1}(n-1)b_0^{n-2}b_p \text{ and} \]
\[ Y^{p+1} : a_1 = (-b_0)^{n-1} \text{ into (**)}, \text{ we get} \]
\[ Y^{p+1} : (-1)^{n-1}nb_0^{n-1}b_p = 0. \]

In this equation \(-1 \neq 0 \text{ (mod } p), n \neq 0 \text{ (mod } p) \text{ and } b_0 \neq 0 \text{ (mod } p) \text{ (from the equation } a_1b_0 = -1). \text{ It means that } b_p = 0. \]

**Step 2.** Suppose \( b_p = b_{2p} = ... = b_{(s-1)p} = 0. \) We show that \( b_{sp} = 0. \) Consider
\[ Y^{(n-2)t+sp+1} : a_{(n-3)t+sp+1} + b_0a_{(n-2)t+sp+1} + b_sp a_{(n-2)t+1} = 0. \] (*)&n
We have seen that
\[ Y^{(n-1)t+sp+1} : a_{(n-2)t+sp+1} + b_sp = 0 \text{ so } a_{(n-2)t+sp+1} = -b_sp \text{ and} \]
\[ Y^{(n-1)t+1} : a_{(n-2)t+1} = -b_0. \]

Substituting these into the equation (*), we get
\[ Y^{(n-2)t+sp+1} : a_{(n-3)t+sp+1} - b_0b_sp - b_0b_sp = 0 \text{ so } a_{(n-3)t+sp+1} = 2b_0b_sp. \]
Generally we can write
\[ Y^{lt+sp+1} : a_{lt+sp+1} + b_0a_{lt+sp+1} + b_sp a_{lt+1} = 0 \text{ (**)} \text{ for } l = n - 1, n - 2, ..., 1. \]

Substituting
\[ Y^{(l+1)t+sp+1} : a_{lt+sp+1} = (-1)^{n-l}(n-l-1)b_0^{n-l-2}b_sp \text{ and} \]
\[ Y^{(l+1)t+1} : a_{lt+1} = (-b_0)^{n-l} \text{ into the equation (**)}, \text{ we get} \]
\[ Y^{lt+sp+1} : a_{lt+sp+1} = (-1)^{n-l}(n-l)b_0^{n-l-1}b_sp \text{ for } l = n - 1, n - 2, ..., 1. \]
If \( l = 0 \) it means
\[ Y^{sp+1} : a_{sp+1}b_0 + a_1b_sp = 0. \] (***)

Substituting
\[ Y^{t+sp+1} : a_{sp+1} = (-1)^{n-1}(n-1)b_0^{n-2}b_sp \text{ and} \]
\[ Y^{t+1} : a_1 = (-b_0)^{n-1} \text{ into (***)}, \text{ we get} \]
\[ Y^{sp+1} : (-1)^{n-1}nb_0^{n-1}b_sp = 0. \]

In this equation \(-1 \neq 0 \text{ (mod } p), n \neq 0 \text{ (mod } p) \text{ and } b \neq 0 \text{ (mod } p) \text{ (from the equation } a_1b_0 = -1). \text{ It means that } b_sp = 0. \]

So we have got \( b_p = b_{2p} = ... = b_{mp} = 0. \text{ It means that } f(Y) \text{ is of the form} \]
\[ f(Y) = Y^t + b_0, \text{ and that } t|q - 1 \text{ so } t = \frac{q-1}{n} \text{ and } (-b_0)^n = 1. \text{ Hence} \]
14. Arcs, Segre

A \((k, n)\)-arc in a projective plane is a set of \(k\) points such that each line intersects it in at most \(n\) points. It is \textit{complete} if it cannot be extended to a \((k + 1, n)\)-arc.

Considering \((k, n)\)-arcs, Barlotti [24] showed that for \(1 < n < q + 1\), \(k \leq qn - q + n\) and equality can only hold when \(n\) divides \(q\).

**Exercise 14.1.** Verify Barlotti’s bound. Observe that in case of equality each line intersects the \((k, n)\)-arc in either 0 or \(n\) points and so \(n | q\).

In this section we consider the case \(n = 2\), so simply \(k\)-arcs. Note that, by Exercise 14.1, \((q + 2)\)-arcs exist only if \(q\) is a power of 2. So if \(q\) is odd then arcs are of size \(\leq q + 1\). In some sense Segre’s theory was a starting point of modern Galois geometry.

**Exercise 14.2.** Let the lines \(\ell_1, \ell_2\) and \(\ell_3\) form a triangle in \(\text{PG}(2, q)\). Prove that there exists a set \(\{m_1, ..., m_{q-1}\}\) of lines \((m_i \neq \ell_j)\), covering the non-vertex points of the triangle if and only if \(q\) is even.

The Segre curve is not used in general as a polynomial in three variables, but as an object with general, local or global, algebraic-geometric properties. Strictly speaking it is not obvious why to include the “Segre method” to this book. I decided to treat it here as well because of (i) historical reasons; (ii) it inspired directly or indirectly the outburst of the polynomial methods; (iii) there are results where Segre-like arguments can be used together with other polynomial methods, see e.g. Section 17.

A generalization of the theorem of Menelaos is the following.

Let \(T\) be an arbitrary triangle in \(\text{PG}(2, q)\). The points on the sides of \(T\) may be identified by coordinates as follows. Take \(T\) as fundamental triangle (i.e. the vertices of \(T\) are \(A_1(1, 0, 0), A_2(0, 1, 0)\) and \(A_3(0, 0, 1)\)), and place the unit point \((1, 1, 1)\) arbitrarily (not on a side of \(T\) of course). Points on the side \(A_2A_3\) are of form \((0, 1, c)\), points on the side \(A_3A_1\) are of form \((a, 0, 1)\), and points on the side \(A_1A_2\) are of form \((1, b, 0)\). These coefficients will be called the “coordinates” of the points. Note that these three points are collinear (so they are contained in an algebraic curve of degree \(one\)) precisely when \(abc = -1\).

More generally, we have the following:
Theorem 14.3. A necessary and sufficient condition that $3n$ points, distributed in three $n$-tuples on the three sides of $T$ (some possibly coinciding with each other, but none with any vertex of $T$) are contained in an algebraic curve $C$ of degree $n$, is that the product of their “coordinates” is

$$
\prod_{i=1}^{n} a_i \prod_{i=1}^{n} b_i \prod_{i=1}^{n} c_i = (-1)^n
$$

(*).

If a point $P$ appears $m$ times in an $n$-tuple then we require that at $P$ the intersection multiplicity of $C$ and the corresponding line is precisely $m$. (It also implies that $C$ does not contain any side of the triangle.)

Proof: We are looking for a curve of form

$$
f(X, Y, Z) = \sum_{i+j+k=n} \alpha_{ijk} X^i Y^j Z^k.
$$

Let $\{P_s = (1, b_s, 0) : s = 1, \ldots, n\}$ be the given (multi)set of points on $A_1A_2$. Then $F(X, Y, 0)$ must factor to $d_3(b_1X - Y)(b_2X - Y) \cdots (b_nX - Y)$; similarly $F(0, Y, Z) = d_1(c_1Y - Z)(c_2Y - Z) \cdots (c_nY - Z)$ and $F(X, 0, Z) = d_2(a_1Z - X)(a_2Z - X) \cdots (a_nZ - X)$, where $d_1, d_2$ and $d_3$ are suitable non-zero constants. These equations determine all the coefficients $\alpha_{ij0}, \alpha_{i0k}, \alpha_{0jk}$. In particular, $\alpha_{n00} = d_3b_1b_2 \cdots b_n = d_2(-1)^n$, $\alpha_{0n0} = d_1c_1c_2 \cdots c_n = d_3(-1)^n$ and $\alpha_{00n} = d_2a_1a_2 \cdots a_n = d_1(-1)^n$. The product of these equations gives exactly (*).

On the other hand, if (*) holds, let’s fix one of the constants, say $d_1 = 1$, then $d_2, d_3$ and all the coefficients $\alpha_{ij0}, \alpha_{i0k}, \alpha_{0jk}$ are determined. The remaining coefficients $\alpha_{ijk}, i, j, k \neq 0$ can be chosen arbitrarily.

As it is used frequently, we formulate the dual version of the above, which is then a generalization of the theorem of Ceva.

Let $T$ be an arbitrary triangle in $\text{PG}(2, q)$. The lines through the vertices of $T$ may be identified by coordinates as follows. Take $T$ as fundamental triangle (i.e. the vertices of $T$ are $A_1(1, 0, 0), A_2(0, 1, 0)$ and $A_3(0, 0, 1)$), and place the unit point $(1, 1, 1)$ arbitrarily (not on a side of $T$ of course). Lines through the vertices of $T$ other than the sides will have an equation of the form $X_2 = -bX_3$, $X_3 = -cX_1$ and $X_1 = -aX_2$, with $a, b, c \in \text{GF}(q)^*$. This coefficient will be called the “coordinate” of the line. Note that these three lines, i.e. $[0, 1, b]$, $[c, 0, 1]$ and $[1, a, 0]$ are concurrent (so they are contained in a pencil, i.e. an algebraic envelope of degree one) precisely when $abc = -1$. More generally, we have the following dual version:

Result 14.4. A necessary and sufficient condition that $3n$ lines, distributed in three $n$-tuples through the three vertices of $T$ (some possibly coinciding with each other, but none with any side of $T$) are contained in an algebraic envelope $C$ of degree $n$ containing no side of $T$, is that the product of their “coordinates” is $(-1)^n$. 

\[\text{Ceva: } n = 1\]
We are especially interested in the following extension:

**Result 14.5.** (Segre) Let us consider any number \( k (\geq 3) \) of lines \( L = \{L_1, \ldots, L_k\} \) in \( \text{PG}(2, q) \) no three of which are concurrent (that is a dual \( k \)-arc), and on each line \( L_i \) a set \( G_i \) of \( n \) points, not necessarily distinct, but each on one line of \( L \) only. In order that there exists an algebraic curve \( C \) of degree \( n \), containing each \( G_i \) but not containing any line of \( L \) it is necessary and sufficient that each of the \( \binom{k}{3} \) triplets of sets \( G_i \) satisfies the condition in the previous Result 14.3.

Finally, we remark that if \( k > n \), then the curve \( C \) is unique, for if \( C_\infty \) and \( C \) both satisfy the requirements above, the same holds for any linear combination of them. Now form a linear combination \( C \) that contains an extra point \( P \) on one of the lines \( L_i \). Since \( C \) intersects the line \( L_i \) in too many points it will contain the line \( L_i \) as a factor, and since it introduces more intersections with the other lines as well, all lines of \( L \) will factor into \( C \) but \( C \) only has degree \( n \) and \( k > n \).

Let us also underline that the curve does not contain any point which is on two lines of the dual \( k \)-arc \( A \).

The most general form of this theorem we are aware of is the following.

**Result 14.6.** [134] Let us consider any number \( k (\geq 3) \) of lines \( L = \{L_1, \ldots, L_k\} \) in \( \text{PG}(2, q) \), and on each line \( L_i \) a set \( G_i \) of \( n \) points, not necessarily distinct, but each on one line of \( L \) only. Suppose that for each \( J \subseteq \{1, 2, \ldots, k\} \) of the following type there is a curve \( C_J \) of degree \( n \) intersecting the lines \( L_j : j \in J \) at the given points \( G_j \) with the required multiplicities:

(a) \( \{L_j : j \in J\} \) is a triangle;
(b) \( \{L_j : j \in J\} \) are all concurrent.

Then there exists an algebraic curve \( C \) of degree \( n \), intersecting each \( L_i \) in the given points \( G_i \) with the required multiplicities. In this case, if \( k > n \) then the curve \( C \) is unique.

**Exercise 14.7.** Prove unicity, so the last sentence of the result.

Note that the result does not hold any more if we require (b) for a bounded number of concurrent lines of \( L \) only. But if the hypothesis holds for any \( t \) concurrent lines of \( L \), \( t \leq n + 2 \), then it holds in general.

Note also that if we know that a curve \( C \) of degree \( n \) contains some points \( P_s = (a_s, b_s, c_s), s = 1, 2, \ldots \) then each \( f(a_s, b_s, c_s) = 0 \) gives a homogeneous linear equation for the coefficients \( \alpha_{ijk}, i + j + k = n \). If the curve is unique then the system of equations has a unique solution (in the projective sense, so up to a constant multiplier). The matrix of the system of linear equations contains entries like \( a_i^k b_i^l c_i^m \).

There are many applications of the results of this section. See Section 17 on sets without tangents, Section 16 on unitals, etc.

We begin with an easy application of Ceva’s theorem.
II. Polynomials in geometry

Proposition 14.8. (Bichara, Korchmáros) Let \( K \subseteq \text{PG}(2, q) \) be a set of \( q+2 \) points, and suppose that \( A_1, A_2, A_3 \in K \) are such that any line meeting \( \{A_1, A_2, A_3\} \) intersects \( K \) in exactly two points. Then \( q \) is even.

Proof: Choose \( A_1, A_2, A_3 \) as the base points of a coordinate frame. Construct a \((q-1) \times 3\)-as matrix \( M \), whose rows are indexed by \( K \setminus \{A_0, A_1, A_2\} \), whose columns are indexed by \( A_0, A_1, A_2 \). The element of \( M \) determined by \((P, A_i)\) will be the coordinate \( \lambda_i(P) \) of the line \( PA_i \). Ceva’s theorem gives that the product of the three elements in one row of \( M \) will be 1. Therefore the product of all elements of \( M \) will also be 1. On the other hand, in each column there are \( q-1 \) pairwise different nonzero element of \( \text{GF}(q) \). This means that in every column we see each nonzero element of \( \text{GF}(q) \). By Wilson’s theorem their product is \((-1)\), whence \( 1 = (-1)^3 \) follows. This implies that \( q \) is even.

Of course the most celebrated application is Segre’s theorem on arcs.

Theorem 14.9. Let \( S \subseteq \text{PG}(2, q) \) be a \((q+1)\)-arc, i.e. a set of \( q+1 \) points, no three of them being collinear. If \( q \) is odd then \( S \) is a conic.

Proof: ([23]) Suppose w.l.o.g. that \( S \) contains the points \((1,0,0), (0,1,0) \) and \((0,0,1) \). Let the tangents at these points be \( Z = cY, X = aZ \) and \( Y = bX \), respectively. Let \( \{S_i \mid i = 1, 2, \ldots, q-2\} \) be the other \( q-2 \) points of \( S \).

Let \((1, b_i, 0)\) be the point that is the intersection of the line \((0,0,1), S_i \) with the line \( Z = 0 \). Let \((0, 1, c_i) \) be the point that is the intersection of the line \((0,0,1), S_i \) with the line \( X = 0 \) and let \((a_i, 0, 1) \) be the point that is the intersection of the line \((0,1,0), S_i \) with the line \( Y = 0 \). Since \( S \) is an oval, the set

\[ \{a_i \mid i = 1, 2, \ldots, q-2\} \cup \{a\} \]

contains every non-zero element of \( \text{GF}(q) \) and similarly for the \( b_i \)'s and the \( c_i \)'s.

The lines \( Y = b_iX, X = a_iZ \) and \( Z = c_iY \) have a point in common (namely \( S_i \)), hence \( a_ib_ic_i = 1 \).

The product of all the non-zero elements of \( \text{GF}(q) \) is \(-1\). Therefore

\[ -1 = \left( \prod_{i=1}^{q-2} a_i \right) a = \left( \prod_{i=1}^{q-2} b_i \right) b = \left( \prod_{i=1}^{q-2} c_i \right) c, \]

\[ \left( \prod_{i=1}^{q-2} a_ib_ic_i \right) abc = -1 \]

hence \( abc = -1 \).

Note that if \(-1 = 1\), so when \( q \) is even then we got a(n algebraic) proof for the (combinatorial) fact, that the tangents of a \((q+1)\)-arc are concurrent (and so their
intersection point, called the nucleus, can be added to the arc, which results in a 
(q + 2)-arc or hyperoval).

Let \( f(X, Y, Z) := -cXY + acYZ + XZ \). The conic defined from \( f = 0 \) contains
the points \((1, 0, 0), (0, 1, 0)\) and \((0, 0, 1)\) and it follows from the fact that
\( abc = -1 \) that it has tangents \( Y = cX, X = bZ \) and \( Z = aY \) at these points.

We have to show that \( f \) (the conic defined by \( f \)) contains another arbitrary point
\( S \) of \( S \) and then we have finished. Let \( \{P, Q, R\} = \{(1, 0, 0), (0, 1, 0), (0, 0, 1)\} \). Let \( f_1 \)
be the quadratic form that defines the conic \( f_1 = 0 \) that contains the points \( P, Q \) and \( S \) and
whose tangents coincide with the tangents of \( S \) at those points. In the same way define \( f_2 \) for the points
\( P, R \) and \( S \).

Let \( t_P \) be the tangent at the point \( P \). The forms \( f, f_1 \) and \( f_2 \) modulo \( t_P \) have a
double zero at \( P \), so we can multiply by a scalar so that the three forms coincide
at all the points of \( t_P \). The forms \( f_1 \) and \( f_2 \) modulo \( t_S \) share a double point at
\( S \) and coincide at \( t_S \cap t_P \), so they coincide at all the points of \( t_S \). In the same way
the forms \( f \) and \( f_1 \) coincide at all the points of \( t_Q \) and the forms \( f \) and \( f_2 \) coincide
at all the points of \( t_R \). But then \( f_1 \) and \( f_2 \) also coincide at \( t_Q \cap t_R \). So in all \( f_1 \)
and \( f_2 \) also coincide on two lines and point not on these lines. Hence the quadratic
form \( f_1 - f_2 \) is zeros on two lines and another point and is therefore identically
zero. So \( f_1 = f_2 \) and in the same way \( f = f_1 = f_2 \). Hence the conic defined by the
equation \( f = 0 \) contains \( S \). \[\]

15 Maximal arcs

After Barlotti’s bound (Exercise 14.1), \((k, n)\) arcs of size \( k = qn - q + n \) are
called maximal. In the Desarguesian projective plane of order \( q \), Denniston [59]
constructed maximal arcs for every divisor of \( q \), when \( q \) is even. Ball, Blokhuis and
Mazzocca [13] proved that for \( q \) odd, there is no maximal arc, see Theorem 15.12.
Their proof was simplified in Ball-Blokhuis [14] and then generalized in [15], as we
have seen in Theorem 13.6.

15.1 Existence: hyperovals

Here we give some information about the case \( n = 2 \) (hence \( q = 2^h \)), i.e. about
hyperovals. For other even values of \( n \), Denniston, Thas and Mathon constructed examples.

Consider a hyperoval \( H_f \) of \( PG(2, q) \), with oval polynomial \( f(X) \), i.e. \( H_f = \{\end{equation}
\( \{(1, 0, 0), (0, 1, 0)\} \cup \{(x, f(x), 1) : x \in GF(q)\} \); we require \( f(0) = 0, f(1) = 1 \).

Exercise 15.1. \( H_f \) is a hyperoval if and only if \( f(X) \) is a permutation polynomial
and \( F_s(X) = \frac{f(X + s) - f(s)}{X} \) is a permutation polynomial for all \( s \in GF(q) \), with
\[N.B.: \]
\( F_s(0) = f'(s) \)
Prove that an oval polynomial is of form
\[ f(X) = a_2 X^2 + a_4 X^4 + \ldots + a_{q-2} X^{q-2}. \]

Exercise 15.2. Prove that an oval polynomial is of form

\[ f(X) = X^r \]

for some \( r \). (Payne, Hirschfeld)

**Exercise 15.3.** \( f(X) = X^r \) is an oval polynomial if and only if \( (r, q-1) = 1 \), \( (r-1, q-1) = 1 \) and \( f(\lambda X) = \lambda f(X) \) is a permutation polynomial.

**Exercise 15.4.** In particular, \( f(X) = X^{2^k} \) is an oval polynomial of \( \text{PG}(2, 2^k) \) if and only if \( (k, h) = 1 \).

It may happen that the graph of \( f \) has the property that the group of translations of \( \text{AG}(2, q) \) acts transitively on it, i.e. for any \( c \in \text{GF}(q) \), \( f(X) + f(c) = f(X + c) \). In this case \( H_f \) is called a translation oval. Then, from Exercise 15.1 we have that \( H_f \) is a translation oval if and only if \( f(X) \) is an additive permutation polynomial, and also \( f(X)/X \) is a permutation polynomial.

Recall Theorem 5.25, saying that every additive function \( \text{GF}(q) \rightarrow \text{GF}(q) \) is a linearized polynomial \( a_0 X + a_1 X^p + a_2 X^{p^2} + \ldots + a_{h-1} X^{p^{h-1}} \). See also Exercise 5.26.

**Exercise 15.5.** The map \( f(X) = \sum_{i=0}^{h-1} a_i X^{p^i} \) is an additive permutation of \( \text{GF}(q) \) such that \( f(X)/X \) is also a permutation, if and only if for the Segre-Bartocci-like matrix

\[
A(\lambda) = \begin{pmatrix}
\lambda & a_1 & \ldots & a_{h-1} \\
ap_1 & \lambda^p & \ldots & a_{h-1}^p \\
ap_2 & \lambda^{p^2} & \ldots & a_{h-2}^p \\
\vdots & \vdots & \ddots & \vdots \\
ap_{h-1} & \lambda^{p^{h-1}} & \ldots & \lambda^{p^{h-1}}
\end{pmatrix}
\]

is additive.

**Proposition 15.6.** (Payne, Hirschfeld) The oval polynomial of a translation oval is of form \( f(X) = X^{2^k} \) (and \( (k, h) = 1 \) of course).

**Proof:** [97] We know that the oval polynomial (being additive) is of the form \( f(X) = a_2 X^2 + a_4 X^4 + a_8 X^8 + \ldots + a_{q/2} X^{q/2} \) and, by Exercise 15.1 now \( f(X)/X \) is a permutation polynomial. We have to prove that only one \( a_i \) can be nonzero.

In Exercise 15.5 \( \deg_A(A(\lambda)) = 2^h - 1 \). It is easy to see that the coefficient of \( \lambda^t, 0 < t < 2^h - 1 \) can be calculated as follows. Let \( t = \sum_{i=1}^{h} t_i 2^{i-1}, t_i \in \{0, 1\} \); and let \( t_{j_1}, \ldots, t_{j_r} \) be precisely the binary digits of \( t \) being equal to zero. Let \( M_{i} \) be the \( r \times r \) principal minor of \( A(\lambda) \) obtained by selecting the rows and columns of indices \( j_1, \ldots, j_r \) and then substituting \( \lambda = 0 \). Then \( \det M_i \) is the coefficient of \( \lambda^t \).
15. Maximal arcs

Hence we need that each $k \times k$ principal minor of $A = \begin{pmatrix} 0 & a_1 & \ldots & a_{h-1} \\ a_{h-1}^p & 0 & \ldots & a_{h-2}^p \\ a_{h-2}^p & a_{h-1}^p & \ldots & a_{h-3}^p \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{p^{h-1}} & a_2^{p^{h-1}} & \ldots & 0 \end{pmatrix}$, $0 < k < 2^{h-1} - 1$ is singular.
Now for $2 \leq k < h$ let $\{i_1, \ldots, i_k\} \subset \{1, \ldots, h\}$. By induction on $k$ one can prove that $a_{i_2-i_1} \cdot a_{i_3-i_2} \cdots a_{i_k-i_{k-1}} \cdot a_{i_1-i_k} = 0$, where the indices are modulo $h$.

The coefficient of $\lambda^0$ is clearly $\det A = 1$. Expanding $\det A$ and using the observation of the previous paragraph on cyclic product, we see that at most (hence precisely) one $a_i$ is nonzero.

Exercise 15.7. If $1 < r, r_1, r_2, r_3 < q - 1$, $rr_1 \equiv 1 \pmod{q - 1}$, $(r-1)(r_2-1) \equiv 1 \pmod{q - 1}$, $r + r_3 \equiv 1 \pmod{q - 1}$, then the hyperovals $H_{X^r}$, $H_{X^{r_1}}$, $H_{X^{r_2}}$ and $H_{X^{r_3}}$ are projectively equivalent.

Exercise 15.8. $H_{X^r}$ is regular (conic + nucleus) iff $r = 2, q/2$ or $q - 2$.

We remark that in $\text{PG}(2, 2^h)$ non-regular hyperovals exist iff $h \geq 4$. As for $h = 5$ and for $h \geq 7$ there exist translation hyperovals; for $n = 4$ Lunelli and Sce found $H_f$ with

$$f(X) = (a^2X^7 + e^7X^6 + e^3X^5 + e^13X^4 + e^3X^3 + e^7X^2 + eX)^2,$$

finally for $h = 6$ we have

$$f(X) = X^{62} + X^{30} + X^{24} + e^{21}(X^{60} + X^{58} + X^{54} + X^{52} + X^{46} + X^{44} + X^{40} + X^{38} + X^{34} + X^{16} + X^{14} + X^{10} + X^8 + X^4) + e^{42}(X^{50} + X^{48} + X^{36} + X^{32} + X^{26} + X^{20} + X^{18} + X^{12} + X^6),$$

where $e^4 = e + 1$.

For $h = 1, 2, 3$ it is easy to check that every hyperoval is regular.

Proposition 15.9. Segre In $\text{PG}(2, 2^h)$ $f(X) = X^6$ is an oval polynomial iff $h$ is odd.

**Proof:** By Exercise 15.3 we have to check whether $\frac{(X+1)^{q^2+1} - X^5}{X} = X^5 + X^3 + X$ is bijective in the case when $h$ is odd. Suppose that for $s \neq t$ $s^5 + s^3 + s = t^5 + t^3 + t$, from this, dividing out by $(s + t)$ and introducing $u = s^2 + t^2, v = st$ we get the quadratic $u^2 + u(v+1) + v^2 + v + 1 = 0$. Dividing by $(v+1)^2$ and introducing $w = \frac{u}{v+1}$ we get $(w + \frac{1}{v+1})^2 + (w + \frac{1}{v+1}) + 1 = 0$. By Exercise 5.6 there is no solution of $Y^2 + Y + 1$ if $\text{Tr}_{2^h-2}(1) = h = 1$, so when $h$ is odd.
We demonstrate the strength of using the Rédei polynomial together with the generalised Newton formulae (NG) from Section 9.4 by giving a short proof for a theorem of Glynn.

It is easy to see that a set of \( q + 2 \) points is a hyperoval if and only if every line meets it in an even number of points. (Through a point of the set in question every line contains at least one more point, but \( 1 + (q + 1) \cdot 1 = q + 2 \), so every line has to meet it in 0 or 2 points.) For even more on even sets (sets of even type) see e.g. Section 23.4. Glynn gave an equivalent description of oval polynomials as follows.

**Theorem 15.10. (Glynn)** A polynomial \( f(x) \) is an oval polynomial if and only if \( \sum_{l=k+1}^{q} x^l f(x)^l = 0 \) for every \( 1 \leq k + l \leq q - 1 \), \( k + l \) odd, \( \{k,l\} \neq \{0,q-1\} \), and \( \sum_{f(x)^q} = 1 \).

**Proof:** (Gács) First suppose \( H = \{(t, f(t)) : t \in \mathbb{F}_q\} \) is a hyperoval in \( PG(2,q) \) and let \( U = \{(t, f(t)) : t \in \mathbb{F}_q\} \) be its affine part. Consider the affine Rédei polynomial

\[
R(X, Y) = \prod_{t \in \mathbb{F}_q} X + tY - f(t) = \sum_{i=0}^{q} r_i(Y) X^{q-i}
\]

of \( U \). \( H \) is a hyperoval precisely if every line meets it in an even number of points.

For lines with direction \( y \neq 0 \) this is equivalent to the condition that \( R(X, y) \) is a square. Since \( q \) is even, \( \deg(r_j) \leq j \), this is equivalent to \( r_j(Y) = 0 \) identically for all \( 1 \leq j \leq q - 3 \), \( j \) odd, and \( r_{q-1}(Y) = Y^{q-1} - 1 \) (since \( R(X,0) = X^q - X \)).

Considering the coefficients of the \( r_j \)'s, we get \( \sigma_{k,l} = 0 \) for all \( 1 \leq k + l \leq q - 1 \), \( k+l \) odd, except for \( k = q - 1 \) or \( l = q - 1 \), when it is \(-1\) (note that since the characteristic is 2, we have \(-1 = 1\)). This implies \( (k + l)\sigma_{k,l} = 0 \) for all \( k \) and \( l \), except for \( \sigma_{0,q-1} = \sigma_{q-1,0} = 1 \).

From this, by induction on \( k + l \) and using (NG), we get the desired condition.

On the other hand, suppose \( f(x) \) is a polynomial satisfying our conditions and let \( H = \{(t, f(t)) : t \in \mathbb{F}_q\} \).

Again induction on \( k + l \) and (NG) give that \( \sigma_{k,l} = 0 \) for all \( 1 \leq k + l \leq q - 1 \), \( k+l \) odd, except for \( k = q - 1 \) or \( l = q - 1 \), when it is \(-1\). This implies that for any fixed \( y \neq 0 \), \( R(X, y) \) is a square, so all lines with slope not in \( \{0, \infty\} \) meet \( H \) in an even number of points. This is also true about vertical lines, since \( f \) is a polynomial and \( (\infty) \) is in \( H \), so what is left is to show that horizontal lines meet \( H \) in one affine point, i.e. \( f \) is bijective.

Note that the bijectivity of \( f \) is equivalent to \( R(X,0) = \prod(X + f(t)) = X^q + X \). Now \( R(X,0) = X^q + \sigma_0 X^{q-1} + \ldots + \sigma_{q-1} = X^q + X + g(X)^2 \) (since \( \sigma_{0,k} = 0 \) for odd \( k \), except for \( k = q - 1 \), when it is 1). But \( H'(X,0) = 1 \), so \( R(X,0) \) cannot have a multiple root, i.e. \( R(X,0) = X^q - X \).
Denniston-arcs

Still in $\text{GF}(q)$, $q = 2^h$, choose $\beta$ which makes $T^2 + \beta T + 1$ an irreducible polynomial. Consider the quadratic curves

$$F_\lambda(X, Y, Z) = X^2 + \beta XY + Y^2 + \lambda Z^2, \quad \lambda \in \text{GF}(q).$$

For $\lambda = 0$ it defines the point $(0, 0, 1)$ only, while for other values these are irreducible conics contained in $\text{AG}(2, q)$. The nucleus of each $F_\lambda$ ($\lambda \neq 0$) is $(0, 0, 1)$.

As the additive group of $\text{GF}(q)$ is elementary abelian, it has subgroups of every size $2^k$, $0 \leq k \leq h$.

**Exercise 15.11.** (Denniston [59]) Let $H$ be a multiplicative subgroup of $\text{GF}(q)$ of size $n = 2^k$, $0 \leq k \leq h$. Define

$$S_H = \bigcup_{\lambda \in H} \{ \text{the points of } F_\lambda \}.$$

Prove that $S_H$ is a $(qn - q + n, n)$-arc (so a maximal arc).

### 15.2 Non-existence

We saw in Section 13.1 a more general statement and its proof. Here we show the proof by Ball and Blokhuis from [14] of the following result:

**Theorem 15.12.** Ball, Blokhuis, Mazzocca [13] In $\text{PG}(2, q)$, with $q$ odd and $n < q$, maximal $(k, n)$-arcs do not exist.

First we can assume that $\mathcal{B}$ is a maximal $(k, n)$-arc contained in $\text{AG}(2, q)$ (external lines always exist if $n < q$), with $|\mathcal{B}| = k = (n - 1)q + n$. As usual, we represent $\text{AG}(2, q)$ by $\text{GF}(q^2)$ so $\mathcal{B} \subset \text{GF}(q^2)$.

For simplicity assume that $0 \not\in \mathcal{B}$ and let $\mathcal{B}^{-1} = \{b^{-1} : b \in \mathcal{B}\}$. Define the polynomial

$$B(T) = \prod_{b \in \mathcal{B}} (1 - bT) = \sum_{i=0}^{\infty} (-1)^i \sigma_i T^i,$$

where $\sigma_i$ is the $i$-th elementary symmetric polynomial of the set $\mathcal{B}$, so $\sigma_i = 0$ if $i > k$. Also define the polynomial

$$F(S, T) = \prod_{b \in \mathcal{B}} (1 - (1 - bT)^{q-1} S) = \sum_{i=0}^{\infty} (-1)^i \hat{\sigma}_i S^i,$$

where $\hat{\sigma}_i$ is the $i$-th elementary symmetric polynomial of the set of polynomials $\{(1 - bT)^{q-1} : b \in \mathcal{B}\}$, so $\deg T \hat{\sigma}_i \leq i(q - 1)$. 

Lemma 15.13. (i) If \( t_0 \in \text{GF}(q^2) \setminus B^{[-1]} \), then \( F(S, t_0) \) is an \( n \)-th power.
(ii) If \( t_0 \in B^{[-1]} \), then \( F(S, t_0) = (1 - S^{q+1})^{n-1} \).

Proof: (i) When \( t_0 = 0 \), the polynomial \( f(s, 0) = \prod_{b \in B} (1 - S) = (1 - S)^k \) and \( n|k \).
When \( t_0 \neq 0 \), then \( t_0^{-1} \) is a point not contained in the arc, whence every line through \( t_0^{-1} \) contains a number of points of \( B \) that is either 0 or \( n \). In the multiset \( \{(t_0^{-1} - b)^{q-1} : b \in B\} \), every element therefore occurs with multiplicity \( n \), so that in \( F(S, t_0) \) every factor occurs exactly \( n \) times.
(ii) Every line passing through the point \( t_0^{-1} \) contains exactly \( n - 1 \) other points of \( B \); hence the multiset \( \{(t_0^{-1} - b)^{q-1} : b \in B\} \) consists of every \( (q + 1) \)-st root of unity repeated \( n - 1 \) times, together with the element 0. This gives

\[
F(S, t_0) = \prod_{b \in B} (1 - (t_0^{-1} - b)^{q-1}) = (1 - t_0^{q-1} S^{q+1})^{n-1} = (1 - S^{q+1})^{n-1}.
\]

Corollary 15.14. (i) The functions \( \hat{\sigma}_i \) are identically zero for \( 0 < i < q \) unless \( n|i \).
(ii) The polynomial \( B \) divides \( \hat{\sigma}_n \), which is not identically zero; the degree of \( \hat{\sigma}_n/B \) is at most \( q - 2n \).

Proof: From the form of \( F \) in both cases of the lemma, it follows that \( \hat{\sigma}_i(t_0) = 0 \) for all \( t_0 \in \text{GF}(q^2) \) with \( 0 < i < q \) unless \( n|i \); since the degree of \( \hat{\sigma}_i \) is at most \( i(q - 1) < q^2 \), these functions are identically zero. Therefore the first coefficient of \( F \) that is not necessarily identically zero is \( \hat{\sigma}_n \).
It is immediate that \( \hat{\sigma}_n(0) = \binom{k}{n} \). With \( q = p^h \), \( n = p^e \),

\[
k = (n - 1)q + n = (p - 1)p^{h+e-1} + \ldots + (p - 1)p^h + p^e;
\]
hence by Lucas’ theorem \( \binom{k}{n} \equiv 1 \pmod{p} \), so is not identically zero. On the other hand, the coefficient of \( S^n \) in \( (1 - S^{q+1})^{n-1} \) is zero; so \( \hat{\sigma}_n(t_0) = 0 \) for \( t_0 \in B^{[-1]} \). Equivalently, \( B \) divides \( \hat{\sigma}_n \). Hence the degree of \( \hat{\sigma}_n/B \) is at most \( n(q - 1) - nq + q - n = q - 2n \).}

Corollary 15.15.

(i) \( F(S, T) = 1 + \sum_{i=1}^{k} (-1)^i \hat{\sigma}_{i, n} S^i + \sum_{i=1}^{k} (-1)^i \hat{\sigma}_{i(q+1)} S^{i(q+1)} \pmod{T - T^{q^2}} \).

(ii) \( BF(S, T) = B + B \sum_{i=1}^{k} (-1)^i \hat{\sigma}_{i, n} S^i \pmod{T - T^{q^2}} \).
Proof: By the previous corollary, the first coefficient of $F$ that is not necessarily identically zero is $\hat{\sigma}_n$. Since, for all $t_0 \in \text{GF}(q^2)$, the function $\hat{\sigma}_j$ vanishes unless $n|j$ or $(q+1)|j$, it follows that $T - T^q | \hat{\sigma}_j$. If $n$ does not divide $j$, then $\hat{\sigma}_j$ still vanishes for $t_0 \in \text{GF}(q^2) \setminus B[1]$, and since $B|\hat{\sigma}_n$, the divisibility relation $T - T^q | \hat{\sigma}_n \hat{\sigma}_j$ follows.

Proof of Theorem 15.12: We shall show that $\hat{\sigma}_n^2$ is a $p$-th power. This, together with (a) $B|\hat{\sigma}_n$ and (b) $\hat{\sigma}_n$ is not identically zero, leads to a contradiction for $p \neq 2$. Calculating the derivative of $B(T)$ gives

$$B'(T) = \sum_{b \in B} \frac{-b}{1 - bT} B(T) = -\left(\sum_{b \in B} \sum_{i=0}^{\infty} b^{i+1} T^i\right) B(T).$$

Since $b^{q^2} = b$, it follows that

$$(T - T^{q^2}) \left(\sum_{b \in B} \sum_{i=0}^{\infty} b^{i+1} T^i\right) = \sum_{b \in B} \sum_{i=0}^{q^2-1} b^i T^i = \sum_{b \in B} (1 - bT)^{q^2-1}.$$

Now, $-\sum_{b \in B} (1 - bT)^{q^2-1}$ takes the value 1 for $T = t_0 \in B[1]$ and is zero for all other elements of $\text{GF}(q^2)$. Since $\hat{\sigma}_{q+1}$ takes the same values and they are both of degree $q^2 - 1$ it follows that $\hat{\sigma}_{q+1} = -\sum_{b \in B} (1 - bT)^{q^2-1}$. This gives

$$(T - T^{q^2}) B' = \hat{\sigma}_{q+1} B.$$

Differentiating it and multiplying by $B$ gives that

$$BB' \equiv B^2 \hat{\sigma}_{q+1}' \pmod{T - T^{q^2}}.$$

However, differentiating $F(S, T)$ with respect to $T$, it follows that

$$\partial_T F(S, T) = \left(\sum_{b \in B} \frac{-b(1 - bT)^{q-2} S}{1 - (1 - bT)^{q-1} S}\right) F(S, T) = \sum_{i=0}^{k} (-1)^i \hat{\sigma}' S^i.$$

Multiplying this by $(1 - S^{q+1})$ and putting $T = t_0 \in \text{GF}(q^2)$, the expression in brackets becomes a polynomial in $S$. Hence

$$F(S, t_0)(1 - S^{q+1}) \partial_T F(S, t_0).$$

Define the quotient of this division to be $R_{t_0}(S)$. It follows that

$$R_{t_0}(S) = -\hat{\sigma}'(t_0) S^n + \hat{R}_{t_0}(S) S^{2n} + \hat{\sigma}'_{q+1}(t_0) S^{q+1},$$
where $\hat{R}_{t_0}(S)$ is an $n$-th power (considered as a function of $S$). Abusing notation we define the polynomial $R(S, T)$ with the property that for $t_0 \in \text{GF}(q^2)$ $R(S, t_0) = R_{t_0}(S)$. Then we have that

$$FR = (1 - S^{q+1}) \partial_T F \pmod{T - T^{q^2}}.$$ 

Multiplying it by $B$, 

$$\left(\sum_{i=1}^{q-q/n+1} (-1)^i B\sigma_n S^{in}\right) R \equiv (1 - S^{q+1}) B\partial_T F \pmod{T - T^{q^2}}. \quad (*)$$

Equating the coefficients of $S^{q+1+n}$ we get 

$$-\hat{\sigma}'_{q+1+n} B + B\hat{\sigma}'_n = -\hat{\sigma}'_{q+1} B\hat{\sigma}_n = -B'\hat{\sigma}_n \pmod{T - T^{q^2}}.$$ 

Hence 

$$B\hat{\sigma}'_{q+1+n} = (B\hat{\sigma}_n)' \pmod{T - T^{q^2}}.$$ 

Equating successively the coefficients of $S^{i(q+1)+n}$ in $(*)$ for $1 < i < n - 1$ gives 

$$B\hat{\sigma}'_{i(q+1)+n} = B\hat{\sigma}'_{(i-1)(q+1)+n} = (B\hat{\sigma}_n)' \pmod{T - T^{q^2}}.$$ 

This implies that $Bp^{-1}$ divides $\hat{\sigma}_n$, which gives a contradiction for $p \neq 2$, since the degree of $\hat{\sigma}_n$ is at most $n(q - 1)$ and it is not identically zero.

### 15.3 Embeddability

There are several improvements on Barlotti’s bound, when $n$ is not a divisor of $q$. Lunelli and Sce [94] showed that $k \leq (n - 1)q + n - 3$ and if $q$ is large enough compared to $n$, then $k \leq (n - 1)q + 8n/13$.

Let $\mathcal{K}$ be an arbitrary $(qn - q + n - \varepsilon, n)$-arc in $\text{PG}(2, q)$. When $n$ divides $q$, a natural question is whether $\mathcal{K}$ is incomplete if $\varepsilon$ is small enough, that is whether it can be completed to a maximal arc. For $\varepsilon = 1$, this was shown by Thas [132]. Ball, Blokhuis [12] showed it for $\varepsilon < n/2$ when $q/n > 3$, for $\varepsilon < 0.476n$ when $n = q/3$ and for $\varepsilon < 0.381n$ when $n = q/2$. This result was improved by Hadnagy and Szőnyi [73], namely they proved it for $\varepsilon \leq 2n/3$, if $q/n$ is large enough.

When $n = 2$, $(k, n)$-arcs are simply called $k$-arcs and maximal arcs (of size $k = q + 2$) are called hyperovals. In this case Segre [106] showed that a $(q + 2 - \varepsilon)$-arc, $\varepsilon \leq \sqrt{q}$, can be extended to a hyperoval. When $4 < q$ is a square, this result is sharp, since there are complete $(q + 1 - \sqrt{q})$-arcs, see Boros and Szőnyi [48], Fisher, Hirschfeld and Thas [63] and Kestenband [85]. The only known example of $(q + 1 - \sqrt{q})$-arcs comes from the cyclic representation of the plane: observe that...
Maximal arcs

\[ q^2 + q + 1 = (q + \sqrt{q} + 1)(q - \sqrt{q} + 1) \] and take every \((q + \sqrt{q} + 1)\)-th point in the Singer-cycle (i.e. a point orbit of a subgroup of size \((q - \sqrt{q} + 1)\) in the cyclic representation), it takes some calculations to prove that they form a complete arc.

It is nice to remark that if you take every \((q - \sqrt{q} + 1)\)-th point instead then you get the \((q + \sqrt{q} + 1)\) points of a Baer subplane \(\text{PG}(2, \sqrt{q})\).

Note that these examples exist for odd square \(q\)-s as well, and it is conjectured that also in the odd case they are the second largest complete arcs, however the best known bound is \(q - \frac{1}{2}\sqrt{q} + 5\) by Hirschfeld and Korchmáros. (For a more detailed description of the known results see e.g. [82].) We remark that Hirschfeld and Korchmáros were also able to prove the stability of the second largest complete arc in the even square case:

**Result 15.16.** [80] A complete arc of \(\text{PG}(2, q)\), \(q = 2^{2e}, e \geq 3\) has size either \(q + 2\), or \(q - \sqrt{q} + 1\), or at most \(q - 2\sqrt{q} + 6\).

The proofs of the Segre or the Hirschfeld-Korchmáros theorems are based on the profound examination of the properties of an algebraic curve associated to the arc.

**Theorem 15.17.** (Weiner) Assume that \(K\) is a \((qp^e - q + p^e - e, p^e)\)-arc in \(\text{PG}(2, q)\), \(q = ph\), \(p\) prime. Suppose also that \(e \leq \sqrt{q}/4\) and \(p^e < \sqrt{q}\). Then \(K\) can be embedded in a maximal arc.

After some hesitation we omit its (nice but lengthy) proof. For \(e = 1\) see Szőnyi [125], his method was improved by Weiner, who proved it for general \(e\) in [137].

For large \(n = p\), the results of Ball-Blokhuis and Hadnagy-Szőnyi turn out to be better, while for small \(p\) Theorem 15.17 is stronger. This and Theorem 15.12 of Ball, Blokhuis and Mazzocca on the non-existence of maximal arcs for \(p > 2\), yield an upper bound on the size of a \((k, p^e)\)-arc.

The following result and proof by Weiner contains some of the key ideas of the proof of Theorem 15.17; it is similar to Segre's idea as it associates an(al other) algebraic curve (envelope) to the arc. The advantage is that this proof seems to be easier and there is a nice way to generalize it to \((k, p^e)\)-arcs of \(\text{PG}(2, q)\) to get Theorem 15.17. We will use Theorem 9.37.

**Theorem 15.18.** Any arc in \(\text{PG}(2, q)\), \(q\) even, of size greater than \(q - \sqrt{q} + 1\) can be embedded in a hyperoval.

**Proof:** ([137]) Assume to the contrary, that \(K\) is not a hyperoval, hence \(|K| = q + 2 - \varepsilon\), where \(1 \leq \varepsilon \leq \sqrt{q}\). If there is a point, not in the arc, through that there pass only 0- and 1-secants, then adding this point to the arc we still get an arc. Repeating this process until there is no more such a point, we obtain an arc \(K\). We show that \(K\) is a hyperoval.

First of all observe that there are exactly \(\varepsilon\) 1-secants passing through a point of \(K\), hence the total number of 1-secants is \(\varepsilon(q + 2 - \varepsilon) \neq 0\).
II. Polynomials in geometry

Define the index of a point as the number of 1-secants through it. Let \( s \) be the index of a point \( P \) on some 0-secant \( \ell \), we show that \( s \) is at most \( \varepsilon \).

Let \( \ell \) be the line \( X = 0 \) (so \([1,0,0]\)) and \( R(X,Y,Z) \) be the Rédei polynomial of \( K \). For a fixed \((0,-z,y)\in \ell \), consider a root \( x \) of \( R(X,y,z) \), its multiplicity is 1 or 2 according as the line \([x,y,z]\) is a 1- or a 2-secant. If \( x \) is a root of multiplicity 2 then its multiplicity as a root of \( \partial X R(X,y,z) \) is still at least 2, so \( R(X,y,z) \) is fully reducible. \( \deg(\text{g.c.d.}(R(X,y,z), \partial X R(X,y,z))) \) is exactly \((q+2-\varepsilon)-(\text{the number of 1-secants through the point } (0,-z,y)) \).

For some \( s \) now write up the resultant \( R(Y,Z) = R_s(R(X,Y,Z), \partial X R(X,Y,Z)) \) as in Section 9.5, its (homogeneous) degree is \( s(s-1) \). We have to give an upper bound for the points on \( \ell \) with index less than \( s \): if \( t_{y,z} \) denotes the number of 1-secants through \((0,-z,y)\) then

\[
\sum_{(0,-z,y) \in \ell} \min\{s-t_{y,z},0\} \leq s(s-1).
\]

So counting the 1-secants through the points of \( \ell \) we get at least \((q+1) s - s(s-1)\), that is at most \( \varepsilon(q+2-\varepsilon) \); from which \( s \leq \varepsilon \) or \( s \geq q + 2 - \varepsilon \) follows. Note that there can be no point with index at least \( q + 2 - \varepsilon \) exactly and it could have been added to \( K \). Furthermore, since through each point outside \( K \) there passes at least one 0-secant, the argument above implies that the index of any point is at most \( \varepsilon \).

Hence the 1-secants form a dual \((\varepsilon(q+2-\varepsilon),\varepsilon)\)-arc and so when \( \varepsilon \leq \sqrt{q} \), the contradiction follows by Barlotti’s bound.

In general, probably \( \sqrt{q} \) is not the right order of magnitude for \( \varepsilon \), except for the case \( n = p^e = 2 \). However if we want a bound for \( \varepsilon \) not depending on \( p^e \), the best order of magnitude we can get is \( \sqrt{q} \).

Combining Theorem 15.17 with the result of Ball, Blokhuis and Mazzocca Theorem 15.12 on non-existence of maximal arcs, the next corollary follows:

**Corollary 15.19.** A \((k,p^e)\)-arc in \( \text{PG}(2,q) \), \( q = ph \), \( p > 2 \) prime, has size less than \( qp^e - q + p^e - \frac{1}{4} \sqrt{q} \).  

16 Unital, semiokvals

A unital is a \( 2 - (q^3 + 1, q + 1, 1) \)-design. We use the same name for a pointset \( U \) of \( \text{PG}(2,q^2) \) if it, together with its \( (q+1) \)-secants, forms a unital in the previous sense. It means that we have \( |U| = q^3 + 1 \) points, and every line intersects \( U \) in either 1 or \( q+1 \) points, the size and this intersection property is equivalent to the
definition. It is also obvious by elementary counting that there is a unique tangent line through each point of a unital. Hence unitals are minimal blocking sets (of maximum possible size, in fact) and semiiovals as well.

The absolute points of a unitary polarity of $PG(2, q^2)$ form a unital, it is called the classical unital or a Hermitian curve. This curve is projectively equivalent to

$$X_1^{q+1} + X_2^{q+1} + X_3^{q+1} = 0.$$ 

Note that for a Hermitian curve, the tangent lines of collinear points are concurrent, i.e. they meet in the polar point of that line. We will see below that this property characterizes Hermitian curves, also giving us an opportunity to show an application of Result 14.6 and the Segre technique.

Various characterizations of a Hermitian curve have been given. Lefèvre-Percsy and independently Faina and Korchmáros proved the following:

**Result 16.1.** Let $H$ be a unital in $PG(2, q^2)$. If every $(q+1)$-secant of $H$ meets $H$ in a Baer subline then $H$ is a Hermitian curve.

Hirschfeld, Storme, Thas and Voloch gave a characterization in terms of algebraic curves:

**Result 16.2.** In $PG(2, q^2)$, $q \neq 2$, any algebraic curve of degree $(q+1)$, without linear components, and with at least $q^3 + 1$ points in $PG(2, q^2)$ must be a Hermitian curve.

Thas [133] proved the following

**Theorem 16.3.** Let $H$ be a unital in $PG(2, q^2)$. If the tangents of $H$ at collinear points of $H$ are concurrent, then $H$ is a Hermitian curve.

The next lemma was the first step in Thas’ proof:

**Lemma 16.4.** Let $H$ be a unital in $PG(2, q^2)$ with the property that the tangents of $H$ at collinear points of $H$ are concurrent. Let $P_1, P_2, P_3$ be non-collinear points of $H$ and let $L_i$ be the tangent of $H$ at $P_i$. Choose the coordinates in such a way that $L_1 \cap L_2 = (0, 0, 1)$, $L_2 \cap L_3 = (1, 0, 0)$, $L_1 \cap L_3 = (0, 1, 0)$. If $P_1 = (0, b, 1)$, $P_2 = (1, 0, c)$ and $P_3 = (a, 1, 0)$ then $(abc)^{q+1} = 1$.

The proof is a nice example of the Segre-like arguments, see the first part of Theorem 14.9. We leave it as an exercise.

**Exercise 16.5.** Prove the lemma of Thas above!

In his original proof Thas showed, using this lemma, that every $(q+1)$-secant meets $H$ in a Baer subline, then by Result 16.1 $H$ is classical. Here we follow the proof of [134], which uses Result 16.2 instead.

**Proof of Theorem 16.3, sketch.** Let $L_1, L_2$ and $L_3$ be non-concurrent tangents of $H$ at the tangent points $P_1, P_2$ and $P_3$. By the lemma and Segre’s Theorem
II. Polynomials in geometry

14.3, there is an algebraic curve \( C' \) intersecting each \( L_i \) at \( P_i \) with intersection multiplicity \( q + 1 \). Next, let \( Q \not\in H \) and let \( M_1, M_2, ..., M_{q+1} \) the tangents of \( H \) through \( Q \). Then the tangent points \( Q_1, Q_2, ..., Q_{q+1} \) are collinear, let \( \ell \) be the line containing them. The curve of degree \( q + 1 \), consisting of \( \ell \) counted \( q + 1 \) times, intersects \( M_i \) at \( Q_i \) with intersection multiplicity \( q + 1 \). Now from Result 14.6 it follows that there exists a curve \( C \) of degree \( q + 1 \) intersecting each tangent of \( H \) at its tangent point with intersection multiplicity \( q + 1 \). As \( C \) contains all points of \( H \), it has at least \( q^3 + 1 \) points. If \( C \) contains a linear component \( L \), then \( L \) contains all the \( q^3 + 1 \) points of \( H \), a contradiction. Now by Result 16.2 of Hirschfeld, Storme, Thas and Voloch, if \( q \neq 2 \) then \( C \) is a Hermitian curve. As \( |C| = |H| = q^3 + 1 \), \( C = H \) and \( H \) is a Hermitian curve. The case of \( q = 2 \) is easy to check.

A semioval is a set of points such that there is a unique tangent at each point. A semioval is regular if all non-tangent lines intersect it in either 0 or a constant number \( a \) of points.

A semioval is called almost oval if there are exactly \( q - 1 \) 2-secants through each of its points. This means that an almost oval semioval \( C \) has \( q + a \) points and through each point of \( C \) there is a unique tangent and a unique \( (a + 1) \)-secant \((a > 1)\). For \( a = 1 \) these sets were called seminuclear sets by Blokhuis and Bruen in [45].

In [34] Blokhuis characterizes almost oval semiovals.

**Theorem 16.6.** (Blokhuis) Let \( C \) be an almost oval semioval in \( PG(2, q) \), \( |C| = q + a \). Then either \( q = a + 2 \) and \( C \) consists of the symmetric difference of two lines, with one further point removed from each line, or \( q = 2a + 3 \) and \( C \) is projectively equivalent to the projective triangle, that is the set defined in Example 18.2.

The proof of this theorem is based on two propositions, the first one can be proved using the Rédéi polynomial.

**Proposition 16.7.** Let \( \ell \) be an \((a + 1)\)-secant of an almost oval semioval \( C \), \( |C| = q + a \). Then the tangents of \( C \) at the different points of \( \ell \cap C \) are concurrent.

**Proof:** Choose coordinates so that \( \ell = \ell_\infty \) and let \( U = C \setminus \ell \). Let \( U = \{(a_i, b_i) : i = 1, \ldots, q - 1\} \) and consider the affine Rédéi polynomial \( R(X, Y) \) of \( U \). For an \((m) \in \ell \cap C \) we have that \( R(X, m)(X^q - X) \). Since \( \deg X(R) = q - 1 \), for these \((m)\)’s the quotient \((X^q - X)/R(X, m)\) can be computed; it has to be \( X - r_1(m) \). This means that the line \( Y = mX + r_1(m) \) is the tangent of \( C \) at \((m)\). Since \( \deg(r_1) = 1 \), \( r_1(m) = am + b \), so the tangents are the lines \( Y = mX + am + b \). These lines pass through \((-a, b)\).

The following generalization of Proposition 16.7 can be proved in exactly the same way as the original one.
Proposition 16.8. Let $U$ be a set of $q - 1$ points in $\text{AG}(2, q)$, which determines at most $q - 1$ directions. Then there is a unique point $w$ such that $U \cup \{w\}$ determines the same directions as $U$.

Proof: Take an infinite point $(m)$ not determined by $U$. Then there is a unique line $t_m$ with slope $m$ which does not meet $U$. These lines pass through a point $w$; this can be proved exactly as in the proof of Proposition 16.7. (The details are left as an exercise.)

This result can be generalized further, namely for sets of size less than $q - 1$. This will be discussed in Theorem 23.1.

Not much is known about semiovals, Thas proved lower and upper bounds for their size (and nonexistence results for their higher dimensional analogues). For regular semiovals Blokhuis and Szőnyi [40] showed that $a$ has to divide $q - 1$ and the points not on the semiovals are on 0 or $a$ tangents. Thus in this case there is a dual (regular) semioval. For regular semiovals in $\text{PG}(2, q)$ more can be said.

Proposition 16.9. [40] Let $S$ be a regular semioval in $\text{PG}(2, q)$. Then $S$ is a unital, or the tangents at collinear points of $S$ are concurrent.

Proof: (Hint:) Try to copy the proof of the previous two propositions.

We have seen above that unitals with the property that tangents at collinear points are concurrent were characterized by Thas as classical unitals (i.e. Hermitian curves).

Using the results of Blokhuis and Szőnyi, and applying an approach similar to Thas’ above, Gács in [68] could give a nice proof of Segre-type for the following.

Theorem 16.10. In $\text{PG}(2, q)$ any regular semioval is either an oval or a unital.

To end this section we show an easy non-existence result.

Theorem 16.11. For $q$ odd there exist no semioval of size $q + 2$, i.e. a set $S \subset \text{PG}(2, q)$ with the property that through each point of $S$ there pass exactly one tangent.

Proof: Observe that through any point of $S$ there pass exactly one 3-secant, and the tangent and 3-secant lines together cover the points of the plane, as $q + 2$ is odd, hence counting the points of $S$ on the lines through any point $P \notin S$ we have to find an odd number of odd secants. Therefore they form a dual blocking set of size $q + 2 + \frac{q + 2}{3}$. It is minimal and does not contain a dual line (pencil),
hence by Szönyi’s Corollary 21.21, every dual line intersects it in 1 mod $p$ points. But there are intersections of size 2 (with pencils centered at the points of $S$), contradiction.

17 Sets without tangents: where Segre meets Rédei

This section is based on [42], [41] and [130]. Sets without tangents were introduced by Blokhuis, Seress and Wilbrink [42], who called them untouchable sets. As a set of size $\leq q + 1$ always has a 1-secant (through each point of it), an untouchable set has at least $q + 2$ points. For $q$ odd, Blokhuis, Seress and Wilbrink proved that the size of a set without tangents in $\text{PG}(2, q)$ is at least $q + \frac{1}{4}\sqrt{2q} + 2$. For $q$ even, the plane $\text{PG}(2, q)$ always has a hyperoval, which is an untouchable set of minimum cardinality; here the question is to find the size of the second smallest untouchable set.

When all lines intersect a set in an even number of points, then such a set is a codeword in the dual code of the plane. For codewords of small weight, see Chapter 6 of the book [3] by Assmus and Key. Note that the cardinality $q + 4$ can be realized in the planes of order 4, 8 and 16, but probably in no other planes.

All known examples have at least $q + \sqrt{q}$ points, see Korchmáros, Mazzocca [88]. They constructed $q + t$-sets of type $(0, 2, t)$ for $t \geq \sqrt{q}$. More examples and a proof that the $t$-secants are concurrent for such sets can be found in Gács, Weiner [70], see Theorem 13.12.

As mentioned in [42], there are untouchable sets of size $2q$, and this is best possible for $q = 3, 5$. Smaller examples were also constructed, the best one for odd $q$’s has size $2q - q/p$, where $q = p^n$. For more constructions in the case $q$ odd, and for planes of small order, we refer to the original paper [42]. For $q$ even see some examples from [41] at the end of this section.

The method introduced in the paper by Blokhuis, Seress and Wilbrink is to associate a curve to an untouchable set, whose points correspond to the lines intersecting the set in at least 3 points. This is a nice application of Segre’s Lemma of tangents. Their bound follows from estimating the number of singular points of this curve. For $q$ even, the construction of the curve still works, but typically we have no information on the number of its singular points. In the next section we briefly recall the construction of these curves.

The Segre-curve, here containing exactly the > 2-secants of a pointset is, intuitively, the Rédei-curve minus the points corresponding to 2-secants (if there are no tangents). The result we are going to prove here is the following.

**Theorem 17.1.** Let $S$ be a set of points in $\text{PG}(2, q)$, without tangents. Then

(a) if $q$ is odd then $|S| > q + 2 + \sqrt{\frac{1}{5}q}$;
(b) if \( q \) is even and \( S \) has an odd line then \( |S| > q + 2 + \sqrt{\frac{1}{6}q} \).

In Section 17.2 we show an improvement by the Szőnyi-Weiner resultant method. In the case when \( q \) is even they proved that a set without tangents, having an odd line, is of size \( > q + 3\lfloor \sqrt{q} \rfloor - 7 \) if \( q > 16 \). Their proof is very short, and elegant, but it is based on other strong results of their stability method.

17.1 The proof using Segre’s method

Curves associated to untouchable sets using Segre’s method

Let \( S \) be a set without tangents in \( \text{PG}(2, q) \), \( 2 \mid q \), \( |S| = q + 2 + \varepsilon \). Throughout this section we suppose that \( q > 6\varepsilon^2 + 5\varepsilon + 1 \), at some points we only need that \( \varepsilon \) is less than \( \sqrt{q}/6 \). Since \( |S| \) is close to \( q + 2 \), and the set has no tangents, almost all lines intersect it in 0 or 2 points. We wish to show that the lines intersecting \( S \) in more than 2 points are contained in an algebraic envelope of degree \( \varepsilon \). For this we will need the generalization of the theorem of Ceva, see Theorems 14.5, 14.3.

Let’s remember that if \( k > n \), then the envelope \( C \) of Segre is unique. Let us also underline that the envelope does not contain any 2-secant of the \( k \)-arc \( A \).

Lemma 17.2. Let \( T \) be any triangle contained in \( S \), \( (S \) is a set without tangents and \( |S| = q + 2 + \varepsilon \)\), with the property that the sides of this triangle are 2-secants.

(a) Suppose that \( q \) is even. Consider the \( i \)-secants through the vertices of \( T \), each with multiplicity \( (i - 2) \). Then these lines are contained in an algebraic envelope of degree \( \varepsilon \).

(b) Suppose that \( q \) is odd. Consider the \( i \)-secants through the vertices of \( T \), each with multiplicity \( 2(i - 2) \). Then these lines are contained in an algebraic envelope of degree \( 2\varepsilon \).

Proof: Looking at \( S \) from a vertex of \( T \) we see that the sum of the multiplicities of the \( i \)-secants through this vertex is just \( \varepsilon \). Consider a \( (q - 1 + \varepsilon) \times 3 \) matrix whose rows are indexed by the points of \( S \setminus T \), and the columns are indexed by the vertices \( A_0, A_1, A_2 \) of \( T \). As the notation suggests, choose \( T \) as the fundamental triangle. Put the “coordinate” of the line \( PA_i \) in position \( (P, A_i) \) of this matrix. Then the product of the coordinates in each row will be \(-1\). In each column we see the coordinates of the \( i \)-secants \((i - 1)\) times each, and every other element of \( \text{GF}(q) \) once. Since the product of the elements of \( \text{GF}(q) \) is \(-1\), the product of the remaining elements is \((-1)^{q+\varepsilon} \). This simply means that the \( i \)-secants with multiplicity \((i - 2)\) satisfy the condition in Result 14.3 if \( q \) is even (i.e. \(-1 = 1\)), but they do not satisfy it when \( q \) is odd. However, by the argument above, the \( i \)-secants with multiplicity \( 2(i - 2) \) will satisfy the required condition, we pay for it by taking square, i.e. the resulting curve will be of degree \( 2\varepsilon \).
Note that when \( \varepsilon \) is small then most of the lines will be 2-secants or skew to \( S \). We want to collect, as usual when using Segre-curves, the “rare”, “irregular” lines in one curve (envelope).

**Lemma 17.3.** If \( 6\varepsilon^2 + 5\varepsilon + 1 < q \), then there exists an algebraic envelope of degree \( \varepsilon \) in the even and \( 2\varepsilon \) in the odd case, containing all the \( i \)-secants of \( S \) with \( i > 2 \), but containing no 2-secants of \( S \).

**Proof:** On the points of \( S \) we form a graph \( \Gamma \) as follows: vertices of \( \Gamma \) are the points of \( S \), two points are adjacent if the line joining them is an \( i \)-secant with \( i > 2 \). Since the number of \( i \)-secants through a point of \( S \) is at most \( \varepsilon \), there are at least \( q + 1 - \varepsilon \) lines through the points which are 2-secants. Hence the degree of a point is at most \( 2\varepsilon \). One can show that there is a set \( A \subset S \) of at least \( 3\varepsilon \) independent points, for which Result 14.5 can be applied, and one can glue together the locally obtained curves if \( (2\varepsilon + 1)(3\varepsilon + 1) > q \).

The proof in the \( q = \) odd case

We have a curve \( C \) of degree \( 2\varepsilon \) with the property that it intersects each pencil of \( S \) in any \( i \)-secant line \( \ell \) of it with multiplicity \( 2(i - 2) \). As for each of the \( i \) points (pencils) on \( \ell \), \( C \) has a multiple intersection in \( \ell \), it follows that \( \ell \) cannot be a simple “point” of \( C \). We are going to use Result 10.3, stating that a curve without multiple components can only have a very limited number of multiple points: for a projective plane curve \( F \) of degree \( n \) without multiple components \( \sum_{P \in F} m_P(m_P - 1) \leq \binom{n}{2} \) holds.

So we get rid of the multiple components: write \( C = E \cdot D^2 \), where \( E \) no longer contains multiple components. The essential observation is that \( E \) is of positive (even) degree as otherwise \( D \) would be a curve of degree \( \varepsilon \) with the property that it intersects each pencil of \( S \) in every one of its \( i \)-secant lines \( \ell \) with multiplicity \( (i - 2) \), but we have seen that such a curve does not exist. As \( C \) fully intersects every pencil \( P \in S \) (since \( \sum_{\ell \in P} 2(i - 2) = 2\varepsilon \)), the same holds for \( E \). It follows from the fact that the intersection numbers are still even (we subtracted an even number from \( 2(i - 2) \)) and if an the intersection number is positive for one pencil \( P \) containing \( \ell \) then \( \ell \in E \) so the intersection number is positive (and \( \geq 2 \)) for all \( i \ell \) points on \( P \). As a consequence, \( \ell \) is a multiple point of \( E \).

For \( \ell \in E \) let \( \mu(\ell) \) denote the multiplicity of \( \ell \) on \( E \) and for a pencil \( P \in S \) let \( \mu(\ell, P) \) be the intersection multiplicity of \( E \) and the pencil \( P \) at \( \ell \). Then \( \mu(\ell, P) \geq \mu(\ell) \), where “\( \geq \)” holds if and only if the pencil \( P \) is a “tangent” of \( E \) at \( \ell \). Also the number of pencils \( P \in S \) that are tangents at \( \ell \) is at most \( \mu(\ell) \). Let the degree of \( E \) be \( 2m \); since \( E \) fully intersects each pencil \( P \in S \), we get

\[
\sum_{P \in S} \sum_{\ell \in P} \mu(\ell, P) = 2m(q + 2 + \varepsilon).
\]
Let’s change the order of summation and use the following estimate:

$$\sum_{P \in \ell} \mu(\ell, P) \leq \mu(\ell) (\varepsilon - \mu(\ell)) + 2m \mu(\ell) \leq 3\varepsilon \mu(P).$$  

\text{(**)}

This estimate is obtained as follows: if the pencil $P$ is a tangent (here we mean tangent in the algebraic sense, so this neither implies or is implied by $|E \cap \text{pencil } P| = 1$) of $E$ at $\ell$, then we know no better than that $\mu(\ell, P) \leq 2m$, and this happens at most $\mu(\ell)$ times. For the remaining points of $\ell$ we have $\mu(\ell, P) = \mu(\ell)$. Finally we used $2m \leq 2\varepsilon$. Using Result 10.3 we obtain

$$\sum_{\ell \in E} \mu(\ell)(\mu(\ell) - 1) \leq 2m(2m - 1).$$

\text{(***)}

We now combine (**) and (***) where in (**) we restrict ourselves to those $\ell \in E$ that are on a point of $S$. For those $\ell$, we have that $\mu(\ell) \geq 2$, so certainly $\sum_{\ell} \mu(\ell) \leq 2m(2m - 1)$. Combining this with (*) we get

$$(2m - 1)3\varepsilon \geq q + 2 + \varepsilon.$$  

Since $2m \leq 2\varepsilon$, we get $q \leq 6\varepsilon^2 - 4\varepsilon - 2 < 6\varepsilon^2 + 5\varepsilon + 1$, a contradiction. 

\textbf{The proof in the $q = \text{even case: Segre and Rédei hand in hand}}$

Here the idea is to combine the above method with a Rédei polynomial approach introduced for $(k, n)$-arcs in [125]. Besides the Segre-curve of the previous sections, another curve will be associated to the untouchable set, with many similar properties as the Segre-curve, implying that they have many points in common.

Finally, we can show that the two curves have a common linear component and derive a contradiction from this fact, if the size of the set is not far from $q + 2$. This second method does not work when the set is contained in the dual of the code generated by the lines of $\text{PG}(2, q)$, that is when each line intersects our untouchable set in an even number of points.

Now another curve will be associated to the untouchable set. This method relies on the paper [125]. Again, the geometric statements will be proved and we will use the algebraic results of Section 9.5.

Consider a line $\ell$ which will be the line at infinity. Let $U = S \setminus \ell = \{(a_i, b_i) : i = 1, \ldots, |U|\}$ and write the Rédei polynomial as

$$R(X, Y) = \prod_{i=1}^{|U|} (X + a_i Y - b_i) = \sum_{j=0}^{|U|} r_j(Y) X^{|U| - j}.$$
II. Polynomials in geometry

Note that \( \deg_Y(r_j) \leq j \). First let us try to interpret in terms of \( R(X,y) \) the fact that through \( (y) \) there pass exactly \( s \) odd lines. (Here an odd line is an \( i \)-secant with \( i \) odd. Note that \( i \geq 3 \) automatically.) From now on the index of a point will be the number of odd lines passing through it.

**Lemma 17.4.** The point \((y) \notin S\) has index \( s \) if and only if the greatest common divisor of \( R(X,y) \) and \( \partial_X R(X,y) \) has degree exactly \(|U| - s\).

**Proof:** Since the characteristic is 2, for \((y) \notin S\) the polynomial \( R(X,y) \) has roots with even multiplicity, and roots corresponding to the odd lines. If we consider \( \partial_X R(X,y) \), then the roots of even multiplicity remain with at least this multiplicity and the multiplicity of the other roots decreases by 1. In other words, the greatest common divisor of \( R(X,y) \) and \( \partial_X R(X,y) \) has degree exactly \(|U| - s\).

Bounds for the number of odd lines is also needed in the proof.

**Lemma 17.5.** The total number of odd lines is at most \( \varepsilon |S|/3 \) and at least \( q + 1 \).

**Proof:** As we have seen in the previous part, the number of \( i \)-secants, with \( i \geq 3 \), through any point of \( S \) is at most \( \varepsilon \). Therefore, the total number of odd lines is at most \( \varepsilon |S|/3 \). For the lower bound note that when \(|S|\) is even then the number of odd lines passing through any point is even, hence the odd secants form a dual even set. When \(|S|\) is odd, the number of odd lines passing through a point is odd, so they form a dual blocking set. It is well-known that a blocking set of \( \text{PG}(2,q) \) is of size at least \( q + 1 \).

The main idea of the proof is that for a fixed \( Y = y \) the polynomial

\[
b(X,y) = R(X,y) / \gcd(R(X,y), \partial_X R(X,y))
\]

can be expressed using the coefficients \( r_1(y), \ldots \) of \( R(X,Y) \). Choose a parameter \( s \) and consider the polynomial \( b = b_s \) of degree \( s \) in \( X \), which is obtained by solving the system of linear equations in the proof of Theorem 9.34 (\( s \) is not fixed yet!). We will try to choose a typical index \( s \) for the line at infinity; that is an \( s \) for which through most of the points there pass exactly \( s \) odd lines. The next lemma says that such a typical index exists.

**Proposition 17.6.** Assume that \( \ell \) intersects \( S \) in 0 or 2 points. Then there is a unique \( s = s(\ell) \) such that \( s \leq \varepsilon \) and at least \( q - \varepsilon \sqrt{q} \) points on \( \ell \) have index at most \( s \) and at least \( \frac{q}{2} \varepsilon \) of them have index exactly \( s \).

**Proof:** Since there are at most \( \varepsilon |S|/3 \leq \varepsilon q/2 \) odd lines, the average index of a point is at most \( \varepsilon /2 \). Hence there are at least \( \frac{q+1}{2} \) points on the line at infinity with index at most \( \varepsilon \). Go down from \( \varepsilon \) and stop at the largest \( s \leq \varepsilon \), where there
are points of index $s$. Then the determinant of $R = R_s$ in Theorem 9.34 is not identically zero as a polynomial in $Y$, and we know the following from Theorems 9.34 and 9.35:

(A) There are at most $s(s-1)$ points for which $\det R = 0$.

(B) The points whose index is less than $s$ are among these points, and $\det R \neq 0$ for points of index $s$.

Hence there are at least $q + 1$ points with index exactly $s$. Using the same trick, the first $t > s$ for which there can be points of index $t$ must satisfy $t(t-1) \geq q + 1$. Since for the points of index at most $s$ the determinant of $R_t$ in Theorem 9.34 must vanish. This implies $t \geq \sqrt{q}/2$. Since the average index is at most $\varepsilon|S|/(3(q + 1))$, there are at most $\varepsilon|S|\sqrt{2}/(3\sqrt{q})$ points having index larger than $s$. This is certainly at most $\sqrt{2\varepsilon(\sqrt{q} + 1)}/3 \leq \varepsilon\sqrt{q}$, since $\varepsilon \leq \sqrt{q}/6$. We already saw in (A) that there are at most $s(s-1) \leq q/6$ points of index less than $s$, so the result follows.

**Proposition 17.7.** Let $s$ be the typical index for the line $\ell$ at infinity. Then there is a curve $c^\ell(X,Y,Z)$ with the following properties:

1. $\deg_X(c^\ell) \leq s$, $\deg(c^\ell) \leq s^2$;
2. $c^\ell(x,y,1) = 0$ implies that $[y,-1,x]$ is an odd line, if the point $(1,y,0)$ has index $s$.

**Proof:** Denote the typical index by $s$. By Lemma 17.4 this means that the g.c.d. of $R(X,Y)$ and $\partial_X R(X,Y)$ has degree $\deg_X R - s$. Consider $c^\ell$ as a homogeneous polynomial constructed in the proof of Theorem 9.34. By Result 9.35, the polynomial $c(X)\det R = c^\ell$ has $X$-degree $s$ and total degree at most $s^2$. If a fixed point $(1,y,0)$ of the line at infinity has index $s$, then the odd lines through it correspond to the roots of $c_s^\ell(X,y)$. This also shows (2).

**The two curves have a common component**

In this section we would like to choose the line at infinity to be a 2-secant of $S$, so that the typical index of it $s > 0$ holds. Next we show that such 2-secants exist.

**Lemma 17.8.** Assume that there is a line intersecting $S$ in an odd number of points. Then there exists a 2-secant of $S$, such that the typical index for it is not zero.

**Proof:** The envelope $C(X_0, X_1, X_2)$ obtained by Segre’s method has degree less than $\sqrt{q}/6$ and it contains all the odd secants of $S$, hence by Bézout’s theorem.
any pencil with vertex having index at least $\sqrt{q/2}$ must be a component of $C$. So there are at most $\sqrt{q/6}$ points with index at least $\sqrt{q/2}$.

Choose a 2-secant $\ell$ that contains no point with index at least $\sqrt{q/2}$. (Such a 2-secant exists, since through a point of $S$ there pass at least $(q+1-\varepsilon)$ 2-secants and there are only $\sqrt{q/6}$ points with index at least $\sqrt{q/2}$.) Assume that the typical index of $\ell$ is zero. Note that there are no points of $\ell \setminus S$ with index greater than the typical index of $\ell$. (Since by the proof of Proposition 17.6 such a point would have index at least $\sqrt{q/2}$.) Hence each point of $\ell \setminus S$ has index zero and the odd lines intersect $\ell$ in the points of $S \cap \ell$. So there can be at most $2\varepsilon$ odd lines in total, which contradicts our lower bound for the number of odd lines, see Lemma 17.5.

Let the line at infinity be a 2-secant of $S$ and assume that for the typical index $s > 0$ holds. Then the curve $C(X_0, X_1, X_2)$ obtained by Segre’s method has $X_2$-degree $\varepsilon$ (which is its total degree). Substitute $X_0 = Y$, $X_1 = -1$, and $X_2 = X$ in $C$ to get the curve $g(X, Y)$. According to the results in the second section, this curve contains all odd lines. Similarly, let us denote by $c(X, Y)$ the curve constructed in the previous section.

**Lemma 17.9.** The curves $c$ and $g$ have a common component.

**Proof:** The curve $c$ has at least $(\frac{5}{6}q - \varepsilon \sqrt{q})s$ points, which correspond to odd lines. These points are also points of the curve $g$. If the two curves had no common component, then Bézout’s theorem would give that

$$s(\frac{5}{6}q - \varepsilon \sqrt{q}) \leq s^2 \varepsilon,$$

which is impossible, since $s \leq \varepsilon$.

Now we are able to prove our main theorem.

**Theorem 17.10.** The size of an untouchable set in $\text{PG}(2, q)$, $q$ even, having odd lines, is at least $q + 1 + \sqrt{q/6}$.

**Proof:** Assume to the contrary, that there exists an untouchable set in $\text{PG}(2, q)$, having odd lines, with size $q + 2 + \varepsilon$, where $\varepsilon < \sqrt{q/6} - 1$. Note that then $6\varepsilon^2 + 5\varepsilon + 1 < q$. Consider a common (absolutely irreducible) component of $c$ and $g$ guaranteed by the previous lemma. Let the $X$-degree of this component be $u$, which is its total degree. Then the component has at least $(\frac{5}{6}q - \varepsilon \sqrt{q})u$ points. Using the Weil bound one immediately sees that this component has to be linear. But that implies the existence of a point with at least $(\frac{5}{6}q - \varepsilon \sqrt{q})u$ odd lines through it. This is a contradiction, since such a set would have at least $3(\frac{5}{6}q - \varepsilon \sqrt{q})$ points.
17. Sets without tangents: where Segre meets Rédei

17.2 Untouchable sets in Galois planes of even order

Here we improve Theorem 17.1 in the case when \( q \) is even. The proof is based on Theorem 23.22.

First we show that a not too large untouchable set is very close to be a set of even type, hence we can apply Theorem 23.22 to such sets.

**Lemma 17.11.** Let \( U \) be a set without tangents in \( \text{PG}(2, q) \), \( q \) even. Assume that \( U \) has \( q + 2 + \varepsilon \) points, then the number of odd-secants is at most \( \varepsilon |U| / 3 \).

**Proof:** Through any point of \( U \) there pass at most \( \varepsilon \) odd-secants. An odd-secant contains at least 3 points of \( U \), therefore the total number of odd-secants is at most \( \varepsilon |U| / 3 \).

**Theorem 17.12.** (Szönyi-Weiner [130]) The size of an untouchable set \( U \) in \( \text{PG}(2, q) \), \( 16 < q \) even, having odd lines, is larger than \( q + 3[\sqrt{q}] - 7 \).

**Proof:** Assume that \( |U| \leq q + 3[\sqrt{q}] - 7 \). By Lemma 17.11, the number of odd-secants, \( \delta \) of \( U \) is less than \( (\lfloor \sqrt{q} \rfloor + 1)(q + 1 - \lfloor \sqrt{q} \rfloor) \). By Theorem 23.22, we can construct a set of even type from \( U \) by modifying \( \lceil \frac{\delta}{q + 1} \rceil \geq 1 \) points. If \( P \) is a modified point, then through \( P \) there pass at least \( q + 1 - (\lfloor \frac{\delta}{q + 1} \rfloor - 1) \) odd-secants of \( U \). But then counting the points of \( U \) on the lines through \( P \) we get that \( |U| > 2(q - \lfloor \sqrt{q} \rfloor) \), when \( P \in U \), and \( |U| > 3(q - \lfloor \sqrt{q} \rfloor) \), when \( P \notin U \); which is a contradiction.

**Concluding remarks**

In this section first we give examples for small sets without tangents but having odd lines. First of all note that the union of two non-disjoint hyperovals \( \mathcal{H}_1 \) and \( \mathcal{H}_2 \) is always such a set of size \( 2(q + 2) - |\mathcal{H}_1 \cap \mathcal{H}_2| \). In [86] it was showed that in \( \text{PG}(2, 16) \) there exist two hyperovals (a Lunelli-Sce and a regular one) intersecting each other in 8 points; hence there is a non-even type, untouchable set of size 28 in \( \text{PG}(2, 16) \). By the construction method introduced in [70], the above set can be used to obtain non-even type, untouchable sets in \( \text{PG}(2, 16^h) \), \( (h \geq 2) \), of size \( \frac{7}{4} \cdot 16^h - 16^{h-1} \) and of size \( \frac{7}{4} \cdot 16^h \).

For untouchable sets in planes of even order we were lucky in the sense that both Segre’s method and Rédei’s method worked. The Rédei method can be generalized to the following situation: let \( S \) be a set having only 0-secants and \( i \)-secants, where \( i \geq p \), \( q = p^h \). Then the size of \( S \) is at least \( qp - q + p \), and in case of equality \( S \) is a maximal arc. By Theorem 15.12 of Ball, Blokhuis and Mazzocca [13], such an arc does not exist if \( p \) is odd. Even in that case, one can show that \( |S| \) has to be at least \((qp - q + p + \varepsilon)\) with \( \varepsilon \geq \sqrt{q}/2 \), if \( S \) has an \( i \)-secant for which \( i \) is
not divisible by $p$. For this, one has to copy more or less the entire proof in [125]. The reason why the result is weaker than for our case $p = 2$, is that the method based on Segre’s lemma of tangents does not seem to work in this case. Similarly, instead of $i \geq p$ one can suppose that $i \geq p^r$ and the situation is more or less the same in this case, too.

When $p^r > \sqrt[q]{q}/2$, then a better bound can be obtained by simple counting arguments:

**Exercise 17.13.** Let $S$ be a set of size $nq + n - q + \varepsilon$ which intersects every line in either 0 or at least $n$ points for some $n = p^r$. Then $\varepsilon \geq n$.

## 18 Directions

The theory of directions determined by a pointset is one of the most prominent ones in finite geometry. There are several applications of it, within geometry (e.g. blocking sets of Rédei type), in group theory (Hajós-Rédei type results), for permutations, etc. One can see the original question from at least four points of view.

Consider a pointset $U = \{P_i(a_i, b_i) : i = 1, \ldots, |U|\} \subset \AG(2, q)$. One can say that $U$ determines the direction/infinite point $(m) \in \ell_\infty$, where $m \in \GF(q) \cup \{\infty\}$ if there are points $P_i$ and $P_j$ such that $m = \frac{b_j - b_i}{a_j - a_i}$. The set of determined directions will be denoted by $D$, its cardinality by $N = |D|$. When $|U| > q$ then $D = \ell_\infty$ (i.e. $N = q + 1$) by the pigeon hole principle, as through any $(m) \in \ell_\infty$ there are $q$ affine lines, so at least one of them will contain at least two points of $U$, determining $(m)$; this shows that only $|U| \leq q$ is interesting. The most examined case is when $|U| = q$, we are going to discuss it in details, but some results concerning smaller $U$ can be found in this book, like Theorem 23.1, etc. The general feeling is that if $|U|$ is close to $q$ then it can be extended to a $q$-set determining the same directions, while small pointsets $U$ can behave “as they want”. Note that a random pointset of size at least $\sqrt{2q \log(q)}$ determines every direction with high probability.

Suppose $U$ is a set of $q$ points which does not determine all directions. Then applying an affine transformation, we can achieve that the direction of vertical lines is not determined. But this means that our point set in question can be considered as the graph of a function $f(X)$, over the underlying field. Since over a finite field every function can be represented by a polynomial, we may assume $f \in \GF(q)[X]$. (Note that lines correspond to linear polynomials.) We will say that a polynomial $f$ determines a direction, if its graph determines it, which means that the set of determined directions is $D_f = D = \{(\frac{f(x) - f(y)}{x - y} : x \neq y\}$. This was the original question Rédei considered, he tried to determine the number of difference quotients a polynomial can have.

It is easy to verify that $D = \{c \in \GF(q) : f(X) - cX \text{ is not bijective}\}$, so a third formulation of our problem is to look for polynomials, for which there are many
c-s such that \( f(X) - cX \) is a permutation. Compare with the definition of \( M_f \) in Section 9.

In his book [103] Rédei proved deep theorems about fully reducible, lacunary polynomials. As an application of his algebraic results, he considered the problem of determining the possible values \( N = N_f = |D_f| \) can take, that is, how many different directions a point set can determine. For an arbitrary prime-power \( q \), he proved that for \( N_f < \frac{q+1}{2} \), \( N_f \) cannot take all values, it has to be an element of the union of some intervals.

For \( q = p \) prime, he proved much more, namely that unless \( U \) is a line (and hence \( N = 1 \)), \( N \) is at least \( \frac{p+1}{2} \). Later Megyesi realised that the case \( \frac{p+1}{2} \) is impossible, so their result can be formulated as follows:

**Theorem 18.1.** (Rédei and Megyesi [103]) If a set of \( p \) points in \( \text{AG}(2,p) \) is not a line, then it determines at least \( \frac{p+3}{2} \) directions.

This bound is sharp, as the (unique) Example 18.2, constructed by Megyesi, shows, see below. Unicity is proved by Lovász and Schrijver, see Theorem 19.1. For the proof of Theorem 18.1, which is a classical lacunary polynomial argument, see the first part of Theorem 18.14.

Now we present a series of examples constructed by Megyesi [103] for arbitrary prime-powers.

**Example 18.2.** For a \( d \) \( |q-1| \), \( 1 < d < q - 1 \), let \( G \) be the multiplicative subgroup of \( \text{GF}(q) \) of order \( d \). Set \( U = \{(x,0) : x \in G\} \cup \{(0,x) : x \notin G\} \), that is put \( G \) and the complement of \( G \) on the \( x \) and \( y \) axes, respectively. An easy calculation shows that the number of determined directions is \( q + 1 - d \).

Perhaps it is useful to give Example 18.2 in the graph form as well. In general, a polynomial giving the example on two lines with \( N = q + 1 - d \) is \( X \chi_G \), where \( \chi_G \) is the characteristic function of \( G \), the multiplicative subgroup of order \( d \). A polynomial having \( N = \frac{q+3}{2} \) is \( f(X) = X^{\frac{q+1}{2}} \).

We remark that the Megyesi example belonging to \( N = \frac{q+3}{2} \), together with the determined directions as points at infinity, is called the *projective triangle*. It is a set of size \( \frac{3}{2}(q+1) \) in \( \text{PG}(2,q) \).

After the publication of Rédei’s book, it turned out that the problem of determining the possible values of \( N \) and looking for sets determining a small number of directions has an important application: a certain type of blocking sets (called *blocking sets of Rédei type*) in \( \text{PG}(2,q) \) of size \( q + N \) is equivalent to a set of \( q \) points in \( \text{AG}(2,q) \) determining \( N \) directions.

**Exercise 18.3.** Show that for a blocking set \( B \subset \text{PG}(2,q) \) and a line \( \ell \), \( |B \setminus \ell| \geq q \) holds, and in case of equality \( B \setminus \ell \), considered as a pointset of \( \text{AG}(2,q) = \text{PG}(2,q) \setminus \ell \), determines (as determined directions) the “necessary” points of \( B \cap \ell \).
In the general case today everything is known for $N < \frac{q+3}{2}$: Ball, Blokhuis, Brouwer, Storme and Szönyi [43], and then the beautiful improved proof of Ball [9] determined all possible values, see Theorem 18.14.

### 18.1 When $D$ is (contained in) a subgroup of $\text{GF}(q)^*$

Given $D \subseteq \ell_\infty = \text{GF}(q) \cup \{\infty\}$, let $F_D$ denote the set of all polynomials $f$ determining directions from $D$, i.e. for which $D_f \subseteq D$.

**Lemma 18.4.** [56] Let $D$ be a non-trivial subgroup of the multiplicative group $\text{GF}(q)^*$. Then the polynomials in $F_D$, with the operation of composition, form a permutation group of the ground set $\text{GF}(q)$.

**Proof:** As $(0) \not\in D$, each $f \in F_D$ is a permutation. Let $f, g \in F_D$, then

$$f(g(x) - f(g(y)) = \frac{f(g(x)) - f(g(y))}{g(x) - g(y)},$$

so the product of two elements of $D$, hence also in $D$. 

**Exercise 18.5.** Prove that the permutation group $F_D$ is 3/2-transitive on $\text{GF}(q)$, moreover, even the subgroup $F_D^{\text{lin}} = \{f(X) = aX + b : a \in D, b \in \text{GF}(q)\} \subseteq F_D$ is 3/2-transitive on $\text{GF}(q)$.

**Exercise 18.6.** [56] Prove that if $D \subseteq \text{GF}(p^\ell)^*$ for some subfield $\text{GF}(p^\ell) < \text{GF}(q)$ then $F_D = F_D^{\text{lin}}$, i.e. the only functions determining directions from $D$ are the linear ones with slope from $D$.

As the multiplicative group $\text{GF}(q)^*$ is cyclic, its subgroups are exactly of the form $D = \{x : x^d = 1\}$ for some $d | (q-1)$. We are going to prove the following theorem of Carlitz, McConnel, Bruen and Levinger [56]:

**Theorem 18.7.** If $D_f \subseteq D = \{x : x^d = 1\}$ for some $d | (q-1)$ then $f$ is of the form $f(X) = a + bX^p^\ell$, where $a \in \text{GF}(q), b \in D$ and $m = \frac{q-1}{d}$ divides $(p^\ell - 1)$.

**Proof:** ([56]) Let $V$ denote the vectorspace of functions $\text{GF}(q) \rightarrow \text{GF}(q)$, or, equivalently, the space of polynomials in $\text{GF}(q)[X]$ of degree $\leq q-1$. The element $g$ of $F_D$ acts on $f \in V$ as $f^g(X) = f(g(X))$. This proof will go in four steps.

The first is about the linear space of homomorphisms $V \rightarrow V$, which commute with elements of the permutation group $F_D$; that is let

$$\text{Hom}_{F_D}(V, V) = \{ \Phi : V \rightarrow V \mid \Phi(f(g(X))) = \Phi(f)(g(X)) \text{ for all } f \in V, g \in F_D \}.$$ 

Define also the monomial functions $\varphi_i(X) = X^{id}$ for $i = 0, 1, \ldots, m = \frac{q-1}{d}$. Finally recall $\mu_a(X) = 1 - (X - a)^{q-1}$, the characteristic function of the set $\{a\}$, see Section 5.3.
Step 1. If $\Phi \in \text{Hom}_{F_D}(V, V)$ then $\Phi(\mu_0)$ can be written as a linear combination of the monomials $\varphi_i$, $i = 0, \ldots, m$. Conversely, given any linear combination $\sum_{i=0}^{m} \lambda_i \varphi_i$, there is a unique element $\Phi \in \text{Hom}_{F_D}(V, V)$ such that $\Phi(\mu_0) = \sum_{i=0}^{m} \lambda_i \varphi_i$.

To prove this we need the following

Exercise 18.8. The dimension of $\text{Hom}_{F_D}(V, V)$ over $GF(q)$ is just the number of the orbits of $(F_D)_0$ (the stabilizer of 0) on $GF(q)$, i.e. $m + 1$.

For $a \in GF(q)$ define the translation $T_a(X) = X - a$. Then $\mu_0^{T_a} = \mu_a$. As any $f \in V$ has the form $f(X) = \sum_{a \in GF(q)} f(a) \mu_a(X) = \sum_{a \in GF(q)} f(a) \mu_0^{T_a}(X)$, for any $\Phi \in \text{Hom}_{F_D}(V, V)$ and $f \in V$ we have

$$\Phi(f) = \sum_{a \in GF(q)} f(a) \Phi(\mu_0^{T_a}) = \sum_{a \in GF(q)} f(a) \Phi(\mu_0)^{T_a},$$

hence $\Phi$ is uniquely determined by the image of $\mu_0$.

To finish Step 1 we have to prove that $\Phi(\mu_0)$ is some linear combination of the monomials $\varphi_i$, $i = 0, \ldots, m$. Let $\Phi(\mu_0)(X) = \sum_{i=1}^{q-1} \lambda_i X^i$ and $f(X) = bX \in F_D^m$ (so $b \in D$). Then $\mu_0(X) = \mu_0(bX) = \mu_0(X)$, so

$$\Phi(\mu_0)(X) = \Phi(\mu_0)(X) = \Phi(\mu_0)^f(X) = \sum_{i=0}^{q-1} \lambda_i (bX)^i.$$  

Thus $\sum_{i=0}^{q-1} \lambda_i (1 - b^i) X^i = 0$, hence all the coefficients $\lambda_i (1 - b^i)$ are zero for $i = 0, 1, \ldots, q - 1$. As $b$ was an arbitrary element of $D$, it means that $\lambda_i = 0$ unless $d|i$ and we are done.

Step 2. We prove that for each $k = 0, 1, \ldots, m$, $U_k = \langle (X - a)^{kd} : a \in GF(q) \rangle$ is an $F_D$-module (i.e. for any $g \in F_D$, $f \in U_k$ also $f^g \in U_k$).

To see this observe that if $\Phi$ is in $\text{Hom}_{F_D}(V, V)$ then $\Phi(V)$ is an $F_D$-module. By Step 1 there exists a $\Phi$ in $\text{Hom}_{F_D}(V, V)$ for which $\Phi(\mu_0)(X) = X^{kd}$. Further

$$\Phi(\mu_a)(X) = \Phi(\mu_0^{T_a})(X) = (\Phi(\mu_0))^{T_a}(X) = (X^a)^{kd}.$$  

Step 3. Recall Exercise 5.8. There we defined $S_\lambda = \langle (X - a)^\lambda : a \in GF(q) \rangle$ and $M_\lambda = \{ \sum_{i=0}^{n-1} \alpha_i p^i : 0 \leq \beta_i \leq \alpha_i \}$. Since $d|q - 1$ we have $(d, p) = 1$ and $1, (d - 1) \in M_\lambda$. In Step 2 we have seen that $S_\lambda$ is an $F_D$-module. Thus, for any $g \in F_D$ and $r \in M_\lambda$, $\varepsilon^r(g(X)) = g(X)^r$ is a polynomial in $S_\lambda$. We are going to use this.

Lemma 18.9. Let $f \in F_D$. Then $f(X) = a + bX^t$, where $a = f(0), b = f(1) - f(0)$ and $td \equiv d \pmod{q - 1}$.
Proof: Let \( a = f(0) \). Since the translation \( T_a \) is in \( F_D \), \( \Psi(X) = T_a(f(X)) = f(X) - a \) is also in \( F_D \) and \( \Psi(0) = 0 \). As \( 1, (d - 1) \in \mathbb{M}_d \), the functions \( \varepsilon_1^\Psi = \Psi \) and \( \varepsilon_1^\Psi = \Psi^{d-1} \) (after reduction) are in \( S_d \). Now, \( \Psi \in F_D \) implies that \( \frac{\Psi(x)}{x} \in D \) for \( x \neq 0 \). From the definition of \( D \), it follows that \( X^d = \Psi(X)^d = \Psi(\frac{X^2}{\Psi}) \Psi(X)^{d-1} \). But \( X^d \) can be a product of two polynomials of degree \( \leq d \) only if \( \Psi(X) = bX^t \) and \( \Psi(X)^{d-1} = b'X^{d-t} \), where \( bb' = 1 \) and \( 0 < t < d \). Then \( \Psi^d(X) = b^dX^{td} = X^d \), if and only if \( td \equiv d \mod q - 1 \) and \( b^d = 1 \). Further, \( b = \Psi(1) = f(1) - a = f(1) - f(0) \).

Step 4. We now show that the only possible choices for \( t \) above are \( t = p^j \). W.l.o.g. we may assume that \( f \in F_D \) has the form \( f(X) = X^t \). \( F_D \) is a group containing the translations \( T_a \). Thus for any fixed \( \alpha \neq 0 \), \( h(X) = f(T_\alpha(X)) = (X - \alpha)^t \) is in \( F_D \). By Step 3, \( h(X) = a + bX^t = (X - \alpha)^t \), where \( a = h(0) = (-\alpha)^t \) and \( b = h(1) - h(0) \). We have the equation \( (X - \alpha)^t - (a + bX^t) = 0 \) as it is of degree \( < q - 1 \). Hence \( t = t', b = 1 \) and \( (X - \alpha)^t = X^t + (-\alpha)^t \). Since \( \alpha \) was arbitrary, this shows that \( f(x + \alpha) = (x + \alpha)^t = x^t + \alpha^t \) for all \( x, \alpha \in GF(q) \), so \( f \) is an automorphism of \( GF(q) \), hence \( t = p^j \) and by Step 3, \( d(p^j - 1) \equiv 0 \mod q - 1 \).

Exercise 18.10. Prove that if \( D = \{ x \in GF(q) : x^d = \lambda \} \) for some fixed \( \lambda \) for which \( \lambda^\frac{q-1}{d} = 1 \), then \( F_D \) consists of the functions \( f(X) = a + bX^p \) where \( a, b \in GF(q) \) and \( b \in D \).

The theorem above has some further applications in geometry. In Section 18.4 we will see that pointsets of size \( q \) determining at most \( \frac{q+1}{2} \) directions can be classified: they are \( GF(p^e) \)-linear pointsets in \( AG(2, q) \), where \( GF(p^e) \) is a subfield of \( GF(q) \). It also means that the set \( D \) of determined directions is a \( GF(p^e) \)-linear pointset of (the line at infinity \( \cong \) PG(1, q), generated by \( \frac{h}{e} + 1 \) points. (For the definition of generation see Section 20.) So one can use that we are in the situation that \( \{ (x^d) : x \in GF(q) \} \supseteq \langle (a_1), ... , (a_{m+1}) \rangle_{GF(p^e)} \) for some \( a_1, ..., a_{m+1} \in GF(q) \).

One can also try to alter the proof above a little bit to prove the following

Conjecture 18.11. If \( D_f \subseteq D = \{ x : x^d = 1 \} \cup \{ 0 \} \) for some \( d(q - 1) \) then \( f \) is of the form \( f(X) = a + bX^p \), where \( a \in GF(q) \), \( b \in D \) and \( m = \frac{q-1}{d} \) divides \( (p^i - 1) \).

It follows from Theorem 18.1 of Rédie and Megyesi that if \( q = p \) is a prime then the Conjecture holds and \( f \) is a linear function.

Exercise 18.12. Suppose that a set of disjoint parabolas \( \{ Y = a_i X^2 + b_i : i = 1, ..., q \} \) partition \( AG(2, q) \). Then (i) the \( b_i \)-s are all distinct; (ii) writing \( a_i = f(b_i) \), the directions determined by the function \( f \) are minus non-squares and possibly \( 0 \); finally (iii) if \( q = p \) is a prime and we do not allow a line as a degenerate parabola then all \( a_i \)-s are equal and they are the vertical translates of the same parabola.
18. Directions

18.2 When \( D \) is (contained in) a subgroup of \( \sqrt{\sqrt{1}} \subset \text{GF}(q^2)^* \)

Well, it almost never happens, if we mean proper subgroups, see Theorem 29.5. For this being meaningful we have to put our pointset \( U \) into the affine plane \( \text{AG}(2, q) \) which is identified with \( \text{GF}(q^2) \) and the directions with the \((q+1)\)-th roots of unity. Theorem 29.5 says that, given \( 1 < d < q + 1 \), if \( U \) determines directions from one coset of the multiplicative subgroup of order \( d \), then \( U \) is a line.

Aart Blokhuis has recently asked the opposite question: is it possible that \( U \) does not determine any direction of the multiplicative subgroup of order \( d \) (unless \( U \) is a line)? Such (positive or negative) results would give rise several applications. One may feel that such sets \( U \) probably do not exist. For \( d = \frac{q+1}{2} \) Blokhuis’ theorem in [29], so Theorem 29.5 shows this. The next possible case \( d = \frac{q+1}{3} \) is already open as far as I know.

18.3 Sets determining \( \leq \frac{q+1}{2} \) directions: affine linear pointsets

Linear pointsets has gained an important role in the theory of blocking sets. First we give the definition of affine linear pointsets:

**Definition 18.13.** A pointset \( S \subseteq \text{AG}(n, q) \) is called \( \text{GF}(p^e) \)-linear if

(i) \( \text{GF}(p^e) \) is a subfield of \( \text{GF}(q) \), and

(ii) there is an affine space \( \text{AG}(n', q) \) containing \( \text{AG}(n, q) \) such that \( S \) is a one-to-one projection of a subgeometry \( \text{AG}(t, p^e) \subset \text{AG}(n', q) \) from a suitable subspace (“vertex”) \( V \) onto \( \text{PG}(n, q) \).

Algebraically this means that if we suppose that \( S \) contains the origin and has size \( |S| = (p^e)^t \), then one can choose \( t \) points (vectors) \( v_1, \ldots, v_t \) of \( \text{AG}(n, q) \) such that \( S \) is the vectorspace spanned by them over \( \text{GF}(p^e) \), i.e. \( S = \{ \sum_{i=1}^{t} \lambda_i v_i \; : \; \lambda_1, \ldots, \lambda_t \in \text{GF}(p^e) \} \).

Suppose that we have an affine pointset \( S \) with the suspect that it is \( \text{GF}(p^e) \)-linear in the affine sense. W.l.o.g. suppose that the origin is in \( S \). Then \( S \) is \( \text{GF}(p^e) \)-linear iff (i) \( (a_1, b_1), (a_2, b_2) \in S \) implies \( (a_1 + a_2, b_1 + b_2) \in S \) and (ii) \( (ca_1, cb_1) \in S \) for all \( c \in \text{GF}(p^e) \). Now changing the representation to the \( \text{GF}(q^2) \)-one, we conclude that \( S \) is \( \text{GF}(p^e) \)-linear iff substituting \( Y = \omega \in \text{GF}(q^2) \setminus \text{GF}(q) \) into its affine Rédei polynomial \( R(X,Y) \), \( R(X,\omega) \) contains terms with exponents being powers of \( p^e \) only. As \( R \) was defined over \( \text{GF}(q) \), it is equivalent to saying that all the \( X \)-exponents of \( R(X,Y) \) are powers of \( p^e \).

Everything is similar in \( \text{AG}(n, q) \) for bigger \( n \). But it gets much harder if \( S \) is non-affine, see Section 20.
18.4 Small blocking sets of Rédei type are linear

Here we present a short proof of the following theorem of Blokhuis, Ball, Brouwer, Storme and Szönyi [43], which was refined and turned to its current beautiful form by Ball [9]:

**Theorem 18.14.** Let \(|U| = q\) be a pointset in \(\text{AG}(2, q)\), \(q = p^h\), \(p\) prime, and let \(N\) be the number of directions determined by \(U\). Let \(s = p^e\) be maximal such that every line intersects \(U\) in a multiple of \(s\) points. Then one of the following holds:

(i) \(s = 1\) and \(q + 3 \leq N \leq q + 1\);
(ii) \(\text{GF}(s)\) is a subfield of \(\text{GF}(q)\) and \(\frac{q}{s} + 1 \leq N \leq \frac{q - 1}{s - 1}\);
(iii) \(s = q\) and \(N = 1\).

Moreover, if \(s \geq 3\) then \(U\) is a \(\text{GF}(s)\)-linear pointset.

**Proof:** Before proving the lower bounds, note first that the upper bounds are trivial. Let \(P\) be a point of \(U\). If \(s > 1\) then the points of \(U\) lie on lines incident with \(P\) and with a direction in \(D\). Therefore

\[ N(s - 1) + 1 \leq q. \]

The degree of a polynomial \(g\) is denoted by \(g^\circ\). We will require Lemma 5.37 by Rédei on lacunary polynomials, and Lemma 5.41 as well.

Let \(U = \{(a_i, b_i) : i = 1, \ldots, q\}\) be our set determining the directions \(D\). We can assume that \((\infty) \notin D\) (so one may think about \(U\) as a graph of a function \(f(X) : \text{GF}(q) \to \text{GF}(q)\), \(N = |D|\) and \(s = p^e\) is maximal such that every line intersects \(U\) in a multiple of \(s\) points. The (affine) Rédei polynomial is

\[ R(X, Y) = \prod_{i=1}^{q} (X + a_iY - b_i) = \sum_{j=0}^{q} \sigma_j(Y) X^{q-j}. \]

The polynomial in one variable \(R(X, y)\) has a repeated factor if and only if \((y) \notin D\).

Hence for \((y) \notin D\)

\[ R(X, y) = X^q - X, \]

and \(\sigma_j(y) = 0\) for \(j = q\) and \(j = 1, 2, \ldots, q - 2\).

The overall degree of \(R(X, Y)\) is \(q\) and (so) the degree of \(\sigma_j(Y)\) is at most \(j\), and the coefficient of \(Y^j\) in \(\sigma_j(Y)\) is \(\sigma_j(\{a_i\}) = \sigma_j(\text{GF}(q))\). Hence for \(j = 1, 2, \ldots, q - 2\) the degree of \(\sigma_j(Y)\) is at most \(j - 1\) and moreover, from the previous paragraph, has at least \(q - N\) distinct zeros. So the polynomial \(\sigma_j(Y) = 0\) whenever \(j \leq q - N\). Therefore

\[ R(X, Y) = X^q + \sum_{j=0}^{N-1} \sigma_{q-j}(Y) X^j. \]

Let \(y \in D\). The line \(c = yX - Y\) is incident with exactly \(k\) points of \(U\) if and
only if \((X + c)\) is a factor of \(R(X, y)\) with multiplicity exactly \(k\). By assumption this \(k\) is always a multiple of \(s\), hence \(R(X, y)\) is an \(s\)-th power. We can write \(R(X, y)^{1/s} = X^{q/s} + g(X)\) for some \(g(X) = g_y(X)\); since \(s\) was chosen to be maximal there exists a \(y \in D\) such that \(g'_y(X) \neq 0\). It follows from Lemma 5.37 that, for any \(y \in D\) such that \(g'(X) \neq 0\) we have \(q^{s} \geq \frac{q+s}{s(s+1)}\). Let \(N_0\) be maximal such that \(\sigma_{q-N_0}\) is not identically 0. We have shown that

\[
\frac{q + s}{s(s + 1)} \leq N_0 \leq N - 1.
\]

This completes the proof of Rédei and Megyesi for the case \(s = 1\). In the remainder of the proof \(s \geq 2\).

If \(j \neq 1\) and \(s\) does not divide \(j\) then \(\sigma_j(y) = 0\) for all \(y \in \text{GF}(q)\) so \(\sigma_j(Y) = 0\). Therefore

\[
R(X, Y) = X^q + \sum_{j=0}^{N_0/s} \sigma_{q-js}(Y)X^{js} + \sigma_{q-1}(Y)X.
\]

In what follows the Hasse derivatives are taken with respect to \(Y\). The \(k\)-th Hasse derivative of \(R(X, Y)\) is \(\mathcal{H}^k_Y(R(X, Y))\) =

\[
= \sum_{(a_1, a_2, \ldots, a_k) \neq (s_1, s_2, \ldots, s_k)} (X + a_1Y - b_1)(X + a_2Y - b_2) \cdots (X + a_kY - b_k)R(X, Y).
\]

For all \((a_i, b_i)\) and \(y \in D\)

\[
X + a_iy - b_i \mid R(X, y) - (X^q - X) = X + \sum_{j=0}^{N_0/s} \sigma_{q-js}(y)X^{js}.
\]

Note that \(\sigma_{q-1}(y) = 0\) for \(y \in D\) as \(R(X, y)\) is an \(s\)-th power.

If we evaluate the equation (1) for \(y \in D\) and multiply by the polynomial above \(k\) times then we get an equality of polynomials in \(X\) the right-hand side of which contains a factor \(R(X, y)\) which divides the left-hand side. That is

\[
R(X, y) \mid (X + \sum_{j=0}^{N_0/s} \sigma_{q-js}(y)X^{js})k\mathcal{H}^k_Y(R)(X, y).
\]

The polynomial

\[
\mathcal{H}^k_Y(R)(X, y) = \sum_{j=0}^{N_0} \mathcal{H}^k_Y(\sigma_{q-j})(y)X^j
\]

has degree at most \(N_0\) so the right-hand side of (2) has degree at most \((k + 1)N_0\).
The polynomial $X + \sum_{j=0}^{N_0/s} \sigma_{q-j}(y)X^j$ is not zero as this would imply $s = 1$. If $(k+1)N_0 \leq q - 1$ then the left hand side of (2) has degree larger than the right-hand side and we conclude that

$$\mathcal{H}_Y^k(\sigma_{q-j})(y) = 0 \text{ for all } 0 \leq j \leq N_0/s.$$ 

Let us assume that $N \leq q/s$.

Now $N_0 \leq N - 1 \leq q/s - 1$ and $(k+1)N_0 \leq sN_0 \leq q - s < q - 1$ whenever $k \leq s - 1$. Hence for $k \leq s - 1$ the $k$-th Hasse derivatives of the polynomials $\sigma_{q-j}$ are zero when evaluated at $y \in D$. We shall show that they are in fact identically zero when $js = N_0$.

It follows immediately from the definition of Hasse derivatives that $\mathcal{H}_Y^{s-1}(f)$ is an $s$-th power for any polynomial $f$. A zero of an $s$-th power is a zero of multiplicity at least $s$. Hence there are at least $sN$ zeros of the polynomial $\mathcal{H}_Y^{s-1}(\sigma_{q-N_0})$. However the degree of this polynomial is less than $q - N_0 < sN_0 < sN$. Hence $\mathcal{H}_Y^{s-1}(\sigma_{q-N_0})(y) \equiv 0$. But $\mathcal{H}_{s-2}(\sigma_{q-N_0})$ is then an $s$-th power, it also has at least $sN$ zeros and is therefore identically zero. We continue by induction. Assume that $\mathcal{H}_{s-i}(\sigma_{q-N_0}) \equiv 0$ for $i = 1, 2, ..., j - 1$. Then $\mathcal{H}_{s-j}(\sigma_{q-N_0})$ is an $s$-th power and if $j < s$ then it has at least $sN$ zeros and is therefore identically zero. Finally for $j = s$ we have that $\sigma_{q-N_0}$ itself is an $s$-th power. However $\sigma_{q-N_0}$ is zero for all $y \notin D$ and so has at least $s(q - N)$ zeros which is far greater than its degree. But $\sigma_{q-N_0} \not\equiv 0$ by assumption, a contradiction. Hence $N \geq q/s + 1$, the lower bound is proved.

Now we are going to prove that $\mathbf{GF}(s)$ is a subfield. Without loss of generality we can assume that $(0,0) \in U$.

Note that

$$\mathcal{H}_X^k(R)(X, y)' = \mathcal{H}_X^k(\sigma_{q-1})(y),$$

where $f'$ is the derivative with respect to $X$, and note that the polynomial

$$\sigma_{q-1}(Y) = \prod_{i=1}^{q}(a_i Y - b_i).$$

Moreover, $y$ is a zero of $\sigma_{q-1}$ exactly $k$ times if and only if the line joining $y$ to $(0,0)$ contains exactly $k$ points, other than $(0,0)$, of $U$.

Let $D^\infty \subseteq D$ be such that for all $y \in D^\infty$ the point $(y)$ is joined to $(0,0)$ by an $s$-secant. Then $\mathcal{H}_Y^k(\sigma_{q-1})(y) = 0$ for all $k = 0, 1, ..., s - 2$ and $\mathcal{H}_Y^{s-1}(\sigma_{q-1})(y) \not\equiv 0$. Hence $\mathcal{H}_Y^{s-1}(R)(X, y) = 0$.

Counting points of $U$ on lines through the origin

$$|D \setminus D^\infty| \leq \frac{q-1-N(s-1)}{s} \leq \frac{q}{s} - 1.$$
18. Directions

Hence \(|D^\infty| \geq N - \frac{q}{s^2} + 1\).

Let \(Q(X)\), a polynomial of degree at most \(sN_0 - q\), be the quotient in the divisibility

\[ R(X, y) \mid (X + \sum_{j=0}^{N_0/s} \sigma_{q- js}(y)X^{js})^{s-1}H_Y^{s-1}(R)(X, y), \]

where \(y \in D^\infty\) and so \(\mathcal{H}_Y^{s-1}(R)(X, y) \neq 0\). Differentiating with respect to \(X\) we get

\[ R(X, y)Q'(X) = (X + \sum_{j=0}^{N_0/s} \sigma_{q- js}(y)X^{js})^{s-1}H_Y^{s-1}(\sigma_{q- 1})(y) - (X + \sum_{j=0}^{N_0/s} \sigma_{q- js}(y)X^{js})^{s-2}H_Y^{s-1}(R)(X, y). \]

The right-hand side of this equation has degree at most \((s-1)N_0 < q\) while if \(Q' \neq 0\) then the left-hand side has degree at least \(q\). We conclude \(Q' = 0\) and

\[ \mathcal{H}_Y^{s-1}(R)(X, y) = \mathcal{H}_Y^{s-1}(\sigma_{q- 1})(y)(X + \sum_{j=0}^{N_0/s} \sigma_{q- js}(y)X^{js}). \]

Extracting \(s\)-th roots and incorporating any constant multiple in the quotient \(Q\) we have

\[ R^{1/s}Q^{1/s} = X + \sum_{j=0}^{N_0/s} \sigma_{q- js}(y)X^{js}. \]

Differentiating again with respect to \(X\) we see \(R^{1/s}(Q^{1/s})' + (R^{1/s})'Q^{1/s} = 1\). Now \(((Q^{1/s})')^{s} \leq N_0/s - 1 + N_0 - q/s < q/s\) and the degree of \(R^{1/s}\) is \(q/s\) so \((Q^{1/s})' = 0\). Therefore \(Q^{1/s}\) and \((R^{1/s})'\) are constant and hence for some \(\gamma \in \text{GF}(q)\)

\[ R(X, y) = \gamma(X + \sum_{j=0}^{N_0/s} \sigma_{q- js}(y)X^{js})^{s}. \]

Now it is easy to check that since

\[ R(X, y) = X^q + \sum_{j=0}^{N_0/s} \sigma_{q- js}(y)X^{js} \]

we have

\[ R(X, y) \in \langle 1, X^s, X^{s^2}, ..., X^{q/s}, X^q \rangle_{\text{GF}(q)}. \]

In particular this implies that \(q\) is a power of \(s\) and equivalently that \(\text{GF}(s)\) is a subfield of \(\text{GF}(q)\).
If \( j \neq s^i \) for some \( i \) then \( \sigma_j(y) = 0 \) for all \( y \in (\text{GF}(q) \setminus D) \cup D^\infty \). By comparing the degree of \( \sigma_j \) with the number of zeros of \( \sigma_j \) we see that \( \sigma_j \equiv 0 \) whenever \( j - 1 \leq q - N + N - q/s^2 + 1 \).

Let \( y \in D \setminus D^\infty \) be such that \( R(X, y) \in \text{GF}(q)[X^t] \setminus \text{GF}(q)[X^s] \). Then \( R(X, y)^{1/s} = X^{q/s} + g(X) \) and by Lemma 5.37 we know that \( g^r \geq \frac{q}{s(s+1)} \). However by the previous paragraph if \( g^r \neq q/s^2 \) then \( g^r < q/s^3 \) which contradicts this. Hence \( g^r = q/s^2 \) and \((g^r)^r < q/s^3 \). If \( s > 2 \) then Lemma 5.41 implies that

\[
R(X, y) \in \langle X^s, X^{s^2}, X^{q/s}, X^q \rangle_{\text{GF}(q)}.
\]

In the final part of the proof we show that \( U \) is a \( \text{GF}(s) \)-linear set.

Let \( D_t \subseteq D \) be the subset of elements of \( D \) for which \( y \in D_t \) implies

\[
R(X, y) \in \text{GF}(q)[X^t] \setminus \text{GF}(q)[X^p].
\]

Counting points of \( U \) on lines incident with a point of \( U \) gives

\[
| \bigcup_{t > s} D_t | \leq \frac{q - 1 - N(s - 1)}{t - s} \leq \frac{q - s^2}{s(t - s)}.
\]

If \( s \neq s^i \) for some \( i \) then \( \sigma_{q-j}(y) = 0 \) for all \( y \in \text{GF}(q) \setminus (\bigcup_{t > s} D_t) \). By degrees \( \sigma_{q-j} \equiv 0 \) for \( j \geq \frac{q-s^2}{s(s-t)} \).

Let \( t > s \) be minimal such that \( D_t \neq \emptyset \) and let \( y \in D_t \). Write

\[
R(X, y) = X^q + g(X) + h(X)^t
\]

where \( g(X) \) has non-zero terms of degree \( s^j \) for some \( j \). We have that

\[
(h^t)^r < \frac{q - s^2}{s(s-t)}.
\]

If \( t \) is not a power of \( s \) then \( s^i < t < s^{i+1} \) for some \( i \). Extracting \( t \)-th roots and following the proof of Lemma 5.37 we get

\[
R^{1/t}(X + g + h^t)h^t.
\]

For \( 1 \leq j \leq i \) we have that

\[
X^{q/s^j} + g^{1/s^j} + h^{1/s^j} = 0 \pmod{R^{1/t}}.
\]

The polynomial \( g^{1/s^j} \) has degree at most \( q/s^{i+1} \) and has terms of degrees that are powers of \( s \). We can reduce \( g \) in the divisibility modulo \( R^{1/t} \) to a polynomial in

\[
\langle X, X^s, X^{s^2}, ..., X^{q/s^{i+1}}, h^{1/s}, ..., h^{1/s^i} \rangle.
\]
Note that
\[ \theta h^o \leq \frac{q - s^2}{s(t - s)} \leq \frac{q}{s^{t+1}}. \]
So the right-hand side of the divisibility has degree less than \( q/t \) after the reduction of \( g \) and is therefore zero. However \( h' \neq 0 \) and so
\[ h^t \in \langle X, X^s, X^{s^2}, \ldots, X^{q/s^{t+1}}, h^{t/s}, \ldots, h^{t/s^i} \rangle \]
which is impossible since \( t \) is not a power of \( s \).

If \( t = s^i \) for some \( i > 1 \) then we go through the same argument replacing \( h' \) by \((g^1/t + h')\) and concluding that some linear combination of
\[ X, X^s, X^{s^2}, \ldots, X^{q/s^{t+1}}, h, h^s, \ldots, h^{s^{i-1}} \]
is zero. It follows from this that
\[ h \in \langle X, X^s, X^{s^2}, \ldots, X^{q/s^i} \rangle. \]

Hence for all \( y \in \mathbb{GF}(q) \) we have \( R(X, y) \in \langle X, X^s, X^{s^2}, \ldots, X^{q} \rangle \).

Let \( \omega \in \mathbb{GF}(q^2) \setminus \mathbb{GF}(q) \) and map \( \mathbb{AG}(2, q) \) to \( \mathbb{GF}(q^2) \) by \((a, b) \mapsto -a \omega + b\). The images of the points of \( U \) under this map are zeros of
\[ R(X, \omega) = \prod_{i=1}^{q} (X + a_i \omega - b_i) \in \langle X, X^s, X^{s^2}, \ldots, X^{q} \rangle_{\mathbb{GF}(q^2)}. \]

Now \( R(X_1 + X_2, \omega) = R(X_1, \omega) + R(X_2, \omega) \) and \( R(\alpha X, \omega) = \alpha R(X, \omega) \) for all \( \alpha \in \mathbb{GF}(s) \).

We will show a more geometric proof for this theorem, see Corollary 21.27.

This result has an analogue for arbitrary dimensional \( k \)-blocking sets of Rédei type:

**Theorem 18.15.** Storme, Sziklai [108] Let \( U \subseteq \mathbb{AG}(n, q) \), \( |U| = q^k \), and let \( D \subseteq H_\infty \) be the set of directions determined by \( U \). If \( D \leq \frac{q+3}{2} q^{k-1} + q^{k-2} + q^{k-3} + \ldots + q^2 + q \), then \( U \) is a \( \mathbb{GF}(p^e) \)-linear set for some subfield \( \mathbb{GF}(p^e) \) of \( \mathbb{GF}(q) \).

Note that this theorem is sharp, as the cone (cylinder), with base the \( q \) affine points of a projective triangle in a plane \( \Pi \not\subset H_\infty \), and with a \((k - 2)\)-dimensional vertex subspace contained in \( H_\infty \setminus \Pi \), has \( q^k \) points and determines \( \frac{q+3}{2} q^{k-1} + q^{k-2} + q^{k-3} + \ldots + q^2 + q + 1 \) directions. For a strong improvement of this result consult Theorems 24.14 and 24.19.
II. Polynomials in geometry

19 Over prime fields: the Gács method

For the $q = p$ prime case, as we have seen in Theorem 18.1, $U \subset \AG(2,p)$ determines either 1 direction (i.e. $U$ is an affine line), or at least $\frac{p^2+3}{2}$ directions. It was possible to characterize equality here already in 1981:

**Theorem 19.1.** (Lovász and Schrijver [91]) For every prime $p > 2$, up to affine transformation there is a unique set of $p$ points in $\AG(2,p)$ determining $\frac{p^2+3}{2}$ directions.

Choosing $d = \frac{q-1}{2}$ in the construction of Megyesi we get an example with $N = \frac{q^2+3}{2}$, so this should be the unique set in the theorem above. Note that the analogue over $\mathbb{R}$, i.e. the union of three halflines $\{(a,0,1), (1,-a,0), (0,1,a) : a \geq 0\} \subset \PG(2,\mathbb{R})$ is still a blocking set. It is also worth to write the (affine part of the) Megyesi example as the graph of the function $X^{\frac{q-1}{2}}$. The analogue of it over $\mathbb{R}$ is the absolute value function $|X|^\frac{q-1}{2}$. Theorem 19.3. Gács [67] For every prime $p$, besides lines and the example characterized by Lovász and Schrijver, any set of $p$ points in $\AG(2,p)$ determines at least $\left[\frac{p^2-1}{3}\right] + 1$ directions.

One may recall Megyesi’s construction 18.2, there $N = q + 1 - d$ where $d|q - 1$ is the size of a multiplicative subgroup of $\GF(q)$. So after $q + 1 - \frac{q-1}{2} = \frac{q^2+3}{2}$ one gets $q + 1 - \frac{q-1}{3} = 2\frac{q-1}{3} + 2$ (whenever $3|q - 1$), so for primes the bound in Theorem 19.3 is one less than a possible sharp result.

The examples of Megyesi are all contained in the union of two lines. This property was characterized by Szönyi. For primes the result can be formulated as follows:
Theorem 19.4. (Szönyi [121]) Suppose $U$ is a set of $p$ points in $\mathbb{A}G(2, p)$, $p$ prime, which is contained in the union of two lines and denote by $N$ the number of determined directions. If $1 < N < p - 1$, then $N = p + 1 - d$ for a $d | p - 1$, and after linear transformation, $U = \{(x, 0) : x \in K\} \cup \{(0, x) : x \notin K\}$, where $K$ is the union of some cosets of the multiplicative subgroup of $\mathbb{G}F(p)$, of order $d$.

For another description of pointsets covered by two lines see Theorem 9.32 of Biró from [28] as well, which also shows the limits of the method we are using.

From now on our underlying field will be $\mathbb{G}F(p)$, where $p$ is a prime. For any polynomial $f$, $N = N_f$ will denote the number of directions $f$ determines. As it was pointed out in the section on symmetric polynomials, if $f$ and $g$ are affine transforms of each other (that is $f(X) = ag(bX + c) + dX + e$, where $a, b, c, d, e \in \mathbb{F}$, $a, b \neq 0$), or if $f$ and $g$ are bijective and $f^{-1} = g$, then $N_f = N_g$ and $W_f = W_g$.

Our next duty is to recall the parameter $W_f$ on polynomials over finite fields (introduced in Section 9.4), which has a close relationship with $N$ as $W_f + N_f \geq p + 1$ (see Lemma 9.31), and which will help us to take the advantages of the algebraic terminology:

$$W_f = \min\{k + l : \sum_{x \in \mathbb{G}F(p)} x^k f(x)^l \neq 0\}.$$  

Here $k$ and $l$ are non-negative integers; for $k = 0$ or $l = 0$, $X^0$ or $f(X)^0$ is defined to be the polynomial 1. Remember that $W_f$ is the smallest $k + l$, for which $X^k f(X)^l$ has reduced degree $p - 1$.

Throughout this section the result of Exercise 5.7 will be used without mentioning it; i.e. for any subspace $V$ of $\mathbb{G}F(q)[X]$, $\text{dim}(V) = |\{\deg(f) : f \in V\}|$.

Theorem 19.3 will be proved, in a slightly more general form, as Theorem 19.6. We will follow the arguments of Ball-Gács-Sziklai [17] in the following sections.

There are some natural ways to generalize Theorem 19.3. One is to consider the problem in $\mathbb{A}G(2, q)$ for any prime-power $q$. After the classification result in [43, 9] (see Theorem 18.14) for the case $N < \frac{q + 3}{2}$, one should ask, whether Theorem 19.3 is true in general and is there a gap in the possible values of $N$ after $\frac{q + 3}{2}$. A proof is known for the case $q = p^2$ only.

Proposition 19.5. (Gács-Lovász-Szönyi) For any prime $p$, in $\mathbb{A}G(2, p^2)$ the only point set determining $\frac{p^2 + 3}{2}$ directions is the one coming from Example 18.2. There are no examples for $\frac{p^2 + 3}{2} < N < \frac{p^2 + p}{2} + 1$.

This result is sharp, there is a construction by Polverino, Szönyi and Weiner [102] for a pointset determining $\frac{q + 1}{2} + 1$ directions, whenever $q$ is a square.
19.1 Permutation polynomials

Let \( p \) be a prime. We say that \( f \in \text{GF}(p)[X] \) is a permutation polynomial if the mapping \( x \mapsto f(x) \) is a permutation of \( \text{GF}(p) \), and by \( M_f \) we denoted the number of elements \( a \in \text{GF}(p) \) for which \( f(X) + cX \) is a permutation polynomial. The connection with the directions determined by \( f(X) \) is straightforward. Namely, the set of parallel lines defined by the equation \( cX_1 + X_2 = a \), where \( a \) runs through the elements of \( \text{GF}(p) \), all contain exactly one point of the graph of \( f \) if and only if \( f(X) + cX \) is a permutation polynomial. Thus the direction of these lines is not a direction determined by \( f \). Hence \( M_f + N_f = p \).

Therefore the Rédei-Megyesi result 18.1 says that if \( M_f \geq (p - 1)/2 \) then \( f(X) = cX + d \) for some \( c, d \in \text{GF}(p) \); in other words, the graph of \( f \), \( \{(x, f(x)) : x \in \text{GF}(p)\} \), is a line.

Similarly Theorem 19.3 says that if \( M_f \geq 2\lceil p^{1/2}\rceil + 1 \), then \( (f(X) - (cX + d))(f(X) - (bX + e)) = 0 \) for some \( b, c, d, e \in \text{GF}(p) \); in other words, the graph of \( f \) is contained in the union of two lines. The new method, invented by Gács was very fruitful, it became the key technique of other results as well, see below.

In the Megyesi examples 18.2, \( G \) is a multiplicative subgroup of \( \text{GF}(p) \) of size \( d \) and \( f(X) = X \chi_G(X) \), where \( \chi_G(X) \) is the characteristic function of \( G \). Here if \( 1 < d < q - 1 \) then \( M_f = d - 1 \).

In Theorem 19.4 Szönyi proved that if the graph of \( f \) is contained in the union of two lines and \( M_f \geq 2 \), then the graph of \( f \) is affinely equivalent to a generalised example of Megyesi detailed above. In the generalised Megyesi example \( G \) can be replaced by a union of cosets of a multiplicative subgroup of \( \text{GF}(p) \). In the generalised example the value of \( M_f \) is again \( d - 1 \) for some divisor \( d \) of \( p - 1 \).

Thus, the above results imply that, either \( M_f \leq 2\lceil p^{1/2}\rceil \), \( f \) is affinely equivalent to \( X \chi_G(X)^{-1/2} \), or \( f \) is linear.

In Theorem 19.6 and on, we will follow [17] when proving a version of the “planar” Gács result. Then in Theorem 19.15 a “3-dimensional” version will be stated. We shall prove that if there are more than \( (2\lceil p^{1/2}\rceil + 1)(p + 2\lceil p^{1/2}\rceil))/2 \approx 2p^2/9 \) pairs \( (c, d) \in \text{GF}(p)^2 \) with the property that \( x \mapsto f(x) + cg(x) + dx \) is a permutation of \( \text{GF}(p) \) then there are elements \( a, b, c \in \text{GF}(p) \) such that \( f(x) + ag(x) + bx + c = 0 \), for all \( x \in \text{GF}(p) \); in other words the graph of \( (f, g) \), \( \{(x, f(x), g(x)) | x \in \text{GF}(p)\} \), is contained in a plane.

The situation is analogous to the planar case. The set of parallel planes defined by the equation \( dX_1 + X_2 + cX_3 = a \), where \( a \) runs through the elements of \( \text{GF}(p) \), all contain exactly one point of the graph of \( (f, g) \) if and only if \( f(X) + cg(X) + dX \) is a permutation polynomial.
19. Over prime fields: the Gács method

19.2 Directions in the plane

In [67] it was proved that if \( M_f > (p-1)/4 \) and \( W_f \geq 2\left\lceil \frac{p-1}{6} \right\rceil + 2 \) then the graph of \( f \) is contained in the union of two lines.

Let

\[
\pi_k(Y) = \sum_{x \in \mathbb{GF}(p)} (f(x) + xY)^k.
\]

It’s a simple matter to check (see Section 5.1), that if \( x \mapsto f(x) + ax \) is a permutation then \( \pi_k(a) = 0 \) for all \( 0 < k < p - 1 \). Since the polynomial \( \pi_k(Y) \) has degree at most \( k - 1 \) (the coefficient of \( Y^k \) is \( \sum_{x \in \mathbb{GF}(p)} x^k = 0 \) it is identically zero for all \( 0 \leq k - 1 < M_f \), unless \( M_f = p - 1 \) in which case \( f \) is linear. Hence if \( f \) is not linear then \( W_f - 1 \geq M_f \).

The original proof of Theorem 19.3 [67] showed that if \( M_f \geq 2\left\lceil \frac{p-1}{6} \right\rceil + 1 \), then the graph of \( f \) is contained in the union of two lines.

In this section we shall prove the following, slightly stronger theorem.

**Theorem 19.6.** [17] If \( M_f \geq (p-1)/6 \) and \( W_f \geq 2\left\lceil \frac{p-1}{6} \right\rceil + 2 \) then the graph of \( f \) is contained in the union of two lines.

The values \( W_f \) and \( M_f \) are invariant under affine transformations and inversion. Replacing \( f \) by its inverse is the transformation which switches coordinates, in other words if we switch coordinates then the graph of \( f \), \( \{(x, f(x)) \mid x \in \mathbb{GF}(p)\} \), becomes the graph of \( f^{-1} \). Let \( E(f) \) denote the set of all polynomials that can be obtained from \( f \) by applying affine transformations and inversions.

Let \((f^i)^{\circ}\) be the degree of the polynomial \( f^i \) modulo \( X^p - X \). Unless stated otherwise all equations are to be read modulo \( X^p - X \).

Note that for any polynomial \( g \) of degree less than \( p \) the sum \( -\sum_{x \in \mathbb{GF}(p)} g(x) \) is equal to the coefficient of \( X^{p-1} \) of \( g \).

**Lemma 19.7.** If \( 3 \leq f^o \leq (p-1)/2 \) then \( W_f \leq (p+1)/3 \).

**Proof:** Write \( p - 1 = af^o + b \) with \( 0 \leq b < f^o \). The degree of \( f(X)^aX^b \) is \( p - 1 \), so we have \( W_f \leq a + b \).

If \( f^o = 3 \) then \( a + b \leq (p-2)/3 + 1 = (p+1)/3 \).

If \((p+1)/3 \leq f^o \leq (p-1)/2\) then \( a + b = 2 + p - 1 - 2f^o \leq (p+1)/3 \).

If \((p+1)/4 \leq f^o \leq (p-1)/3 \) then \( a + b = 3 + p - 1 - 3f^o \leq 3 + p - 1 - 3(p+1)/4 = (p+1)/4 + 1 \leq 1 \) for \( p \geq 11 \).

If \( 4 \leq f^o \leq (p+1)/4 \) then \( a + b \leq (p-b-1)/f^o + b \leq p/f^o + (bf^o - b - 1)/f^o \leq p/f^o + f^o - 2 \). This is at most \( (p+1)/3 \) if and only if the quadratic inequality \( 3(f^o)^2 - (p + 7)f^o + 3p \leq 0 \) is satisfied. For \( p \geq 20 \), the inequality is satisfied for both \( f^o = 4 \) and \( f^o = (p+1)/4 \), so it holds for all values between 4 and \( (p+1)/4 \).
For $p < 20$ a case by case analysis suffices to show that $a + b \leq (p + 1)/3$.

Note that for $f^o = 2$ we have $W_f = (p - 1)/2$ and $M_f = 0$ and for $f^o = 1$ we have $W_f = p - 1$ and $M_f = p - 1$.

**Lemma 19.8.** If $f^o = (p+1)/2$ then either $W_f \leq (p+5)/4$ or $f$ is affinely equivalent to $X^{p+1}/2$.

**Proof:** After applying a suitable affine transformation we can suppose that $f(X) = X^{f^o} + g(X)$ where $g^o \leq (p - 3)/2$.

If $g^o \leq 1$ then by applying another linear transformation we can subtract $g$ from $f$ and hence $f$ is affinely equivalent to $X^{f^o}$.

Suppose $g^o \geq 2$. Write $(p - 3)/2 = ag^o + b$ with $0 \leq b < g^o$ and consider the polynomial

$$f(X)^{a+1}X^b = \sum_{i=0}^{a+1} \binom{a+1}{i} X^{i\frac{p+1}{2}+b}g(X)^{a+1-i}.$$ 

We claim that the only term in the sum that has a term of degree $X^{p-1}$ (modulo $X^p - X$) is $g(X)^{(2)g^o} - X^{b+1}$. Let $r(X) = g(X)^{(2)g^o} + X^{b+1}$ (modulo $X^p - X$), a typical term in the sum (note that all the binomial coefficients are non-zero). If $i$ is even then $r(X) = g(X)^{(2)g^o} + X^{b+1}$, which has degree $(a + 1 - i)g^o + b + i = (p - 3)/2 + g^o - (g^o - 1)i < p - 1$. If $i \neq 1$ is odd then $r(X) = g(X)^{(2)g^o} + (p - 1)/2 + b + p - 2 + g^o - (g^o - 1)i < p - 1$.

Hence $f(X)^{a+1}X^b$ has degree $p - 1$ which implies $W_f \leq a + b + 1$.

Finally, note that $a + b \leq (p - 3)/(2g^o) + g^o - 1$, which is at most $(p + 1)/4$ if $2 \leq g^o \leq (p - 3)/4$. If $g^o > (p - 3)/4$ then $a = 1$ and $b = (p - 3)/2 - g^o < (p - 3)/4$ and so $a + b < (p + 1)/4$.

Let $s = \lceil (p - 1)/6 \rceil$.

We will assume from now on that $W_f \geq 2s + 2$. By the definition of $W_f$ the sum

$$\sum_{x \in GF(p)} x^bf(x)$$

has no term of degree $X^{p-1}$, for all $k = 0, 1, \ldots, 2s$, and therefore the degree of $f$ is at most $p - 2s - 2$. By Lemma 19.7 and Lemma 19.8 the degree of $f$ is at least $(p + 3)/2$.

**Lemma 19.9.** There is polynomial in $h \in E(f)$ with one of the following properties. Either

(i) for all $i$ such that $1 \leq i \leq 2s$, $(h^i)^o \leq h^o + i - 1$ and $(h^2)^o = h^o + 1$, or
(ii) for all $i$ such that $1 \leq i \leq 2s$, $(h^i)^o \leq (h^2)^o + i - 2$ and $(h^3)^o = (h^2)^o + 1$, and $h$ has no root in $GF(p)$.

**Proof:** Let

$$d(f) = \max\{(f^i)^o - i \mid 1 \leq i \leq 2s\}$$

and let $d = d(f_1)$ be maximal over all polynomials in $E(f)$. The fact that $f^o \geq (p + 3)/2$ implies that $d \geq (p + 1)/2$.

Let $\pi(Y) = \pi_{p-1-d}(Y)$. The coefficient of $Y^{p-1-d-j}$ is $(p-1-d)\sum_{x \in GF(p)} x^{p-1-d-j} f^j$ which, by the definition of $d$, is non-zero for at least one $j$ where $1 \leq j \leq 2s$. Hence $\pi(Y) \neq 0$.

If for all $a$ such that $f(X) + aX$ is a permutation polynomial we have $\pi(a) = \pi'(a) = \pi''(a) = 0$ then $(Y - a)^3$ divides $\pi(Y)$ and since $M_f \geq (p - 1)/6$ the degree of $\pi$, $\pi^o = p - 1 - d \geq 3M_f \geq (p - 1)/2$ which isn’t the case.

Since $0 < p - 1 - d < p - 1$ we have already seen that $\pi(a) = 0$, so either $\pi'(a) \neq 0$ or $\pi''(a) \neq 0$ for some $a$.

Let $f_2$ be the inverse of the function $f(X) + aX$.

If

$$0 \neq \pi'(a) = -(d + 1) \sum_{x \in GF(p)} x(f + ax)^{p-2-d}$$

then $\sum_{z \in GF(p)} f_2(z)z^{p-2-d} \neq 0$ and so $f_2^o \geq d + 1$. By the maximality of $d$, $f_2^o = d + 1$ and so $(f_2^2)^o - i \leq f_2^2 - 1$. If $(f_2^2)^o \leq f_2^o$ then let $f_3 = f_2 + cX$ where $c$ is chosen so that $(f_3^2)^o \geq f_3^2 + 1$ and $f_3$ is not a permutation polynomial. Note that $f_3^2 = f_2^2 + 2cXf_2 + c^2X^2$.

If

$$0 \neq \pi''(a) = (d + 1)(d + 2) \sum_{x \in GF(p)} x^2(f + ax)^{p-3-d}$$

then $\sum_{z \in GF(p)} (f_2(z))^2z^{p-3-d} \neq 0$ and so $(f_2^3)^o \geq d + 2$. By the maximality of $d$, $(f_2^3)^o = d + 2$ and so $(f_3^2)^o - i \leq (f_3^2)^o - 2$. If $(f_3^2)^o \leq (f_3^2)^o$ then let $f_3 = f_2 + cX$ where $c$ is chosen so that $(f_3^2)^o \geq (f_3^2)^o + 1$ and $f_3$ is not a permutation polynomial.

Finally, let $e$ be an element not in the image of $f_3$ and let $f_4 = f_3 - e$. Then $f_4$ has no root in $GF(p)$.

**Lemma 19.10.** There is a polynomial in $h \in E(f)$ for which there exist polynomials $F$, $G$ and $H$, where $H^o - 2 = F^o - 1 = G^o = r \leq s - 2$, $(F,G) = 1$ and

$$Fh + Gh^2 = H.$$
Note that this implies that \( h \) satisfies the conditions of Lemma 19.9 (i).

**Proof:** Let \( h \) be a polynomial satisfying the conditions of Lemma 19.9. Since \( W_h \geq 2s + 2 \) we have \((h^i)^o \leq p - 2s - 3 + i\).

Define subspaces of the vector space of polynomials of maximum degree \( p - 1 \)

\[
\psi_j = \{ Fh + Gh^2 \mid F^o \leq j, \ G^o \leq j - 1 \},
\]

where \( j \leq s - 1 \). If there are polynomials \( F \) and \( G \) such that \( Fh + Gh^2 = 0 \) then since \( h \) has no root \( F + Gh = 0 \) which is impossible since \((hG)^o \) is at least \( 3s \) and at most \( 5s - 3 < p - 1 \). Thus the dimension of \( \psi_j \) is \( 2j + 1 \).

Since \( W_h \geq 2s + 1 \) and \( 2(j + 1) \leq 2s \), the sum over \( GF(p) \) of the evaluation of the product of any two elements of \( \psi_j \) is zero, hence the sum of the degrees of any two elements of \( \psi_{s - 1} \) is not equal to \( p - 1 \). The maximum degree of any element of \( \psi_{s - 1} \) is \( p - s - 3 \) and so only half of the degrees in the interval \([s + 2, \ldots, p - 1 - (s + 2)]\) can occur. But \( \dim \psi_{s - 1} = 2s - 1 > (p - 1 - (s + 2) - (s + 1))/2 \) and so there is an element \( H \) of degree at most \( s + 1 \) in \( \psi_{s - 1} \).

Let \( H \) be of minimal degree, so \((F, G) = 1\).

If \( h \) satisfies case (i) of Lemma 19.9 then \((h^2)^o = h^o + 1 \) and \( r = G^o = F^o - 1 \). Moreover \( Fh^2 + Gh^3 = Hh \) and \((h^3)^o \leq h^2 + 2 \) implies \( H^o \leq r + 2 \).

If \( h \) satisfies case (ii) of Lemma 19.9 then \((h^3)^o = (h^2)^o + 1 \geq h^o + 2 \) and \((h^4)^o \leq (h^2)^o + 2 \). Let \( F^o = r + 1 \) and so \( G^o \leq r \). The equation \( Fh^3 + Gh^4 = Hh^2 \) implies \( H^o \leq r + 2 \). If \( G^o \leq r - 1 \) then \( Fh^2 + Gh^3 = Hh \) implies \( r + 2 + h^o \geq H^o + h^o = r + 1 + (h^2)^o \) and so \((h^2)^o = h^o + 1 \). But then \( Fh + Gh^2 = H \) implies \( G^o = r \).

Either way we have \( r = G^o = F^o - 1 \geq H^o - 2 \).

Let \( r_1 = h + aX \) and \( F_1 = F - 2aXG, G_1 = G \) and \( H_1 = H - a^2X^2G + aXF \). Then \( F_1r_1 + G_1r_1^2 = H_1 \) and we can choose \( a \) so that \( H_1 \) has degree \( r + 2 \). Now when we look at \( \psi_{r+1} \) for \( r_1 \) we find \( F_1, G_1 \) and \( H_1 \) as required. Note that \((F, G) = 1\) implies \((F_1, G_1) = 1\).

We wish to prove \( r = 0 \). So let us assume \( r \geq 1 \) and define \( i \) to be such that \((i - 2)r + 1 \leq s < (i - 1)r + 1 \) for \( r \geq 2 \) and \( s \) for \( r = 1 \). Note that \( r \leq s - 2 \) implies \( i \geq 3 \) and that \( s + r - 1 \leq 2s - i \) if \( i = 3 \) or \( i = s \) and also if both \( i \geq 4 \) and \( r \geq 2 \), since \( r \leq (s - 1)/2 \) and \( i \leq (s - 1)/2 \).

**Lemma 19.11.** There is a polynomial \( h \in E(f) \) and a polynomial \( G \), where \( G^o = r \leq s - 2 \), such that for all \( j = 2, \ldots, i \), there is an \( F_j \) and an \( H_j \) with the property that \((F_j, G) = 1\),

\[
F_jh + G^{i - 1}h^i = H_j,
\]

\[
F_j^o \leq (j - 1)(r + 1), \ H_j^o \leq (j - 1)r + j \ and \ H_j^o = (i - 1)r + i.
\]

**Proof:** Let \( r_1 \) satisfy the conditions of Lemma 19.10. We start by proving that there is an \( h \in E(f) \) for which \((h^{i - 1})^o \geq h^o + i - 2\).
If $(r_1^{-1})^o \leq r_1^o + i - 3$ then let $h = r_1 + aX$. Choose $a$ so that $h^{i-1} = \sum_{j=0}^{i-1} (i-j)(aX)^{i-j-1}r_1^j$ has degree at least $h^o + i - 2$ while at the same time the degree of $F - 2aXG$ is $r + 1$ and the degree of $H - a^2X^2G + aXF$ is $r + 2$.

We will prove the lemma by induction. Lemma 19.10 implies that for $j = 2$ we can take $F_2 = F$ and $H_2 = H$.

Define $F_j = -(F_{j-1}F + H_{j-1}G)$ and $H_j = -HF_{j-1}$. It can be checked by induction, multiplying by $Gh$ and using $Gh^2 = H - Fh$, that

$$F_jh + G^{j-1}h^j = H_j.$$

The degrees satisfy $F_j^o \leq (j-1)(r+1)$ and $H_j^o \leq (j-1)r + j$ and $(F_j, G) = 1$, since $(F, G) = 1$ by Lemma 19.10 and $(F_{j-1}, G) = 1$ by induction.

Now $(h^{i-1})^o \geq h^o + i - 2$ and the equation $F_{i-1}h + G^{i-2}h^{i-1} = H_{i-1}$ implies that $F_{i-1}^o \geq (i-2)(r+1)$ and so $F_{i-1}^o = (i-2)(r+1)$. Finally $H_i = -HF_{i-1}$ implies $H_i^o = (i-1)r + i$.

Let $h$ satisfy the conditions of Lemma 19.11. Note that this implies that $h$ satisfies the conditions of Lemma 19.10 and Lemma 19.9 (i). Define

$$\phi_j = \{Ah+Bh^i \mid A^o \leq j, \ B^o \leq j + 1 - i\}.$$

Note that $H_i \in \phi_{(i-1)r+i-1}$ and that $(i-1)r + i - 1 \leq s + r + i - 2 \leq 2s - 1$.

**Lemma 19.12.** For $j \leq 2s-1$ all polynomials of $\phi_j$ have degree at least $H_i^o$ and those of degree at most $p - 2 - h^o$ are multiples of $H_i$.

**Proof:** If $Ah + Bh^i = 0$ then, since $h$ has no root in GF$(p)$, $A + Bh^{i-1} = 0$. The degree of $Bh^{i-1}$ is at most $p - 4$ and at least $(p+3)/2$ and so $A = B = 0$. Thus the dimension of $\phi_j$ is $2j + 3 - i$.

Suppose that $\phi_j$ contains a polynomial $C$ of degree $n$ but no polynomial of degree $n+1$. Then $\phi_{j+1}$ contains a polynomial of degree $n+1$, $X \cdot C$ for example, and a polynomial of degree one more than the maximum degree of an element of $\phi_j$. However $\dim \phi_{j+1} = \dim \phi_j + 2$, so $n$ is unique. Moreover, the polynomials of degree $n+1$ in $\phi_{j+1}$ are multiples of a polynomial of degree $n$ in $\phi_j$.

Since $j \leq 2s - 1$, $\phi_j$ contains no element of degree $p - 1 - h^o$. Now $H_i \in \phi_{(i-1)r+i-1}$ and is a polynomial of degree less than $p - 1 - h^o$. It is not a multiple of any polynomial in $\phi_j$ for $j < (i-1)r+i-1$, since if it were there would be a non-constant polynomial $K$ and polynomials $A$ and $B$ with the property that $(KA)h + (KB)h^i \in \phi_{(i-1)r+i-1}$, with $(KA)^o \leq (i-1)r+i-1$ and $(KB)^o \leq (i-1)r$, which would be a constant multiple of $H_i$. This is not possible since $(F_i, G) = 1$. Thus all polynomials in $\phi_j$ of degree at most $p - 2 - h^o$ are multiples of $H_i$ and in particular have degree at least $H_i^o$. 


The following lemma contradicts the previous one which implies that our assumption that \( r \geq 1 \) was incorrect.

**Lemma 19.13.** There is a non-zero polynomial of degree less than \( H_i^o \) in \( \phi_j \) for some \( j \leq 2s - 2 \).

**Proof:** Suppose \( r \geq 2 \) and so \( i \leq s \). Let
\[
\Delta = \{A^i + B_2h^2 + \ldots + B_{i-1}h^{i-1} + Ch^i \mid A^o \leq s - 1, B^o \leq r - 1, C^o \leq s - i\}.
\]
Since \( W_h \geq 2s + 1 \) the sum of the degrees of any two elements of \( \Delta \) is not equal to \( p - 1 \). The maximum degree of any element of \( \Delta \) is \( p - s - 3 \) and so only half of the degrees in the interval \([s + 2, \ldots, p - 1 - (s + 2)]\) can occur, in other words at most \( \lfloor (p - 4 - 2s)/2 \rfloor \leq 2s - 2 \) of the degrees in this interval occur. If \( \dim\Delta = (i - 2)r + 2s - i + 1 \) then there is a polynomial
\[
E = Ah + B_2h^2 + \ldots + B_{i-1}h^{i-1} + Ch^i
\]
in \( \Delta \) of degree at most \( s + 2 - ((i - 2)r + 2s - i + 1 - (2s - 2)) = s - (i - 2)r + i - 1 \). If \( \dim\Delta < (i - 2)r + 2s - i + 1 \) then \( E = 0 \in \Delta \) non-trivially. Either way there is a polynomial \( E \in \Delta \) with not all \( A, B, C \) zero where \( E^o \leq s - (i - 2)r + i - 1 \).

Substituting \( G^{i-1}h^i = H_j - hF_j \) we have
\[
G^{i-2}E = G^{i-2}Ah + CG^{i-2}h^i + \sum_{j=2}^{i-1} B_j G^{i-1-j}(H_j - hF_j)
\]
and rearranging
\[
G^{i-2}E - \sum_{j=2}^{i-1} B_j G^{i-1-j}H_j = (G^{i-2}A - \sum_{j=2}^{i-1} B_j F_j G^{i-1-j})h + CG^{i-2}h^i.
\]
Checking the degrees on the right-hand side we see that the left-hand side is a polynomial in \( \phi_j \) for some \( j \leq 2s - 2 \).

The degree of the left-hand side is at most \( \max\{s + i - 1, ir - r + i - 2\} \) which is less than \( H_i^o = (i - 1)r + i \).

If \( r = 1 \) then take \( i = s \) and define \( \Delta \) as above. There is a polynomial \( E \) in \( \Delta \) of degree at most \( s + 1 \) and the degree of \( G^{i-2}E \) is at most \( 2s - 1 \) which is the degree of \( H_s \). If we have equality then by Lemma 19.12 the polynomial
\[
(G^{s-2}A - \sum_{j=2}^{s-1} B_j F_j G^{s-1-j})h + CG^{s-2}h^s
\]
is a constant multiple of \( F_s h + G^{s-1}h^s \) which implies \( CG^{s-2} \) is a constant multiple of \( G^{s-1} \) which it is not since one has degree \( s - 2 \) and the other \( s - 1 \).
19. Over prime fields: the Gács method

We can now prove Theorem 19.6.

**Proof:** By the previous lemmas there exist polynomials \( h \in E(f) \) and \( F \) of degree 1 and \( H \) of degree 2 such that \( h^2 + Fh = H \). Thus \( (h + F/2)^2 = H + F^2/4 \). All values of \( H + F^2/4 \) are squares and so \( H + F^2/4 = (aX + b)^2 \). Hence \((h + F/2 - aX - b)(h + F/2 + aX + b) = 0 \) and the graph of \( h \) (and so the graph of \( f \) too) is contained in the union of two lines.

### 19.3 Linear combinations of three permutation polynomials

Let \( M(f, g) \) be the number of pairs \((a, b) \in \text{GF}(p)^2\) for which \( f(X) + ag(X) + bX \) is a permutation polynomial. Let

\[
W(f, g) = \min\{k + l + m \mid \sum_{x \in \text{GF}(p)} x^k f(x)^l g(x)^m \neq 0 \}.
\]

Let again \( s = \lceil \frac{p-1}{e} \rceil \). Before we prove the main result of this section we need the following lemma.

**Lemma 19.14.** [17] If \( M(f, g) > (2s+1)(p+2s)/2 \) then \( W(f, g) \geq 2s + 2 \) or there are elements \( c, d, e \in \text{GF}(p) \) such that \( f(x) + cg(x) + dx + e = 0 \) for all \( x \in \text{GF}(p) \).

**Proof:** Let \( \pi_k(Y, Z) = \sum_{x \in \text{GF}(p)}(f(x) + g(x)Y + xZ)^k \).

By Section 5.1, if \( f(X) + ag(X) + bX \) is a permutation polynomial then \( \pi_k(a, b) = 0 \) for all \( 0 < k < p - 1 \). Write

\[
\pi_k = \prod \sigma_j(Y, Z),
\]

where each \( \sigma_j \) is absolutely irreducible. Then \( \sum \sigma_j^2 = \pi_k^2 \leq k \).

Let \( N_j \) be the number of solutions of \( \sigma_j(a, b) = 0 \) in \( \text{GF}(p) \) for which \( f(X) + ag(X) + bX \) is a permutation polynomial.

If \( \lambda \sigma_j \in \text{GF}(p)[Y, Z] \), for some \( \lambda \) in an extension of \( \text{GF}(p) \), and \( \sigma_j^2 \geq 2 \) then by Theorem 10.9(i) \( N_j \leq \sigma_j^2(p + \sigma_j^2 - 1)/2 \).

Suppose \( \sigma_j^2 = 1 \) and there are at least \((p + 1)/2\) pairs \((a, b)\) for which \( \sigma_j(a, b) = 0 \) and \( f(X) + ag(X) + bX \) is a permutation polynomial. Let \( \sigma_j = \alpha Y + \beta Z + \gamma \).

If \( \alpha \neq 0 \) then there are \((p + 1)/2\) elements \( b \in \text{GF}(p) \) with the property that \( \alpha f(X) - (\beta b + \gamma) g(X) + boX = \alpha f(X) - \gamma g(X) + b(\alpha X - \beta) \) is a permutation polynomial. By Rédei and Megyesi’s theorem mentioned in the introduction, this implies that \( \alpha f(X) - \gamma g(X) \) is linear and hence there are elements \( c, d, e \in \text{GF}(p) \) such that \( f(x) + cg(x) + dx + e = 0 \) for all \( x \in \text{GF}(p) \). If \( \alpha = 0 \) then there are \((p + 1)/2\) elements \( a \in \text{GF}(p) \) with the property that \( \beta f(X) - \gamma X + a \beta g(X) \) is a permutation polynomial. The set of \( p \) points \( \{(\beta f(x) - \gamma x, \beta g(x)) \mid x \in \text{GF}(p)\} \)
may not be the graph of a function but it is a set of \( p \) points that does not determine at least \((p + 1)/2\) directions. Thus it is affinely equivalent to a graph of a function that does not determine at least \((p - 1)/2\) directions and so by Rédéi and Megyesi’s theorem, it is a line. Hence, there are elements \( c, d \) and \( e \) with the property that \( c(βf(x) − γx) + dβg(x) + e = 0 \) for all \( x ∈ GF(p) \). Thus, either there are elements \( c, d, e ∈ GF(p) \) such that \( f(x) + cg(x) + dx + e = 0 \) for all \( x ∈ GF(p) \) or \( N_j ≤ (p - 1)/2 \).

Suppose \( λσ_j ∉ GF(p)[Y, Z] \) for any \( λ \) in any extension of \( GF(p) \). The polynomials \( σ_j = ∑α_{nm}Y^nZ^m \) and \( π_j = ∑α'_{nm}Y^nZ^m \) have at most \((σ_j)^2\) zeros in common by Bézout’s theorem. However if \((y, z) ∈ GF(p)^2 \) and \( σ_j(y, z) = 0 \) then \( τ_j(y, z) = 0 \). Hence

\[
N_j ≤ (σ_j)^2 ≤ σ_j^2(p + σ_j - 1)/2,
\]

whenever \( σ_j^2 ≤ (p - 1)/2 \).

Thus if \( π_k ≠ 0 \) and \( k ≤ (p - 1)/2 \) then \( N(π_k) \), the number of solutions of \( π_k(y, z) = 0 \) in \( GF(p) \) for which \( f(X) + ag(X) + bX \) is a permutation polynomial, satisfies

\[
N(π_k) ≤ ∑ N_j ≤ ∑ σ_j^2(p + σ_j - 1)/2 ≤ k(p - 1)/2 + 1/2 \sum (σ_j^2)^2 ≤ k(p - 1)/2 + 1/2 (\sum σ_j^2)^2 = (k(p - 1) + k^2)/2.
\]

By hypothesis \( π_k ≡ 0 \) or

\[
(2s + 1)(p + 2s)/2 < N_k ≤ (k(p - 1) + k^2)/2,
\]

which gives \( k ≥ 2s + 2 \). Now

\[
π_k(Y, Z) = ∑_{l=0}^{k} ∑_{m=0}^{k-l} \binom{k}{l} \binom{k-l}{m} \left( ∑_{x ∈ GF(p)} x^{k-l-m}f(x)^lg(x)^m \right) Y^m Z^{k-l-m},
\]

and so \( W(f, g) ≥ 2s + 2 \).

**Theorem 19.15.** [17] If \( M(f, g) > (2s + 1)(p + 2s)/2 \) then there are elements \( c, d, e ∈ GF(p) \) such that \( f(X) + cg(X) + dX + e = 0 \).

**Proof:** If \( p = 3 \) and \( M(f, g) > (2s + 1)(p + 2s)/2 = 15/2 \) then there is a \( c \) such that \( f(X) + cg(X) + bX \) is a permutation polynomial for all \( b ∈ GF(p) \), which can only occur if there is a constant \( e \) such that \( f(X) + cg(X) + e = 0 \).

So suppose \( p ≥ 5 \) and that there are no elements \( c, d, e ∈ GF(p) \) with the property that \( f(X) + cg(X) + dX + e = 0 \).

Clearly \( W_{f+ag} ≥ W(f, g) \) for all \( a ∈ GF(p) \) and \( W(f, g) ≥ 2s + 2 \) by Lemma 19.14.
There is an $a_1 \in \mathbb{GF}(p)$ with the property that
\[ M_{f+a_1g} \geq M(f,g)/p \geq (p-1)/6. \]

By Theorem 19.6 there are constants $c,d,c',d' \in \mathbb{GF}(p)$ with the property that
\[ (f + a_1g + cX + d)(f + a_1g + c'X + d') = 0 \]
so the graph of $(f,g)$, the set of points $\{(x, f(x), g(x)) \mid x \in \mathbb{GF}(p)\}$, is contained in the union of two planes.

By Rédei and Megyesi’s theorem, since we have assumed that the graph of $f + a_1g$ is not a line, $M_{f+a_1g} \leq (p-1)/2$ and so there is an $a_2 \neq a_1$ with the property that
\[ M_{f+a_2g} \geq (M(f,g) - (p-1)/2)/(p-1) \geq (p-1)/6. \]

Thus the graph of $(f,g)$ is contained in the union of two other planes, different from the ones before. The intersection of the two planes with the two planes is four lines and so the graph of $(f,g)$ is contained in the union of four lines.

Similarly, since $(M(f,g) - (p-1)/2)/(p-2) \geq (p-1)/6$ and $(M(f,g) - 3(p-1)/2)/(p-3) \geq (p-1)/6$, there is an $a_3$ and an $a_4$ with that property that $M_{f+a_3g} \geq (p-1)/6$ and $M_{f+a_4g} \geq (p-1)/6$ and so the graph of $(f,g)$ is contained in two other distinct pairs of planes. The four lines span three different pairs of planes and so the graph of $(f,g)$ is contained in the union of two lines and hence a plane, which is a contradiction.

\[ \Box \]

There is an example when $q$ is an odd prime (power) congruent to 1 modulo 3 with $M(f,g) = 2(q-1)^2/9 - 1$ where the graph of $(f,g)$ is not contained in a plane, which shows that the bound is the right order of magnitude.

Let $E = \{ e \in \mathbb{GF}(q) \mid e^{(q-1)/3} = 1 \} \cup \{0\}$. Then the set $S = \{(e,0,0), (0,e,0), (0,0,e) \mid e \in E\}$ is a set of $q$ points. If $\pi$, the plane defined by
\[ X_1 + aX_2 + bX_3 = c, \]
is incident with $(e,0,0)$ for some $e \in E$ then $e \in E$. Likewise if it is incident with $(0,e,0)$ for some $e \in E$ then $a/c \in E$ and if it is incident with $(0,0,e)$ for some $e \in E$ then $b/c \in E$.

If $\pi$ is incident with two points of $S$ then either $a \in E$, $b \in E$ or $a/b \in E$. Thus if $a, b$ and $a/b$ are not elements of $E$ then $\pi$ and all the planes parallel to $\pi$ are incident with exactly one point of $S$. There are $2(q-1)^2/9$ such sets of parallel lines.

If we make a change of coordinates so that $\{x_1 = x \mid x \in \mathbb{GF}(q)\}$ is one such set of parallel planes then there are functions $f$ and $g$ for which $S = \{(x, f(x), g(x)) \mid x \in \mathbb{GF}(q)\}$. Each other set of parallel planes with the above property corresponds to a pair $(a, b)$ such that $f(X) + ag(X) + bX$ is a permutation polynomial. Thus
II. Polynomials in geometry

\[ M(f, g) = 2(q - 1)^2 / 9 - 1. \] Explicitly the functions \( f \) and \( g \) can be defined by
\[ f(x) = \chi_H(x)x \text{ and } g(x) = \chi_{\varepsilon H}(x)x, \] where \( \chi_H \) is the characteristic function of \( H = \{ t^3 \mid t \in \text{GF}(p) \} \) and \( \varepsilon \) is a primitive third root of unity.

20 Projective linear pointsets

In Section 18.3 we defined affine linear pointsets. The general geometric definition in the projective case is the following:

**Definition 20.1.** A pointset \( B \subseteq \text{PG}(n, q) \) is called \( \text{GF}(p^e) \)-linear if

(i) \( \text{GF}(p^e) \) is a subfield of \( \text{GF}(q) \), and

(ii) there is a projective space \( \text{PG}(n', q) \) containing \( \text{PG}(n, q) \) such that \( B \) is a projection of a subgeometry \( \text{PG}(t, p^e) \subset \text{PG}(n', q) \) from a suitable subspace ("vertex" or "center") \( V \) to \( \text{PG}(n, q) \).

Note that here \( \dim V = n' - n - 1 \) and the projection is not necessarily one-to-one.

Projective linear pointsets are more complicated than affine ones. One way of the algebraic description is that \( B \) is \( \text{GF}(p^e) \)-linear iff one can choose \( t + 2 \) points (vectors) \( \underline{v}_0, \underline{v}_1, ..., \underline{v}_{t+1} \) of \( \text{PG}(n, q) \) such that \( B \) is the "span" of them over \( \text{GF}(p^e) \), i.e.

1. their homogeneous coordinates are chosen in such a way that \( \underline{v}_0 = \underline{v}_1 + \underline{v}_2 + ... + \underline{v}_{t+1} \);
2. \( \underline{v}_1, ..., \underline{v}_{t+1} \) are independent over \( \text{GF}(p^e) \);
3. \( B = \langle \underline{v}_0, \underline{v}_1, ..., \underline{v}_{t+1} \rangle_{\text{GF}(p^e)} = \{ \sum_{i=1}^{t+1} \lambda_i \underline{v}_i : \lambda_1, ..., \lambda_{t+1} \in \text{GF}(p^e), (\lambda_1, ..., \lambda_{t+1}) \neq (0, 0, ..., 0) \} \).

(As usual, for any \( \mu \in \text{GF}(q)^* \) and any vector \( \underline{u} \), the point \( \mu \underline{u} \) represents the same point). So we get \( (\text{GF}(p^e))^{t+1-1} \) points, possibly counted with multiplicities.

In this case some points may well coincide. Let’s examine the structure of multiple points! For any point \( \underline{u} \in B \) consider the (homogeneous) \( t + 1 \)-tuples \( L_{\underline{u}} = \{ (\lambda_1, ..., \lambda_{t+1}) \} \subseteq \text{PG}(t, p^e) \) defining it with \( \underline{u} = \sum_{i=1}^{t+1} \lambda_i \underline{v}_i \). Obviously any \( L_{\underline{u}} \) is a projective subspace of \( \text{PG}(t, p^e) \) (so all the multiplicities are of the form \( (\text{GF}(p^e))^{i+1-1} \) for \( i \in \{0, 1, ..., t\} \)), and \( \{ L_{\underline{u}} : \underline{u} \in B \} \) is a partition of \( \text{PG}(t, p^e) \).

**Exercise 20.2.** Prove that, because of (2) above, most of the subspaces \( L_{\underline{u}} \) are in fact points of \( \text{PG}(t, p^e) \).

Define the matrix
\[ U = (\underline{v}_1^T, \underline{v}_2^T, ..., \underline{v}_{t+1}^T), \]
then \( B = \langle \varepsilon_0, \varepsilon_1, ..., \varepsilon_{t+1} \rangle_{\text{GF}(p^e)} \) is the image of \( \text{PG}(t, p^e) = \{(\lambda_1, ..., \lambda_{t+1}) \neq (0, 0, ..., 0) : \forall \lambda_i \in \text{GF}(p^e)\} \) under the map \( \lambda \mapsto U\lambda^T \).

Two linear combinations \( P = \sum_{i=1}^{t+1} \lambda_i \varepsilon_i \) and \( Q = \sum_{i=1}^{t+1} \mu_i \varepsilon_i \) define coinciding points if there exists an \( \alpha \in \text{GF}(q) \) such that \( P = \alpha Q \), so \( \sum_{i=1}^{t+1} (\lambda_i - \alpha \mu_i) \varepsilon_i = 0 \). It can happen if the \( \varepsilon_i \)-s are dependent over \( \text{GF}(q) \) (as usually they are). Consider the \( ((n+1) \times (t+1)) \) matrix \( U \) defined above. Let \( W \) be the projective subspace of \( \text{PG}(t, q) \) consisting of nonzero vectors \( w \) for which \( Uw^T = 0 \). (It may be the empty set if \( n \geq t \)) If \( W = \emptyset \) then all the points of \( B \) are distinct.

Note that, counting without multiplicities, the number of points of \( B \) satisfies

\[
|B| \leq \frac{(p^e)^{t+1} - 1}{p^e - 1};
\]

and the author conjectures that if \( \text{GF}(p^e) \) is the “maximum subfield of linearity” then

\[
(p^e)^t + (p^e)^{t-1} + 1 \leq |B| \leq \frac{(p^e)^{t+1} - 1}{p^e - 1}
\]

holds as well. Intuitively it would mean that we cannot lose more than a \((t-2)\)-dimensional subspace, collapsing into one point.

**Theorem 20.3.** The Rédei polynomial of \( B \) is

\[
R(X, Y, ..., T) = \prod_{(\lambda_1, ..., \lambda_{t+1}) \in \text{PG}(t, p^e)} \sum_{i=1}^{t+1} \lambda_i \varepsilon_i V = \sum_{\pi \in \text{Sym}(1, 2, ..., t+1)} \text{sgn}(\pi) \prod_{i=1}^{t+1} (\varepsilon_i V)^{(p^e)^{\tau(\pi)}} = \\
= \det \left( \begin{array}{cccc}
\varepsilon_1 V & \varepsilon_2 V & \ldots & \varepsilon_{t+1} V \\
(p^e \varepsilon_1 V)^{p^e} & (p^e \varepsilon_2 V)^{p^e} & \ldots & (p^e \varepsilon_{t+1} V)^{p^e} \\
\vdots & \vdots & \ddots & \vdots \\
(p^e \varepsilon_1 V)^{p^{2e}} & (p^e \varepsilon_2 V)^{p^{2e}} & \ldots & (p^e \varepsilon_{t+1} V)^{p^{2e}} \\
\end{array} \right) = \text{MRD}(\varepsilon_1 V, \varepsilon_2 V, ..., \varepsilon_{t+1} V).
\]

**Proof:** To prove this first observe that both \( R \) and the determinant is of degree \( 1 + p^e + p^{2e} + ... + p^{te} \). Hence it is enough to prove that each factor \((\sum_{i=1}^{t+1} \lambda_i \varepsilon_i) V\) of \( R \) appears in the determinant as well.

W.l.o.g. suppose that \( \lambda_i \neq 0 \). Multiply the first column of the determinant by the constant \( \lambda_1 \), then successively add \( \lambda_2 \cdot \) (the second column), ..., \( \lambda_{t+1} \cdot \) (the \((t+1)\)-th column) to the first column, this process does not change the determinant essentially. Now the first column is \((\sum_{i=1}^{t+1} \lambda_i \varepsilon_i) V, \ldots, (\sum_{i=1}^{t+1} \lambda_i \varepsilon_i) V)^{p^e}, \ldots, (\sum_{i=1}^{t+1} \lambda_i \varepsilon_i) V)^{p^{te}}\), so each entry in it is divisible by the factor \((\sum_{i=1}^{t+1} \lambda_i \varepsilon_i) V\), hence the same holds for the
determinant as well.

Suppose that a hyperplane \( \pmb{x} = [x, y, ..., t] \) contains precisely one point \( \pmb{P} = \sum_{i=1}^{t+1} \lambda_i \pmb{v}_i \) point of \( B (\lambda_i \in \text{GF}(p^e)) \). It means that

\[
0 = \pmb{P} \cdot \pmb{x} = \sum_{i=1}^{t+1} \lambda_i \pmb{v}_i \cdot \pmb{x}.
\]

Take the \((p^e)^j\)-th power of this equation, it is \( \sum_{i=1}^{t+1} \lambda_i (\pmb{v}_i \cdot \pmb{x})^{p^e j} = 0 \), meaning that linear combination of the columns of the determinant above (after substituting \( \pmb{V} = \pmb{x} \), with the same \( \lambda_i \)-s, result in the zero vector, hence the value of the determinant is zero.

**Exercise 20.4.** Prove the other direction, i.e. if the determinant is zero for some substitution \( \pmb{V} = \pmb{x} = (x, y, ..., t) \) then there is a point \( \pmb{P} = \sum_{i=1}^{t+1} \lambda_i \pmb{v}_i \in B \) on the hyperplane \([x, y, ..., t]\).

Intuitively, if a hyperplane \([x, y, ..., t]\) contains \( (p^e)^{k+1} - 1 \) points of \( B \), as the intersection is a linear set generated by some \( \pmb{u}_0, \pmb{u}_1, ..., \pmb{u}_{k+1} \in B \), then it means that there are \( k+1 \) independent equations for the columns of the determinant above (i.e. \( k+1 \) independent vectors \( \pmb{\lambda} = (\lambda_1, ..., \lambda_{t+1}) \), each coming from a \( \pmb{u}_j \), expressed from the \( \pmb{v}_i \)-s), hence the rank of the matrix is \((t+1) - (k+1)\).

**Exercise 20.5.** Prove that it implies that \((x, y, ..., t)\) is a point of \( R(X, Y, ..., T) \) with multiplicity \( \frac{(p^e)^{k+1} - 1}{p^e - 1} \) precisely (as it has to be).

If for example \( p^e = q \) then \( B \) is a blocking set with respect to hyperplanes, since for any hyperplane \([x, y, ..., t]\) the Rédei polynomial \( R(x, y, ..., t) \) vanishes: the first and the last rows of the determinant above are identical after the substitution.

Note that now \( R(X, Y, ..., T) \) may contain multiple factors. (Removing all but one copies of a multiple point the blocking property remains intact.)

### 21 Blocking sets

A blocking set with respect to \( k \)-dimensional subspaces is a pointset meeting every \( k \)-subspace. As a blocking set plus a point is still a blocking set, we are interested in minimal ones (with respect to set-theoretical inclusion) only. Note that in a (projective) plane the only interesting case is \( k = 1 \).

In any projective plane of order \( q \) the smallest blocking set is a line (of size \( q + 1 \)). In \( \text{PG}(2, q) \) there exist minimal blocking sets of size \( \frac{3}{4}q \); the projective triangle of size \( 3(q+1)/2 \) if \( q \) is odd and the projective triad (which is a linear pointset in fact) of size \( 3q/2 + 1 \) if \( q \) is even. In general, in \( \text{PG}(n, q) \) it is easy to construct
a blocking set with respect to \( k \)-dimensional subspaces; it is straightforward to prove that the smallest example is a subspace of dimension \( n - k \) (so consisting of \( q^{n-k+1} - 1 \) \( q \) points), this example is called trivial. Another easy one is a cone, with a planar blocking set as a base and an \((n-k-2)\)-dimensional subspace as vertex; if the base was of size \( \frac{3}{2}q \) then the blocking set will be of size \( \frac{3}{2}q^{n-k} \) roughly. A blocking set with respect to \( k \)-dimensional subspaces of \( \text{PG}(n, q) \) is said to be small if it is smaller than \( \frac{3}{2}(q^n + 1) \), in particular in the plane it means that \( |B| < 3(q + 1)/2 \).

A most interesting question of the theory of blocking sets is to classify the small ones. A natural construction (blocking the \( k \)-subspaces of \( \text{PG}(n, q) \)) is a subgeometry \( \text{PG}(h(n-k)/e, p^e) \), if it exists (recall \( q = p^h \), so \( 1 \leq e \leq h \) and \( e|h \)). It is one of the earliest results concerning blocking sets, due to Bruen [51], that a nontrivial blocking set of a projective plane of order \( q \) is of size \( \geq q + \sqrt{q} + 1 \), and equality holds if and only if it is a Baer subplane (i.e. a subgeometry of order \( \sqrt{q} \)). It is easy to see that the projection of a blocking set, w.r.t. \( k \)-subspaces, from a vertex \( V \) onto an \( r \)-dimensional subspace of \( \text{PG}(r, q) \), is again a blocking set, w.r.t. the \((k+r-n)\)-dimensional subspaces of \( \text{PG}(r, q) \) (where \( \dim(V) = n-r-1 \) and \( V \) is disjoint from the blocking set).

A blocking set of \( \text{PG}(r, q) \), which is a projection of a subgeometry of \( \text{PG}(n, q) \), is called linear. (Note that the trivial blocking sets are linear as well.) Linear blocking sets were defined by Lunardon, and they were first studied by Lunardon, Polito and Polverino [93], [98].

**Conjecture 21.1. The Linearity Conjecture.** In \( \text{PG}(n, q) \) every small blocking set, with respect to \( k \)-dimensional subspaces, is linear.

There are some cases of the Conjecture that are proved already.

**Theorem 21.2.** For \( q = p^h \), every small minimal non-trivial blocking set w.r.t. \( k \)-dimensional subspaces is linear, if

(a) \( n = 2, k = 1 \) (so we are in the plane) and

(i) (Blokhuis [33]) \( h = 1 \) (i.e. there is no small non-trivial blocking set at all);

(ii) (Szőnyi [123]) \( h = 2 \) (the only non-trivial example is a Baer subplane with \( p^2 + p + 1 \) points);

(iii) (Polverino [99]) \( h = 3 \) (there are two examples, one with \( p^3 + p^2 + 1 \) and another with \( p^3 + p^2 + p + 1 \) points);

(iv) (Blokhuis, Ball, Brouwer, Storme, Szőnyi [43], Ball [9]) if \( p > 2 \) and there exists a line \( \ell \) intersecting \( B \) in \( |B \cap \ell| = |B| - q \) points (so a blocking set of Rédei type);
(b) for general $k$:

(i) (Szönyi and Weiner) \[129\] if $h(n-k) \leq n$, $p > 2$ and $B$ is not contained in an $(h(n-k)-1)$-dimensional subspace;

(ii) (Storme-Weiner \[110\] (for $k = n-1$), Bokler and Weiner \[138\]) $h = 2$, $q \geq 16$;

(iii) (Storme-Sziklai \[108\]) if $p > 2$ and there exists a hyperplane $H$ intersecting $B$ in $|B \cap H| = |B| - q^{n-k}$ points (so a blocking set of Rédei type).

There is an even more general version of the Conjecture. A $t$-fold blocking set w.r.t. $k$-subspaces is a pointset which intersects each $k$-subspace in at least $t$ points. Multiple points may be allowed as well.

**Conjecture 21.3.** The Linearity Conjecture for multiple blocking sets: In $\text{PG}(n,q)$ any $t$-fold blocking set $B$, with respect to $k$-dimensional subspaces, is the union of some (not necessarily disjoint) linear pointsets $B_1, ..., B_s$, where $B_i$ is a $t_i$-fold blocking set w.r.t. $k$-dimensional subspaces and $t_1 + ... + t_s = t$; provided that $t$ and $|B|$ are small enough ($t \leq T(n,q,k)$ and $|B| \leq S(n,q,k)$ for two suitable functions $T$ and $S$).

Note that there exists a $(\sqrt{q}+1)$-fold blocking set in $\text{PG}(2,q)$, constructed by Ball, Blokhuis and Lavrauw \[19\], which is not the union of smaller blocking sets. (This multiple blocking set is a linear pointset.)

First we study 1-fold (planar) blocking sets.

As an appetizer, we present here Blokhuis’ theorem, which was a real breakthrough at 1994. It was conjectured by Jane di Paola in the late 1960’s.

**Theorem 21.4.** (Blokhuis \[33\]) In $\text{PG}(2,p)$, $p$ prime, the size of a non-trivial blocking set is at least $3(p+1)/2$.

**Proof 1:** Let $B = U \cup D$, $U = B \cap \text{AG}(2,p) = \{(a_i,b_i) : i = 1, ..., p+s\}$ with $s \geq 1$ and $D = B \setminus \text{AG}(2,p) = \{(\infty),(y_1),..., (y_{k-s})\}$, so $|B| = p + 1 + k$, and suppose that $B$ is a minimal non-trivial blocking set. Consider the affine Rédei polynomial

$$R(X,Y) = \prod_{i=1}^{p+s}(X + a_i Y + b_i) = \sum_{j=0}^{p+s} r_j(Y) X^{p+s-j}$$

of $U$, where $\deg_Y r_j(Y) \leq j$ and $r_0(Y) = 1$. If $(y) \not\in B$ then the affine lines of slope $y$ should be blocked by $U$. It means that $R(X,y)$ vanishes for all $X = x \in \text{GF}(p)$ hence $R(X,y) = (X^p - X)t(X)$ for some $t(X)$ of degree $s$. Consequently, $R(X,y)$ does not contain terms of exponent $s + 2, s + 3, ..., p - 1$, so the polynomials $r_{s+1}(Y), ..., r_{p-2}(Y)$ vanish for all $y \not\in D$, so for $p - k + s$ values. It means that
21. Blocking sets

\(r_{s+1}(Y) = \ldots = r_{p-k+s-1}(Y) = 0\) identically, so the terms \(X^{k+1}, \ldots, X^{p-1}\) are all missing even from \(R(X,Y)\).

Now consider a point at infinity from \(D\), i.e. some \(y_r\). As \(R(X,y_r)\) still do not contain the terms \(X^{k+1}, \ldots, X^{p-1}\), we have

\[R(X,y_r) = X^p g(X) + h(X), \deg(g) = s, \deg(h) \leq k.\]

It is almost the situation of Exercise 5.39, excepting that \(g(X)\) and \(h(X)\) may have a common factor. Dividing out the common factors we get \(X^p g_1(X) + h_1(X)\), which is still totally reducible, \(\deg(g_1) \leq s, \deg(h_1) \leq k\). As \(s \leq k\), Exercise 5.39 gives \(k \geq \frac{p+1}{2}\), so \(|B| = p + k + 1 \geq \frac{3}{2}(p+1)\). The only cases we have to exclude are (i) \(X^p g_1(X) + h_1(X) = (aX + b)^p\) and (ii) \(X^p - X \mid X^p g_1(X) + h_1(X)\). Both are impossible as (i) would imply that \(B\) contains a whole line, while (ii) would mean that \(X^p - X \mid R(X,y_r)\) so the point \((y_r)\) could be deleted without loss of the blocking property, contradicting the minimality of \(B\).

**Proof 2:** Let \(B = \{(a_i, b_i) : i = 1, \ldots, p + k\} \cup \{(\infty)\}\). The affine Rédei polynomial

\[R(X,Y) = \prod_{i=1}^{p+k} (X + a_i Y + b_i)\]

vanishes for all \(X = x, Y = y, \ x, y \in \mathbb{GF}(p)\). Hence \(R(X,Y)\) is in the ideal \(\langle (X^p - X), (Y^p - Y) \rangle\) and we can write \(R(X,Y) = (X^p - X) F(X,Y) + (Y^p - Y) G(X,Y)\), where \(f\) and \(g\) are of total degree \(k\). Let \(R_0\) denote the part of \(R\) that is homogeneous of total degree \(p + k\), and let \(F_0\) and \(G_0\) denote the parts of \(F\) and \(G\) resp. that are homogeneous of total degree \(k\). Now \(R_0 = X^p F_0 + Y^p G_0\). As the equation is homogeneous let’s put \(Y = 1\), and define \(h(X) = R_0(X,1), f(X) = F_0(X,1)\) and \(g(X) = G_0(X,1)\).

So \(f(X) = \prod_i (X + a_i) = X^p f(X) + g(X)\) is a fully reducible polynomial with \(f^p, g^p \leq k\). Using Exercise 5.39 after dividing out the common factors of \(f\) and \(g\) we can finish the argument as in Proof 1.

These proofs seem to be very similar, the first treats the case \(s \geq 1\), the second the case \(s = 0\). The little “philosophical” difference led to different trains of thought, as we will see later. This theorem somehow become aprobe of new ideas examining blocking sets, at least two more proofs will be presented, see Theorem 21.4 and Corollary 21.22.

One can formulate the chase for minimal (nontrivial) blocking sets (in \(\text{PG}(2, q)\)) in an algebraic way as follows. Consider the polynomial ring \(\mathbb{GF}(q)[X, Y, Z]\) and its subset \(\mathbb{GF}(q)[X, Y, Z]_{\text{hom}}\), the homogeneous polynomials of any degree. The fully reducible polynomials form the multiplicative sub-semigroups \(\mathcal{R}\) and \(\mathcal{R}_{\text{hom}}\).
in them. Let $\text{GF}(q)[X, Y, Z]_0$ and $\text{GF}(q)[X, Y, Z]_{\text{hom}, 0}$ denote the sets (ideals) of polynomials vanishing everywhere in $\text{GF}(q) \times R \times \text{GF}(q) \times \text{GF}(q)$.

Both $\text{GF}(q)[X, Y, Z]_0$ and $\text{GF}(q)[X, Y, Z]_{\text{hom}, 0}$, as ideals, can be generated by three polynomials from $R$ (and $R_{\text{hom}}$, resp.), for example $\text{GF}(q)[X, Y, Z]_0 = \langle (X^q - X); (Y^q - Y); (Z^q - Z) \rangle$ and $\text{GF}(q)[X, Y, Z]_{\text{hom}, 0} = \langle (Y^q Z - YZ^q); (Z^q X - ZX^q); (X^q Y - XY^q) \rangle$. Note also that for any $a, b, c \in \text{GF}(q)$ the polynomial $a(Y^q Z - YZ^q) + b(Z^q X - ZX^q) + c(X^q Y - XY^q)$ is still totally reducible. (It is the Rédei polynomial of the pointset consisting of the points of the line $[a, b, c]$.)

The trivial blocking sets, as we have seen, correspond to the minimal polynomials $a(Y^q Z - YZ^q) + b(Z^q X - ZX^q) + c(X^q Y - XY^q)$.

### 21.1 One curve

So let $|B| = q + k$ be our blocking set. We often suppose that $|B| < 2q$. Recall the Rédei polynomial of $B$:

$$R(X, Y, Z) = \prod_{(a_i, b_i, c_i) \in B} (a_i X + b_i Y + c_i Z) = \sum_{j=0}^{q+k} r_j(Y, Z)X^{q+k-j}.$$ 

**Definition 21.5.** ([47], [123]) Let $C$ be the curve of degree $k$ defined by

$$f(X, Y, Z) = r_0(Y, Z)X^k + r_1(Y, Z)X^{k-1} + \ldots + r_k(Y, Z).$$

Note that as $\deg(r_j) = j$ (or $r_j = 0$), the polynomial $f(X, Y, Z)$ is homogeneous of degree $k$ indeed.

**Lemma 21.6.** If the line $L_X[1, 0, 0]$ contains the points $\{ (0, b_{ij}, c_{ij}) : j = 1, \ldots, N_X \}$ then

$$r_{N_X}(Y, Z) = \prod_{a_s \neq 0} a_s \prod_{j=1}^{N_X} (b_{ij} Y + c_{ij} Z) \mid R(X, Y, Z);$$

$$r_{N_X}(Y, Z) \mid f(X, Y, Z);$$

so $f$ can be written in the form $f = r_{N_X} \tilde{f}$, where $\tilde{f}(X, Y, Z)$ is a homogeneous polynomial of total degree $= X$-degree $= k - N_X$. In particular, if $L_X$ is a Rédei line then $f = r_{N_X}$. One can write $R(X, Y, Z) = r_{N_X}(Y, Z)R(X, Y, Z)$ as well.

**Proof:** obvious from the definitions: $r_{N_X} | r_i \forall i$. Indeed, $r_{N_X}$ contains the $X$-free factors of $R$; $N_X$ is the smallest index $j$ for which $r_j$ is not identically zero. As, by
definition, \( r_j \) is gained from \( R = \prod(a_iX + b_iY + c_iZ) \) by adding up all the partial products consisting of all but \( j \) \((b_iY + c_iZ)\) factors and \( j \) non-zero \( a_i \) factors, each of these products will contain all the factors of \( r_{NX} \), so \( r_{NX} | r_j \forall j \).

Note that the curve \( r_{NX} \) consists of \( N_X \) lines on the dual plane, all passing through \([1, 0, 0]\).

On the other hand if \( k < q \) then

\[
\begin{align*}
f &= \mathcal{H}_X^q R = \sum_{\{s_1, s_2, \ldots, s_q\}} a_{s_1}a_{s_2} \ldots a_{s_q} \prod_{j \not\in \{s_1, s_2, \ldots, s_q\}} (a_jX + b_jY + c_jZ).
\end{align*}
\]

Obviously it is enough to sum for subsets \( \{P_{s_1}, P_{s_2}, \ldots, P_{s_q}\} \subseteq B \setminus L_X \).

If one coordinatizes \( B \) such that each \( a_i \) is either 0 or 1, then

\[
\begin{align*}
f &= r_{NX} \bar{f} = r_{NX} \sum_{J \subseteq \{1, 2, \ldots, q+k\}} |J| = k - N_X \prod_{a_j \neq 0 \forall j \in J} (X + b_jY + c_jZ).
\end{align*}
\]

Also

\[
\begin{align*}
r_{NX} &= \mathcal{H}_X^{q+k-N_X} R = \mathcal{H}_X^{k-N_X} f.
\end{align*}
\]

The next proposition summarizes some important properties of the Rédei polynomial and of this curve.

**Theorem 21.7.** ([123])

(1.1) For a fixed \((y, z)\), \((0, -z, y) \not\in B\), the element \( x \) is an \( r \)-fold root of \( R_{y, z}(X) = R(X, y, z) \) if and only if the line with equation \( xX + yY + zZ = 0 \) intersects \( B \) in exactly \( r \) points.

(1.2) Suppose \( R_{y, z}(X) = 0 \), i.e. \((0, -z, y) \in B\). Then the element \( x \) is an \((r-1)\)-fold root of \( R(X, y, z) \) if and only if the line with equation \( xX + yY + zZ = 0 \) intersects \( B \) in exactly \( r \) points.

(2.1) For a fixed \((0, -z, y) \not\in B\) the polynomial \((X^q - X)\) divides \( R_{y, z}(X) \). Moreover, if \( k < q - 1 \) then \( R_{y, z}(X) = (X^q - X)f(X, y, z) \) for every \((0, -z, y) \not\in B\); and \( f(X, y, z) \) splits into linear factors over \( \mathbb{GF}(q) \) for these fixed \((y, z)\)’s.

(2.2) If the line \([0, -z, y]\) \((0, -z, y) \not\in B)\ meets \( f(X, Y, Z) \) at \((x, y, z)\) with multiplicity \( m \), then the line with equation \( xX + yY + zZ = 0 \) meets \( B \) in exactly \( m + 1 \) points.

This theorem shows that the curve \( f \) has a lot of \( \mathbb{GF}(q)\)-rational points and helps us to translate geometric properties of \( B \) into properties of \( f \).
II. Polynomials in geometry

Proof: (1.1) and (1.2) are straightforward from the definition of the Rédei polynomial. The multiplicity of a root $X = x$ is the number linear factors in the product defining $R(X, Y, Z)$ that vanish at $(x, y, z)$, which is just the number of points of $B$ lying on the line $[x, y, z]$. The first part of (2.1) follows from (1.1) and the well-known fact that $\prod_{x \in \mathbb{F}(q)} (X - x) = X^q - X$. The rest of (2.1) is obvious.

To prove (2.2) note that if the intersection multiplicity is $m$, then $x$ is an $(m + 1)$-fold root of $R_{y,z}(X)$. Now the assertion follows from (1.1).

The facts given in Theorem 21.7 will be used frequently without further reference.

The next lemma shows that the linear components of $\bar{f}$ (or the curve $\bar{C}$ defined by $\bar{f} = 0$) correspond to points of $B$ which are not essential.

Lemma 21.8. ([123])

(1.1) If a point $P(a, b, c) \in B \setminus L_X$ is not essential, then $aX + bY + cZ$ divides $\bar{f}(X, Y, Z)$ (as polynomials in three variables).

(1.2) Conversely, if $N_X < q + 2 - k$ and $aX + bY + cZ$ divides $\bar{f}(X, Y, Z)$, then $(a, b, c) \in B \setminus L_X$ and $(a, b, c)$ is not essential.

(2.1) If a point $P(0, b, c) \in B \cap L_X$ is not essential, then $X^q - X$ divides $\bar{R}(X, -c, b)$ (as polynomials in three variables).

(2.2) Conversely, if $X^q - X$ divides $\bar{R}(X, -c, b)$, then $(0, b, c)$ cannot be an essential point of $B$.

Proof: (1.1): Take a point $Q(0, -z_0, y_0) \notin B$. For this $Q(0, -z_0, y_0)$ there are at least two points of $B$ on the line $PQ$, hence $(aX + bY + cz_0)$ divides $\bar{f}(X, y_0, z_0)$. In other words, the line $L : aX + bY + cZ$ and $\bar{C}$ have a common point for $(Y, Z) = (y_0, z_0)$. This happens for $q + 1 - N_X$ values of $(y_0, z_0)$, so Bézout's theorem implies that $L$ is a component of $\bar{C}$.

(1.2): Conversely, if $aX + bY + cZ$ divides $\bar{f}(X, Y, Z)$, then for every $Q(0, -z_0, y_0) \notin B$ the line through $Q$ and $(a, b, c)$ intersects $B$ in at least two points. If $(a, b, c) \notin B$, then $|B| \geq 2(q + 1 - N_X) + N_X$. Putting $|B| = q + k$ gives a contradiction. Hence $(a, b, c) \in B$. Since every line through $(0, -z_0, y_0) \notin B$, contains at least two points of $B$, the point $(a, b, c)$ cannot be essential.

(2.1) and (2.2) can be proved in a similar way as (1.1) and (1.2).

If the line $[1, 0, 0]$ is a tangent, or if $B$ is a small blocking set, then the previous lemma simply says that there are no linear components of $\bar{f}$ if $|B| < 2q$. Note that also in Segre's theory there is a lemma corresponding to this one (see [77], Lemmas 10.3.2 and 10.4.), and it plays an important role in proving the incompleteness of arcs.
Recall also a lower bound on the number of $\mathbb{GF}(q)$-rational points of certain components of $f$, see Blokhuis, Pellikaan, Szönyi [47].

**Lemma 21.9.** ([47]) (1) The sum of the intersection multiplicities $I(P; f \cap \ell_P)$ over all $\mathbb{GF}(q)$-rational points of $f$ is at least $\deg(f)(q+1) - \deg(f)N_X$, where $\ell_P$ denotes the line through $P$ and $(1,0,0)$ (the “horizontal line”). If $g$ is a component of $f$, then the corresponding sum for $g$ is at least $\deg(g)(q+1) - \deg(\bar{g})(N_X)$, where $g_0 = \gcd(g, r_{N_X})$ and $g = g_0\bar{g}$.

(2) Let $g(X,Y,Z)$ be a component of $f(X,Y,Z)$ and suppose that it has neither multiple components nor components with zero partial derivative w.r.t. $X$. Then the number of $\mathbb{GF}(q)$-rational points of $g$ is at least

$$\deg(g)(q+1) - \deg(\bar{g})(N_X + \deg(\bar{g}) - 1)$$

**Proof:** Let $g = g_0\bar{g}$, where $g_0$ contains the product of some linear components (hence $g_0|r_{N_X}$) and $\bar{g}$ has no linear component; $s = \deg(g)$, $\bar{s} = \deg(\bar{g})$. First note that the linear components of $r_{N_X}$ all go through $(1,0,0)$ while $\bar{g}$ does not. For any fixed $(Y,Z) = (y,z)$, for which $(0,-z,y) \notin B$, the polynomial $f(X,y,z)$ is the product of linear factors over $\mathbb{GF}(q)$, hence the same is true for every divisor $g$ of $f$. So the number of points, counted with the intersection multiplicity of $g$ and the horizontal line at that point, is at least $\bar{s}(q+1 - N_X) + \deg(g_0)(q+1)$. To count the number of points without this multiplicity we have to subtract the number of intersections of $\bar{g}$ and $\bar{g}_X$ (see [47]); Bézout’s theorem then gives the result. Note also that in this counting the common points of $\bar{g}$ and $\bar{g}_X$ are counted once if the intersection multiplicity $I(P; \bar{g} \cap \ell_P)$ is not divisible by $p$, and the points with intersection multiplicity divisible by $p$ are not counted at all. Hence we have at least $\bar{s}(q+1 - N_X) + (s - \bar{s})(q+1) - \bar{s}(\bar{s} - 1)$ points of $g$. 

These elementary observations already yield interesting results on blocking sets. We mention without a proof that Lemma 21.9, combined with the Weil-estimate on the number of rational points of a curve gives the result of Bruen $|B| \geq q + \sqrt{q} + 1$.

We repeat a lemma of Blokhuis and Brouwer.

**Proposition 21.10.** ([44]) There are at most $k^2 - k + 1$ lines that meet $B$ in at least two points.

**Proof:** Exercise 12.5, with $|B| = q + k$, gives that the total number of tangents is at least $(q + k)(q + 1 - k)$, which means that there are at most $k^2 - k + 1$ lines intersecting $B$ in at least two points. 

Now we are ready to prove Blokhuis’ theorem 21.4 in the prime case.

**Theorem 21.11.** (Blokhuis [33]) In $\text{PG}(2,p)$, $p$ prime, the size of a non-trivial blocking set is at least $3(p+1)/2$. 

II. Polynomials in geometry

Proof: Take a component \( g = \tilde{g} \) (of degree \( s \)) of \( \tilde{f} \). Since \( p \) is prime, it cannot have zero partial derivative with respect to \( X \). Therefore it has at least \( s(p+1) - s(N_X + s - 1) \) points by Lemma 21.9. On the other hand, again since \( p \) is prime, it cannot be non-classical with respect to lines. Therefore, by the Stöhr-Voloch theorem 10.9, it has at most \( s(p + s - 1)/2 \) \( \mathbb{GF}(p) \)-rational points. This implies

\[
s(p + 1) - s(N_X + s - 1) \leq s(p + s - 1)/2,
\]

which means \( s \geq (p + 5 - 2N_X)/3 \). In particular, if \(|B| < p + 1 + 2(p + 3)/3\) and we choose \( L_X \) to be a tangent, then the curve \( \tilde{f} \) must be (absolutely) irreducible. Now Lemma 21.9 can be applied to \( f \) itself and it says that \( \tilde{f} \) has at least \((k - 1)(p + 1) - (k - 1)(k - 1)\) points. On the other hand, the previous lemma shows that it can have at most \( k^2 - k + 1 \) points over \( \mathbb{GF}(p) \). Solving the inequality \( pk - k(k - 1) \leq k^2 - k + 1 \) implies \( k \geq (p + 2)/2 \).

Let us repeat the interesting observation that for \(|B| < p + 1 + 2(p + 3)/3\) the curve \( \tilde{f} \) itself must be irreducible. A second proof of a slightly weaker bound will be given in Proposition 21.20. In case of a prime-power \( q \) the same argument shows that for \(|B| \leq p + (p + 3)/3\) each component of \( f \) whose partial derivative with respect to \( X \) is not identically zero must be non-classical with respect to lines. However, the existence of such non-classical components can be excluded by using a pair or triple of curves, as we shall see soon.

21.2 Three new curves

In this subsection we introduce three nice curves. We use the notation \( V = (X,Y,Z); V^q = (X^q,Y^q,Z^q) \) and \( \Psi = V \times V^q \equiv ((Y^qZ - YZ^q),(Z^qX - ZX^q),(X^qY - XY^q)) \). Let \( B \) be a minimal blocking set of \( PG(2,q) \). Since \( R(X,Y,Z) \) vanishes for all homogeneous \((x,y,z) \in \mathbb{GF}(q) \times \mathbb{GF}(q) \times \mathbb{GF}(q) \), we can write it as

\[
R(X,Y,Z) = \Psi \cdot g = \det(V, V^q, g) =
\]

\[
(X^qZ - YZ^q) g_1(X,Y,Z) + (Z^qX - ZX^q) g_2(X,Y,Z) + (X^qY - XY^q) g_3(X,Y,Z),
\]

where \( g_1, g_2, g_3 \) are homogeneous polynomials of degree \( k - 1 \) in three variables and \( g = (g_1, g_2, g_3) \). Note that \( g \) is not determined uniquely, it can be changed by \( g' = g + g_0 V \) for any homogeneous polynomial \( g_0 \in \mathbb{GF}(q)[X,Y,Z] \) of total degree \( k - 2 \), if \( k < q \) and for \( g' = g + g_0 V + g_{00} V^q \) for arbitrary homogeneous polynomials \( g_0 \) of degree \( k - 2 \) and \( g_{00} \) of degree \( k - q - 1 \).

Why is this a most natural setting? For example observe that if \( B \) is the line \([a,b,c] \) then \( R = (a,b,c) \cdot \Psi \).

Now one can define \( f = V \times g \). Then \( f \cdot (V^q - V) = f_1(X^q - X) + f_2(Y^q - Y) + f_3(Z^q - Z) = R \), and \( f_1, f_2, f_3 \) are homogeneous polynomials of degree \( k \). If \( k < q \) then, by this “decomposition” of \( R \), \( f \) is determined uniquely. Conversely, if for
some $g'$ also $f = V \times g'$ holds then $g' = g + gV$ for some homogeneous polynomial $g$ of degree $k - 2$.

We also remark that, as $V \cdot (V \times g) = 0$, we have $Vf = 0$. For another proof see 21.16.

If $k \geq q$ then $f$ is not necessarily unique in the decompositon of $R$. But if we choose $f = V \times g$ for some $g$ then 21.16 remains valid (otherwise it may happen that $V \cdot f$ is not the zero polynomial).

The following lemma summarizes some fundamental properties of $g$.

**Proposition 21.12.** (1.1) If a point $P(a, b, c) \in B$ is not essential, then there exists an equivalent $g' = g + g_0V$ (or $g' = g + g_0V + g_0V^q$) of $g$ such that $aX + bY + cZ \text{ divides } g_i(X, Y, Z)$, $i = 1, 2, 3$ (as polynomials in three variables).

(1.2) Conversely, if $N_X < q + 2 - k$ and $aX + bY + cZ \text{ divides each } g_i(X, Y, Z)$, $i = 1, 2, 3$, then $(a, b, c) \in B$ and $(a, b, c)$ is not essential.

(2) If $B$ is minimal then $g_1, g_2$ and $g_3$ have no common factor.

**Proof:** (1.1) In this case $R_0 = R/(aX + bY + cZ)$ still vanishes everywhere, so it can be written in the form $R_0 = g_0\Psi$, so $\Psi \cdot (g_0(aX + bY + cZ) - g) = 0$.

(1.2) Now $aX + bY + cZ \text{ divides } R$ as well, so $(a, b, c) \in B$. Deleting it, the Rédéi polynomial of the new pointset is $(Y^qZ - YZ^q) \frac{g_2(X, Y, Z)}{aX + bY + cZ} + (Z^qX - ZX^q) \frac{g_2(X, Y, Z)}{aX + bY + cZ} + (X^qY - XY^q) \frac{g_2(X, Y, Z)}{aX + bY + cZ}$, so it remains a blocking set.

(2) Such a factor would divide $R$ as well, which splits into linear factors. Then for a linear factor see (1.2).

We want to “evaluate” $R$ along a line $[a, b, c]$ of the dual plane (so we examine the lines through $(a, b, c)$ of the original plane). We use the notation

$$
\phi(X, Y, Z)\bigg|_{[a, b, c]} = \phi(bZ - cY, cX - aZ, aY - bX).
$$

In general $f(X, Y, Z)\bigg|_{[a, b, c]} = f(-bY - cZ, aY, aZ) = f(bX, -aX - cZ, bZ) = f(cX, cY, -aX - bY)$, where e.g. $f(-bY - cZ, aY, aZ)$ can be used if $a \neq 0$ etc.

**Theorem 21.13.** (1)

$$
R\bigg|_{[a, b, c]} = \left( a g_1\bigg|_{[a, b, c]} + b g_2\bigg|_{[a, b, c]} + c g_3\bigg|_{[a, b, c]} \right) \left( (ZY^q - Z^qY)\bigg|_{[a, b, c]} \right)
$$

(the last factor should be changed for $(XZ^q - X^qZ)\bigg|_{[a, b, c]}$ if $a = 0$ and $b \neq 0$ and for $(YX^q - Y^qX)\bigg|_{[a, b, c]}$ if $a = b = 0$ and $c \neq 0$, “normally” these factors are identical when restricting to $aX + bY + cZ = 0$).
(2) \((a, b, c) \in B\) if and only if \(a g_1_{[a, b, c]} + b g_2_{[a, b, c]} + c g_3_{[a, b, c]} = 0\). It means that if one considers this equation as an equation in the variables \(a, b, c\) then the points of \(B\) are exactly the solutions of it.

(3) If \((a, b, c) \in B\) then consider

\[
R_{aX + bY + cZ} = \left( a g_1_{[a, b, c]} + b g_2_{[a, b, c]} + c g_3_{[a, b, c]} \right) \left( Z Y^q - Z^q Y \right)_{[a, b, c]}
\]

(4) Suppose \((a, b, c) \notin B\) then if a line \([x, y, z]\) through \((a, b, c)\) is an \(r\)-secant of \(B\), then \((x, y, z)\) is a root of \(a g_1_{[a, b, c]} + b g_2_{[a, b, c]} + c g_3_{[a, b, c]}\) with multiplicity \(r - 1\).

Proof: Easy calculations. For instance to prove (2) we simply need

\[
R_{[a, b, c]} = a g_1_{[a, b, c]} + b g_2_{[a, b, c]} + c g_3_{[a, b, c]} = 0.
\]

See Example 7.4 for showing the use of (2) above: there we get that the equation of the “canonical” Baer subplane is

\[
G_{a, b, c}(X, Y, Z) = X V^q (cVb - cbV) + Y V^q (aVb - abV) + Z V^q (aVc - acV) = 0,
\]

meaning that the Baer subplane is just \(\{(a, b, c) \in \text{PG}(2, q) : G_{a, b, c}(X, Y, Z) \equiv 0\}\).

The map \([x, y, z] \mapsto [g_1(x, y, z), g_2(x, y, z), g_3(x, y, z)]\), acting on the lines, is a remarkable one.

Proposition 21.14. Let \([x, y, z]\) be a tangent line to \(B\) at the point \((a_t, b_t, c_t) \in B\). Then \([g_1(x, y, z), g_2(x, y, z), g_3(x, y, z)]\) is also a line through \((a_t, b_t, c_t)\), different from \([x, y, z]\).

If \([x, y, z]\) is a secant line then \([g_1(x, y, z), g_2(x, y, z), g_3(x, y, z)]\) is either \([x, y, z]\) or meaningless (i.e. \([0, 0, 0]\)).

Obviously, if \(g(x, y, z) = [0, 0, 0]\) then \([x, y, z]\) is a \(\geq 2\)-secant as the \(\leq 1\)-st derivatives are 0.

Proof: Recall Theorem 7.10, here we have

\[
(a_t, b_t, c_t) = (\partial X R)(x, y, z), (\partial Y R)(x, y, z), (\partial Z R)(x, y, z) = (-yg_3(x, y, z) + zg_2(x, y, z), xg_3(x, y, z) - zg_1(x, y, z), yg_1(x, y, z) - xg_2(x, y, z)).
\]

Now the scalar product with \((g_1(x, y, z), g_2(x, y, z), g_3(x, y, z))\) vanishes.
or:
=(a_t, b_1, c_t)\cdot g(x, y, z) = (\nabla R)(x, y, z)\cdot g(x, y, z) = ((x, y, z)\times g(x, y, z))\cdot g(x, y, z) = 0.

Here \((x, y, z) \neq g(x, y, z)\) as their cross product is \((a_t, b_1, c_t)\).

If \([x, y, z]\) is a secant line then there are more than one components of \(R\) going through \((x, y, z)\) (see Theorem 7.10) hence
\[
0 = (\nabla R)(x, y, z) = (x, y, z) \times g(x, y, z).
\]

or: we can use Theorem 21.13.

We also calculate \(\nabla R\) for future use: \(\nabla R = \Psi(\nabla \circ g) + V^q \times g\).

The following is true as well. We will see (Theorem 21.19, Corollary 21.23) that if \(B\) is small, then \(R\) can be written in the form
\[
X^q(Yg_{XY} + Zg_{XZ}) + Y^q(Xg_{XY} + Zg_{YZ}) + Z^q(Xg_{ZX} + Yg_{YZ}),
\]
where the polynomials \(g_{XY},\ldots\) contain only exponents divisible by \(p\). Surprisingly or not, \(g_{XY} = -g_{YX},\ldots\), as \(0 = Xf_1 + Yf_2 + Zf_3 = XY(g_{XY} + g_{YX}) + YZ(g_{YX} + g_{YZ}) + ZX(g_{XZ} + g_{XY})\). One can take \(\partial X\partial Y, \partial Y\partial Z, \partial Z\partial X\) of both sides.

Now \(g = (g_{YX}, g_{ZX}, g_{XY})\), which is a kind of “natural choice” for \(g\).

Or: \(g_{XY} = \partial_X f_1 = -\partial_X f_2,\ldots\), or similarly (if \(p \neq 2\)) \(g = \nabla \times f\) and \(f = \nabla \times (\nabla \times f)\); \(g = \nabla^1 R \times (\nabla^q H R)\).

### 21.3 Three old curves

In this section we will present the method using three old algebraic curves. As an application we show Szőnyi’s result [123] that blocking sets of size less than \(3(q + 1)/2\) intersect every line in 1 modulo \(p\) points. This immediately implies Blokhuis’ theorem for blocking sets in \(\text{PG}(2, p)\).

Let now \(B\) be a minimal blocking set of \(\text{PG}(2, q)\). Since \(R(X, Y, Z)\) vanishes for all \((x, y, z) \in \text{GF}(q) \times \text{GF}(q) \times \text{GF}(q)\), we can write it as
\[
R(X, Y, Z) = (X^q - X)f_1(X, Y, Z) + (Y^q - Y)f_2(X, Y, Z) + (Z^q - Z)f_3(X, Y, Z) = W \cdot f,
\]
where \(f = (f_1, f_2, f_3)\) and \(\deg(f_i) \leq k\) as polynomials in three variables. Note that \(f_1\) here is the same as the polynomial \(f\) defined in Definition 21.5 and examined in Section 21.1; while \(f_2\) and \(f_3\) behave very similarly.

**Proposition 21.15.** (Lovász, Szőnyi) Let \([x, y, z]\) be a tangent line to \(B\) at the point \((a_t, b_1, c_t) \in B\). Then
\[
f(x, y, z) = (f_1(x, y, z), f_2(x, y, z), f_3(x, y, z)) = (a_t, b_1, c_t)
\]
as homogeneous triples.
**Proof:** Recall Theorem 7.10, here we have

\[
((\partial_X R)(x, y, z), (\partial_Y R)(x, y, z), (\partial_Z R)(x, y, z)) = -(f_1(x, y, z), f_2(x, y, z), f_3(x, y, z))
\]

Or:

\[
(a_t, b_t, c_t) = (\nabla R)(x, y, z) = (\nabla(W \cdot f))(x, y, z) = ((\nabla \circ W)\nabla f + (\nabla \circ f)W)(x, y, z) = -f(x, y, z) + 0 = -f(x, y, z).
\]

**Lemma 21.16.** If \(k < q - 1\) then \(V \cdot f = Xf_1 + Yf_2 + Zf_3 = 0\). (Hence \(R = V^2 f\) as well).

**Proof:** If \([x, y, z]\) is a tangent then by 21.15 \(V \cdot f\) vanishes, and by the end of Theorem 7.10 it also vanishes if \([x, y, z]\) is at least a 2-secant. As the degree is less than \(q\) we are done. **Or:** it is just Theorem 7.10 (6) with \(r = 1\).

**Note** also that \(f = \nabla^1_{\mathcal{H}} R\); and \(-f = (\nabla \circ f) V\). Moreover, in general \(-\nabla^{q-1} f = (\nabla^q \circ f) V\). It follows from the derivation of \(f \cdot V = 0\).

From Theorem 7.10 (5) one can see that each of the curves \(f_1, f_2, f_3\) go through the point \((x, y, z)\) of the dual plane corresponding to a secant line \([x, y, z]\). Where are the other (extra) points of e.g. \(f_1\)? They are exactly the points of \(r_{NX}\) of Lemma 21.6, so points on factors corresponding to points with \(a_s = 0\).

If one fixes \((Y, Z) = (y, z)\) then \(R(X, y, z)\) is divisible by \((X^q - X)\). If \(R(X, y, z) \neq 0\), so if \((0, y, z) \notin B \cap L_X\) then for an \((x, y, z) \in GF(q) \times GF(q) \times GF(q)\) if the line with equation \(xX + yY + zZ = 0\) intersects \(B\) in at least two points (cf. Proposition 21.7 (2.2)) then \(f_1(x, y, z) = 0\). One can repeat the same reasoning for \(f_2, f_3\) and this immediately gives the following lemma:

**Lemma 21.17.** ([123]) The curves \(f_i\) have almost the same set of \(GF(q)\)-rational points. The exceptional points correspond to lines intersecting \(L_X, L_Y\) or \(L_Z\) in a point of \(B\).

**Proof:** Since this observation is crucial, a direct proof is also included. Consider the Rédei polynomial \(R(X, Y, Z)\). For an element \((x, y, z) \in GF(q) \times GF(q) \times GF(q)\) we get \(-f_1(x, y, z) = \partial_X R(x, y, z)\) and similarly \(-f_2(x, y, z) = \partial_Y R(x, y, z)\) and \(-f_3(x, y, z) = \partial_Z R(x, y, z)\).

Since \(R\) is a product of linear factors and \(R(x, y, z) = 0\), \(\partial_X R(x, y, z) = 0\) if and only if there are two linear factors vanishing at \((x, y, z)\), or if \(R(X, y, z) = 0\) (i.e. \((0, -z, y) \in B\)). The similar statement holds for \(\partial_Y R\), hence the two derivatives are zero for the same values \((x, y, z)\), except in the cases described in the statement.

**Lemma 21.18.** ([123]) If \(k < q - 1\) then the polynomials \(f_1, f_2\) and \(f_3\) cannot have a common factor. Moreover, e.g. \(f_1\) and \(f_2\) have a common factor \(g\) iff \((0, 0, 1) \in B\) and \(g = Z\).
21. Blocking sets

**Proof:** Such a common factor must divide \( R(X, Y, Z) \), hence it must be divisible by \( a_iX + b_iY + c_iZ \) for some \( i \). Lemma 21.8 (2) gives \( (N = 1, k \leq q - 2) \) that the point \( (a_i, b_i, c_i) \) can be deleted, a contradiction.

Suppose that \( q \) is a common factor of \( f_1 \) and \( f_2 \), then from \( Xf_1 + Yf_2 + Zf_3 = 0 \) we have \( g|Zf_3 \).

Therefore, \( (f_1, f_2, f_3) \) is a triple of polynomials (curves) having no common factor (component), but they pass through almost the same set of \( GF(q) \)-rational points. Using Bézout’s theorem it immediately gives Lemma 21.10 back.

### 21.4 Small blocking sets

Lemmas 21.17 and 21.18 can also be used to show that all the components of \( f \) have identically zero partial derivative with respect to \( X \). Note that for any component \( h \) of \( f \) the total degree of \( h \) is the same as its degree in \( X \).

**Theorem 21.19.** \((123)\) If \( k \leq (q+1)/2 \) and \( g(X, Y, Z) \) is an irreducible polynomial that divides \( \bar{f}_1(X, Y, Z) \), then \( g_X = 0 \).

**Proof:** Suppose to the contrary that \( g \) is a component of \( \bar{f}_1 \) with nonzero partial \( X \)-derivative, denote its degree by \( \deg(g) = s \). By Theorem 21.19 the number of \( GF(q) \)-rational points on \( g \) is at least \( s(q + 2 - N_X - s) \). Since these points are also on \( f_2 \), Bézout’s theorem gives \( s(q + 2 - N_X - s) \leq sk \), since by Lemma 21.18, if \( f_2 \) and \( g \) has a common component (i.e. \( g \) itself) then it cannot be a component of \( f_3 \) and one can use Bézout for \( g \) and \( f_3 \) instead. This immediately implies \( q + 2 \leq k + N_X + s \) and from \( N_X + s \leq k \) it follows that \( k \geq (q + 2)/2 \), a contradiction.

Note that it implies that all the \( X \)-exponents appearing in \( f_1 \) are divisible by \( p \) (as \( r_{N_X} \) does not involve \( X \)); and a similar statement holds for the \( Y \)-exponents of \( f_2 \) and for the \( Z \)-exponents of \( f_3 \). Let’s define \( e \), the \((algebraic)\) exponent of \( B \), as the greatest integer such that \( f_1 \in GF(q)[X^{p^e}, Y, Z] \), \( f_2 \in GF(q)[X, Y^{p^e}, Z] \) and \( f_3 \in GF(q)[X, Y, Z^{p^e}] \). By the Theorem \( e \geq 1 \).

**Proposition 21.20.** If \( q = p \) is a prime and \( |B| < p + 2p+4-N_X \), then the curve \( \bar{f}_1 \) is irreducible (and similarly for \( \bar{f}_2, \bar{f}_3 \)).

**Proof:** Suppose to the contrary that e.g. \( \bar{f}_1 \) is not irreducible, and let \( g \) be a component of \( \bar{f}_1 \) of degree at most \( (k - N_X)/2 \). The proof of Theorem 21.19 gives \( p + 2 \leq k + N_X + \deg(g) \leq 3k/2 + N_X/2 \), that is \( 2(p+2)-N_X \leq k \).
Corollary 21.21. ([123]) If $B$ is a blocking set of size less than $3(q + 1)/2$, then each line intersects it in 1 modulo $p$ points.

Proof: Take a line $\ell$ and coordinatise such that $\ell \cap L_X \cap B = \emptyset$. If $\ell = [x, y, z]$ then $r_{N_X}(y, z) \neq 0$. Since all the components of $f_1$ contain only terms of exponent (in $X$) divisible by $p$, for any fixed $(Y, Z) = (y, z)$ the polynomial $f_1(X, y, z) = r_{N_X}(y, z)f_1(X, y, z)$ itself is the $p$-th power of a polynomial. This means that at the point $P(x, y, z)$ the “horizontal line” (i.e. through $P$ and $(1, 0, 0)$) intersects $f_1(X, Y, Z)$ with multiplicity divisible by $p$ (and the same is true for $f_1$), so by Corollary 21.21 the line $[x, y, z]$ intersects $B$ in 1 modulo $p$ points.

Note that now we have $|B| \equiv 1 \pmod{p}$. Of course, this theorem also implies Blokhuis’ theorem in the prime case.

Corollary 21.22. (Blokhuis [33]) If $q = p$ is a prime, then $|B| \geq 3(q + 1)/2$ for the size of a non-trivial blocking set.

Corollary 21.23. If $B$ is a blocking set of size less than $3(q + 1)/2$, then the $X$-exponents in $f_1$, the $Y$-exponents in $f_2$ and the $Z$-exponents in $f_3$ are 0 (mod $p^e$); moreover all the exponents appearing in $R(X, Y, Z)$, $f_1, f_2, f_3; r_{N_X}(Y, Z), r_{N_Y}(X, Z), r_{N_Z}(X, Y)$, are 0 or 1 (mod $p^e$).

Proof: The first statement is just Theorem 21.19. From this the similar statement follows for $f_1$: the $X$-exponents in $f_1$, the $Y$-exponents in $f_2$ and the $Z$-exponents in $f_3$ are 0 (mod $p^e$).

Consider a term $aX^{\alpha p^e + 1}Y^\beta Z^\gamma$ of $Xf_1$ in the identity $Xf_1 + Yf_2 + Zf_3 \equiv 0$. It should be cancelled by $Yf_2$ and $Zf_3$, which means that it should appear in either one or both of them as well with some coefficient. It cannot appear in both of them, as it would imply exponents like $X^{\alpha p^e + 1}Y^\beta Z^\gamma$, but the exponents must add up to $k + 1$, which is 2 mod $p^e$, a contradiction. So this term is cancelled by its negative, for example contained in $Yf_2$, then it looks like $-aX^{\alpha p^e + 1}Y^\beta Z^\gamma$, where the exponents, again, add up to $k + 1$, which is 2 mod $p^e$, hence $\gamma \equiv 0 \pmod{p^e}$, so the original term of $f_1$ was of the form $aX^{\alpha p^e}Y^\beta Z^\gamma Z^\gamma$.

For $r_{N_X}(Y, Z), r_{N_Y}(X, Z)$ and $r_{N_Z}(X, Y)$ recall that they are also homogeneous polynomials of total degree 1 (mod $p^e$) and for instance $f_1 = r_{N_X}f_1$ and $\deg f_1 = \deg X f_1$, so in $f_1$ the terms of maximal $X$-degree have 0 or 1 mod $p^e$ exponents (as terms of $f_1$), on the other hand they together form $r_{N_X}X^{k-N_X}$.

Finally $R = X^q f_1 + Y^q f_2 + Z^q f_3$ so $R$ has also 0 or 1 mod $p^e$ exponents only.

Note that in $\tilde{f}_1$ other exponents can occur as well. Comparing the exponents one can find $Y \partial_Y \tilde{f}_1 + Z \partial_Z \tilde{f}_1 = X \partial_X \tilde{f}_1 + Y \partial_Y \tilde{f}_1 + Z \partial_Z \tilde{f}_1 = 0$ as well.
The (geometric) exponent \( e_P \) of the point \( P \) can be defined as the largest integer for which each line through \( P \) intersects \( B \) in 1 mod \( p^{e_P} \) point. It can be proved (e.g. [39]) that the minimum of the (geometric) exponents of the points in \( B \) is equal to \( e \) defined above.

**Theorem 21.24.** [118] Let \( B \) be a blocking set with exponent \( e \). If for a certain line \( \ell \cap B = p^e + 1 \) then \( \text{GF}(p^e) \) is a subfield of \( \text{GF}(q) \) and \( \ell \cap B \) is \( \text{GF}(p^e) \)-linear.

**Proof:** Choose the frame such that \( \ell = L_X \) and \( (0, 0, 1); (0, 1, 0); (0, 1, 1) \in \ell \cap B \). Consider \( f = f_1 \), now \( r_N X(Y, Z) \) is a homogeneous polynomial of (total) degree \( p^e + 1 \), with exponents \( 0, 1, p^e \) or \( p^e + 1 \), so of form \( \alpha Y p^{e+1} + \beta Y Z p^e + \gamma Y^2 Z + \delta Z p^{e+1} + 1 \). As \( r_N X(0, 1) = r_N X(1, 0) = r_N X(1, -1) = 0 \) we have \( r_N X = Y p^{e+1} Z - Y Z p^e \). \( \Box \)

Now we can disclose one of our main goals: to get as close as we can to the proof of the conjecture that every small blocking set is linear.

By the following proposition, a blocking set with exponent \( e \) has a lot of \( (p^e + 1) \)-secants (so “nice substructures”). Similar arguments can be found in [37].

**Proposition 21.25.** Let \( P \) be any point of \( B \) with exponent \( e_P \).

(1) (Blokhuis) There are at least \( (q - k + 1)/p^{e_P} + 1 \) secant lines through \( P \).

(2) Through \( P \) there are at most \( 2(k - 1)/p^{e_P} - 1 \) long secant lines, i.e. lines containing more than \( p^{e_P} + 1 \) points of \( B \) (so at least \( q/p^{e_P} - 3(k - 1)/p^{e_P} + 2 \) \( (p^{e_P} + 1) \)-secants).

(3) There are at most \( 4k - 2p^{e_P} - 4 \) points \( Q \in B \setminus \{P\} \) such that \( PQ \) is a long secant.

(4) There are at least \( q - 3k + 2p^e + 4 \) points in \( B \) with \((\text{point-})\text{-exponent } e \).

**Proof:** (1) was proved by Blokhuis using lacunary polynomials. To prove (2) denote by \( s \) the number of \( (p^{e_P} + 1) \)-secants through \( P \) and let \( r \) be the number of \( (\geq 2p^{e_P} + 1) \)-secants through \( P \). Now \( sp^{e_P} + 2p^{e_P} + 1 \leq q + k \). From (1) \( s + r \geq (q - k + 1)/p^{e_P} + 1 \), so \( q/p^{e_P} - (k - 1)/p^{e_P} + r + 1 \leq s + 2r \leq q/p^{e_P} + (k - 1)/p^{e_P} + 2 \). Hence \( r \leq 2(k - 1)/p^{e_P} + 1 \) and \( s \geq q/p^{e_P} - (k - 1)/p^{e_P} + 1 \geq q/p^{e_P} - 3(k - 1)/p^{e_P} + 2 \).

For proving (3) subtract the number of points on \( (p^{e_P} + 1) \)-secants through \( P \) from \( |B| \), it is \( q + k - (q/p^{e_P} - 3(k - 1)/p^{e_P} + 2)p^{e_P} - 1 = 4k - 2p^{e_P} - 4 \). There is at least one point \( P \in B \) for which \( e_P = e \). On the \( p^e + 1 \)-secants through it (by (2)) we find at least \( 1 + p^e(q/p^{e} - 3(k - 1)/p^{e} + 2) \) points, each of exponent \( e \), it proves (4). \( \Box \)

Recall that there are at least \( q + 1 - k \) tangent lines through \( P \), so at most \( k \) secants.

We also know from Szőnyi [123] that \( q/p^{e_P} + 1 \leq k \leq q/p^e + q/p^{2e} + 2q/p^{3e} + \ldots \). Now
“almost all” line-intersections of $B$ are $\text{GF}(p^e)$-linear (in fact they are isomorphic to $\text{PG}(1,p^e)$ in the non-tangent case).

**Corollary 21.26.** [118] For the exponent $e$ of the blocking set, $e|h$ (where $q = p^h$).

**Proof:** By Proposition 21.25 $B$ has a lot of short secants. By Theorem 21.24 these intersections are all isomorphic to $\text{PG}(1,p^e)$, so $\text{GF}(p^e)$ is a subfield of $\text{GF}(p^h) = \text{GF}(q)$.

Now we can give a very short proof for Theorem 18.14 in the case when $p^e > 13$.

**Corollary 21.27.** [118] Small blocking sets of Rédei type, with $p^e > 13$, are linear.

**Proof:** Suppose $L_Z$ is the Rédei-line, $O = (0,0,1) \in B$, $e_O = e$, and take any $P \in B \setminus L_Z$, with $e_P = e$, and any $\alpha \in \text{GF}(p^e)$. **Claim:** $\alpha P$ (affine point!) is also in $B$. If $OP$ is a short secant then it is obvious.

Consider the short secant through $P$, there are at least $q/p^e - 3(k - 1)/p^e + 2$. Most of them, at least $q/p^e - 3(k - 1)/p^e + 2 - 4k - 2p^e - 4 < q/p^e - 7k - 3k/p^e$, say \{\ell_i : i \in I\}, contain at least two points $Q_1, Q_2 \in B$, such that $OQ_1$ and $OQ_2$ are short secants.

For any of them, say $\ell_i$, take $\alpha \ell_i$, it contains $\alpha P$. If all of $\{\alpha \ell_i : i \in I\}$ were long secants then they would contain at least $2p^e(q/p^e - 7k - 3k/p^e) > q + k$ points of $B$, contradiction if $p^e > 13$. Say $\alpha \ell$ is a short secant, then $\alpha P \in B \cap \alpha \ell$ and $e_{\alpha P} = e$ as well.

Let $U_0$ be the set of affine points of $B$ with exponent $e$. Now we have that $U_0$ is invariant for magnifications from any center in $U_0$ and with any scale $\alpha \in \text{GF}(p^e)$, so it forms a vectorspace over $\text{GF}(p^e)$. As its size is $q - 3k + 2p^e + 4 \leq |U_0| \leq q$ we have $|U_0| = q$ and it contains all the affine points of $B$.

**Consequences**

The bounds for the sizes of small blocking sets are now the following.

**Corollary 21.28.** Let $B$ be a minimal blocking set of $\text{PG}(2,q)$, $q = p^h$, of size $|B| < 3(q + 1)/2$. Then there exists an integer $e$, called the exponent of $B$, such that

$1 \leq e|h$,

and

$q + 1 + p^e(\frac{q}{p^e+1}) \leq |B| \leq \frac{1+(p^e+1)(q+1)-\sqrt{(1+(p^e+1)(q+1))^2-4(p^e+1)(q^2+q+1)}}{2}.$

If $|B|$ lies in the interval belonging to $e$ and $p^e \neq 4$ then each line intersects $B$ in $1$ modulo $p^e$ points. Most of the secants are $(p^e + 1)$-secants, they intersect $B$ in a pointset isomorphic to $\text{PG}(1,p^e)$. 

These bounds are due to Blokhuis, Polverino and Szőnyi, see [99, 123], and asymptotically they give $q + \frac{q}{p} - \frac{q^s}{p^s} + \frac{q}{p^s} - \ldots \leq |B| \leq q + \frac{q}{p} + \frac{q}{p^s} + 2\frac{q}{p^s} + \ldots$. Note that for $q = p^{2s}$ and $q = p^{3s}$, where $s$ is a prime, the lower bound is sharp: $|B| \geq q + q/p^s + 1$ and $|B| \geq q + q/p^{2s} + 1$, resp.

The $1 \mod p^r$ property was established by Szőnyi; our Theorem 21.26 shows that only a very few of the intervals of Szőnyi, Blokhuis, Polverino contain values from the spectrum of blocking sets, i.e. only those with $e|h$. The linearity of short secants is Theorem 21.24, on their number see Proposition 21.25.

Let $S(q)$ denote the set of possible sizes of small minimal blocking sets in $PG(2, q)$.

**Corollary 21.29.** Let $B$ be a minimal blocking set of $PG(n, q)$, $q = p^h$, with respect to $k$-dimensional subspaces, of size $|B| < \frac{1}{2}(q^{n-k} + 1)$, and of size $|B| < \sqrt{2}q^{n-k}$ if $p = 2$. Then

- $|B| \in S(q^{n-k})$;
- if $p > 2$ then $(|B| - 1)(q^{n-k})^{n-2} + 1 \in S((q^{n-k})^{n-1})$.

If $p > 2$ then there exists an integer $e$, called the exponent of $B$, such that

$$1 \leq e|h,$$

for which every subspace that intersects $B$, intersects it in 1 modulo $p^r$ points. Also $|B|$ lies in an interval belonging to some $e' \leq e$, $e'|h$. Most of the $k$-dimensional subspaces intersecting $B$ in more than one point, intersect it in $(p^r + 1)$ points precisely, and each of these $(p^r + 1)$-sets is a collinear pointset isomorphic to $PG(1, p^r)$.

Most of this was proved by Szőnyi and Weiner in [129]. Consider the line determined by any two points in a $(p^r + 1)$-secant $k$-subspace, this line should contain $p^r + 1$ points. Then the technique of [129] can be used to derive a planar minimal blocking set (in a plane of order $q^{n-k}$) with the same exponent $e$: firstly embed $PG(n, q)$ into $PG(n, q^{n-k})$ where the original blocking set $B$ becomes a blocking set w.r.t. hyperplanes, then choose an $(n-3)$-dimensional subspace $\Pi \subset PG(n, q^{n-k})$ not meeting any of the secant lines of $B$ and project $B$ from $\Pi$ onto a plane $PG(2, q^{n-k})$ to obtain a planar minimal blocking set, for which Theorem 21.24 and Proposition 21.25 can be applied, implying $e|h(n-k)$.

Now in $PG(n+1, q) \supseteq PG(n, q)$ build a cone $B^*$ with base $B$ and vertex $V \in PG(n+1, q) \setminus PG(n, q)$; then $B^*$ will be a (small, minimal) blocking set in $PG(n+1, q)$ w.r.t. $k$-dimensional subspaces. The argument above gives $e|h(n + 1 - k)$, so $e \mid \gcd(h(n-k), h(n+1-k)) = h$.

**Exercise 21.30.** Let $B \subset PG(2, q)$ be a double blocking set of size $2q + k$. Then

$$R(X, Y, Z) = W F(X, Y, Z) W^T,$$

where $F(X, Y, Z) = (f_{ij}(X, Y, Z))_{3 \times 3}$. 

22 Multiple blocking sets

In this section we give a generalization of the Rédei-polynomial approach of blocking sets. Some of the statements below (and much more) can be found in [37], some others in [62].

Let $B = \{(a_i, b_i, c_i)\}$ be a $t$-fold blocking set in $\text{PG}(2, q)$, having possibly weighted (i.e. multiple) points, $|B| = tq + k$.

We use the very same Rédei polynomial as we did before.

$$R(X, Y, Z) = \prod_{i=1}^{\mid B \mid} (a_i X + b_i Y + c_i Z)$$

$$= \sum_{j=0}^{\mid B \mid} X^{\mid B \mid - j} f_j(Y, Z)$$

$$= \sum_{0 \leq j_1, j_2, j_3 \leq t} f_{j_1,j_2,j_3}(X, Y, Z) (X^q - X)^{j_1} (Y^q - Y)^{j_2} (Z^q - Z)^{j_3}, \quad (\ast)$$

where $\deg(r_j) \leq j$, $j = 0, \ldots, |B|$, and each $f_{j_1,j_2,j_3}$, if present, is a homogeneous polynomial of degree $k$, for $0 \leq j_1, j_2, j_3 \leq t$, $j_1 + j_2 + j_3 = t$. The latter equation above follows from the fact that this Rédei polynomial is zero $t$ times everywhere in $\text{PG}(2, q)$.

The polynomials $f_{j_1,j_2,j_3}$ satisfy a (low degree) polynomial equation:

**Lemma 22.1.** If $k + t < q$ then

$$\sum_{0 \leq j_1, j_2, j_3 \leq t \atop j_1 + j_2 + j_3 = t} X^{j_1} Y^{j_2} Z^{j_3} f_{j_1,j_2,j_3}(X, Y, Z) = 0$$

and

$$R(X, Y, Z) = \sum_{0 \leq j_1, j_2, j_3 \leq t \atop j_1 + j_2 + j_3 = t} f_{j_1,j_2,j_3}(X, Y, Z) X^{j_1} Y^{j_2} Z^{j_3}.$$

**Proof:** For the second equation observe that in $(\ast)$ the left hand side is homogeneous of degree $tq + k$ so all the terms on the right hand side with degree $\neq tq + k$ must vanish.

As a special case, consider the lowest degree terms of $(\ast)$, they are of degree $k + t$, and they must disappear after summing them, this proves the first equation.

As a corollary note that $f_{j_1,j_2,j_3} = \mathcal{H}_X^{j_1} \mathcal{H}_Y^{j_2} \mathcal{H}_Z^{j_3} R$ as polynomials, and also for every $x, y, z \in \text{GF}(q)$ we have $f_{j_1,j_2,j_3}(x, y, z) = -\left(\mathcal{H}_X^{j_1} \mathcal{H}_Y^{j_2} \mathcal{H}_Z^{j_3} R\right)(x, y, z)$. 


We would like to understand what the (GF(q)-rational points of the) curves \( f_{j_1,j_2,j_3} \) mean. For \( f_{000} \) it is obvious: \((x,y,z)\) is a point of it if and only if the line \([x,y,z]\) is either an \((\geq t+1)\)-secant (this is the typical case), or if \([x,y,z]\) intersects the line \([1,0,0]\) in a point of \( B \). Similar statements hold for \( f_{0u0} \) and \( f_{ou0} \).

**Proposition 22.2.** If the line \([x,y,z]\) is an \((\geq t+1)\)-secant then \( f_{j_1,j_2,j_3}(x,y,z) = 0 \) for all \( 0 \leq j_1,j_2,j_3 \leq t, \ j_1 + j_2 + j_3 = t \).

**Proof:** Fix \( 0 \leq j_1,j_2,j_3 \leq t \), \( j_1 + j_2 + j_3 = t \) and some \((\geq t+1)\)-secant line \([x,y,z]\). Recall Theorem 7.10 (3) stating that \( \left( \mathcal{H}^{l_1}_{X} \mathcal{H}^{l_2}_{Y} \mathcal{H}^{l_3}_{Z} R \right)(x,y,z) = 0 \) and also \( f_{j_1,j_2,j_3}(x,y,z) = -\left( \mathcal{H}^{l_1}_{X} \mathcal{H}^{l_2}_{Y} \mathcal{H}^{l_3}_{Z} R \right)(x,y,z) \). \( \square \)

### 22.1 A \( t \pmod{p} \) result

Let \( B \) be a minimal weighted \( t \)-fold blocking set in \( \text{PG}(2,q) \), with \(|B| = tq + t + k\), where \( 2t + k < q + 2 \). From now on we are going to use a “more affine” point of view, still based on [37] and [62].

Assume that the line \( l_\infty \) is an \( m \)-secant to \( B \). Consider \( \text{PG}(2,q) \) as the affine plane \( \text{AG}(2,q) \) with \( l_\infty \) as the line at infinity. Assume that \( B \cap l_\infty = D = \{ (\infty), \ldots, (\infty), (y_1), \ldots, (y_{m-s}) \} \), where \((\infty)\) is a point of weight \( s \) of \( B \) (\( 1 \leq s \leq t \)), where some of the other points of \( D \) might be multiple points of \( B \), and that \( U = B \setminus D = \{ (a_i,b_i) : i = 1, \ldots, tq + t + k - m \} \), where \( U \) is a multiset when \( B \) has affine multiple points.

Now we redefine the Rédei polynomial associated to the \( t \)-fold blocking set \( B \), (with \((\infty)\) deleted).

**Definition 22.3 (The Rédei polynomial of the set \( B \)).**

\[
R(X,Y) = \prod_{j=1}^{m-s}(Y - y_j) \prod_{i=1}^{tq+t+k-m}(X + a_iY - b_i)
\]

\[
= \prod_{j=1}^{m-s}(Y - y_j) \sum_{i=0}^{tq+t+k-m} X^{i+q+k-m-i} r_i(Y)
\]  

\[= (X^q - X)^t f_0(X,Y) + (X^q - X)^{t-1}(Y^q - Y)f_1(X,Y)
\]

\[+ \cdots + (Y^q - Y)^t f_t(X,Y), \tag{2.2} \]

where \( \deg(r_i) \leq i, i = 0, \ldots, tq + t + k - m, \) and \( \deg(f_i) \leq k + t - s, i = 0, \ldots, t. \)

Choose a point \((b,m), b \neq b_i, m \neq y_j\). Consider \( R(X,m) = (X^q - X)^t f_0(X,m) \). By the properties of the Rédei polynomial, the line \( Y = mX + b \) intersects \( U \) in more than \( t \) points iff \( X = b \) is a root of \( R(X,m) \) with multiplicity \( \geq t+1 \) iff \((b,m)\)
is a point of the algebraic curve $f_0(X, Y)$. Considering $R(b, Y) = (Y^q - Y)^t f_t(b, Y)$ instead, we get that the line $Y = mx + b$ intersects $U$ in more than $t$ points if $(b, m)$ is a point of the algebraic curve $f_t(X, Y)$.

Therefore, these two algebraic curves $f_0$ and $f_t$ have essentially the same set of $\text{GF}(q)$-rational points.

If $m = y_j$ or $b = b_j$, and the line $Y = mx + b$ intersects $U$ in more than $t$ points, then still $f_0(b, m) = f_t(b, m) = 0$. Because of the above mentioned divisibilities, $f_0(b, m) = 0$ or $f_t(b, m) = 0$ does not imply that $Y = mx + b$ intersects $U$ in more than $t$ points.

In this section we will assume that there is no line contained in $B$. As the following theorems will show, this is no restriction when $2t + k < q + 2$.

**Theorem 22.4.** Let $B$ be a minimal weighted $t$-fold blocking set of $\text{PG}(2, q)$, with $|B| = tq + t + k$, where $2t + k < q + 2$, containing a line $\ell$. Then $B$ is the sum of the line $\ell$ and the minimal weighted $(t - 1)$-fold blocking set $B^*$, obtained from $B$ by reducing the weight of every point $P$ of $\ell$ by one.

**Proof:** Since $\ell \subseteq B$, $|\ell \cap B| \geq q + 1$.

If $|\ell \cap B| \geq q + t$, then after reducing the weight of every point of $\ell$ by one, a new weighted set $B^*$ is obtained which still intersects every line in at least $t - 1$ points. Since $B$ is a minimal weighted $t$-fold blocking set, also $B^*$ is a minimal weighted $(t - 1)$-fold blocking set.

Assume now that $q + 1 \leq |B \cap \ell| < q + t$. Reduce again the weight of every point on $\ell$ by one, and add a minimal number of simple points $P_1, \ldots, P_t$ of $\ell$ back so that again a weighted $(t - 1)$-fold blocking set $B^*$ is obtained, hence $|B^* \cap \ell| = t - 1$. We need to add at most $t - 1$ points $P_i, \ldots, P_t$ to achieve this, hence $|B^*| \leq tq + t + k - (q + 1) + t - 1 = (t - 1)q + 2(t - 1) + k$. A particular feature of a point $P_i, i = 1, \ldots,$ is that the line $\ell$ is the only $(t - 1)$-secant to $B^*$ passing through $P_i$.

Finally, we show that through $P_i$ there pass at least two $(t - 1)$-secants, hence the above case cannot occur. Now we choose our coordinate system in such a way that $(\infty) \in B$, $P_i$ is an affine point $(a, b)$, and $(\ell_{\infty} \cap \ell) \notin B^*$ and $(\infty)$ has multiplicity $s$. Suppose that $|\ell_{\infty} \cap B^*| = m$ and write up the Rédei polynomial. Since $B^*$ is a $(t - 1)$-fold blocking set, we get that:

$$R(X, Y) = \prod_{j=1}^{m-s} (Y - y_j) \prod_{i=1}^{tq + t + k - (m - s)} (X + a_i Y - b_i)$$

$$= (X^q - X)^{t-1} f_0(X, Y) + (X^q - X)^{t-2} (Y^q - Y) f_1(X, Y)$$

$$+ \cdots + (Y^q - Y)^{t-1} f_{t-1}(X, Y),$$

(2.3)

where $\deg(f_i) \leq |B^*| - q(t - 1) - s = 2(t - 1) + k - 1$, $i = 0, \ldots, t - 1$. 

II. Polynomials in geometry
The argument before this theorem shows that if a line $Y = mX + b$ intersects $B^*$ in more than $(t - 1)$ points, then $(b, m)$ is a point of the curve $f_0$. Each line except $\ell$ through the point $P_t(a, b)$ intersects $B^*$ in at least $t$ points. These lines are points of the line $X + aY - b$ in the dual plane. Hence $X + aY - b$ intersects $f_0$ in at least $q - 1$ points (we do not see the vertical line here). Since $\deg f_0 < q - 1$, Bézout’s theorem implies that the line $X + aY - b$ is a component of $f_0$. Suppose that $\ell$ is the line $\ell = Y + m'X + b'$. Then $f_0(b', m') = 0$ and since $\ell \cap \ell_\infty \notin B^*$, $\ell$ intersects $B^*$ in at least $t$ points. This is a contradiction, hence $q + 1 \leq |B \cap \ell| < q + t$ does not occur.

As the next example shows, the above theorem is sharp.

**Example 22.5.** Let $S$ be the set of points lying on the lines of a dual hyperoval in $PG(2, q)$, $q$ even. Then $S$ is a $(\frac{q}{2} + 1)$-fold blocking set of size $(\frac{q}{2} + 1)q + (\frac{q}{2} + 1)$ (each point in $S$ has multiplicity one). Note that now $t = \frac{q}{2} + 1$, $k = 0$ and $2t + k = q + 2$. If we delete a line of $S$, then the resulting point set is not a $\frac{q}{2}$-fold blocking set.

**Remark 22.6.** Theorem 22.4 has several important applications.

1. It first of all shows that when characterizing minimal weighted $t$-fold blocking sets of size $tq + t + k$, where $2t + k < q + 2$, in $PG(2, q)$, it is possible to assume that they do not contain any lines.

2. Moreover, also when proving the $t \pmod{p}$ result for a minimal weighted $t$-fold blocking set $B$, $|B| = tq + t + k$, where $2t + k < q + 2$, it is possible to assume that there are no lines contained in $B$. For, if there is a line $\ell$ contained in $B$, Theorem 22.4 shows that it is possible to reduce the weight of every point of $\ell$ by one in order to obtain a new minimal weighted $(t - 1)$-fold blocking set $B^*$. Proving the $t \pmod{p}$ result for $B$ is now reduced to proving the $(t - 1) \pmod{p}$ result for $B^*$.

3. We are also now able to characterize weighted minimal $t$-fold blocking sets of size $tq + t$ and to exclude the existence of minimal $t$-fold blocking sets of size $tq + t + 1$.

**Theorem 22.7.** A weighted $t$-fold blocking set $B$ in $PG(2, q)$, of size $|B| = tq + t$, where $2t < q + 2$, is a sum of $t$ lines.

There does not exist a weighted minimal $t$-fold blocking set $B$ in $PG(2, q)$ of size $|B| = tq + t + 1$, $2t + 1 < q + 2$.

**Proof:** Suppose that $tq + t \leq |B| \leq tq + t + 1$. Then counting the incidences of the points of $B$ with the lines through a point $R$ not in $B$, we have that through $R$ all the lines are $t$-secants if $|B| = tq + t$ and there is exactly one $(t + 1)$-secant and $q$ $t$-secants if $|B| = tq + t + 1$. Counting the incidences of the points of $B$ with the lines through a point $R' \in B$, we get that $R'$ lies on at least one line $\ell$ completely contained in $B$, when $|B| = tq + t$ and $R'$ lies on at least one line $\ell$ completely contained in $B$ or $R'$ lies on $q + 1$ $(t + 1)$-secants, when $|B| = tq + t + 1$. This latter
case means that \( R' \) is not minimal, hence we can assume that each point of \( B \) lies on at least one line completely contained in \( B \).

Now the \( t \) points of any \( t \)-secant (which must exist) and Theorem 22.4 show that \( B \) contains the sum of \( t \) lines, which is a \( t \)-fold blocking set already, of size \( tq + t \).

Remark 22.8. One can observe now that a weighted \( t \)-fold blocking set in \( \text{PG}(2, q) \), of size \( tq + t \), where \( 2t < q + 2 \), intersects every line in \( t \) \((\mod p)\) points; also that through any point of it there pass at least \( q + 1 \) \( t \)-secants.

By the theorem above, from now on we can (and will) assume that \( k \geq 2 \) for the minimal blocking sets considered.

In this section, from now on, we assume that \( B \) does not contain any line, hence \( |B| = tq + t + k \geq tq + t + 2 \), and we suppose that \( |B| < tq + (q+3)/2 \). (Note that since \( k \geq 2 \), we still have \( 2t + k < q + 2 \).) Furthermore, we choose our coordinate system so that \( \ell_{\infty} \) is a \( t \)-secant and the point \((\infty)\) in \( B \) has multiplicity \( s \), where \( 1 \leq s \leq t \).

Lemma 22.9. The polynomial \( \prod_{j=1}^{t-s}(Y - y_j) \) divides \( f_0(X, Y) \).

Proof: By (2.1),

\[
R(X, Y) = \sum_{i=0}^{tq+k} \left( r_i(Y) \cdot \prod_{j=1}^{t-s} (Y - y_j) \right) X^{tq+k-i}.
\]

So every coefficient polynomial of a term \( X^{tq+k-i} \) is divisible by \( \prod_{j=1}^{t-s} (Y - y_j) \). By (2.2), the high degree part \( \prod_{j=1}^{t-s} (Y - y_j) \cdot X^{tq+k} + \cdots + r_k(Y) \cdot \prod_{j=1}^{t-s} (Y - y_j) \cdot X^{tq} \) must be equal to \( X^{tq} f_0(X, Y) \), when one compares the \( X \)-degrees of the two expressions (2.1) and (2.2) for \( R(X, Y) \). So \( \prod_{j=1}^{t-s} (Y - y_j) \) divides \( f_0(X, Y) \).

If \( X = 0 \) intersects \( U \) in the, possible weighted, points \((0, b_j), \ j = 1, \ldots, z\), then a similar argument shows that \( \prod_{b_j} (X - b_j) \) divides \( f_t(X, Y) \), where the product is taken over the values \( b_j \), according to their weights.

Theorem 22.10. Let \( B \) be a minimal weighted \( t \)-fold blocking set of \( \text{PG}(2, q) \), with \( |B| = tq + t + k < tq + (q+3)/2 \) and \( k \geq 2 \). Then every point of \( B \) lies on at least \( q + 1 - k - t \) different \( t \)-secants.

Proof: Let \( P = (a, b) \in U \) and suppose \((\infty) \in B, \ |l_{\infty} \cap B| = t \). Assume that \( P \) lies on more than \( k + t \) different lines sharing at least \( t + 1 \) points with \( B \). Then
more than \( k \) of those lines intersect \( l_\infty \) in a point not belonging to \( B \). Each of these latter lines defines a point of \( f_0(X,Y)/\prod_{j=1}^{t+1} (Y - y_j) \). More precisely, they define intersection points, in the dual plane, of the algebraic curve \( f_0(X,Y)/\prod_{j=1}^{t+1} (Y - y_j) = 0 \) with the line \( X + aY - b = 0 \). The polynomial \( f_0(X,Y)/\prod_{j=1}^{t+1} (Y - y_j) \) has at most degree \( k \), so by Bézout’s theorem, the linear term \( X + aY - b \) is a factor of \( f_0(X,Y)/\prod_{j=1}^{t+1} (Y - y_j) \).

Consider a line through \( P \) with slope \( m \neq y_j, m \neq \infty \), so that we can use the arguments above.

Plugging \( Y = m \) into \( R(X,Y) \), we get

\[
R(X,m) = \prod_{j=1}^{t+1} (m - y_j) \prod_{i=1}^{t+1} (X + a_im - b_i) = (X^q - X)^t f_0(X,m).
\]

The fact that \( X + aY - b \) is a linear factor of \( f_0 \) means geometrically that the lines through \( P \) with slope \( m \neq y_j, m \neq \infty \), intersect \( U \) in at least \( t + 1 \) points.

Assume that a line \( \ell \) through \( P \) with slope \( m = y_j \) or \( m = \infty \) is a \( t \)-secant. Then replace the line at infinity \( l_\infty \) by a new line at infinity \( l'_\infty \) not intersecting \( \ell \) in a point of \( B \), and containing exactly \( t \) points of \( B \).

In the affine plane with \( l_\infty^* \) as line at infinity, we use the same notations, but in combination with the symbol \( * \) to make the distinction with the notations used in the original affine plane. The theorem of Bézout will now lead to the desired contradiction.

Through \( P \), there pass at least \( q + 1 - t \) lines that intersect \( B \) in at least \( t + 1 \) points. Whenever a line contains at least \( t + 1 \) affine points of \( B \), it defines a point of \( f_0^* \) (see the reasoning at the beginning of this section). This implies that if the coordinates of \( P \) in the new coordinate system are equal to \((a^*, b^*)\), then the line \( X^* + a^*Y^* - b^* = 0 \) meets the curve \( f_0^* \) in at least \( q + 1 - t - t \) points.

We subtracted \( t \) from \( q + 1 - t \) since \( t \) of those lines through \( P \) could contain a point of \( B \) belonging to \( l_\infty^* \). Then such a line through \( P \), not containing a point at infinity of \( B \), and containing at least \( t + 1 \) affine points \((a^*_i, b^*_i)\) defines a point of the polynomial \( f_0^*(X^*,Y^*)/\prod_{j=1}^{t+1} (Y^* - y_j^*) \). This latter polynomial has degree at most \( k < (q + 3)/2 - t \).

Then, if \( q + 1 - 2t \geq (q + 3)/2 - t > k \geq \deg(f_0^*) \), Bézout’s theorem implies that this linear component \( X^* + a^*Y^* - b^* \) is a component of \( f_0^* \), so also the line \( \ell \) through \( P \) intersects \( U^* \) in at least \( t + 1 \) points, since its point at infinity in the new coordinate system does not lie in \( B \), and so the observations made before this theorem apply. Note that the condition \( q + 1 - 2t \geq (q + 3)/2 - t \) implies that \( t \leq (q - 1)/2 \).

We have proved that all lines through \( P \in B \) are at least \((t + 1)\)-secants to \( B \); this contradicts the minimality of \( B \). So a point of \( B \) lies on at most \( k + t \) lines sharing more than \( t \) points with \( B \).
Corollary 22.11. Let $B$ be a weighted $t$-fold blocking set of $\text{PG}(2,q)$, with $|B| = tq + t + k < tq + (q + 3)/2$ and $2t < q + 2$. Assume that $P$ is an essential point of $B$. Then there are at least $q + 1 - k - t$ different $t$-secants through $P$.

Proof: Delete the non-essential points of $B$ one-by-one until a minimal $t$-fold blocking set $B'$ is obtained. By Theorem 22.10 and Remark 22.8, there will be at least $q + 1 - (|B'| - tq)$ different $t$-secants of $B'$ through $P$. Now if we add back the points of $B \setminus B'$, then through $P$, we will see at least $q + 1 - (|B'| - tq) - |B \setminus B'|$ $t$-secants to $B$.

Let $B$ be a minimal weighted $t$-fold blocking set of size $tq + t + k$, where $t + k < (q + 3)/2$ and $k \geq 2$. Recall the definition of the Rédei polynomial from the beginning of this section, the following lemma is straightforward.

Lemma 22.12. If a line $Y = mX + b$ intersects $B \cap U$ in more than $t$ points, then $f_0(b, m) = \cdots = f_t(b, m) = 0$.

We will also need

Lemma 22.13. The algebraic curve $f_0(X, Y) = 0$ does not have linear components depending on the variable $X$.

Proof: Such a linear component depending on $X$ should have the form $X + aY - b = 0$. The proof of Theorem 22.10 then shows that the point $P = (a, b)$ is a non-essential point of $B$; which contradicts the minimality of $B$.

Lemma 22.14. If $B$ is minimal, then the polynomials $f_0, \ldots, f_t$ cannot have a common divisor different from $Y - y_j$.

Proof: Such a polynomial would divide $R(X, Y)$; so would be linear. This can only be of the form $Y - y_j$.

We now come to the main theorem of this section: the proof of the $t \ (\text{mod} \ p)$ result.
22. Multiple blocking sets

Theorem 22.15. Let $B$ be a minimal weighted $t$-fold blocking set in $\text{PG}(2, q)$, $q = p^h$, $p$ prime, $h \geq 1$, with $|B| = tq + t + k$, $t + k < (q + 3)/2$, $k \geq 2$. Then every line intersects $B$ in $t \pmod p$ points.

Proof: By Remark 22.6, it is possible to assume that $B$ does not contain any lines. We will assume that the line at infinity intersects $B$ in $t$ points. Let $h(X, Y)$ be an absolutely irreducible component of $f_0(X, Y)/\prod_{j=1}^{t-s}(Y - y_j)$ of degree larger than one. Similar arguments as in the case $t = 1$ imply that $\partial_X h \equiv 0$.

If $Y = m \neq y_i$, we obtain $R(X, m) = (X^q - X)^i f_0(X, m)$, having $t \pmod p$ solutions since $f_0(X, m)$ is a $p$-th power. So every line $Y = mX + b$, not containing a point of $B$ at infinity, intersects $B$ in $t \pmod p$ points.

For every line $\ell$ of which we are not yet sure that it intersects $B$ in $t \pmod p$ points, it is possible to find a new line at infinity intersecting $B$ in $t$ points and intersecting $\ell$ in a point not belonging to $B$. Repeating the previous arguments now shows that also $\ell$ intersects $B$ in $t \pmod p$ points.

The next corollary follows from Theorem 22.10 and Remark 22.8.

Corollary 22.16. Let $B$ be a weighted $t$-fold blocking set in $\text{PG}(2, q)$, $q = p^h$, $p$ prime, $h \geq 1$, with $|B| = tq + t + k$, $t + k < (q + 3)/2$, $2t < q + 2$. Assume that all the points of $B$ on the line $\ell$ are essential. Then $\ell$ intersects $B$ in $t \pmod p$ points.

When each line intersects $B$ in $t \pmod q$ points, then the characterization of $B$ is immediate.

Proposition 22.17. Let $B$ be a minimal weighted $t$-fold blocking set in $\text{PG}(2, q)$ of size $tq + t + k$, where $t + k < (q + 3)/2$, $k \geq 2$. Assume that each line intersects $B$ in $t \pmod q$ points. Then $B$ is a sum of $t$ (not necessarily different) lines.

Proof: Let $\ell$ be a line of $\text{PG}(2, q)$ not contained in $B$. Let $P \in \ell \setminus B$. Since all the lines, different from $\ell$, through $P$ contain at least $t$ points of $B$, $\ell$ contains at most $t + k$ points of $B$.

Every point $R$ of $B$ lies on at least one line containing more than $t$ points of $B$, so on a line $\ell$ containing at least $t + q$ points of $B$. Since $t + k < t + q$, the preceding paragraph implies that $\ell$ is contained in $B$. By Theorem 22.4, $B$ is the sum of this line $\ell$ and a $(t - 1)$-fold blocking set $B^*$ intersecting every line in $(t - 1) \pmod q$ points. Repeating the above argument shows that $B$ is a sum of $t$ lines.

These results are enough to give a determine a lower bound on the size of a minimal weighted $t$-fold blocking set $B$ in $\text{PG}(2, q)$, $q = p^h$, $p$ prime, $h \geq 1$. 

We again assume that \( B \) does not contain any lines, for it is trivially possible to construct a minimal weighted \( t \)-fold blocking set in \( \text{PG}(2, q) \) by taking a sum \( B \) of \( t \) lines. Then \( |B| = t(q + 1) \).

**Theorem 22.18.** Let \( B \) be a minimal weighted \( t \)-fold blocking set in \( \text{PG}(2, q) \), \( q = p^h \), \( p \) prime, \( h \geq 1 \), with \( |B| = tq + t + k \), \( t + k < (q + 3)/2 \), containing no lines.

Assume that \( h(X, Y) \) is a component of \( f_0 \), which can be written as \( h(X, Y) = g(X^{p^r}, Y) \) with \( g'_X \neq 0 \). Then \( k \geq \frac{2 + p^r}{p^r + 1} - t + 1 \).

We omit the details now, the interested reader may see Proposition 3.6 in [37] for all the ideas needed.

# 23 Stability

We start with a result of [113], which is a generalization of the main result of [124]. Let \( D \) be a set of directions in \( \text{AG}(2, q) \). A set \( U \subseteq \text{AG}(2, q) \) is called a \( D \)-set if \( U \) determines precisely the directions belonging to \( D \).

**Theorem 23.1.** Let \( U \) be a \( D \)-set of \( \text{AG}(2, q) \) consisting of \( q - \varepsilon \) points, where \( \varepsilon \leq \alpha \sqrt{q} \) and \( |D| < (q + 1)(1 - \alpha) \), \( 1/2 \leq \alpha \leq 1 \). Then \( U \) is incomplete, i.e. it can be extended to a \( D \)-set \( Y \) with \( |Y| = q \).

**Proof:** In the proof we follow the method of Section 11.

Let \( U = \{(a_i, b_i) : i = 1, ..., q - \varepsilon\} \), suppose \((\infty) \in D\).

If \((y) \not\in D\) then the values \(a_iy - b_i\) are all distinct elements of \( \text{GF}(q) \). Define the Rédei polynomial of \( U \) as

\[
R(X, Y) = \prod_{i=1}^{q-\varepsilon}(X + a_iY - b_i) = \sum_{j=0}^{q-\varepsilon} r_j(Y)X^{q-\varepsilon-j}.
\]

Then \( \deg(r_j) \leq j \). Let \( R_y(X) = R(X, y) \), then \( R_y|_{(X^q - X)} \) if and only if the elements in \( A(y) = \{-a_iy + b_i : i = 1, ..., q - \varepsilon\} \) are pairwise distinct, that is, when \((y) \not\in D\). (We define \( A(Y) \), a set of linear polynomials, in the similar way.)

In this case let \( \sigma_j = \sigma_j(A(y)) \) be the \( j \)-th elementary symmetric polynomial of the elements in \( A(y) \), and \( \sigma^*_j = \sigma^*_j(A(y)) = \sigma_j(\text{GF}(q) \setminus A(y)) \) be the \( j \)-th elementary symmetric polynomial of the remaining elements. Note that \( \sigma_j = (-1)^jr_j \), and by induction, using the recursive formula

\[
\sigma^*_j = -\sigma_j - \sum_{k=1}^{j-1} \sigma_k \sigma^*_{j-k},
\]

hence in principle \( \sigma^*_j \) can be expressed by the \( \sigma_i \)-s, so by the \( r_i \)-s \((i = 0, ..., j)\), which means that \( \sigma^*_j \) can be considered as a polynomial in \( Y \). Now the recursive formula shows that \( \deg_Y(\sigma^*_j) \leq j \) as well. (See also Section 25 on nuclei.)
Define the polynomial \( f(X, Y) = X^\varepsilon - \sigma_1^* X^{\varepsilon-1} + \sigma_2^* X^{\varepsilon-2} - + + (1)^\varepsilon \sigma_\varepsilon^* \). Here \( f \) is of total degree \( \varepsilon \) and if \((y_0) \notin D\), then \( R(X, y_0)f(X, y_0) = X^q - X \). For such \( y_0 \)-s, we have
\[
f(X, y_0) = \prod_{\beta \in GF(q) \setminus A_{y_0}} (X - \beta),
\]
so the curve \( \mathcal{F} \) defined by \( f(X, Y) = 0 \) has precisely \( \varepsilon \) distinct simple points \((x, y_0)\). So \( \mathcal{F} \) has at least
\[
N \geq (q + 1 - |D|)\varepsilon > (q + 1)\alpha\varepsilon
\]
simple points in \( PG(2, q) \).

Now, using Lemma 10.15 with the same \( \alpha \), we have that \( \mathcal{F} \) has a linear component \( X + aY - b \) over \( GF(q) \). Then \(-ay + b \notin A_y\) if \((y) \notin D\). Let \( U^* = U \cup \{(a, b)\} \), then \( R^*(X, y) = R(X, y)(X + ay - b) \) divides \( X^q - X \) for all \((y) \notin D\), as \( X^q - X = R(X, y)f(X, y) \) and \((X + aY - b)|f(X, Y)\). Hence \( U^* \) does not determine any directions not in \( D \), so \( U^* \) is also a \( D \)-set. Repeating this procedure we end up with a \( D \)-set consisting of \( q \) points.

Comparing this to Theorem 18.14 one can see that if \( U \subset AG(2, q) \) determines \( N \leq \frac{q+1}{\delta} \) directions and \( U \) is of size \( q - \varepsilon \), with \( \varepsilon \) small then still we know the structure of \( U \).

The analogue of Theorem 23.1 is the following version of the results of [69, 47]:

**Theorem 23.2.** Let \( U \subset AG(2, q) \) be a pointset of size \(|U| = q + \varepsilon\), where \( \varepsilon \leq \alpha \sqrt{q} - 1 \) and \( \frac{1}{2} + \frac{1}{\sqrt{q}} \leq \alpha \leq 1 \). Suppose that there are more than \( \alpha(q + 1) \) points on \( \ell_\infty \), through which every affine line contains at least one point of \( U \); let the complement of this pointset on \( \ell_\infty \) be called \( D \). Then one can find \( \varepsilon \) points of \( U \), such that deleting them the remaining \( q \) points will still block all the affine lines through the points of \( \ell_\infty \setminus D \).

**Proof:** Let \( U = \{(a_i, b_i) : i = 1, \ldots, q + \varepsilon\} \), suppose \((\infty) \in D\). Define the Rédei polynomial of \( U \) as
\[
R(X, Y) = \prod_{i=1}^{q+\varepsilon} (X + a_i Y - b_i) = \sum_{j=0}^{q+\varepsilon} r_j(Y)X^{q+\varepsilon-j},
\]
Then \( \deg(r_j) \leq j \). Let \( R_y(X) = R(X, y) \), then \( (X^q - X) R_y \) if and only if \( GF(q) \subset A(y) = \{-a_i y + b_i : i = 1, \ldots, q + \varepsilon\} \) for the multiset \( A(y) \), that is, when \((y) \notin D\). Similarly, let \( A(Y) = \{-a_i Y + b_i : i = 1, \ldots, q + \varepsilon\} \), a set of linear polynomials. In this case let \( \sigma_j = \sigma_j(A(y)) \) be the \( j \)-th elementary symmetric polynomial of the elements in \( A(y) \), and \( \bar{\sigma}_j = \bar{\sigma}_j(A(y)) = \sigma_j(A(y) \setminus GF(q)) \) be the \( j \)-th elementary symmetric polynomial of the “extra” elements. Note that \( \sigma_j = (-1)^j r_j \), and like in Section 11, we have \( \bar{\sigma}_j = \sigma_j \), and we can define
\[
\bar{\sigma}_j(Y) \overset{\text{def}}{=} \sigma_j(Y) = (-1)^j r_j(Y).
\]
Define the polynomial \( f(X, Y) = X^\varepsilon - \bar{\sigma}_1 X^{\varepsilon-1} + \bar{\sigma}_2 X^{\varepsilon-2} - \ldots + (-1)^{\varepsilon} \bar{\sigma}_\varepsilon \). Here \( f \) is of total degree \( \varepsilon \) and if \((y_0) \notin D\) then \( R(X, y_0) = (X^q - X)f(X, y_0) \). For such \( y_0 \)-s, we have
\[
f(X, y_0) = \prod_{\beta \in A \setminus \text{GF}(q)} (X - \beta),
\]
so the curve \( F \) defined by \( f(X, Y) = 0 \) has precisely \( \varepsilon \) distinct simple points \((x, y_0)\).

So \( F \) has at least \( N \geq (q + 1 - |D|)\varepsilon > (q + 1)\alpha\varepsilon \)
simple points in \( \text{PG}(2, q) \).

Now, using Lemma 10.15 with the same \( \alpha \), we have that \( F \) has a linear component \( X + aY - b \) over \( \text{GF}(q) \). Then \(-ay + b\) has multiplicity at least two in \( A(y) \) if \((y) \notin D\). Now \((X^q - X)(X + ay - b)\) divides \( R(X, y) \) for all \((y) \notin D\), as \( R(X, y) = (X^q - X)f(X, y) \) and \((X + aY - b)f(X, Y)\). Suppose that the point \((a, b) \notin U\).

Then counting the points of \( U \) on the lines connecting \((a, b)\) to the points of \( \ell_{\infty} \setminus D \),
we find at least \( 2|\ell_{\infty} \setminus D| \geq q + 1 + \varepsilon \) points (at least 2 on each), a contradiction.

Hence \((a, b) \in U\), and one can delete \((a, b)\) from \( U \).
Repeating this procedure we end up with a set consisting of \( q \) points and still not determining any direction in \( \ell_{\infty} \setminus D \).

\[ \]

Usually it is difficult to prove that, when one finds the “surplus” element(s), then they can be removed, i.e. they were there in the original set. Here the “meaning” of a non-essential point (i.e. each line through it is an \( \geq 2 \)-secant) helped.

**Exercise 23.3.** Prove that if \( S_1, S_2 \subseteq \text{PG}(2, q) \) are two pointsets, with characteristic vectors \( v_{S_1}, v_{S_2} \) and weight (or line-intersection) vectors \( m_{S_1} = Av_{S_1}, m_{S_2} = Av_{S_2} \), then
\[
||m_{S_1} - m_{S_2}||^2 = ||v_{S_1} - v_{S_2}|| + q \cdot ||v_{S_1} \triangle v_{S_2}||
\]
where ||\( x || = \sqrt{\sum x_i^2} \) and \( \triangle \) denotes symmetric difference.

Note that it means that the (euclidean) distance of the line-intersection vectors of any two pointsets is at least \( \sqrt{q} \).

The next sections are taken from Szönyi-Weiner [130], which is a collection of wonderful stability results, most (but not all) of them based on the new resultant method of the authors.

### 23.1 Stability theorems for small blocking sets and the Szönyi-Weiner method

If we delete a few (say, \( \varepsilon \)) points from a blocking set, then we get a point set intersecting almost all except of at most a few (\( \varepsilon q \)) lines. A point set which is “close” to be a blocking set is a point set that intersects almost all lines. A stability
23. Stability

The type question asks whether all point sets having only a few 0-secants can be obtained from a blocking set by deleting a few points of it. Of course, if we only had a few 0-secants, then by adding one-one point to each of these lines (hence in total still only a few points), we obtain a blocking set. So we have to be careful by choosing sensible bounds in such stability theorems.

The next result is about the stability of the smallest blocking sets, that is, about the lines.

**Result 23.4.** (Erdős and Lovász, [61]) A point set of size \( q + 1 \) in \( \text{PG}(2, q) \), with less than \( q\sqrt{q} - q \) skew lines always contains at least \( q - \sqrt{q} \) points from a line.

Note that this result is sharp, since if we delete \( \sqrt{q} \) points from a Baer subplane, then the resulting set will have \( q\sqrt{q} - q \) skew lines exactly and it has at most \( \sqrt{q} + 1 \) collinear points.

By the result of Blokhuis and Brouwer (Exercise 12.5) we know that through an essential point of a blocking set \( B \) there pass at least \( 2q + 1 - |B| \) tangents. This result helps to estimate the number of 0-secants we get by deleting an essential point from a small blocking set. So if we delete \( \varepsilon \) essential points from a small blocking set then we get at least \( \varepsilon \frac{q}{2} \) skew lines. The main result of this section is the following theorem.

**Theorem 23.5.** Let \( B \) be a point set in \( \text{PG}(2, q) \), \( q \geq 81 \), of size less than \( \frac{3}{2}(q + 1) \). Denote the number of 0-secants of \( B \) by \( \delta \), and assume that it is at most \( \frac{1}{3}q\sqrt{q} \), when \( |B| < q + \sqrt{q} \) and at most \( \frac{q^2}{6(|B| - q)} \) otherwise. Then \( B \) can be obtained from a blocking set by deleting at most \( \frac{2\delta}{q} \) points of it.

Note that the assumptions in this theorem are chosen such that \( \delta \leq \frac{1}{3}q\sqrt{q} \) and \( \delta \leq \frac{q^2}{6(|B| - q)} \), \( q \geq 81 \) will both hold whenever \( |B| < \frac{3}{2}(q + 1) \).

When the size of \( B \) is large, the theorem above is immediate.

**Lemma 23.6.** Assume that for the size of \( B \), \( \frac{3}{4}q \leq |B| < \frac{3}{2}(q + 1) \) holds and \( \delta \leq \frac{q^2}{6(|B| - q)} \), \( q \geq 81 \). Then \( B \) can be obtained from a blocking set by deleting at most \( \frac{2\delta}{q} \) points of it.

**Proof:** Since any two lines intersect, we can add at most \( \frac{q}{2} \) points to \( B \) so that we get a blocking set \( B' \). This blocking set will have size at most \( |B| + \frac{q^2}{6(|B| - q)} \). This function takes its maximum at \( |B| = \frac{3}{4}q \) when \( |B| \) is in the interval \( \left[ \frac{3}{8}q, \frac{3}{2}q + 1 \right] \) (and \( q \geq 81 \)). Hence \( |B'| \leq \frac{23}{12}q \) and so by Result 12.5, through each of its essential point there pass at least \( \frac{1}{12}q \) tangents. Since \( \delta \leq \frac{4}{3}q \), this shows that indeed we could have added at most \( \frac{4}{3}q / \frac{1}{12}q = 16 \) points to \( B \) to obtain a blocking set of size at most \( \frac{1}{2}q + 17 \). Again by Result 12.5, through each of its essential point there pass at least \( \frac{1}{2}q - 16 \) tangents, hence again Result 12.5 implies that indeed
we needed less than 5 points (here we use again that $q \geq 81$). Repeating this argument once more, we see that we need at most 2 ($\leq \frac{2\sqrt{q}}{q}$) points.

As the above lemma shows, Theorem 23.5 is weak when the size of $B$ is in the upper part of the given interval. The aim of the next two sections is to improve on this result, when $|B|$ is relatively large.

To prove Theorem 23.5 we need the following two lemmas.

**Lemma 23.7.** Let $S$ be a point set of size less than $2q$ in $\text{PG}(2, q)$, $q \geq 81$, and assume that the number of external lines $\delta$ of $S$ is less than $(q^2 - q)/2$.

1. Denote by $s$ the number of external lines of $B$ passing through a point $P$. Then $(2q + 1 - |S| - s)s \leq \delta$.

2. If $|S| \leq \frac{5}{4}q$ and $\delta \leq \frac{1}{3}\sqrt{q}q$, then through any point there are at most $\frac{\delta}{2} + \frac{1}{2}$ or at least $2q + 1 - |S| - \frac{\delta}{2} - \frac{1}{2}$ external lines to $S$.

**Proof:** Let $\ell_\infty$ be a line intersecting $S$ in $k > 0$ points and let $(\infty) \in S$. Furthermore, assume that $|S| - k \neq q$. This can be done, otherwise every line that intersects $S$ would intersect it in $k$ points. Since $|S| < 2q$, counting the points of $S$ through a point in $S$, we get that $k = 2$. Hence $S$ is a hyperoval, but this contradicts our assumption on $\delta$.

Assume that there is an ideal point different from $(\infty)$ through that there pass $t$ affine lines intersecting $S \setminus \ell_\infty$ in at least 1 point. Denote by $n_{t+h}$, the number of ideal points different from $(\infty)$ through that there pass $(t+h)$ affine lines intersecting $S \setminus \ell_\infty$. Hence by Lemma 12.6, $\sum_{h=1}^{q-t}hn_{t+h} \leq (|S| - k - t)(q - t)$.

Suppose that $P$ is a point of $\ell_\infty \setminus S$ and assume that through $P$ there pass $q - t$ affine lines not intersecting $S \setminus \ell_\infty$. Denote by $r_{(q-t)-h}$, the number of ideal points different from $(\infty)$ through that there pass $(q - t) - h$ affine skew lines. Through these points there pass $t+h$ affine lines intersecting $S \setminus \ell_\infty$, hence $\sum_{h=1}^{q-t}hr_{(q-t)-h} = \sum_{h=1}^{q-t}hn_{t+h}$ and from above this is at most $(|S| - k - t)(q - t)$. Hence by counting the number of skew lines through the points of $\ell_\infty \setminus S$, we get a lower bound on $\delta$:

$$
(q + 1 - k)(q - t) - \sum_{h=1}^{q-t}hr_{(q-t)-h} \leq \delta. 
$$

Using $\sum_{h=1}^{q-t}hr_{(q-t)-h} = \sum_{h=1}^{q-t}hn_{t+h} \leq (|S| - k - t)(q - t)$ and substituting $s = (q - t)$, we get the first part of the lemma:

$$
(2q + 1 - |S| - s)s \leq \delta. 
$$

To prove the second part of the lemma, we estimate the discriminant of (2.5) (from below) by $(2q + 1 - |S|) - (\frac{2\sqrt{q}}{q} + 1)$ (here we use the fact that $\delta \leq \frac{1}{3}q\sqrt{q}$).
Hence $s \leq \frac{\delta}{2q+1-|S|} + \frac{1}{2}$ or $s \geq 2q + 1 - |S| - \frac{\delta}{2q+1-|S|} - \frac{1}{2}$.

**Lemma 23.8.** Assume that $|B| \leq \frac{5}{4} q$. Let $N$ be the set of points through that there are at least $2q + 1 - |B| - \frac{\delta}{2q+1-|B|} - \frac{1}{2}$ external lines to $B$. Then $B \cup N$ is a blocking set.

**Proof:** Assume to the contrary that there exists a line $\ell$ external to $B$, so that through each point of $\ell$ there pass less than $2q + 1 - |B| - \frac{\delta}{2q+1-|B|} - \frac{1}{2}$ external lines of $B$. Then by Lemma 23.7 (2), through each of these points there pass at most $\frac{\delta}{2q+1-|B|} + \frac{1}{2}$ external lines (including $\ell$). Counting the external lines of $B$ through the points of $\ell$, we get an upper bound on $\delta$.

$$\delta \leq 1 + (q + 1)(\frac{\delta}{2q+1-|B|} - \frac{1}{2}) = \delta + \frac{\delta(|B| - q)}{2q+1-|B|} - \frac{q+1}{2} + 1 \quad (2.6)$$

This is a contradiction, since $\delta \leq \frac{q^2}{4(|B| - q)}$. Hence on each of the external lines, there is at least one point through that there pass at least $2q + 1 - |B| - \frac{\delta}{2q+1-|B|} - \frac{1}{2}$ external lines.

**Proof of Theorem 23.5:** By Lemma 23.6, we may assume that $|B| \leq \frac{5}{4} q$. We construct the point set $B'$, by adding the points through that there pass at least $2q + 1 - |B| - \frac{\delta}{2q+1-|B|} - \frac{1}{2}$ external lines to $B$. Since $\delta \leq \frac{1}{4} q \sqrt{q}$ and $|B| \leq \frac{5}{4} q$, there pass at least $\frac{11}{4} q$ skew lines through such points. Counting the external lines through these points, we see at least $\frac{11}{4} q + (\frac{11}{4} q - 1) + (\frac{11}{4} q - 2) + \ldots$ 0-secants, which shows that there were less than $\lceil \frac{3}{4} q \rceil$ such points (here we use that $q \geq 81$). Hence $|B'| < 3q/2$. By Lemma 23.8, $B'$ is a blocking set. Let $\varepsilon$ be the minimum number of points we need to add to $B$ in order to obtain a blocking set $B^*$. ($|B^*| \leq |B'| < 3q/2$). By Result 12.5, through each essential point of this blocking set (such are the points of $B^* \setminus B$) there pass at least $2q + 1 - |B| - \varepsilon \geq q/2$ tangents, i.e., external lines to $B$. Hence in total $B$ has at least $\varepsilon q/2$ external lines, which shows that $\varepsilon \leq 2\delta/q$.

**23.2 Stability theorems for blocking sets: the prime case**

In this section we will improve on the stability theorem of the previous section, when the order of the plane is prime. Blokhuis ([33]) proved that a blocking set with less than $\frac{3}{4} (q + 1)$ points must contain a line. We are going to show that if $B$ is a point set with $|B| \leq \frac{3}{4} (q + 1)$, then it contains a huge part of a line. Here $\varepsilon$ can be even be $cq$, where $c$ is a small constant. The proof is motivated by [33].
Lemma 23.9. Let $B$ be a point set in $\text{PG}(2, q)$, $|B| < \frac{3}{2}(q + 1)$. Assume that there are at most $\varepsilon(q + 1)$ skew lines to $B$. Then the total number $\tau$ of 1-secants of $B$ is at least $(q + 1)(2q - |B| - 2\varepsilon)$. Hence there is a point $P$ of $B$ so that there are at least $\frac{3}{2}(2q - |B| - 2\varepsilon)$ 1-secants through $P$.

Proof: Take a 0-secant $\ell$ of $B$. If there is no such line then $B$ is a blocking set and (by Result 12.5) through any essential point of $B$ there pass at least $\frac{1}{2}(q + 1) - 1$ tangents. Let the points of $\ell$ be denoted by $P_1, \ldots, P_{q+1}$ and let $\nu_i$ be the number of 0-secants, $\tau_i$ be the number of tangents through $P_i$. Looking at $B$ from $P_i$ one gets that $q - (\nu_i + \tau_i) \leq (|B| - \tau_i)/2$, which implies that $2\nu_i + \tau_i \geq 2q - |B|$. Summing over all $i$ we get that $(q + 1)(2q - |B|) \leq 2\varepsilon(q + 1) + \tau$, from which $\tau \geq (q + 1)(2q - |B| - 2\varepsilon)$ follows. On the other hand, if we add up the number of tangents at the points of $B$, we get $\tau$, so there is a point which has at least the average number of tangents.

Theorem 23.10. Let $\Delta$ be the integer part of $\sqrt{2\varepsilon(q + 1)} - 1$. Let $B$ be a set of points of $\text{PG}(2, q)$, $q = p$ prime, that has at most $\varepsilon(q + 1)$ 0-secants for some $\varepsilon < \frac{1}{4}(q - 6)$. Suppose that $|B| < \frac{3}{2}(q + 1 - \Delta)$. Then there is a line that contains at least $q - 2\varepsilon$ points of $B$.

Proof: Choose the coordinate system in such a way that $(\infty)$ is a point of $B$ with at least $\frac{3}{2}(2q - |B| - 2\varepsilon)$ tangents, one of them being the line at infinity. Let $U = \{(a_i, b_i) : i = 1, \ldots, |B| - 1\}$ be the affine part of $B$. The 0-secants of $B$ can be written as $Y = m_jX + b_j$, $j = 1, \ldots$. Consider the polynomial $a(x, y)$ of smallest degree $\Delta$, which vanishes at the points $(b_j, m_j)$, $j = 1, \ldots, \varepsilon(q + 1)$. By Exercise 10.2, $\Delta \leq \sqrt{2\varepsilon(q + 1)} - 1$. Now write up the polynomial

$$R(X, Y) = \left(\prod_i (X + a_iY - b_i)\right) a(X, Y).$$

The first product is the Rédei polynomial of $U$. This polynomial $R$ vanishes for every $(x, y)$, hence it can be written as

$$R(X, Y) = (X^q - X)f(X, Y) + (Y^q - Y)g(X, Y),$$

where $\deg(f), \deg(g) \leq |B| - 1 - q + \Delta$. As in Blokhuis [33], consider the terms of highest degree of this equation and substitute $Y = 1$ in it. Then we get a polynomial equation

$$r^*(X) = \left(\prod_i (X + a_i)\right) a^*(X) = X^q f^*(X) + g^*(X),$$

where $X^q \nmid g^*(X)$. We may suppose that $f^*$ and $g^*$ are coprime, since otherwise we could divide by their greatest common divisor and obtain an equation of the
same type with smaller degrees. Denote by $s$ the maximum of the degrees of $f^*$ and $g^*$ after this division. Now we can continue copying Blokhuis’ proof. The roots of $r^*(X)$ in $\text{GF}(q)$ are also roots of $Xf^*(X) + g^*(X)$. The multiple roots of $r^*(X)$ in $\text{GF}(q)$ are also roots of $X^s(f^*(X))' + (g^*(X))'$. The roots not in $\text{GF}(q)$ are roots of $a^*(x)$. Hence

$$r^*(X)|((Xf^*(X) + g^*(X)) - (g^*(X))'f^*(X))a^*(X). \quad (2.7)$$

If the polynomials on the right hand side of (2.7) are non-zero, then comparing the degrees gives $q + s \leq s + 1 + 2s - 2 + \Delta$, that is $s \geq (q + 1 - \Delta)/2$. Since $s \leq |B| - 1 - q + \Delta$, it gives that $|B| \geq \frac{3}{2}(q + 1) - \frac{3}{2}\Delta$; which is a contradiction. The third term on the right hand side of (2.7) cannot be the zero polynomial, since the terms of highest degree of $a(X,Y)$ formed a homogeneous polynomial and so $(Y - 1)$ cannot be a factor of it.

If the first term on the right hand side of (2.7) is the zero polynomial then $r^*(X)$ is divisible by $(X^q - X)$. Since $a^*(X)$ has degree at most $\Delta$, the remaining $q - \Delta$ factors of $(X^q - X)$ must come from the product $\prod(X + a_i)$. Geometrically this would imply that through the point $(\infty)$ there passed at most $\Delta + 1$ tangents, which contradicts the choice of $(\infty)$. (Here we use that $\Delta + 1 < \frac{3}{2}(2q - |B| - 2\varepsilon).$)

If the second term is zero, then, since $f^*$ and $g^*$ are coprime, $(f^*(X))' = 0$. For $q = p$ prime, it implies that either $|B| \geq 2q + 1 - \Delta$ (which is not possible by our upper bound on $|B|$) or $aX^q + b$ divides $r^*(X)$. Since $aX^q + b = (aX + b)^q$, and at most $\Delta$ of these factors can come from $a^*(X)$, it implies that there is a line $\ell$ (through $(\infty)$) that contains at least $q + 1 - \Delta$ points of $B$. Finally, assume that $|\ell \cap B| = q + 1 - k$, $k \leq \Delta$. Then the 0-secants pass through the $k$ missing points of $\ell$. Since $|B| \leq \frac{3}{2}q + 1 - \frac{3}{2}\Delta$, the number of 0-secants is at most $k(q - \left(\frac{3}{2}q + 1 - \frac{3}{2}\Delta - q - 1 + k\right)) \leq \frac{1}{2}k(q + 1)$.

Hence $k \leq 2\varepsilon$.

Note that there is no restriction on how small $\varepsilon$ can be. Chosing $\varepsilon$ to be slightly less than $\frac{1}{q + 1}$ one gets Theorem 21.4 of Blokhuis.

**Remark 23.11.** (1) The condition $\varepsilon < \frac{1}{q}(q - 6)$ is not really necessary. Indeed, fix the size of $B$. Determine the largest $\varepsilon$ so that $|B| < \frac{3}{2}(q + 1 - \Delta)$. Then $\varepsilon < \frac{1}{q}(q - 6)$ will automatically hold if $|B| > q/2$ (a more exact bound comes from $|B| < \frac{3}{2}(q + 1 - \Delta)$). On the other hand, if a set $B$ has size $cq$ for some $c < 1$ then the number of 0-secants is at least $(1 - c)q(q + 1)$. This can be seen by counting 0-secants through points of a fixed 0-secant. Hence our theorem gives a non-trivial bound only if $(1 - c)q(q + 1) < \varepsilon(q + 1)$, where $|B| = cq = \frac{3}{2}(q + 1 - \Delta)$. Roughly speaking this gives that for a fixed $c < 1$, the value of $\varepsilon$ has to be smaller than $(1 - \frac{3}{2}c)^2q/2$, which gives the equation $4c^2 + 6c - 9 = 0$ for the critical value of $c$. The positive root of the equation is $(-3 + \sqrt{45})/2$. Since it is bigger than $\frac{1}{2}$, this shows that $\varepsilon = (q - 6)/4$ is never reached. Let us underline that
the result gives a non-trivial stability theorem also for sets of size $cq$, $c < 1$ (but $c > (-3 + \sqrt{75})/4 \approx 0.927$).

(2) However, even when $|B| = q + 1$, one cannot expect only $\varepsilon$ missing points. Indeed, if we take an affinely regular $\delta$-gon $K$, inscribed in an ellipse of $AG(2, q)$, and the set of $q + 1 - \delta$ directions $N$ not determined by $K$, then the number of 0-secants $\delta = K \cup N$ is exactly $\delta(q - \delta)$, so when $\delta \geq \sqrt{q}$, then this is smaller than $\delta q$. For example, if $\delta = (q + 1)/2$, then $\delta(q - \delta)$ is roughly $q\delta/2$. The bound on $\varepsilon$ in Theorem 23.10 does not allow this value, but it shows that the combinatorial argument at the end of the proof cannot really be improved.

23.3 Stability theorems for blocking sets: the non-prime case

As mentioned before, in this section we are going to improve on Theorem 23.5, when the size of our point set is relatively large. The proof is guided by the ideas of the paper [123], where it is shown that each line intersects a small minimal blocking set in $1 \mod p$ points. In case of an almost blocking set $B$, a very similar argument to those in [123] will show that $B$ contains a point set intersecting almost every line $1 \mod p$ points and so its size cannot be too large. Finally, using resultants (see Section 9.5), we show that we can add a few points to $B$ so that we obtain a blocking set.

**Theorem 23.12.** Let $B$ be a point set in $PG(2, q)$, $q = p^h$, $h > 1$, $q \geq 81$, and suppose that the number of 0-secants, $\delta$, of $B$ is at most $1000pq$. Assume that $|B| < \frac{3}{2}(q + 1) - \frac{(p+3)}{2}\sqrt{2q}$. Then $B$ can be obtained from a blocking set by deleting at most $\frac{2q}{9}$ points of it.

Note that when $|B| > q + \frac{1000}{3}p$, then this theorem is an improvement on Theorem 23.5.

To prove the theorem our main aim is first to show that $B$ can be embedded in a blocking set of size less than $\frac{3}{2}(q + 1)$, and then the result will follow immediately. For the points $(a_v, b_v, c_v)$ of $B$, consider the three-variable Rédéi polynomial.

$$ R_B(X, Y, Z) = \prod_{v=1}^{[B]} (c_vX + a_vY - b_vZ) = \sum_{j=0}^{[B]} r_j(Y, Z)X^{[B]-j}. \quad (2.8) $$

Note that $r_j(Y, Z)$ is a homogeneous polynomial of degree $j$. As in the case of the two variable Rédéi polynomial, this polynomial also encodes the intersection multiplicities of $B$ and the lines:

*For a fixed $(z, y, 0) \in \ell$, the element $x \in \mathbf{GF}(q)$ is an $r$-fold root of $R(X, y, z)$ if and only if the line with equation $zY = yX + xZ$ intersects $U$ in exactly $r$ points.*

Hence the line $wY = uX + vZ$ is a 0-secant of $B$, if and only if $R(u, v, w) \neq 0$. The following lemma is similar to Exercise 10.2.
Lemma 23.13. There exists a three-variable homogeneous polynomial \( \tilde{a}(X, Y, Z) \) over \( \text{GF}(q) \), of degree at most \( \sqrt{25} - 1 \), such that for each skew line \( wY = uX + vZ \) to \( B \), where \( w, u, v \in \text{GF}(q) \), \( \tilde{a}(u, v, w) = 0 \).

Delete each linear component \((c_iX + a_iY - b_iZ)\) of \( \tilde{a} \) and add the corresponding projective point \((a_i, b_i, c_i)\), if it was not in \( B \), to \( B \). We will denote the new polynomial by \( \tilde{a}_1 \) and the new set by \( B_1 \). Hence \( |B_1| < 3(q + 1)/2 - \frac{p + 1}{2} \sqrt{25} - 1 \).

First of all, note that if \( B_1 \) has at most one 0-secant, then by putting one point on this line, we obtain a blocking set of size less than \( \frac{3}{2}(q + 1) \) containing \( B \). So from now on we assume that \( B_1 \) has at least two 0-secants, and we choose our new coordinate system in such a way, that the lines \( Z = 0 \) and \( X = 0 \) are skew to \( B_1 \).

Note that, in this new coordinate system, \( B_1 \) is an affine point set. Let \( a^*(X, Y, Z) \) be the polynomial \( \tilde{a}_1(X, Y, Z) \) in this new coordinate system. From now on we will substitute \( Z = 1 \), hence we will consider the two variable (affine) Rédei polynomial \( R_{B_1}(X, Y) \) and the two variable polynomial \( a^*(X, Y) \). By the construction of \( a^* \), the polynomial \( R_{B_1}a^* \) vanishes for all \((x, y) \in \text{GF}(q) \times \text{GF}(q)\). If there is a factor \( d(X, Y) \) of \( a^*(X, Y) \), so that \( (R_{B_1}\tilde{a}^*)(x, y) = 0 \) for every \((x, y)\) pair, then we delete this factor from \( a^* \). We repeat this process until there is such factor.

Remark 23.14. Hence we obtained a polynomial \( a(X, Y) \), such that \( t := \text{deg}a = \text{deg} \tilde{a} - (|B_1| - |B|) \leq \sqrt{25} - 1 \), \( \text{deg}(R_{B_1}a) < 3(q + 1)/2 - \frac{p + 1}{2} \sqrt{25} - 1 \), and \( a(X, Y) \) has no linear component. Furthermore, \( R_{B_1}(x, y)a(x, y) = 0 \) for every pair \((x, y) \in \text{GF}(q) \times \text{GF}(q)\), and \( a \) is minimal in the sense that this property will not hold if we delete any factor of \( a \).

Hence, we can write \( R_{B_1}a \) as:

\[
R_{B_1}(X, Y)a(X, Y) = (X^q - X)f(X, Y) + (Y^q - Y)g(X, Y),
\]

where \( \text{deg}(f), \text{deg}(g) \leq |B_1| - q + \text{deg}(a) = |B_1| - q + t < (q + 1)/2 - \frac{p + 1}{2} \sqrt{25} \).

Denote by \( C(X, Y) \) the product of the common factors (with multiplicity) of \( f(X, Y) \) and \( g(X, Y) \).

\[
R_{B_1}(X, Y)a(X, Y) = C(X, Y)((X^q - X)f(X, Y) + (Y^q - Y)g(X, Y)),
\]

where \( \tilde{f} \) and \( \tilde{g} \) have no common factors. Furthermore, \( \text{deg}(\tilde{f}), \text{deg}(\tilde{g}) \) and \( \text{deg}(C) \) are at most \( |B_1| - q + \text{deg}(a) = |B_1| - q + t < (q + 1)/2 - \frac{p + 1}{2} \sqrt{25} \). By the minimality of \( a \), the polynomials \( C \) and \( a \) cannot have a common factor, hence \( C(X, Y)\mid R_{B_1}(X, Y) \).

Corollary 23.15. All the factors of \( C(X, Y) \) have multiplicity one and are of form \((X + a_kY - b_k)\). Furthermore, the points \((a_k, b_k, 1)\) corresponding to the linear factors of \( C(X, Y) \) are in \( B_1 \).
Let \( \mathcal{C} \) denote the set of these points, hence \(|\mathcal{C}| = \deg_X C\). From above, \( \mathcal{C} \subset B_1 \).

Denote the point set \( B_1 \setminus \mathcal{C} \) by \( B_2 \). Note that \( B_2 \) is an affine point set and construct the Rédei polynomial \( R_{B_2}(X, Y) \) of \( B_2 \). Then:

\[
R_{B_2}(X, Y)a(X, Y) = (X^q - X)\tilde{f}(X, Y) + (Y^q - Y)\tilde{g}(X, Y),
\]

(2.11)

As the next lemma shows, through each point of \( \mathcal{C} \), there pass a few 1-secants only.

**Lemma 23.16.** If \( (X+a_k Y - b_k) \) is a factor of \( C(X, Y) \) then the number of 1-secants of \( B_1 \) through \((a_k, b_k, 1) \) \((\in B_1)\) is at most \( t + 1 \).

**Proof:** We have seen that \((X + a_k Y - b_k)\) cannot divide \( a(X, Y) \). Hence by Bézout’s theorem, \( a \) and \((X + a_k Y - b_k)\) have at most \( t \) common points.

For any value \( y \), \( x = b_k - a_k y \) is an at least 2-fold root of the right hand side of equation (2.10), and so this also holds for the left hand side. Hence from above, there are at least \( q - t \) values \( y \), such that \( x = b_k - a_k y \) is an at least 2-fold root of \( R_{B_k}(X, y) \). For these values, the line \( Y = yX + x \) (through \((a_k, b_k, 1)\)) intersects \( B_1 \) in at least two points. Now the lemma follows, since the lines through \((a_k, b_k, 1)\) are either of type \( Y = yX + x \) or vertical.

**Lemma 23.17.** For any \((x, y) \in \text{GF}(q) \times \text{GF}(q)\), if \( \tilde{f}(x, y) = 0 \), then \( \tilde{g}(x, y)a(x, y) = 0 \).

**Proof:** Suppose that for a fixed \( Y = y \), \( x \) is a root of \( \tilde{f}(X, y) \). Then, by equation (2.11), the intersection multiplicity of \( R_{B_2}(X, Y)a(X, Y) \) and the line \( Y = y \) in \((x, y)\) is at least two. Now assume that \( a(x, y) \neq 0 \), then by the properties of Rédei polynomials we have that the line \( Y = yX + x \) intersects \( B_2 \) in at least two points. Hence the intersection multiplicity of the line \( X = x \) and \( R_{B_2}(X, Y) \) in \((x, y)\) is also at least two, and so by equation (2.11), \( \tilde{g}(x, y) = 0 \).

**Lemma 23.18.** Let \( r_i(X, Y) \) be irreducible polynomials over the algebraic closure \( \text{GF}(q) \) dividing \( \tilde{f} \). If \( \frac{\partial \tilde{f}}{\partial X} \neq 0 \) then \( \sum_i \deg_X r_i \leq \frac{2}{p} \).

**Proof:** Let \( \overline{\text{GF}}(q) \) denote the algebraic closure of \( \text{GF}(q) \), and assume that \( \deg_X r_i = s_i \). Then for any \( i \), the sum of the intersection multiplicities \( I(P, r_i \cap \ell_P) \) over \( \overline{\text{GF}(q)} \times \text{GF}(q) \) is exactly \( s_i q \), where \( \ell_P \) denotes the horizontal line through \( P \).

First we show that the above sum over \( \overline{\text{GF}(q)} \times \text{GF}(q) \) is less than \( s_i q - s_i pt \). Assume to the contrary that the sum of these intersection multiplicities is at least \( s_i q - s_i pt \). To get the number of points of \( r_i \) over \( \overline{\text{GF}(q)} \times \text{GF}(q) \) without multiplicities, we have to subtract the number of intersections of \( r_i \) and \( \frac{\partial r_i}{\partial X} \). Hence by Bézout’s theorem, we get that \( r_i \) has at least \( s_i q - s_i pt - s_i(s_i - 1) \) \( \text{GF}(q) \)-rational points. By Lemma 23.17, these points are also on \( \tilde{g}a \). Now we show that \( r_i \nmid \tilde{g}a \). Since \( \tilde{f} \)}
and $\tilde{g}$ have no common factors, if $r_i | \tilde{g}a$, then $r_i | a$. Hence $r_i$ also divides the right hand side of equation (2.11) and so it divides $(Y^q - Y)\tilde{g}(X,Y)$. Again as $\tilde{f}$ and $\tilde{g}$ have no common factors, $r_i | (Y^q - Y)$ and so $r_i = Y - m, m \in \text{GF}(q)$; but this is not possible since $r_i | a$ and $a$ has no linear component. Hence we can apply Bézout’s theorem on the polynomials $r_i$ and $\tilde{g}a$:

$$s_i q - s_i pt - s_i(s_i - 1) \leq s_i\left(\frac{q + 1}{2} - \frac{(p - 1)}{2}\sqrt{2\delta}\right).$$

After simplifying the inequality, we get that $(q + 1)/2 - \frac{p+1}{2}\sqrt{2\delta} \leq s_i$; which is a contradiction since $s_i \leq \deg_x \tilde{f} < (q + 1)/2 - \frac{p+1}{2}\sqrt{2\delta}$.

Hence the sum of the intersection multiplicities $I(P, r_i \cap \ell_P)$ over $(\text{GF}(q) \setminus \text{GF}(q)) \times \text{GF}(q)$ is at least $s_i pt$. For any fixed $Y = y$, $R_{B_2}(X, y)$ splits into linear factors, hence $\tilde{f}(X, y)$ can have at most $t$ roots that are not from $\text{GF}(q)$. So the sum of the intersection multiplicities $I(P, f \cap \ell_P)$ over $(\text{GF}(q) \setminus \text{GF}(q)) \times \text{GF}(q)$ is at most $tq$, from which $pt \sum_i s_i \leq tq$ follows.

Hence for a fixed $Y = y$, $\tilde{f}(X, y)$ is almost a $p$-th power.

$$\tilde{f}(X, y) = (w_y(X))^pu_y(X), \quad (2.12)$$

where $\deg_X u_y \leq q/p$. Using equations (2.11) and (2.12), we get that for any $y \in \text{GF}(q)$,

$$R_{B_2}(X, y)a(X, y) = (X^q - X)\tilde{f}(X, y) = (X^q - X)(w_y(X))^pu_y(X). \quad (2.13)$$

As the next lemma shows, this equation helps to bound the size of $B_2$.

**Lemma 23.19.** The size of $B_2$ is less than $q + 7q^2/p$.

**Proof:** We will estimate the sum $S$ of the intersection multiplicities $I(P, \tilde{f} \cap r_P)$, where $r_P$ are the horizontal lines through those points $P \in \text{GF}(q) \times \text{GF}(q)$, where these intersection multiplicities are at least $p$.

For a fixed value $y \in \text{GF}(q)$, $\tilde{f}(X, y) = (w_y(X))^pu_y(X)$ splits into linear factors over $\text{GF}(q)$, hence the sum $S$ of the above intersection multiplicities is at least $q(\deg_X(\tilde{f}) - \max_y\deg(u_y))$. By Lemma 23.18 and by equation (2.13), this is at least $q(|B_2| + t - q - q/p)$.

Now we will give an upper bound for $S$. First of all note that

$$I(P, \tilde{f} \cap r_P) = I(P, R_{B_2} \cap r_P) + I(P, a \cap r_P) - 1,$$

for all points $P$. By Bézout’s theorem, the sum of the intersection multiplicities $I(P, a \cap r_P)$ over all points $P \in \text{GF}(q) \times \text{GF}(q)$ is at most $q\deg a = qt$. To give an
upper bound for the sum of the intersection multiplicities \( I(P, R_{B_2} \cap r_P) \) (when for each \( P \), \( I(P, \overline{f} \cap r_P) \geq p \)), we will distinguish between the points \( P \) according as \( I(P, R_{B_2} \cap r_P) \geq (p + 2)/2 \) and \( I(P, R_{B_2} \cap r_P) < (p + 2)/2 \).

By the fundamental properties of the Rédei polynomial, the first case considers those points \( P(x, y) \) that correspond to lines \( Y = yX + x \) intersecting \( B_2 \) in at least \((p + 2)/2 \) points. Hence for these points \( P \), the sum of the intersection multiplicities \( I(P, R_{B_2} \cap r_P) \) is exactly the number of incident point-line pairs, where the point lies in \( B_2 \) and the line is \( a \geq (p + 2)/2 \)-secant. The number of \((p + 2)/2 \)-secants through a point of \( B_2 \) is at most \( 2(|B_2| - 1)/p \), hence the number of these incident point-line pairs is at most \((p + 2)/2 \) points. Hence for these points \( P \), we have that \( |B_2| \geq q \).

Now we bound the sum of the intersection multiplicities \( I(P, R_{B_2} \cap r_P) \) over the points \( P \), for that \( I(P, R_{B_2} \cap r_P) < (p + 2)/2 \) (and \( I(P, \overline{f} \cap r_P) \geq p \)). For these points, \( I(P, a \cap r_P) \geq p/2 \) and so \( I(P, a \cap \overline{f}) \geq p/2 \). Hence by Bézout’s theorem the number of such points \( P \) is at most \((\deg f \cdot \deg g)/p \). For each of these points \( P \), \( I(P, R_{B_2} \cap r_P) \leq (p + 1)/2 \), hence the sum of these intersection multiplicities is at most \((p + 1)/p \cdot \deg f \cdot \deg g = \frac{p + 1}{p} \cdot (|B_2| - q)t \). Hence:

\[
q(|B_2| + t - q - \frac{q}{p}) \leq S \leq \frac{2|B_2|(|B_2| - 1)}{p} + \frac{p + 1}{p}(|B_2| - q)t + qt.
\]

Subtract \( q(|B_2| + t - q - \frac{q}{p}) \) from both sides of the above inequality.

\[
0 \leq \frac{2|B_2|(|B_2| - 1)}{p} + \frac{p + 1}{p}(|B_2| - q)t - q(|B_2| - q - \frac{q}{p})
\]

When \( q = p^h, h > 2 \), (using that \(|B_2| \leq \frac{3}{2}q \)), this inequality yields immediately that \(|B_2| < q + \frac{7q}{p} \).

So now we only consider the case \( q = p^2 \). For \(|B_2| \), the right hand side of the above inequality is a quadratic expression which is positive when \(|B_2| = q \) and negative when \(|B_2| = q + \frac{7q}{p} \) (the lemma is only interesting if \( q + \frac{7q}{p} < \frac{3}{2}q \) since \(|B_2| \leq \frac{3}{2}q \) and so we may suppose that \( p > 13 \)). Divide the above inequality by \( \frac{2}{p} \), so the coefficient of the quadratic term is \( 1 \) and the constant term is \((p + 1)qt + q^2p + q^2)/2 \). It follows from the previous argument that one of the roots of this quadratic expression is less than \( q + \frac{7q}{p} < \frac{3}{2}q \); hence the other is larger than \((p + 1)qt + q^2p + q^2)/3q \). This is larger than \( \frac{3}{2}q \), when \( p > 13 \) and since \(|B_2| \leq \frac{3}{2}q \), we get that \(|B_2| < q + \frac{7q}{p} \).

\[ \square \]

**Lemma 23.20.** The number of 0-secants of \( B_2 \), \( \delta' \), is at most \( \frac{1}{1000}pq \).

**Proof:** Originally \( B \) had at most \( \frac{1}{1000}pq \) 0-secants. To obtain \( B_2 \) we added some points and deleted the points of \( \mathcal{C} \). By Lemma 23.16, after deleting the points of \( \mathcal{C} \), we may get at most \(|\mathcal{C}|(t + 1) \leq \frac{9}{4} \sqrt{\frac{2}{1000}pq} \) new 0-secants. Hence \( \delta' \leq \frac{9}{4} \sqrt{\frac{2}{1000}pq} \)\]
The number of finishes our proof.

\[ \frac{q}{2} \sqrt{\frac{2}{1000}pq + \frac{1}{1000}pq} < q \sqrt{\frac{1}{2000}pq} + q \frac{1}{1000} \sqrt{pq}. \]

**Lemma 23.21.** The number of 0-secants of \( B_2 \) through a point is either at most \( \frac{\delta'}{2q+1-|B_2|} + \frac{1}{50}p \) or at least \( 2q + 1 - |B_2| - \left( \frac{\delta'}{2q+1-|B_2|} + \frac{1}{50}p \right). \)

**Proof:** By Lemma 23.7, if through a point \( P \) there pass \( s \) external lines of \( B_2 \), then \( (2q + 1 - |B_2| - s)s \leq \delta' \).\footnote{Assume to the contrary that \( \delta' > \frac{1}{21}pq \). By the construction of \( B_2 \), all the 0-secants of \( B_2 \) that are not skew to \( B \) pass through one of the points of \( C \). There are at least \( \delta' - \frac{1}{1000}\frac{pq}{|C|} \) such 0-secants, hence there exists a point \( P \in C \) through that there pass at least \( \frac{\delta'}{|C|} - \frac{pq}{1000|C|^2} \) 0-secants of \( B_2 \). We show that this contradicts Lemma 23.21. To this, note that \( |B_2| \geq \frac{3\sqrt{2}}{50}q \). Otherwise counting the number of 0-secants through the points of a skew line to \( B_2 \), we get more than \( \frac{1}{\sqrt{10}}q \frac{\sqrt{pq}}{pq} \) skew lines; which is a contradiction by Lemma 23.20.

First we show that \( \frac{\delta'}{|C|} - \frac{pq}{1000|C|^2} > \frac{\delta'}{2q+1-|B_2|} + \frac{1}{50}p \). We may assume, that \( 2q + 1 - |B_2| \geq dq \), where \( \frac{41}{30} \geq d > \frac{1}{2} \). Recall that \( B_1 = B_2 \cup C \) and \( |B_1| \leq \frac{2}{3}q \), so \( |C| \leq (d - \frac{1}{2})q \). Hence it is enough to show that \( \frac{\delta'}{2q+1-|B_2|} - \frac{p}{1000(d-\frac{1}{2})^2} > \frac{\delta'}{2q+1-|B_2|} + \frac{1}{50}p \).

Now \( \delta' > \frac{1}{21}pq \); hence we need to see that \( \frac{1}{21} \left( \frac{1/2}{d-\frac{1}{2}} \right) - \frac{1}{1000(d-\frac{1}{2})^2} > \frac{1}{50} \). After differentiating the left hand side of the above inequality, one can see that it is decreasing in the interval \( (\frac{1}{2}, \frac{41}{30}) \). So for \( d = \frac{41}{30} \), it takes its minimum, which is larger than \( \frac{1}{50} \).

To get a contradiction with Lemma 23.21, now we only have to show that the number of 0-secants of \( B_2 \) through any point of \( C \) is less than \( 2q + 1 - |B_2| - \frac{\delta'}{2q+1-|B_2|} \).
(\frac{\delta'}{2q+1-|B_2|} + \frac{1}{50} p). By Lemma 23.16, there are at most \( t + 1 < \sqrt{\frac{2pq}{100}} \) 0-secants through any point of \( C \). Using Lemma 23.20 and that \( |B_2| \leq \frac{3}{2} q \), we get the \( t + 1 < 2q + 1 - |B_2| - (\frac{\delta'}{2q+1-|B_2|} + \frac{1}{50} p) \).

Hence by Theorem 23.5, we can add at most \( \frac{2}{3} p < p \) points to \( B_2 \), so that we obtain a blocking set. Note that we constructed \( B_2 \) from \( B \) by adding at most \( \deg \tilde{a} < \sqrt{2q} \) points to \( B \) and deleting some points. Hence in total we can add at most \( \sqrt{2q} + p \) points to \( B \) in order to get a blocking set. This blocking set will have size less than \( \frac{3}{2} q + 1 \) (here we assume that \( \delta > 1 \), see the beginning of this section). Hence similarly as at the end of the proof of Theorem 23.5, we get that \( \varepsilon \leq \frac{\delta}{q} \).

### 23.4 Stability theorem for sets of even type

A set of even type \( U \) is a point set intersecting each line in even number of points. By counting the points of \( S \) on the lines through a point of \( S \) and on the lines through a point not in \( S \), one can see immediately that \( q \) must be even. Hence from now on in this section we will assume that \( 2|q| \). The smallest sets of even type are the hyperovals, they have \( q + 2 \) points. All other examples known to the authors have at least \( q + \sqrt{q} \) points; see Korchmáros, Mazzocca \[88\]. They constructed \((q + t)\)-sets of type \((0, 2, t)\) for \( t \geq \sqrt{q} \). More examples and a proof that the \( t \)-secants are concurrent for such sets can be found in Gács, Weiner \[70\].

It is easy to see that the symmetric difference of any two sets of even type is a set of even type.

A set of almost even type is a point set having only a few odd-secants. If we delete a point from a set of even type \( U \) then the new point set will have \( q + 1 \) odd-secants, and of course this will be also the case when we add a point to \( U \). If we modify \( \varepsilon \) points then we will get at least \( \varepsilon(q + 1) \) and at most \( \varepsilon(q + 1) \) odd-secants.

In this section we are going to prove the following stability theorem.

**Theorem 23.22.** Assume that the point set \( H \) in \( \text{PG}(2, q) \), \( 16 < q \) even, has \( \delta \) odd-secants, where \( \delta < (\lfloor \sqrt{q} \rfloor + 1)(q + 1 - \lfloor \sqrt{q} \rfloor) \). Then there exists a unique set \( H' \) of even type, such that \(|(H \cup H') \setminus (H \cap H')| = \lceil \frac{\delta}{q+1} \rceil \).

**Remark 23.23.** Note that a complete arc of size \( q - \sqrt{q} + 1 \) has \((\sqrt{q} + 1)(q + 1 - \sqrt{q})\) odd-secants, which shows that Theorem 23.22 is sharp, when \( q \) is a square. (Since the smallest sets of even type are hyperovals.) For the existence of such arcs see \[48\], \[63\] and \[85\].

Let \( \ell_\infty \) be the line at infinity intersecting the point set \( M \) in even number of points, furthermore let \( M \setminus \ell_\infty = \{(a_v, b_v)\}_{v} \) and \( M \cap \ell_\infty = \{(y_i)\}_{i} \). Consider the
23. Stability

following polynomial:

\[
g(X, Y) = \sum_{v=1}^{\ell_\infty} (X+a_v Y-b_v)^{q-1} + \sum_{y_i \in M \cap \ell_\infty} (Y-y_i)^{q-1} + |M| = \sum_{i=0}^{q-1} r_i(Y)X^{q-1-i},
\]  

(2.15)

Note that \( \text{deg} r_i \leq i \).

**Lemma 23.24.** Assume that the line at infinity contains even number of points of \( M \). Through a point \((y)\) there pass \( s \) odd-secants of \( M \) if and only if the degree of the greatest common divisor of \( g(X, y) \) and \( X^q - X \) is \( q - s \).

**Proof:** To prove this lemma we only have to show that \( x \) is a root of \( g(X, y) \) if and only if the line \( \gamma = yX + x \) intersects \( M \) in even number of points. To this, for the \((x, y)\) pairs, one has to count the parity of zero and non-zero terms.

**Remark 23.25.** Assume that the line at infinity is an even-secant and suppose also that there is an ideal point, different from \((\infty)\), with \( s \) odd-secants. Let \( n_h \) denote the number of ideal points different from \((\infty)\), through that there pass \( s - h \) odd-secants of the point set \( M \). Then Lemma 23.24 and Corollary 12.6 imply that \( \sum_{h=1}^{s-1} h n_h \leq s(s - 1) \).

**Lemma 23.26.** Let \( M \) be a point set in \( PG(2, q) \), \( 16 < q \) even, having less than \((\lfloor \sqrt{q} \rfloor + 1)(q + 1 - \lfloor \sqrt{q} \rfloor)\) odd-secants. Then the number of odd-secants through any point is at most \( \lfloor \sqrt{q} \rfloor + 1 \) or at least \( q - \lfloor \sqrt{q} \rfloor \).

**Proof:** Pick a point \( P \) with \( s \) odd-secants and let \( \ell_\infty \) be an even-secant of \( M \) through \( P \). (If there was no even-secant, then the lemma follows immediately.) By Remark 23.25, counting the number of odd-secants through \( \ell_\infty \setminus (\infty) \), we get that:

\[ qs - s(s - 1) \leq \delta. \]

This is a quadratic inequality for \( s \), where the discriminant is larger then \( q + 1 - 2(\lfloor \sqrt{q} \rfloor + 2) \). Hence \( s < \lfloor \sqrt{q} \rfloor + 2 \) or \( s > q + 1 - (\lfloor \sqrt{q} \rfloor + 2) \).

**Proposition 23.27.** Let \( M \) be a point set in \( PG(2, q) \), \( 16 < q \) even, having less than \((\lfloor \sqrt{q} \rfloor + 1)(q + 1 - \lfloor \sqrt{q} \rfloor)\) odd-secants. Assume that through each point there pass at most \( 3\lfloor \sqrt{q} \rfloor \) odd-secants. Then the total number of odd-secants \( \delta \) of \( M \) is at most \( \lfloor \sqrt{q} \rfloor q - q - 2 \lfloor \sqrt{q} \rfloor + 1 \).

**Proof:** Assume to the contrary that \( \delta > \lfloor \sqrt{q} \rfloor q - q + 2 \lfloor \sqrt{q} \rfloor + 1 \). Pick a point \( P \) and let \( \ell_\infty \) be an even-secant of \( M \) through \( P \). Assume that there are \( s \) odd-secants through \( P \). If there is a point \( Q \) on this even-secant through which there
pass at least \( s \) odd-secants, then choose the coordinate system so that \( Q \) is \((\infty)\). Then by Remark 23.25, counting the number of odd-secants through \( \ell \), we get a lower bound on \( \delta \):

\[
(q + 1)s - s(s - 1) \leq \delta.
\]

Since \( \delta < ((\lceil \sqrt{q} \rceil + 1)(q + 1 - \lceil \sqrt{q} \rceil)), \) from the above inequality we get that \( s < \lceil \sqrt{q} \rceil + 1 \) (hence \( s \leq \lceil \sqrt{q} \rceil \)) or \( s > q + 1 - \lceil \sqrt{q} \rceil \), but by the assumption of the proposition the latter case cannot occur.

Now we show that through each point there are at most \( \lfloor \sqrt{q} \rfloor \) odd-secants. The above argument and Lemma 23.26 show that on each even-secant there is at most \( \lfloor \sqrt{q} \rfloor + 1 \) odd-secants and through the rest of the points there are at most \( \lceil \sqrt{q} \rceil \) of them. Assume that there is a point \( R \) with \( \lfloor \sqrt{q} \rfloor + 1 \) odd-secants. Since \( \delta > \lfloor \sqrt{q} \rfloor + 1 \), we can find an odd-secant \( \ell \) not through \( R \). From above, the number of odd-secants through the intersection point of an even-secant on \( R \) and \( \ell \) is at most \( \lfloor \sqrt{q} \rfloor \). So counting the odd-secants through the points of \( \ell \), we get at most \((q - \lfloor \sqrt{q} \rfloor)(\lceil \sqrt{q} \rceil - 1) + (\lceil \sqrt{q} \rceil + 1)\lceil \sqrt{q} \rceil + 1\), which is a contradiction, so there was no point with \( \lfloor \sqrt{q} \rfloor + 1 \) odd-secants.

This means that the odd-secants form a dual \( \lfloor \sqrt{q} \rfloor \)-arc, hence \( \delta \leq (\lfloor \sqrt{q} \rfloor - 1)(q + 1) + 1 \), which is a contradiction again; whence the proof follows.

**Proof of Theorem 23.22** By Lemma 23.26, through each point there pass either at most \( \lfloor \sqrt{q} \rfloor + 1 \) or at least \( q - \lfloor \sqrt{q} \rfloor \) odd-secants. Consider the points through that there pass at least \( q - \lfloor \sqrt{q} \rfloor \) odd-secants. If such a point was in \( \mathcal{H} \) then delete it, otherwise add it to \( \mathcal{H} \). Denote this new set by \( \mathcal{H}' \). Note that the number of modified points is less than \( 2 \lfloor \sqrt{q} \rfloor \), hence through each point there pass at most \( 3 \lfloor \sqrt{q} \rfloor \) odd-secants of \( \mathcal{H}' \). Denote by \( \delta' \), the number of odd-secants of \( \mathcal{H}' \). Note that when we modify (delete or add) a point then each odd-secant through that point will become an even-secant and vice-versa. Hence, if through a point there passed \( s \geq q - \lfloor \sqrt{q} \rfloor \) odd-secants of \( \mathcal{H} \), then at least \( s - 3 \lfloor \sqrt{q} \rfloor \) of them will be an even secant of \( \mathcal{H}' \). So through this point there will pass at most \( q + 1 - (s - 3 \lfloor \sqrt{q} \rfloor) \) new odd-secants. Since, when \( q > 16 \), \( s \geq q + 1 - (s - 3 \lfloor \sqrt{q} \rfloor) \), the number of odd secants \( \delta' \) of \( \mathcal{H}' \) is at most \( \delta \). By Proposition 23.27, \( \delta' \leq \lfloor \sqrt{q} \rfloor q - q + 2 \lfloor \sqrt{q} \rfloor + 1 \).

Our first aim is to show that \( \mathcal{H}' \) is a set of even type.

Let \( P \) be an arbitrary point with \( s \) odd-secants, and let \( \ell_\infty \) be an even-secant through \( P \). Assume that there is a point on \( \ell_\infty \) with at least \( s \) odd-secant through it. Then as in Proposition 23.27, counting the number of odd-secants through \( \ell \), we get a lower bound on \( \delta' \):

\[
(q + 1)s - s(s - 1) \leq \delta'.
\]

This is a quadratic inequality for \( s \), where the discriminant is larger then \( (q + 2 - \frac{\delta' + q}{q + 1}) \). Hence \( s < \frac{\delta' + q}{q + 1} \) or \( s > q + 2 - \frac{\delta' + q}{q + 1} \), but by the construction of \( \mathcal{H}' \), the latter case cannot occur.
Now we show that there is no point through that there pass at least \( \delta' + \frac{q}{q+1} \) odd-secants. On the contrary, assume that \( T \) is a point with \( \delta' + \frac{q}{q+1} \leq s \) odd-secants. We choose our coordinate system, so that the ideal line is an even-secant through \( T \) and \( T \neq (\infty) \). Then from above, through each ideal point, there pass less than \( s(\geq \delta' + \frac{q}{q+1}) \) odd-secants. First we show that there exists an ideal point through that there pass exactly \( (s-1) \) odd-secants. Otherwise by Remark 23.25, \( 2(q-1) \leq s(s-1) \); but this is a contradiction since by Lemma 23.26, \( s \leq \lfloor \sqrt{q} \rfloor + 1 \). Let \( (\infty) \) be a point with \( (s-1) \) odd-secants. Then as before, we can give a lower bound on the total number of odd-secants of \( H' \):

\[
(s-1) + qs - s(s-1) \leq \delta'
\]

Bounding the discriminant (from below) by \( (q+2 - 2\frac{\delta' + q}{q+1}) \), it follows that \( s < \delta' + \frac{q}{q+1} \) or \( s > q + 2 - \frac{\delta' + q}{q+1} \). This is a contradiction, since by assumption, the latter case cannot occur and the first case contradicts our choice for \( T \).

Hence through each point there pass less than \( \delta' + \frac{q}{q+1} \) odd-secants. Assume that \( \ell \) is an odd-secant of \( H' \). Then summing up the odd-secants through the points of \( \ell \) we get that \( \delta' < (q+1)\frac{\delta' - 1}{q+1} + 1 \), which is a contradiction. So \( H' \) is a set of even type.

To finish our proof we only have to show that \(|(H \cup H') \setminus (H \cap H')| = \lfloor \frac{\delta}{q+1} \rfloor \). As we saw at the beginning of this proof, the number \( \varepsilon \) of modified points is smaller than \( 2\lfloor \sqrt{q} \rfloor \). On one hand, if we construct \( H \) from the set \( H' \) of even type, then we see that \( \delta \geq \varepsilon(q+1 - (\varepsilon - 1)) \). Solving the quadratic inequality we get that \( \varepsilon < \lfloor \sqrt{q} \rfloor + 1 \) or \( \varepsilon > q + 1 - \lfloor \sqrt{q} \rfloor \), but from above this latter case cannot happen. On the other hand, \( \delta \leq \varepsilon(q+1) \). From this and the previous inequality (and from \( \varepsilon \leq \lfloor \sqrt{q} \rfloor \)), we get that \( \frac{\delta}{q+1} \leq \varepsilon \leq \frac{\delta}{q+1} + \frac{\sqrt{q}(\lfloor \sqrt{q} \rfloor - 1)}{q+1} \). Hence the theorem follows.

For applications of Theorem 23.22 see the next section and also Section 17.2.

### 23.5 Number of lines meeting a \((q+2)\)-set

Stability of hyperovals was already studied by Blokhuis and Bruen. A hyperoval is not only nice in the sense that it intersects each line in even number of points, but it is also extremal in the sense that considering point sets of size \( q+2 \), a hyperoval intersects the least number of lines, that is \( \binom{q+2}{2} \). The next result shows that a \((q+2)\)-set intersecting a bit more than \( \binom{q+2}{2} \) lines can always be constructed by modifying a hyperoval a little bit.

**Result 23.28.** (Blokhuis, Bruen [44]) Let \( H \) be a point set in \( PG(2,q) \), \( q \) even, of size \( q+2 \). Assume that the number of lines meeting \( H \) in at least 1 point is \( \binom{q+2}{2} + \nu \), where \( \nu \leq \frac{q}{2} \). Then \( H \) is a hyperoval or there exist two points \( P \) and \( Q \), so that \( (H \setminus P) \cup Q \) is a hyperoval.
Now we will try to improve on this result. Hence we will consider \((q+2)\)-sets intersecting a bit more than \(\frac{q+2}{2} + \frac{q}{2}\) lines.

**Theorem 23.29.** Let \(\mathcal{H}\) be a point set in \(\text{PG}(2, q)\), \(16 < q\) even, of size \(q+2\). Assume that the number of lines meeting \(\mathcal{H}\) in at least \(1\) point is \(\frac{q+2}{2} + \nu\), where \(\nu < \frac{1}{4}([\sqrt{q}] + 1)(q+1-|\sqrt{q}|)\). Then there exists a set \(\mathcal{H}^*\) of even type, such that \(|(\mathcal{H} \cup \mathcal{H}^*) \setminus (\mathcal{H} \cap \mathcal{H}^*)| = \lceil \frac{4\nu}{q+1} \rceil\).

**Proof:** First we show that almost all lines meeting \(\mathcal{H}\) intersect it in \(2\) points. Let \(l_i\) denote the number of lines intersecting \(\mathcal{H}\) in \(i\) points. We will do the standard counting arguments to get a lower bound on \(l_2\). That is:

\[
\sum_{i=1}^{q+1} l_i = \binom{q+2}{2} + \nu \quad (2.16)
\]

\[
\sum_{i=1}^{q+1} il_i = (q+2)(q+1) \quad (2.17)
\]

\[
\sum_{i=2}^{q+1} i(i-1)l_i = (q+2)(q+1) \quad (2.18)
\]

Calculating ((2.17)-(2.16)), and then subtracting it twice from (2.18), we get

\[
\sum_{i=2}^{q+1} (i-1)l_i = \binom{q+2}{2} - \nu \quad (2.19)
\]

\[
\sum_{i=3}^{q+1} (i-2)(i-1)l_i = 2\nu \quad (2.20)
\]

Hence from (2.20), we have that \(\sum_{i=3}^{q+1} (i-1)l_i \leq 2\nu\) and so using (2.19), we have that \(l_2 \geq \binom{q+2}{2} + 3\nu\). Hence the total number of odd-secants is at most \(\binom{q+2}{2} + \nu - \left(\binom{q+2}{2} - 3\nu\right) = 4\nu\). So Theorem 23.22 finishes our proof.

\[\blacksquare\]

### 24 Jamison, Brouwer-Schrijver, affine blocking sets

Here we reconstruct the short proof of Brouwer and Schrijver [49] for the theorem on (1-)blocking sets in \(\text{AG}(n, q)\). It was proved independently and in a more general form by Jamison [84].

**Theorem 24.1.** In \(\text{AG}(n, q)\) a blocking set \(B\) with respect to hyperplanes has at least \(|B| \geq n(q-1) + 1\) points.
Note that the bound is sharp: \( n \) concurrent lines form such a blocking set (but there are several other examples as well, no classification of the minimal blocking sets can be hoped for).

**Proof:** We can assume that the origin \( 0 = (0, 0, \ldots, 0) \) is in \( B \), let \( B' = B \setminus \{0\} \). \( B' \) blocks all hyperplanes not through \( 0 \), hence, as any such hyperplane has equation of form \( w_1X_1 + w_2X_2 + \ldots + w_nX_n = 1 \) for some \( w_1, \ldots, w_n \), not all zero, we have that the polynomial

\[
F(Y_1, \ldots, Y_n) = \prod_{b \in B'} (b_1Y_1 + b_2Y_2 + \ldots + b_nY_n - 1)
\]

vanishes at every \((w_1, \ldots, w_n) \neq 0\). It means that for each \( i \) we have \((Y_q - 1 - _1) - F(Y_1, \ldots, Y_n)\), so \( \prod_{i=1}^n(Y_i^{q-1} - 1)F(Y_1, \ldots, Y_n) \). As \( F(0) \neq 0 \), its degree, so \(|B'|| \geq n(q - 1)\).

After removing the origin from \( B \) (w.l.o.g. it was in there), the remaining points block all hyperplanes not through \( 0 \). After dualisation, as Jamison did, one can formulate Theorem 24.1 like:

**Theorem 24.2.** In \( \text{AG}(n, q) \) if a set \( B \) of nonzero hyperplanes cover \( \text{AG}(n, q) \setminus \{0\} \) then it has at least \(|B| \geq n(q - 1)\) hyperplanes.

In fact Jamison proved the following more general result:

**Theorem 24.3.** Any covering of \( \text{AG}(n, q) \setminus \{0\} \) with \( k \)-dimensional affine subspaces not through the origin, contains at least \( q^{n-k} - 1 + k(q - 1) \) subspaces; where \( 0 \leq k < n \). Moreover, this bound is always sharp.

**Proof:** Suppose to the contrary that \( S \) is a family of nonzero \( k \)-subspaces covering \( \text{AG}(n, q) \setminus \{0\} \) and \(|S| < q^{n-k} - 1 + k(q - 1) \). We represent \( \text{AG}(n, q) \) as \( \text{GF}(q^n) \). Let \( p(X) \in \text{GF}(q^n)[X] \) be the product of all root polynomials \( p_L(X) \) as \( L \) ranges though the \( k \)-subspaces of \( S \). As \( p(x) = 0 \) for all \( x \in \text{GF}(q^n)^* \), we have

\[
p(X) = (X^{q^n-1} - 1)t(X)
\]

for some \( t(X) \). Let \( a_j \) be the coefficient of the term of degree \( j(q^n - 1) \) in \( p(X) \) and \( b_j \) the coefficient of the term of degree \( j(q^n - 1) \) in \( t(X) \). From (1) we obtain the recursive relations

\[
a_0 = -b_0 \]

and

\[
a_j = b_{j-1} - b_j \quad \text{for} \quad j > 0.
\]

Since 0 is not covered, \( 0 \neq p(0) = a_0 \) so \( b_0 \neq 0 \). We want to show that \( a_j = 0 \) for \( j \geq 1 \). From this and (2), \( b_j = b_0 \neq 0 \) for all \( j \), which is a contradiction as a polynomial can have finitely many nonzero terms only.
By \( |S| < q^{n-k} - 1 + k(q - 1) \) the degree of \( p(X) \) is strictly less than 
\[
q^k(q^{n-k} - 1 + k(q - 1)) \leq (k + 1)q^n - (k + 1)q^k < (k + 1)(q^n - 1);
\]
whence \( a_j = 0 \) for all \( j \geq k + 1 \). We are going to prove \( a_j = 0 \) for \( 1 \leq j \leq k \).

As \( p(X) \) is the product of root polynomials (each a linearized polynomial plus a constant term), we deduce that if \( a_j \neq 0 \) then
\[
j(q - 1) = c_0 + c_1q + ... + c_kq^k,
\]
where each \( c_i \geq 0 \) and
\[
c_0 + ... + c_k \leq |S| < q^{n-k} - 1 + k(q - 1).
\]

We want to prove that such an expansion (3), (4) cannot hold. Suppose that it does.

As all terms in (3) are nonnegative,
\[
c_k \leq jq^{n-k} - 1,
\]

since otherwise \( jq^{n-k}q^k > j(q^n - 1) \).

Suppose \( j = 1 \). If both in (5) and (6) equalities hold then \( \sum_i c_i = k(q - 1) + q^{n-k} - 1 \), contradicting (4). So one of the inequalities must be strict. Consequently,

\[
\sum_{i=0}^{k} c_iq^i < (q - 1) + (q - 1)q + ... + (q - 1)q^{k-1} + (q^{n-k} - 1)q^k = q^n - 1,
\]

contradicting (3).

Suppose \( j > 1 \). Let \( m \) be the least integer such that \( j \leq q^m \). By induction on \( j \) it is easy to see that \( j \leq q^{j-1} \), hence \( 0 < m \leq j - 1 \leq k - 1 \). Considering (3) modulo \( q^m \) we obtain
\[
q^m - j \equiv c_0 + c_1q + ... + c_{m-1}q^{m-1} \pmod{q^m}.
\]

As \( m - 1 \leq k - 1 \) we can apply (5) here and conclude that the sum on the right hand side lies between 0 and \( q^m - 1 \), so it is not only a congruence but actually an equality. Thus we may write
\[
j(q^n - 1) = q^m - j + c_mq^m + ... + c_kq^k.
\]

If \( c_i = q - 1 \) when \( m \leq i \leq k - 1 \) and \( c_k = jq^{n-k} - 1 \), then
\[
c_m + ... + c_k = (k - m)(q - 1) + jq^{n-k} - 1 \geq (k - m)(q - 1) + q^{n-k} - 1 + mq^{n-k}
\]
This contradicts (4), so either one of the inequalities in (5) must be strict for some \(i\) between \(m\) and \(k-1\), or inequality (6) must be strict. In either case
\[
c_0 + c_1 q + \ldots + c_k q^k < q^m - j + (q-1)q^m + \ldots + (q-1)q^{k-1} + (jq^{n-k} - 1)q^k = jq^n - j,
\]
and this contradicts (3). Therefore the representation (3) is impossible if \(|S| \leq q^{n-k} - 1 + k(q-1)\). Consequently, \(a_j = 0\) for all \(j > 0\).

Note that even if \(|S| = q^{n-k} - 1 + k(q-1)\), then \(a_j\) is nonetheless 0 for all \(j > 1\). Of course, since a covering does exist in this case, \(a_1\) may be nonzero. Therefore \(a_1\) is the critical coefficient.

For \(k = n-1\) Bruen [53] generalized it in the following way for \(t\)-covers (i.e. when each point is covered at least \(t\) times):

**Theorem 24.4.** Any \(t\)-covering of \(AG(n,q) \setminus \{0\}\) with hyperplanes not through the origin, contains at least \((n+t-1)(q-1)\) hyperplanes. Dually:

Any \(t\)-fold blocking set of \(AG(n,q)\) (with respect to the hyperplanes) contains at least \((n+t-1)(q-1) + 1\) points.

**Proof:** Let \(B\) be a set of \(t\)-covering hyperplanes, defined by the linear equations \(f_i = 0, i = 1, \ldots , |B|\). Then \(\prod_{i=1}^{|B|} f_i\) is a polynomial not vanishing at the origin but vanishing \(t\) times elsewhere. Now Exercise 5.12 finishes the proof. For the dual statement suppose w.l.o.g. that the origin is contained in the blocking set, and use the standard duality in \(PG(n,q)\) containing \(AG(n,q)\).

We mention without proof that Bruen generalized Theorem 24.3 for \(t\)-coverings:

**Theorem 24.5.** Any \(t\)-covering of \(AG(n,q) \setminus \{0\}\) with \(k\)-dimensional affine subspaces not through the origin, contains at least
\[
tq^{n-k} - 1 + \sum_{i=0}^{k-1} b_i
\]
subspaces, where \(q^k - t = \sum_{i=0}^{k-1} b_i q^i, 0 \leq b_i < q, kt \leq q^k\).

**Exercise 24.6.** [53] Let \(\pi\) be a dual translation plane of order \(q^2\), with (dual) kernel affine plane of order \(q\). Then any blocking set of \(\pi\) contains at least \(q^2 + 2(q-1)\) points. See also Theorem 27.1.
24.1 Applications of the punctured Nullstellensatz

In this section, which is based on [22], we show applications to the punctured Nullstellensatz by Ball and Serra (see Section 5.5).

Consider two lines ℓ₁ and ℓ₂ of a projective plane over a field ℱ and finite non-intersecting subsets of points $S_i$ of $ℓ_i$. Let $A$ be a set of points with the property that every line joining a point of $S_1$ to a point of $S_2$ is incident with a point of $A$. If we asked ourselves how small can $A$ be then obviously we could simply choose $A$ to be the smaller of the $S_i$ and clearly we can do no better. If, however, we impose the restriction that one of the lines joining a point $P_i$ of $S_1$ to a point $P_2$ of $S_2$ is not incident with any point of $A$ then it is not so obvious how small can $A$ be. We will see that at least $|S_1| + |S_2| - 2$ points are needed, which is clearly an attainable bound, for example take $A$ to be $(S_1 \cup S_2) \setminus \{P_1, P_2\}$. The next theorem provides the bound to arbitrary dimension and to sets that have not just one point incident with the lines joining a point of $S_1$ to a point of $S_2$, but a fixed number $t$ of points.

Let $ℱ$ be an arbitrary field.

**Theorem 24.7.** Let $ℓ_1, ℓ_2, \ldots, ℓ_n$ be $n$ concurrent lines spanning $PG(n, ℱ)$ and let $S_i$ be a subset of points of $ℓ_i$ for each $i$ not containing the point of intersection of the lines $ℓ_i$. Let $A$ be a set of points with the property that every hyperplane $⟨s_1, s_2, \ldots, s_n⟩$, where $s_i \in S_i$ is incident with at least $t$ points of $A$ except those hyperplanes $⟨d_1, d_2, \ldots, d_n⟩$, where $d_i$ is an element of a subset $D_i$ of $S_i$ for all $i$, which may be incident with less than $t$ points of $A$. If there is a hyperplane $⟨d_1, d_2, \ldots, d_n⟩$, where $d_i$ is an element of a subset $D_i$ for all $i$, which is incident with no point of $A$, then for all $j$

$$|A| \geq (t - 1)(|S_j| - |D_j|) + \sum_{i=1}^{n}(|S_i| - |D_i|).$$

**Proof:** Let $H$ be a hyperplane that meets the lines $ℓ_i$ in a point of $S_i$ but is not incident with any point of $A$. Apply a collineation of $PG(n, ℱ)$ that takes $ℓ_1, ℓ_2, \ldots, ℓ_n$ to the axes of $AG(n, ℱ)$, the affine space obtained from $PG(n, ℱ)$ by removing the hyperplane $H$, and takes the point $H \cap ℓ_i$ to the point $⟨e_i⟩$, where $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$.

We can then assume that $A$ is a subset of $AG(n, ℱ)$, the affine space obtained from $PG(n, ℱ)$ by removing the hyperplane $H$. The hyperplane $H$ is defined by the equation $X_{n+1} = 0$.

Let $0 \in T_i$ be the subset of $ℱ$ with the property that $s^{-1} \in T_i \setminus \{0\}$ if and only if $⟨se_i + e_{n+1}⟩$ is a point of $S_i$. Note that the line $ℓ_i$, after applying the collineation, is $⟨e_i, e_{n+1}⟩$ and $|T_i| = |S_i|$. Let $0 \in E_i$ be the subset of $ℱ$ with the property that
\( d^{-1} \in E_i \setminus \{0\} \) if and only if \( \langle de_i + e_{n+1} \rangle \) is a point of \( D_i \). Define

\[
 f(X_1, X_2, \ldots, X_n) = \prod_{a \in A} \left( \left( \sum_{i=1}^{n} a_i X_i \right) - 1 \right).
\]

The affine hyperplanes \( \sum_{i=1}^{n} t_i X_i = 1 \), where \( t_i \in T_i \) are not all zero, are the affine hyperplanes spanned by points \( s_1, s_2, \ldots, s_n \), where \( s_i \in S_i \). By hypothesis there are \( t \) points of \( A \) incident with these hyperplanes, unless \( t_i \in E_i \) for all \( i \), and so \( f \) has a zero of multiplicity \( t \) at \( (t_1, t_2, \ldots, t_n) \), unless \( t_i \in E_i \) for all \( i \).

However \( 0 \in E_i \) for all \( i \) and \( F(0, 0, \ldots, 0) = (-1)^{|A|} \), so there is an element of \( T_1 \times T_2 \times \ldots \times T_n \) where \( f \) does not vanish. Theorem 5.24 implies that for all \( j \)

\[
|A| = \deg(f) \geq (t-1)(|T_j| - |E_j|) + \sum_{i=1}^{n} (|T_i| - |E_i|) = (t-1)(|S_j| - |D_j|) + \sum_{i=1}^{n} (|S_i| - |D_i|).
\]

The above theorem also holds for any multi-set \( A \).

The condition that there is a hyperplane that is not incident with a point of \( A \) is essential. If we do not impose this condition then for \( t < n \) any collection of \( t \) of the sets \( S_i \) would be appropriate for \( A \).

For \( t = 1 \) the bound is tight: take \( A = \bigcup_{i=1}^{n} (S_i \setminus D_i) \).

Theorem 24.7 has some corollaries. The following theorem, which, after Theorem 24.7, can be formulated as an exercise, is due to Bruen [53]. It was initially proven for \( t = 1 \) by Jamison (Theorem 24.1); see also the independent proof found by Brouwer and Schrijver [49].

It is nice to prove Theorem 24.4 again, using Theorem 24.7:

**Exercise 24.8.** If every hyperplane of \( AG(n, q) \) is incident with at least \( t \) points of a set of points \( A \), then \( A \) has at least \( (n + t - 1)(q - 1) + 1 \) points.

The bound in this theorem can be improved slightly in many cases when \( t \leq q \) as was proven in [31]. In Theorem 24.11 we shall investigate when this improvement applies to the more general Theorem 24.10 below.

Firstly let us look at a consequence of Theorem 24.7 for projections.

**Theorem 24.9.** If there are \( m - 1 \) points \( x_1, x_2, \ldots, x_{m-1} \) of \( PG(n, \mathbb{F}) \) that project \( m \) collinear points \( S_1 \) onto \( m \) collinear points \( S_2 \) then there is a further point \( x_m \) which also projects \( S_1 \) onto \( S_2 \).

**Proof:** Suppose that there is no such point \( x_m \) which also projects \( S_1 \) onto \( S_2 \). There are \( m \) lines \( \ell_1, \ldots, \ell_m \) that join a point of \( S_1 \) to a point of \( S_2 \) but are not incident with any of the points \( x_1, x_2, \ldots, x_{m-1} \). The points of \( S_1 \) and \( S_2 \) are all
contained in the same plane and so any two lines \( \ell_i \) and \( \ell_j \) are incident. If they
are not all incident with a common point \( x_m \) then we can choose \( m - 2 \) points
\( y_1, \ldots, y_{m-2} \) such that \( y_i \) is incident with \( \ell_i \) but is not incident with \( \ell_m \) and \( y_{m-2} \) is
the intersection of the lines \( \ell_{m-2} \) and \( \ell_{m-1} \). (We may have to relabel the lines to
ensure that \( \ell_m \) is not incident with the intersection of the lines \( \ell_{m-2} \) and \( \ell_{m-1} \).)
The set \( A = \{x_1, x_2, \ldots, x_{m-1}, y_1, \ldots, y_{m-2}\} \) has the property that every line, except
\( \ell_m \), that joins a point of \( S_1 \) to a point of \( S_2 \) is incident with a point of \( A \), which
contradicts Theorem 24.7.

The following theorem is almost the dual of Theorem 24.7. The proof is shorter
as here we do not need an initial transformation.

**Theorem 24.10.** Let \( A \) be a set of hyperplanes of \( \mathbb{AG}(n, F) \) and let \( D_i \) be a non-
empty proper subset of \( S_i \), a finite subset of \( F \). If every point \((s_1, s_2, \ldots, s_n)\), where
\( s_i \in S_i \), is incident with at least \( t \) hyperplanes of \( A \) except at least one point of
\( D_1 \times D_2 \times \cdots \times D_n \), which is incident with no hyperplane of \( A \), then for all \( j \)

\[
|A| \geq (t - 1)(|S_j| - |D_j|) + \sum_{i=1}^{n}(|S_i| - |D_i|).
\]

**Proof:** Define

\[
f(X_1, X_2, \ldots, X_n) = \prod \left( \sum_{i=1}^{n} a_i X_i - a_{n+1} \right),
\]

where each factor in the product corresponds to a hyperplane, defined by the
equation \( \sum_{i=1}^{n} a_i X_i = a_{n+1} \), in \( A \). By hypothesis the polynomial \( f \) has a zero of
multiplicity \( t \) at all the points of \( S_1 \times S_2 \times \cdots \times S_n \) except at least one point of
\( D_1 \times D_2 \times \cdots \times D_n \) where it is not zero. By Theorem 5.24 the bound follows.

If \( S_i = GF(q) \) and \( D_i = \{0\} \) then Theorem 24.10 implies that a set of hyperplanes
\( A \) with the property that every non-origin point of \( \mathbb{AG}(n, q) \) is incident with at
least \( t \) hyperplanes of \( A \) is a set of at least \( (n + t - 1)(q - 1) \) hyperplanes, which
dualising gives Bruens theorem (Exercise 24.8) again.

We end this section by proving the following theorem which is similar to Theorem
24.10 but in which there are translations of the set of hyperplanes of \( \mathbb{AG}(n, q) \), not
incident with the origin, which also cover most, but not all, of the points of the
grid \( S_1 \times \cdots \times S_n \).

For any \( \lambda \in F^n \) and \( A \), a finite subset of \( F^n \), define \( A + \lambda = \{a + \lambda | a \in A\} \).
In the following a **punctured grid** is a set of points \((S_1 \times \cdots \times S_n) \setminus (D_1 \times \cdots \times D_n)\),
where \( D_i \) is a proper non-empty subset of some subset \( S_i \subseteq F \).
Theorem 24.11. Let $\Lambda$ be a set of vectors of $\mathbb{F}^n$ with the property that $\lambda \in \Lambda$ if and only if there is a finite punctured grid $G^\lambda$, punctured at the origin and whose dimensions do not depend on $\lambda$, with the property that every point of $G^\lambda$ is incident with at least $t$ hyperplanes defined by equations of the form

$$b_1X_1 + \ldots + b_nX_n = 1,$$

for some $b \in A + \lambda$. Let $m$ be minimal such that for all $\lambda \in \Lambda$

$$\prod_{s \in S_i \setminus D_i} (X - s) = 1 + X^m r_\lambda(X)$$

for some polynomial $r_\lambda$, where $G^\lambda$ is the punctured grid $(S_1 \times \ldots \times S_n) \setminus (D_1 \times \ldots \times D_n)$. If there are non-negative integers $j$ and $k$ with the property that either

$$k \leq j \leq \min\{t - 1, m - 1, |\{\lambda_1 | (\lambda_1, \ldots, \lambda_n) \in \Lambda \cap (-A)| - 1\}\}$$

or

$$k + 1 \leq j \leq \min\{t - 1, m - 1, |\{\lambda_1 | (\lambda_1, \ldots, \lambda_n) \in \Lambda\}| - 1\},$$

and

$$\left(\sum_{i=1}^n (|S_i| - |D_i|) + (t - 1)(|S_1| - |D_1|) + k\right) \neq 0$$

then

$$|A| \geq \sum_{i=1}^n (|S_i| - |D_i|) + (t - 1)(|S_1| - |D_1|) + k + 1.$$ 

Proof: Suppose that $|A| = \sum_{i=1}^n (|S_i| - |D_i|) + (t - 1)(|S_1| - |D_1|) + k$. Let

$$f_\lambda(X_1, X_2, \ldots, X_n) = \prod_{a \in A} \left(\left(\sum_{i=1}^n (a_i + \lambda_i)X_i\right) - 1\right).$$

The degree of $f_\lambda$ is $|A| - 1 + \varepsilon$, where $\varepsilon = 0$ if $\lambda = -a$ for some $a \in A$ and $\varepsilon = 1$ if not. By hypothesis the polynomial $f$ has a zero of multiplicity $t$ at all the points of $S_1 \times S_2 \times \ldots \times S_n$ except at least one point of $D_1 \times D_2 \times \ldots \times D_n$ where it is non-zero. Let

$$g_i(X_i) = \prod_{s_i \in S_i} (X_i - s_i) \text{ and } l_i(X_i) = \prod_{d_i \in D_i} (X_i - d_i).$$

By Theorem 5.24

$$f_\lambda(X_1, \ldots, X_n) = \sum_{\tau \in T} g_{\tau(1)} \ldots g_{\tau(t)} h_\tau + u_1 \prod_{i=1}^n \frac{g_i}{l_i},$$
II. Polynomials in geometry

for some polynomial $u_1$ of degree at most $(t - 1)(|S_1| - |D_1|) + k - 1 + \varepsilon$. Since there is a point, the origin, of $D_1 \times D_2 \times \cdots \times D_n$ where $f_\lambda$ is non-zero, the polynomial $u_1$ is non-zero at this point. The polynomial in one variable

$$f_\lambda(X, 0, ..., 0) = g_1^t h + u_2 \frac{g_1}{l_1},$$

for some polynomial $h$ and polynomial $u_2$ of degree at most $\deg u_1$.

By hypothesis $f_\lambda$ has a zero of multiplicity $t$ at all the points $(s_1, 0, ..., 0)$, where $s_1 \in S_1 \setminus D_1$. Therefore $f_\lambda(X, 0, ..., 0)$ is divisible by

$$\left( \frac{g_1}{l_1} \right)^t = (1 + X^m r_\lambda(X))^t.$$

Let $A_1$ be the multiset where $a_1$ appears as an element of $A_1$ the number of times it appears as the first coordinate of an element of $A$. Thus

$$f_\lambda(X, 0, ..., 0) = g_1^t h + u_2 \frac{g_1}{l_1},$$

can be written as

$$\prod_{a_1 \in A_1} ((a_1 + \lambda_1)X - 1) = (1 + X^m r_\lambda)^t(u_3 + hl_1^t),$$

for some polynomial $u_3$ of degree at most $\deg u_2 - (t - 1)(|S_1| - |D_1|)$, which is at most $k - 1 + \varepsilon$. Since $0 \in D_1$ we can write $hl_1^t = X^t h_2$ for some polynomial $h_2$. Thus, the coefficient of $X^j$ in the right hand side of the equation above is zero for all $j$ for which $k + \varepsilon \leq j \leq \min\{m - 1, t - 1\}$. On the left-hand side of this equation the coefficient of $X^j$ is a polynomial in $\lambda_1$ of degree at most $j$ where the term $\lambda_1^j$, if it appears in the polynomial, has coefficient $\binom{|A_1|}{j}$.

If the number of $\lambda_1$ which appear as first coordinate in the vectors in $\Lambda$ is more than $j$, then the coefficient of $X^j$, which is a polynomial in $\lambda_1$ of degree at most $j$, must be identically zero, and so the binomial coefficient is zero.

The following corollary is a slight generalisation of a result of Blokhuis (Theorem 2.2) from [31], see Section 25 as well for this and the next one.

**Corollary 24.12.** A set $A$ of points of $\text{AG}(n, q)$ with the property that every hyperplane is incident with at least $t$ points of $A$, has size at least

$$(n + t - 1)(q - 1) + k + 1,$$

provided that there exists a $j$ with the property that $k \leq j \leq \min\{t - 1, q - 2\}$ and

$$\binom{-n - t + k + 1}{j} \neq 0.$$
Proof: Apply Theorem 24.11 with $\Lambda = -A$, $S_i = \mathbb{GF}(q)$ and $D_i = \{0\}$ for all $i = 1, 2, ..., n$. Note that for all $i$,

$$
\prod_{s \in S_i \setminus D_i} (X - s) = X^{q-1} - 1,
$$

so $m = q - 1$ and that $|\{\lambda_1 | (\lambda_1, ..., \lambda_n) \in \Lambda \cap (-A)\}| = |\{-a_1 | (a_1, ..., a_n) \in A\}| = q$.

We conclude that if there are non-negative integers $j$ and $k$ with the property that $k \leq j \leq \min\{t - 1, q - 2\}$ and

$$
\binom{(n + t - 1)(q - 1) + k}{j} = \binom{-n - t + k + 1}{j} \neq 0,
$$

then $|A| \geq (n + t - 1)(q - 1) + k + 1$. \hfill \blacksquare

The following corollary is from Blokhuis [31] for $(t, q) = 1$ and [8] in general.

Exercise 24.13. A set of points of $\text{AG}(2, q)$ with the property that every line is incident with at least $t$ points of $A$ has size at least $(t + 1)q - (t, q)$.

24.2 Rédei polynomials in three indeterminates

The next two sections come from Ball-Lavrauw [21].

In most of the applications of Rédei polynomials we have a set of points with certain intersection properties with hyperplanes. Now we shall look at how to use Rédei polynomials in situations where we have a set of points that have certain intersection properties with smaller dimensional subspaces. The obvious place to start is in three dimensional affine or projective space, so let $A$ be a pointset of $\text{AG}(3, q)$ and define

$$
R(T, S, U) = \prod_{(x, y, z) \in A} (T + xS + yU + z).
$$

We define polynomials $\sigma_j$ in two indeterminates, of total degree at most $j$, by writing

$$
R(T, S, U) = \sum_{j=0}^{|A|} \sigma_j(S, U) T^{|A| - j}.
$$

Let $a$ and $b$ be any elements of $\mathbb{GF}(q)$ and consider the factors of the polynomial

$$
R(T, aU + b, U) = \prod_{(x, y, z) \in A} (T + (ax + y)U + bx + z).
$$

The point $(x, y, z)$ is incident with the line defined by the hyperplanes $aX + Y = \alpha$ and $bX + Z = \beta$ if and only if $ax + y = \alpha$ and $bx + z = \beta$ if and only if the
corresponding factor in $R(T, aU + b, U)$ is $T + \alpha U + \beta$. Note that for a fixed $a$ and $b$ these $q^2$ lines are parallel. Identifying the affine point $(x, y, z)$ with the projective point $(x, y, z, 1)$ then the line defined by the (hyper)planes $aX + Y = \alpha$ and $bX + Z = \beta$ is incident with point $(1, -a, -b, 0)$. Indeed, every affine line incident with $(1, -a, -b, 0)$ can be defined by the intersection of two planes of the form $aX + Y = \alpha$ and $bX + Z = \beta$, for some $\alpha$ and $\beta$, and this line is incident with $k$ points of $A$ if and only if $T + \alpha U + \beta$ occurs as a factor of $R(T, aU + b, U)$ with multiplicity $k$. Let us fix a situation to see how we can make use of this.

Let $A$ be a set of $q^2$ points that does not determine every direction, so we can assume there is a point $(1, -a, -b, 0)$ whose corresponding parallel class of $q^2$ lines are each incident with exactly one point of $A$. Each factor in $R(T, aU + b, U)$ is distinct and we have

$$R(T, aU + b, U) = \prod_{\alpha, \beta \in \mathrm{GF}(q)} (T + \alpha U + \beta) = T^{q^2} - ((U^q - U)^{q-1} + 1)T^q + (U^q - U)^{q-1}T.$$ 

However, we also have that

$$R(T, aU + b, U) = \sum_{j=0}^{q^2} \sigma_j(aU + b, U)T^{|A|-j}$$

and hence for $1 \leq j \leq q^2 - q - 1$, $\sigma_j(aU + b, U) \equiv 0$.

So we have that $\sigma_j(S, U) \equiv 0 \mod S - aU - b$ from which it follows that

$$S - aU - b \mid \sigma_j(S, U).$$

If there are more pairs $(a, b)$ than the degree of $\sigma_j$ for which this holds then $\sigma_j(S, U) \equiv 0$. So in our situation let $N$ be the number of directions $(1, -a, -b, 0)$ not determined by two points of $A$. Then

$$R(T, S, U) = T^{q^2} + \sum_{j=0}^{q^2-N} \sigma_{q^2-j}(S, U)T^j.$$ 

When we evaluate both $S = s$ and $U = u$ we are looking at the intersection properties of $A$ with planes. Indeed, a factor $T + \alpha$ has multiplicity $k$ in $R(T, s, u)$ if and only if the plane $sX + uY + Z = \alpha$ is incident with $k$ points of $A$. However, $R(T, s, u) = T^{q^2} + g(T)$, where $\deg g \leq q^2 - N$, and moreover factorises into linear factors in $\mathrm{GF}(q)[T]$. In [20] Ball and Lavrauw prove the following

**Theorem 24.14.** If $A$ is a set of $q^2$ points of $\mathbb{A}G(3, q)$ that does not determine at least $p^r q$ directions for some $e$ then every plane meets $A$ in $0 \mod p^{e+1}$ points.

By Theorem 18.15 of Storme and Sziklai we know that if the number of directions determined is less than $q(q + 3)/2$ then the set $A$ is $\mathrm{GF}(s)$-linear for some subfield
24. Jamison, Brouwer-Schrijver, affine blocking sets

$GF(s)$ of $GF(q)$. In the case when $q$ is prime this means that $A$ is a plane. Theorem 24.14 says that in the case when $q$ is prime and we have a set of points that determine less than $q^2 + 2$ directions then every plane contains $0 \mod q$ points. It would be interesting to know if this implies that $A$ is a cone. Some immediate corollaries of Theorem 24.14 relate to ovoids of the generalised quadrangles $T_2(O)$ or $T^*_2(O)$.

Corollary 24.15. [20] Let $O$ be an ovoid of the generalised quadrangle $T_2^*(O)$. The planes of $AG(3, q)$ are incident with zero mod $p$ points of $O$.

Corollary 24.16. [20] Let $O$ be an ovoid of the generalised quadrangle $T_2(O)$ containing the point $(1)$. The planes of $AG(3, q)$ are incident with zero mod $p$ points of $O$.

In the case when $O$ is a conic the generalised quadrangle $T_2(O)$ is isomorphic to $Q(4, q)$. Since we can choose any point of $Q(4, q)$ to be the point $(1)$, the corollary says that every elliptic quadric meets an ovoid of $Q(4, q)$ in $1 \mod p$ points or not at all. (See also Theorem 28.2 in Section 28.2) In fact one can eliminate the possibility that an elliptic quadric and an ovoid are disjoint but that does involve slightly more work, see [18]. A short counting argument leads to the following theorem.

Theorem 24.17. When $q$ is prime an ovoid of $Q(4, q)$ is an elliptic quadric.

Although the Rédei polynomial considered in [18] is the same as we have used here, they used a more roundabout argument involving the Klein correspondence to deduce the fact that for nearly all $j$ the identity $\sigma_j(aU, U - a) \equiv 0$ holds for all $a \in GF(q)$. Now we see that from $\sigma_j(aU + b, U) \equiv 0$, one only needs to substitute $U$ with $U - a$ and put $b = a^2$ to obtain the same equivalence. The previous theorem can be pushed a little further. De Beule and Metsch recently proved the following.

Theorem 24.18. When $q$ is prime a set of $q^2 + 2$ points that blocks every line of $Q(4, q)$ is an elliptic quadric together with a point.

24.3 Rédei polynomials in many indeterminates

Let us prove the natural generalisation of Theorem 24.14 to $AG(n, q)$ by using Rédei polynomials in $n$ variables.

Theorem 24.19. If $A$ is a set of $q^{n-1}$ points of $AG(n, q)$ that does not determine at least $p^e q$ directions for some $e$ then every hyperplane meets $A$ in $0 \mod p^{e+1}$ points.

Proof: Let $A \subset AG(n, q) = PG(n, q) \setminus \pi_{\infty}$ where $\pi_{\infty}$ is defined by the equation $X_0 = 0$. Let $D$ be the set of directions determined by $A$, i.e.

$$D = \{ P \in \pi_{\infty} | P \in \langle Q, R \rangle, Q, R \in A \}.$$
Define the Rédei polynomial as

\[ R(T, X) = \prod_{(a_1, \ldots, a_n) \in A} \left( T + \sum_{i=1}^{n} a_i X_i \right), \]

where \( X = (X_1, \ldots, X_n) \), and define the polynomials \( \sigma_j(X) \) by writing

\[ R(T, X) = \sum_{j=0}^{q^n-1} T^{q^n-1-j} \sigma_j(X). \]

Note that the total degree of \( \sigma_j \) is at most \( j \). Let \( P = (0, y_1, y_2, \ldots, y_n) \in \pi_\infty \setminus D \) be a direction not determined by \( A \) and since \( P \) must have a non-zero coordinate, we may assume that \( y_m = 1 \), for some \( m \). Now consider the Rédei polynomial \( R(T, X) \) modulo \( \sum_{i=1}^{n} y_i X_i \). We get

\[ R(T, X) \equiv \prod_{(a_1, \ldots, a_n) \in A} \left( T + \sum_{i=1}^{n} (a_i - a_m y_i) X_i \right) \mod \sum_{i=1}^{n} y_i X_i. \]

For all \( \gamma \in \text{GF}(q)^{n-1} \), the line defined by the \( n-1 \) equations \( X_i - y_i X_m = \gamma_i X_0 \), where \( i \neq m \), contains the point \( P \), which is a direction not determined by \( A \), and so contains exactly one point of \( A \). Hence there is exactly one \( (1, a_1, \ldots, a_n) \in A \) such that \( a_i - a_m y_i = \gamma_i \) for all \( i \neq m \) and we have

\[ R(T, X) \equiv \prod_{\gamma \in \text{GF}(q)^{n-1}} \left( T + \sum_{i=1, i \neq m}^{n} \gamma_i X_i \right) \mod \sum_{i=1}^{n} y_i X_i. \]

The above polynomial is linear over \( \text{GF}(q) \) in \( T \) and so

\[ R(T, X) \equiv T^{q^n-1} + \sum_{k=0}^{n-2} \sigma_{q^n-1-q^k}(X) T^{q^k} + \sigma_{q^n-1}(X) \mod \sum_{i=1}^{n} y_i X_i \]

and we conclude that \( \sigma_j(X) \equiv 0 \mod \sum_{i=1}^{n} y_i X_i \), whenever \( j \neq q^n-1 \) and \( j \neq q^n-1 - q^k \) for some \( k \). Hence for each \( P = (0, y_1, y_2, \ldots, y_n) \in \pi_\infty \setminus D \)

\[ \sum_{i=1}^{n} y_i X_i \mid \sigma_j(X) \]

in these cases and so \( \sigma_j(X) \equiv 0 \) whenever \( \deg(\sigma_j) \leq j < |\pi_\infty \setminus D| \). By hypothesis \( |\pi_\infty \setminus D| \geq p^e q \) and so we can write

\[ R(T, X) = T^{q^n-1} + \sum_{j=p^e q}^{q^n-1} \sigma_j(X) T^{q^n-1-j}. \]
Now let \( x \in \text{GF}(q)^n \) be any vector in \( n \) coordinates and let \( d \) be maximal such that \( R(T, x) \in \text{GF}(q)[T^{p^d}] \setminus \text{GF}(q)[T^{p^{d+1}}] \). We wish to prove that \( d \geq e + 1 \). Write \( R(T, x) = S(T)^{p^d} \), so \( S \in \text{GF}(q)[T] \setminus \text{GF}(q)[T^p] \) and importantly \( \partial_T S \neq 0 \). Moreover
\[
S(T) = T^{q^{n-1}/p^d} + S_1(T),
\]
where \( \deg(S_1) \leq q^{n-1}/p^d - q^{e-d} \). Since \( S(T) \) is the product of linear factors
\[
S(T) \mid (T^n - T) \partial_T S.
\]
The degree of the right-hand side of this divisibility is less than \( q + \deg(S_1) \leq q + q^{n-1}/p^d - q^{e-d} \). If \( d \leq e \), the degree of the left-hand side, which is the degree of \( S \) and equal to \( q^{n-1}/p^d \), will be greater than the degree of right-hand side and we conclude that the right-hand side of the divisibility must be zero. However this implies that \( \partial_T S \) is zero, a contradiction, hence \( d \geq e + 1 \).

We have shown that for all \( x \in \text{GF}(q)^n \),
\[
R(T, x) = \prod_{(1, a_1, \ldots, a_n) \in A} \left( T + \sum_{i=1}^n a_ix_i \right) \in \text{GF}(q)[T^{p^{e+1}}]
\]
and so all its factors \( T + \alpha \) occur with multiplicity a multiple of \( p^{e+1} \). Hence there are a multiple of \( p^{e+1} \) points of \( A \) satisfying \( \sum_{i=1}^n a_ix_i = \alpha \), or, in other words, there are \( 0 \) modulo \( p^{e+1} \) points of \( A \) on the hyperplane defined by the equation \( \sum_{i=1}^n x_iX_i = \alpha \). This concludes the proof.

Now the following improvement to Theorem 24.19 is given with a shorter and simpler proof from [11]. The main difference here is the use of \( \text{GF}(q) \times \text{GF}(q^{n-1}) \) as a model for \( \text{AG}(n, q) \) in place of the natural \( \text{GF}(q)^n \).

**Theorem 24.20.** Let \( q = p^h \) and \( 1 \leq p^e < q^{n-2} \). If there are more than \( p^e(q - 1) \) directions not determined by a set \( S \) of \( q^{n-1} \) points in \( \text{AG}(n, q) \) then every hyperplane meets \( S \) in \( 0 \) modulo \( p^{e+1} \) points.

In [11] sets of points that reach or almost reach the bound (for some special values of \( e \)) are constructed.

If \( f \) is a function in \( n - 1 \) variables over the finite field \( \text{GF}(q) \) then the set of points \( S = \{(x, f(x))|x \in \text{GF}(q)^{n-1}\} \) is a set of \( q^{n-1} \) points of \( \text{AG}(n, q) \) and the set of directions determined by the function \( f \) is defined to be the set of directions determined by \( S \). We call \( S \) the graph of \( f \), for obvious reasons. Note that for any set \( S \) of \( q^{n-1} \) points which does not determine all the directions, by applying an affine transformation so that the projective point \((0, \ldots, 0, 1)\) is a non-determined direction, we can construct a function whose graph is the set \( S \).

**Proof:** Let us consider the points of \( \text{AG}(n, q) \) as a set of elements of \( \text{GF}(q) \times \text{GF}(q^{n-1}) \) and \( S \) a set of \( q^{n-1} \) points. We can assume, after making an affine
transformation if necessary, that the hyperplane with first coordinate zero does not contain exactly \( q^{n-2} \) points of \( S \). Then the set of directions not determined by \( S \) consists of projective points \((1, m)\) where \( m \) runs through some set \( N \subseteq \text{GF}(q^{n-1}) \).

Let \( x = (x_1, x_2) \) and \( y = (y_1, y_2) \) be two points of \( \text{AG}(n, q) \) with the property that \( x_1 \neq y_1 \) and there is an element \( \mu \in \text{GF}(q^{n-1}) \) such that \( x_1\mu - x_2 = y_1n - y_2 \). Then, \( (x_1 - y_1)\mu = x_2 - y_2 \) and the projective point \((x_1 - y_1, x_2 - y_2) = (1, \mu)\). Thus, \((1, \mu)\) is the direction determined by the points \( x \) and \( y \).

For all \( m \in N \) the projective point \((1, m)\) is not determined by \( S \) and so the set \( \{x_1m - x_2 \mid x = (x_1, x_2) \in S\} \) consists of distinct elements, and hence all elements, of \( \text{GF}(q^{n-1}) \).

Define a polynomial \( r \) in two variables and polynomials \( \sigma_j \), in one variable of degree at most \( j(q-1) \), by

\[
r(X, Y) = \prod_{x \in S} (X - (x_1Y - x_2)^{q-1}) = \sum_{j=0}^{q^n-1} \sigma_j(Y)X^{q^n-1-j}.
\]

Now \( r \) has the property that for all \( m \in N \),

\[
r(X, m) = \prod_{x \in S} (X - (x_1m - x_2)^{q-1}) = \prod_{\lambda \in \text{GF}(q^{n-1})} (X - \lambda^{q-1}) =
\]

\[
= X(X(q^{n-1} - 1)^{q-1} - 1)^{q-1} = X^{q^n-1} + X^{q^{n-1}-(q^{n-1}-1)q-1} + \ldots + X.
\]

Thus, for all \( m \in N \) and \( 1 \leq j < (q^{n-1} - 1)(q-1) \) we have \( \sigma_j(m) = 0 \). However, \( |N| > p^e(q-1) \geq \deg(\sigma_j) \) for all \( j \leq p^e \) and since a polynomial has at most as many zeros as its degree, \( \sigma_j \) is identically zero for all \( 1 \leq j \leq p^e \).

Let \( c_j \) be coefficient of the term of degree \( j(q-1) \) in the polynomial \( \sigma_j(Y) \). Then

\[
\prod_{x \in S} (X - x_1^{-q-1}) = \sum_{j=0}^{q^n-1} c_j X^{q^{n-1} - j} = X^{q^n-1} + c_{p^e+1}X^{q^{n-1} - p^e-1} + \ldots + c_{p^n-1}.
\]

Now \( x_1 \in \text{GF}(q) \) and so \( x_1^{-q-1} = 1 \) unless \( x_1 = 0 \). If we write \( t \) for the number of points of \( x \in S \) with first coordinate zero then

\[
\prod_{x \in S} (X - x_1^{-q-1}) = X^t(X - 1)^{q^n-1-t} = \sum_{j=0}^{q^n-1} \binom{-t}{j}(-1)^j X^{q^n-1-j}.
\]

Comparing the above two equations we see that \( \binom{-t}{r} = 0 \mod p \) for all \( 0 \leq r \leq e \) and so \( t = 0 \mod p^e + 1 \), by Lucas’ Theorem. Thus the number of points of \( S \) incident with the hyperplane with first coordinate zero is \( 0 \) modulo \( p^e + 1 \). However, this hyperplane was chosen arbitrarily among the hyperplanes that do not contain exactly \( q^{n-2} \) points of \( S \). Hence, every hyperplane is incident with \( 0 \) modulo \( p^e + 1 \) points of \( S \).
Corollary 24.21. Let \( q = p^b \) and \( 1 \leq p^e q^t < q^{n-2} \), where \( e, t \in \mathbb{Z} \). If there are more than \( p^e q^t(q - 1) \) directions not determined by a set \( S \) of \( q^{n-1} \) points in AG\((n, q)\) then every \((n - 1 - s)\)-dimensional subspace, where \( 0 \leq s \leq t \), meets \( S \) in \( 0 \) modulo \( p^{e+1}q^t-s \) points.

Proof: Let \( \Sigma_{n-1-s} \) be a \((n - 1 - s)\)-dimensional subspace which does not contain \( q^{n-2-s} \) points of \( S \).

We first prove that there is a hyperplane containing \( \Sigma_{n-1-s} \) which does not contain exactly \( q^{n-2} \) points of \( S \). So we assume \( s \geq 1 \) since otherwise there is nothing to prove. If every subspace of dimension \( n - s \) which contains \( \Sigma_{n-1-s} \) contains exactly \( q^{n-s-1} \) points of \( S \) then

\[
|S| = q^{n-1} = n + (q^{n-s-1} - n)(q^{s+1} - 1)/(q - 1),
\]

where \( n \) is the number of points of \( S \) contained in \( \Sigma_{n-s-1} \). This implies that \( n = q^{n-1} \) which by assumption it is not. Therefore we can find a chain of subspaces \( \Sigma_{n-s-1} \subset \Sigma_{n-s} \subset \ldots \subset \Sigma_{n-1} \) with the property that \( |S \setminus \Sigma_{n-1}| \neq q^{n-2} \). Thus \( \Sigma_{n-1} \) meets the subspace at infinity in a subspace consisting entirely of determined directions.

There are \((q^n - q^{n-1})/(q^{n-s} - q^{n-s-1}) = q^s\) subspaces of dimension \( n - s \) that contain \( \Sigma_{n-1-s} \) and are not contained in \( \Sigma_{n-1} \) and so one of them meets the subspace at infinity in a subspace that contains at least \( p^e q^{t-s}(q - 1) \) non-determined directions. Applying Theorem 24.20 to this subspace, the corollary follows.

24.4 Affine blocking sets

This part is from Ball [8].

The following proposition will be analysed later to provide lower bounds on the sizes of multiple blocking sets with respect to hyperplanes in AG\((n, q)\). For the moment we satisfy ourselves with proving that for \( t \)-fold blocking sets of AG\((n, q)\), which have at most \((n + t - 1)(q - 1)\) points, a set of linear equations has a nontrivial solution. The degree of a polynomial \( f \) will be denoted \( f^\circ \).

Proposition 24.22. Let \( S \), a set of \((t + n - 1)(q - 1) + k - 1 \) points in AG\((n, q)\), be a \( t \)-fold blocking set with respect to hyperplanes. Then there exist \( \sigma_{i(q-1)} \) with \( \sigma_0 = 1 \) such that

\[
\sum_{i=0}^{\lfloor j/(q-1) \rfloor} \binom{aq - q - n + k - t - i(q - 1)}{j - i(q - 1)} \sigma_{i(q-1)} = 0 \pmod{p}
\]

for all \( j \) such that \( k - 1 \leq j < t \).
Theorem: Let $S$, a set of $(t+n-1)(q-1) + k - 1$ points in $\text{AG}(n, q)$, be a $t$-fold blocking set with respect to hyperplanes and assume $0 \in S$. Define
\[ F(X_1, \ldots, X_n) = \prod_{\sigma \in S} (s_1X_1 + \ldots + s_nX_n + 1), \]
then $F^o = |S| - 1 = (t+n-1)(q-1) + k - 2$. Write $F(X) = W(X) + V(X)$, where $V \in J_t$ and all terms divisible by $X_1^{c_1}qX_2^{c_2}q \cdots X_n^{c_n}q$ with $c_1 + \ldots + c_n = t$ appear only in $V$. Note that $W(0) \neq 0$ as $F(0) \neq 0$. By hypothesis we have that $X_1^1F \in J_t$ and hence that $X_1^1W \in J_t$. Moreover, considering the possible terms that can appear in $X_1^1W$, it follows that $X_1^1W = (X_1^q - X_1)W_1$ where $W_1 \in J_{t-1}$. Continuing for $X_2, \ldots, X_n$ we see that we can write
\[ W(X) = U(X) \prod_{i=1}^{n}(X_i^{q-1} - 1), \]
where $U^o \leq (t-1)(q-1) + k - 2$ and $U(0) \neq 0$.

On every hyperplane $X_1 = c$ there exist at least $t$ points of $S$ and therefore $(X_1^{q-1} - 1)^t$ divides
\[ F(X_1, 0, \ldots, 0) = (X_1^{q-1} - 1)U(X_1, 0, \ldots, 0) + (X_1^{q} - X_1)^t\hat{V}(X_1) = \prod_{\sigma \in S} (s_1X_1 + 1), \]
where $V(X_1, 0, \ldots, 0) = (X_1^{q} - X_1)^t\hat{V}(X_1)$. Let $\hat{S}$ be a multi-subset of the multiset $S^{[1]} := \{s_1((s_1, \ldots, s_n) \in S)\}$ of size $|S| - tq$ such that the multi-set $S^{[1]} \setminus \hat{S}$ contains each element of $\text{GF}(q)$ repeated exactly $t$ times. Define the symmetric functions $\sigma_j$ by
\[ \prod_{a \in \hat{S}} (aX + 1) = \sum_{j=0}^{nq - q - n + k - t} \sigma_jX^j. \]

Put $X_1 = X$, $s_1 = a$ and $F(X, 0, \ldots, 0) = (X^{q-1} - 1)^tf(X)$, let $\hat{V}(X, 0, \ldots, 0) = v(X)$ and $U(X, 0, \ldots, 0) = (X^{q-1} - 1)^{t-1}u(X)$ and rewrite the above as
\[ f(X) = u(X) + X^tv(X) = \sum \sigma_jX^j, \]
where $u^o \leq k - 2$. The coefficient of $X^j$ implies that $\sigma_j = 0$ whenever $k - 1 \leq j < t$. For all $\lambda \in \text{GF}(q)$ the set $S_{\lambda} = \{(s_1 + \lambda, s_2, \ldots, s_n) | (s_1, s_2, \ldots, s_n) \in S\}$ is a $t$-fold blocking set with respect to hyperplanes of $\text{AG}(n, q)$ and we can make a shift of the other $n - 1$ coordinates to ensure that $0$ is in $S_{\lambda}$. Let $\sigma_j^{(\lambda)}$ denote the $j$-th symmetric function of the set $\hat{S}_{\lambda} = \{a + \lambda | a \in \hat{S}\}$, then it follows that $\sigma_j^{(\lambda)} = 0$ whenever $k - 1 \leq j < t$. Now
\[ \sigma_j^{(\lambda)}(a_1 + \lambda)(a_2 + \lambda) \cdots (a_j + \lambda) = \sum_{r=0}^{j} \binom{\hat{S} - r}{j - r} \sigma_r \lambda^{j-r}. \]
where the first sum extends over all possible combinations of $a_1 + \lambda$, $a_2 + \lambda$, ..., $a_j + \lambda$ in $S_\lambda$. Hence for $k - 1 \leq j < t$

$$\sum_{r=0}^{k-1} \binom{nq - q - n + k - t - r}{j - r} \sigma_r \lambda^{j-r} = 0 \pmod{p}.$$

This is zero when reduced modulo $\lambda^q - \lambda$ since it is valid for all $\lambda \in \text{GF}(q)$. Therefore

$$\sum_{i=0}^{[j/(q-1)]} \binom{nq - q - n + k - t - i(q-1) - r}{j - i(q-1) - r} \sigma_{i(q-1)+r} = 0 \pmod{p}$$

where $0 \leq r < q - 1$. We are specifically interested in getting equations involving $\sigma_0$, since this is non-zero and so we conclude that for $k - 1 \leq j < t$

$$\sum_{i=0}^{[j/(q-1)]} \binom{nq - q - n + k - t - i(q-1)}{j - i(q-1)} \sigma_{i(q-1)} = 0 \pmod{p}. \quad \blacksquare$$

**Theorem 24.23.** For $t < q$ a t-fold blocking set with respect to hyperplanes in $AG(n, q)$ has at least $(t + n - 1)(q - 1) + k - 1$ points provided there exists a $j$ such that $k - 1 \leq j < t$ and the binomial coefficient $\binom{k-n-t}{j} \neq 0 \pmod{p}$.

**Proof:** In fact this is an almost trivial consequence of Proposition 24.22. Assume that there is a t-fold blocking set with $(t + n - 1)(q - 1) + k - 1$ points. Since $t < q$ we have that $j < q - 1$ and there is only one term in the sum. Lucas’ theorem allows us to ignore the terms in the top of the binomial coefficient divisible by $q$, and we deduce that $\binom{k-n-t}{j} \sigma_0 = \binom{k-n-t}{j} = 0 \pmod{p}$, which gives a contradiction if a $j$ in the condition of the theorem exists. \quad \blacksquare

**Corollary 24.24.** For $t < q$ a t-fold blocking set with respect to hyperplanes in $AG(n, q)$ has at least $(t + n - 1)q - n + 1$ points provided $\binom{n}{t} \neq 0 \pmod{p}$.

**Corollary 24.25.** For $t < q$ a t-fold blocking set with respect to hyperplanes in $AG(n, q)$ has at least $(t + 1)q - p^{e(t)}$ points (where $e(t)$ is maximal such that $p^{e(t)}$ divides $t$).

**Proof:** Let $k = t - p^{e(t)} + 1$ and $j = t - 1$, write $t = t_0p^{e(t)}$ where $p \nmid t_0$. Then $\binom{-p^{e(t)}+1}{t-1} \sigma_0 = \binom{-2p^{e(t)}+p^{e(t)}-1}{t_0-1} = \binom{-2}{t_0-1} \pmod{p}$, which is non-zero. \quad \blacksquare

Now we are well prepared for the next section on nuclei and affine blocking sets as well.
II. Polynomials in geometry

25 Nuclei and affine blocking sets

The theory of nuclei shows a nice application of the \( \text{GF}(q^2) \)-representation.

**Definition 25.1.** \( P \not\in B \) is a \( t \)-fold nucleus of \( B \subset \text{PG}(2, q) \) if all the lines through \( P \) intersect \( B \) in at least \( t \) points.

A 1-fold nucleus is called nucleus simply. The motivation of this notion is that the nucleus of an oval in a plane of even order is a nucleus in this sense as well. Obviously, if \( B \) has a nucleus then \( |B| \geq t(q + 1) \). The set of nuclei is sometimes denoted by \( N(B) \).

It is also interesting to dualise this concept. Given \( L \), a set of lines in \( \text{PG}(2, q) \), a line \( \ell \not\in L \) is a \( t \)-fold nuclear line of it if the lines of \( L \) cover each point of \( \ell \) at least \( t \) times. It means that if you consider \( L \) as a totally reducible algebraic curve, then \( \ell \) intersects it in each point (of \( \ell \)) with multiplicity at least \( t \).

**Theorem 25.2.** If \( B \subset \text{PG}(2, q) \), \( |B| = q + 1 \) and it is not a line then it has at most \( q - 1 \) nuclei.

**Proof 1:** There exists a line disjoint from \( B \) so w.l.o.g. \( B \in \text{AG}(2, q) \) and no infinite point can be a nucleus. Using the \( \text{GF}(q^2) \)-representation of the affine plane, define \( f(X) = \sum_{b \in B} (X - b)^{q-1} \). If \( x \) is a nucleus then the set of \( (X - b)^{q-1} \) is exactly the complete set of \( (q + 1) \)-st roots of unity, so their sum is 0, hence \( x \) is a root of \( f \), which is of degree \( q \). \(\) 

**Proof 2:** Consider the following polynomial defined by \( B \):

\[
F(X, Y, Z) = \sum_{(b_1, b_2, b_3) \in B} (b_1X + b_2Y + b_3Z)^{q-1};
\]

we will prove that if \( (a_1, a_2, a_3) \) is a nucleus of \( B \) then \( (a_1X + a_2Y + a_3Z)|F(X, Y, Z) \). Then it follows that

\[
\prod_{(a_1, a_2, a_3) \in N(B)} (a_1X + a_2Y + a_3Z) \mid F(X, Y, Z),
\]

which is of degree \( q - 1 \).

Take a line \([v_1, v_2, v_3]\) meeting \( B \) in precisely one point. Then \( F(v_1, v_2, v_3) = 0 \) as of the \( q + 1 \) terms of the sum one is zero and the other \( q \) are all 1.

Now w.l.o.g. assume that \( a_1 \neq 0 \) and write \( F(X, Y, Z) = (a_1X + a_2Y + a_3Z)g(X, Y, Z) + G(Y, Z) \) with \( G(Y, Z) \) homogeneous of degree \( q - 1 \) or identically zero. Since \([u, v, w]\) with \( u = -\frac{a_2v + a_3w}{a_1} \) is a line through \((a_1, a_2, a_3)\) and hence contains a unique point of \( B \), so \( F(u, v, w) = 0 \) and \( a_1u + a_2v + a_3w = 0 \). Hence \( G(v, w) = 0 \) for all \( v, w \in \text{GF}(q) \). So \( G \) cannot have degree \( q - 1 \) hence it is
identically zero.

Proof 3: This proof uses the Segre-trick:

Lemma 25.3. (Segre, Korchmáros) Let \( B \subset PG(2, q) \) a pointset of size \( q + 1 \) and \( A_1, A_2, A_3 \) three non-collinear nuclei of \( B \). Write \( B_i = A_j A_k \cap B \), where \( \{i, j, k\} = \{1, 2, 3\} \). Then the three points \( B_1, B_2, B_3 \in B \) are collinear.

Proof of the lemma Let \( A_1, A_2, A_3 \) be the base points of the coordinate frame, let \( B_1 = (0, 1, b_1), B_2 = (b_2, 0, 1), B_3 = (1, b_3, 0) \), where \( b_1 b_2 b_3 \neq 0 \). Apply the Segre-trick for the lines joining \( A_i \) to to points of \( B \setminus \{B_1, B_2, B_3\} \), so build a matrix of size \( (q - 2) \times 3 \), with rows indexed by the points of \( B \setminus \{B_1, B_2, B_3\} \) and with columns indexed by \( A_1, A_2 \) and \( A_3 \). The entry in position \( (P, A_i) \) is the “coordinate” of the line \( PA_i \), so if the equation of the line is \( X_3 = \lambda_1 X_2 \) or \( X_1 = \lambda_2 X_3 \) or \( X_2 = \lambda_3 X_1 \) then this \( \lambda_i \) will appear in the matrix. By Ceva’s theorem, the product of the three elements in any row is 1. On the other hand, in each column all but one elements of the theorem, the product of the three elements in any row is 1. On the other hand, \( \prod_{P \in B} P \) by Wilson’s theorem, the (product of all the entries) times \( \prod_{P \in B} P \) is identically zero.

Now we are ready for Proof 3 (which is due to Blokhuis and Mazzocca): Again we can restrict ourselves to \( AG(2, q) \). Define a map \( f : N(B) \to GF(q)^* \) in the following way: take an arbitrary \( P \in N(B) \) and put \( f(P) = 1 \). If \( P_i \in N(B) \), let \( B = PP_i \cap B \) (which is unique). Now \( B_i = \lambda_i P + (1 - \lambda_i) P_i \) for a suitable \( \lambda_i \in GF(q)^* \setminus \{1\} \). Then put \( f(P_i) = \frac{1}{\lambda_i - 1} \). Denote the affine coordinates like \( P(p^1, p^2), P_i(p^1_i, p^2_i) \) and \( B_i(b^1_i, b^2_i) \). It is easy to check that in \( AG(3, q) \) the points \( (p^1, p^2, f(P)), (p^1_i, p^2_i, f(P_i)) \) and \( (b^1_i, b^2_i, 0) \) are collinear.

The Segre-Korchmáros lemma implies that if \( B' \subset B \) is on the line \( P_i P_j \) then \( B_i, B_j, B' \) and hence \( (p^1, p^2, f(P_i)), (p^1_i, p^2_i, f(P_j)) \) and \( (b^1_i, b^2_i, 0) \) are collinear. In particular \( f \) is injective, so \( |N(B)| \leq q - 1 \).

A more general form of it is the following

Theorem 25.4. (Blokhuis) If \( B \subset AG(2, q) \), \( |B| = t(q + 1) + k - 1, k < q \), then the number of its \( t \)-fold nuclei is at most \( k(q - 1) \), supposing that \( \binom{t+k-1}{k} \neq 0 \) (mod \( p \)) holds.

Proof: As in the previous proof, after identifying \( AG(2, q) \) and \( GF(q^2) \), define the polynomial

\[
F(X, T) = \prod_{b \in B} (T - (X - b)^{q-1}).
\]
II. Polynomials in geometry

(Note that \( \sum (X - b)^{q-1} \), used in the previous proof, is just the coefficient of \( T^{(q+1)+k-2} \).) For a \( t \)-fold nucleus \( x \), the multiset \( \{ (x - b)^{q-1} : b \in B \} \) contains every \((q + 1)\)-st root of unity at least \( t \) times, so the polynomial \( F(x, T) \) in one variable is divisible by \((T^{q+1} - 1)^t\) for each \( t \)-fold nucleus \( x \).

Let \( \sigma_j(X) \) denote the \( j \)-th elementary symmetric polynomial of the terms \((X - b)^{q-1}\). As a polynomial of \( X \), its degree is \( \leq j(q - 1) \), with equality if \( \binom{|B|}{j} \) is nonzero in \( \text{GF}(q) \); for \( j = k \) this is the condition in the statement. As \( F(X, T) = \sum_{j=0}^{|B|} (-1)^j \sigma_j(X) T^{|B| - j} \), in case of \( X = x \) being a \( t \)-fold nucleus, we have

\[
F(x, T) = (T^{q+1} - 1)^t(T^{k-1} + \ldots).
\]

On the right hand side the coefficient of \( T^{t(q+1)-1} \) is zero as \( k < q \), on the left hand side this coefficient is \((-1)^k \sigma_k(x)\). So every \( t \)-fold nucleus \( x \) is a root of \( \sigma_k(X) \), which is of degree \( k(q - 1) \).

A nice refinement and re-frasing is the following

**Theorem 25.5.** (Ball) If \( B \) is a \( t \)-fold blocking set of \( \text{AG}(2, q) \), \( e(t) \) is the maximal exponent for which \( p^{e(t)} \) then \( |B| \geq (t+1)q - p^{e(t)} \).

For \( e(t) = 0 \), i.e. when \( \text{g.c.d.}(t, q) = 1 \), it was proved by Blokhuis. In particular, when \( t = 1 \) it is Jamison’s result 12.2.

**Proof:** First let’s see the connection between nuclei and blocking sets. If \( B \) is a \( t \)-fold blocking set then all the points in its complement are \( t \)-fold nuclei of \( B \).

Suppose to the contrary that \( B \) is a blocking set of size \((t+1)q - p^{e(t)} - 1 = t(q + 1) + (q - t - p^{e(t)}) - 1\), so by the previous theorem \((k = q - t - p^{e(t)})\) it has at most \((q - t - p^{e(t)})(q - 1)\) nuclei, which is less than the size of the complement of \( B \), so \( B \) cannot be a \( t \)-fold blocking set provided \( \binom{t+k-1}{k} \neq 0 \) modulo \( p \). Write \( t = p^{e(t)}c \) where \( p \nmid c \). Using Lucas’ theorem and calculating modulo \( p \) we have

\[
\left( \frac{(t(q + 1) + k - 1)}{t(q + 1) - 1} \right) = \left( \frac{tq + q - p^{e(t)} - 1}{tq + t - 1} \right) =
\]

\[
\left( \frac{q - p^{e(t)} - 1}{cp^{e(t)} - 1} \right) = \left( \frac{q - 2p^{e(t)} + p^{e(t)} - 1}{(c - 1)p^{e(t)} + p^{e(t)} - 1} \right) = \left( \frac{q/p^{e(t)} - 2}{c - 1} \right) \left( \frac{p^{e(t)} - 1}{p^{e(t)} - 1} \right),
\]

which is non-zero mod \( p \) as, using base \( p \), each digit of \( q/p^{e(t)} - 2 \) is \((p - 1)\) except the last one which is \((p - 2)\), but the last digit of \( c - 1 \) cannot be \( p - 1 \) as \( p \nmid c \).

**Corollary 25.6.** If \( K \) is a \((k, n)\)-arc of \( \text{AG}(2, q) \), and \( e \) is the maximal exponent such that \( p^e \) then \(|K| \leq (n - 1)q + p^e \).
25. Nuclei and affine blocking sets

Proof: Let $B$ be the complement of $K$ in $\AG(2,q)$. It is a $t = (q-n)$-fold blocking set and the previous theorem gives the bound.

Lunelli and Sce conjectured that the size of a $(k,n)$-arc $K$ in $\PG(2,q)$ is $k \leq (n-1)q+1$. It was disproved it by Hill and Mason, their counterexample is the disjoint union of some Baer subplanes; but if $\gcd(n,q)=1$ and there exists a line skew to $K$ then the previous Corollary shows that the Lunelli-Sce bound is true.

25.1 Lower nuclei

Now suppose that $B \subset \AG(2,q)$, $|B| = t(q+1) - k + 1$, and we want to investigate its $t$-fold lower nuclei, so the points from which $B$ looks like a $(|B|, t)$-arc. The result is quite similar to the case of nuclei:

**Theorem 25.7.** If $B \subset \AG(2,q)$, $|B| = t(q+1) - k + 1$, then the number of its $t$-fold nuclei is at most $k(q-1)$, supposing that $\binom{t(q+1)}{k} \not\equiv 0 \pmod{p}$ holds.

As we did before, let’s identify $\AG(2,q)$ and $\GF(q^2)$, so $B \subset \GF(q^2)$. Let $E$ be the multiset of $(q+1)$-st roots of unity in $\GF(q^2)$, each with multiplicity $t$. Let $B(X) = \{(X - b_1)^{q-1}, (X - b_2)^{q-1}, ..., (X - b_{|B|})^{q-1}\}$ where $B = \{b_1, ..., b_{|B|}\}$. Then the point represented by $x \in \GF(q^2)$ is a $t$-fold (lower) nucleus of $B$ if and only if it is not in $B$ and $B(x) \subseteq E$ as a multiset.

First we prove two lemmas.

**Lemma 25.8.** Let $S \subset E$, $|S| = t(q+1) - r$, $\sigma_i = \sigma_i(S)$, $\sigma_r^* = \sigma_i(E \setminus S)$. Then

$$\sum_{i=0}^{r} \sigma_i^* \sigma_{r+1-i} = 0.$$

Proof: $$(X^{q+1} - 1)^t = \prod_{a \in E}(X - a) = \prod_{b \in S}(X - b) \prod_{\beta \in (E \setminus S)}(X - \beta) = \sum_{i=0}^{t(q+1) - r} (-1)^i \sigma_i X^{(t(q+1) - r - i)} \sum_{j=0}^{r} (-1)^j \sigma_j^* X^{r-j}.$$ The coefficient of $X^{t(q+1) - u}$ in this expression, $u = 1, 2, ..., q - 2$, is

$$\sum_{i=0}^{r} \sigma_i^* \sigma_{u-i} = 0. \quad (u)$$

From $(u)$, $\sigma_u^*$ can be expressed as

$$\sigma_u^* = -\sum_{i=0}^{u-1} \sigma_i^* \sigma_{u-i}. \quad (u^*)$$
Now the next, \((r + 1)\)-st equality gives the desired relation among the elementary symmetric polynomials, as no more \(\sigma_i^*\) can appear (note that the upper limit is \(r\) instead of \(r + 1\)):

\[
\sum_{i=0}^{r} \sigma_i^* \sigma_{r+1-i}.
\]

We remark that the lemma can be proved in a shorter way, but the equations above will be needed; this way one can see that \((r + 1)\) is the first (i.e. minimal degree) non-trivial condition that can be proved.

**Lemma 25.9.** For \(j \geq 1\)

\[
\sum_{l=0}^{j} (-1)^l \binom{a+l-1}{l} \binom{a}{j-l} = 0
\]

holds.

**Proof:** Since \((X + 1)^a = \sum_{l=0}^\infty \binom{a+l-1}{l} (-1)^l X^l\) and \((X + 1)^a = \sum_{l=0}^\infty \binom{a}{l} X^l\), it follows that

\[
1 = (X + 1)^{-a}(X + 1)^a = \sum_{j=0}^\infty X^j \sum_{l=0}^\infty (-1)^l \binom{a+l-1}{l} \binom{a}{j-l},
\]

which immediately gives the lemma.

Now we are ready for the

**Proof of Theorem 25.7:** Let

\[
G(X) = \sum_{i=0}^{k-1} \sigma_i^* (B(X)) \sigma_{k-i}(B(X)).
\]

If \(x\) is a \(t\)-fold nucleus then Lemma 25.8 applies, that is

\[
G(x) = \sum_{i=0}^{k-1} \sigma_i^* (B(x)) \sigma_{k-i}(B(x)) = 0.
\]

We state that \(G(X)\) has degree \(k(q-1)\). All the nuclei are roots of it. We determine the coefficient of \(X^{k(q-1)}\). Since \(k-1 < q\), all the equations \((u)\) hold for \(u = 1, ..., k\).

Let \(z_i\) denote the coefficient of \(X^{i(q-1)}\) in

\[
\sigma_i^* ((X - b_1)^{q-1}, (X - b_2)^{q-1}, ..., (X - b_{|B|})^{q-1}).
\]

Then for \(i = 1, ..., k - 1\)

\[
z_i = - \sum_{j=0}^{i-1} z_j \binom{a}{i-j}.
\]

By Lemma 25.9 for \(i = 1, ..., k - 1\)

\[
z_i = (-1)^{i+1} \binom{a + i - 1}{i}.
\]
Then for our polynomial \( k \):

\[
\sum_{j=0}^{k-1} z_j \binom{a}{k-j} = -\sum_{j=0}^{k-1} (-1)^{j+1} \binom{a+j-1}{j} \binom{a}{k-j}
\]

from which

\[
z_k = (-1)^{k-1} \binom{t(q+1)}{k} \neq 0
\]

by the assumption of the Theorem. So the polynomial is of degree \( k(q-1) \) exactly, it is not the zero polynomial, hence it has at most so many roots.

\section{Internal nuclei}

A point of \( B \) not contained in a collinear triplet is usually called an \textit{internal nucleus}. The set of internal nuclei is denoted by \( \text{IN}(B) \). Further result on internal nuclei can be found e.g. in \[139\], we only state a nice result of Wettl here. The proof is left to the reader as an exercise.

\textbf{Theorem 25.10.} (Wettl) Let \( q \) be odd, \( B \) be a set of \( q+1 \) points in \( \text{PG}(2,q) \). Then \( \text{IN}(B) \) is contained in a conic.

\textbf{Proof:} (Hint: Show that there is a unique tangent at each \( P \in \text{IN}(B) \). Apply Segre’s lemma for a triangle \( A_1, A_2, A_3 \in \text{IN}(B) \).)

\section{Higher dimensions}

Now we generalize the previous results to higher dimensions. Here we identify \( \text{AG}(n,q) \) with \( \text{GF}(q^n) \).

\textbf{Definition 25.11.} \( P \not\in B \) is a \( t \)-fold nucleus of \( B \subset \text{PG}(n,q) \) if all the lines through \( P \) intersect \( B \) in at least \( t \) points.

A 1-fold nucleus is called nucleus simply. Obviously, if \( B \) has a nucleus then \( |B| \geq t\theta_{n-1} \).

\textbf{Theorem 25.12.} If \( B \subset \text{AG}(n,q) \), \( |B| = \theta_{n-1} \) and it is not a hyperplane then it has at most \( q-1 \) nuclei.

\textbf{Exercise 25.13.} Modify Proof 1 and Proof 2 of Theorem 25.2 as needed!

A more general form of it is the following
Theorem 25.14. Let $B \subseteq \PG(n, q)$, $|B| = t(q + 1) + k - 1$, $k < q$, suppose that there are exactly $i$ points of it on the ideal hyperplane $\PG(n, q) \setminus \AG(n, q)$. Then the number of its $t$-fold nuclei contained in $\AG(n, q)$ is at most $(k+r)(q-1)$ for any $r \geq 0$ such that the binomial coefficient $(t^k - i - 1 \choose k+r) \not\equiv 0 \pmod p$ holds.

It is a generalisation of Blokhuis’ [31]. For $r = 0$ this is in [112].

Exercise 25.15. Modify the proof of Theorem 25.4 as needed!

From 25.12, so in the case $t = k = 1$ we have that there are $q - 1$ nuclei only. However, if $B$ intersects every hyperplane of $\PG(n, q)$, Blokhuis and Mazzocca proved the following.

Theorem 25.16. If $B$ of size $\theta_{n-1}$ intersects every hyperplane of $\PG(n, q)$ then it has at most $q^{n-1} - q^{n-2}$ nuclei; moreover there exist sets attaining this bound.

In the extremal case when $r = q^{n-2} - 1$ we have that $q^{n-2}\theta_{n-1} - i$ or we would have been able to find a smaller $r$ for which the binomial coefficient was non-zero. It follows then that $i \equiv \theta_{n-3} \pmod {q^{n-2}}$ or in words that every hyperplane meets $B$ in $\theta_{n-3} \pmod {q^{n-2}}$ points. From this it can be deduced that the classification of $\theta_{n-1}$-sets with $q^{n-1} - q^{n-2}$ nuclei is equivalent to the classification in the case of $(q + 1)$-sets in $\PG(2, q)$ having $q - 1$ nuclei, see ...

As in the planar case we have the following consequence for affine blocking sets.

Theorem 25.17. (Ball) If $B$ is a $t$-fold blocking set of $\AG(n, q)$, $e(T)$ is the maximal exponent for which $p^e(t) \mid t$ then $|B| \geq (t + 1)q - p^e(t)$.

Exercise 25.18. Modify the proof of Theorem 25.5 as needed!

For $e(t) = 0$, i.e. when g.c.d.$(t, q) = 1$, it was proved by Blokhuis. In particular, when $t = 1$ it is Jamison’s result.

Lower nuclei

Now suppose that $B \subseteq \AG(n, q)$, $|B| = t\theta_{n-1} - k + 1$, and we want to investigate its $t$-fold lower nuclei, so the points from which $B$ looks like a $|B|, t$-cap. The result is quite similar to the case of nuclei:

Theorem 25.19. Let $B \subseteq \PG(n, q)$, $|B| = t(q + 1) - k + 1$, $k < q$, suppose that there are exactly $i$ points of it on the ideal hyperplane $\PG(n, q) \setminus \AG(n, q)$. Then the number of its $t$-fold lower nuclei contained in $\AG(n, q)$ is at most $(k+r)(q-1)$ for any $r > 0$ such that the binomial coefficient $(t+i \choose k+r) \not\equiv 0 \pmod p$ holds.

Exercise 25.20. Modify the proof of Theorem 25.7 as needed!
26 Mixed representations

This part is from [15]. It is a continuation of Section 13.1, where the planar case was arranged. Here we see the high dimensional generalization, and what makes it work is the following “mixed representation” of the space.

Let \( k \geq 4 \). If we view \( \text{GF}(q)^{k-3} \times \text{GF}(q^2) \) as the \((k-1)\)-dimensional vector space over \( \text{GF}(q) \) then the points of \( \text{AG}(k-1, q) \) can be viewed as \( a = (a_0, a_1, a_2, \ldots, a_{k-2}) \) where \( a_{k-2} \in \text{GF}(q^2) \) and the other \( a_i \) are elements of \( \text{GF}(q) \). In the quotient space of \( w_0 = (1, 0, \ldots, 0, y_0), w_1 = (0, 1, 0, \ldots, 0, y_1), \ldots, w_{k-3} = (0, \ldots, 0, 1, y_{k-3}) \) the point \( a \) is given by \((0, \ldots, 0, y_0 - a_{k-2} + \sum_{i=1}^{k-3} a_i y_i) \). As in Section 13.1, the points \( a \) and \( b \) are on the same point in \( \text{PG}(1, q) \) if and only if \((y_0 - a_{k-2} + \sum_{i=1}^{k-3} a_i y_i)^{q-1} = (y_0 - b_{k-2} + \sum_{i=1}^{k-3} b_i y_i)^{q-1} \) if and only if \( \langle w_0, w_1, \ldots, w_{k-3}, a \rangle = \langle w_0, w_1, \ldots, w_{k-3}, b \rangle \). Note that \( y_0 - a_{k-2} + \sum_{i=1}^{k-3} a_i y_i = 0 \) if and only if \( a \in \langle w_0, w_1, \ldots, w_{k-3} \rangle \).

**Theorem 26.1.** A set of points \( S \) in \( \text{PG}(k-1, q) \) which is incident with 0 mod \( r \) points of every hyperplane has at least \((r - 1)q + (p-1)r\) points, where \( 1 < r < q = p^h \) and \( k \geq 4 \).

**Proof:** Either there is a co-dimension 2 subspace that is incident with no points of \( S \) or \(|S| \geq q^2 + q + 1 \) (from which the theorem follows) or every co-dimension 3 subspace is incident with a point of \( S \) (which if were the case either \(|S| > q^3 \) or every co-dimension 4 subspace is incident with a point of \( S \).)

Counting points of \( S \) on hyperplanes containing this co-dimension 2 subspace either \(|S| \geq r(q+1)\) (and hence the theorem is proved) or there is a hyperplane incident with no points of \( S \). Moreover \(|S| = 0 \) mod \( r \).

Let \( s \) be the greatest common divisor of the non-trivial intersections that \( S \) has with the co-dimension 2 subspaces. If \( s > 1 \) then take a co-dimension 2 subspace incident with \( ms \) points of \( S \) and by induction each hyperplane containing this co-dimension 2 subspace contains at least \((s-1)q + (p-1)s - ms\) points of \( S \) and so \(|S| \geq ((s-1)q + (p-1)s - ms)(q+1) + ms > (r+1)q \). Thus there is a co-dimension 2 subspace incident with just one point of \( S \). Counting points of \( S \) on hyperplanes containing this co-dimension 2 subspace we see that \(|S| = 1 + (q+1)(-1) \) mod \( r \). Combining this with \(|S| = 0 \) mod \( r \) we have that \( q = 0 \) mod \( r \).

We can view \( S \) as a subset of \( \text{GF}(q)^{k-3} \times \text{GF}(q^2) \simeq \text{AG}(k-1, q) \) and consider the polynomial

\[
R(X, Y) = \prod_{a \in S} \left( X + (Y_0 - a_{k-2} + \sum_{i=1}^{k-3} a_i Y_i)^{q-1} \right) = \sum_{j=0}^{\left\lfloor \frac{|S|}{2} \right\rfloor} \sigma_j(Y) X^{|S|-j}.
\]

For all \( y = (y_0, y_1, \ldots, y_{k-3}) \in \text{GF}(q^2)^{k-2} \) the points \( w_0 = (1, 0, \ldots, 0, y_0), w_1 = (0, 1, 0, \ldots, 0, y_1), \ldots, w_{k-3} = (0, \ldots, 0, 1, y_{k-3}) \) and \( b \) are on the same hyperplane if and only if \((y_0 - a_{k-2} + \sum_{i=1}^{k-3} a_i y_i)^{q-1} = (y_0 - b_{k-2} + \sum_{i=1}^{k-3} b_i y_i)^{q-1} \neq 0 \).
Suppose that $W = \langle w_0, w_1, \ldots, w_{k-3} \rangle$ is a $(k-3)$-dimensional subspace is incident with $t$ points of $S$. By hypothesis every $(k-2)$-dimensional subspace contains a multiple of $r$ points of $S$ and so

$$R(X, y) = X^t(X^{q+1} - 1)^{r-t_0}g(X)^r,$$

where $t_0 = t \mod r$.

For all $y \in \mathbf{GF}(q^2)^{k-2}$ the polynomial $\sigma_j(y) = 0$ whenever $0 < j < q$ and $r$ does not divide $j$. However $\sigma_j$ has degree at most $j(q-1)$ and so, for $0 < j < q$ and $r$ does not divide $j$, the polynomial $\sigma_j \equiv 0$.

Let $|S| = (r-1)q + \kappa r$.

For future reference note that if $t = 0$ then $\sigma_{q+1}(y) = 0$. If $t = 1$ then $\sigma_{q+1}(y) = 1$ and $\sigma_{kr}(y) = 0$ since the degree of $g$ in this case is at most $\kappa - 1$.

Let $'$ be differentiation with respect to any one of the variables $Y_i$. As in the proof of the planar case, Theorem 13.6, we have

$$R(X, y) \mid (X^{q+1} - 1)\frac{\partial R}{\partial Y}(X, y).$$

If $|W \cap S| = 0$ then $R(X, y)$ is an $r$-th power and in exactly the same way as in the proof of Theorem 13.6 we have

$$\sigma_{kr}\sigma'_{q+1} = -\sigma'_{kr}.$$

Let

$$f(Y) = \prod_{a \in S} (Y_0 - a_{k-2} + \sum_{i=1}^{k-3} a_i Y_i).$$

If $|W \cap S| > 0$ then $f(y) = 0$ and if $|W \cap S| = 0$ then $\sigma_{q+1}(y) = 0$, therefore $f\sigma_{q+1} = 0$ for all $y \in \mathbf{GF}(q^2)^{k-2}$. So there are polynomials $r_i$ for $i = 1, \ldots, k-2$ such that

$$f\sigma_{q+1} = \sum_{i=1}^{k-2} (Y_i^{q^2} - Y_i)r_i(Y),$$

and the degree of $r_i$ is at most $\deg f + \deg \sigma_{q+1} - q^2 \leq |S| - 1$.

Now choose any $(y_1, \ldots, y_{k-3}) \in \mathbf{GF}(q^2)^{k-3}$ and $b \in S$ and set $y_0 = b_{k-2} - \sum_{i=1}^{k-3} b_i y_i$. Then $b \in W$ so $|W \cap S| \geq 1$. Differentiate $f\sigma_{q+1}$ with respect to $Y_i$ and evaluate at $y$. Since $|W \cap S| \geq 1$ it follows that $f(y) = 0$ and so $\sigma_{q+1}f' = -r_i$.

If $|W \cap S| > 1$ then $f'(y) = 0$ and hence $r_i(y) = 0 = -f'(y)$. If $|W \cap S| = 1$ then $\sigma_{q+1} = 1$ and $r_i(y) = -f'(y)$. Thus the polynomial $r_i + f'$ has at least $|S|q^{2(k-3)}$ zeros but is a polynomial of degree at most $|S| - 1$ over $\mathbf{GF}(q^2)$ in $k-3$ indeterminates and is either zero or has at most $(|S| - 1)q^{2(k-3)}$ zeros. Thus $r_i = -f'$ and

$$f\sigma_{q+1} = -\sum_{i=1}^{k-2} (Y_i^{q^2} - Y_i)\frac{\partial f}{\partial Y_i}.$$
Now again differentiate $f^\sigma q_{q+1}$ but now evaluate for $y \in \text{GF}(q^2)^{k-2}$ where $|W \cap S| = 0$. Then $\sigma_{q+1}(y) = 0$ and
\[ \sigma'_{q+1} = f'/f. \]
Combining this with $\sigma_{kr}\sigma'_{q+1} = -\sigma'_{kr}$ we have that $(f\sigma_{kr})' = 0$.
Returning to the case where $|W \cap S| = 1$ we have that $\sigma_{kr}(y) = f(y) = 0$ and so $(f\sigma_{kr})' = 0$. And in the case $|W \cap S| = t > 1$ the polynomial $f$ has a zero of degree $t$ and so again $(f\sigma_{kr})' = 0$. The polynomial $(f\sigma_{kr})'$ is zero for all $y \in \text{GF}(q^2)^{k-2}$ but is a polynomial of degree at most $|S| + kr(q-1) < q^2$. Thus $(f\sigma_{kr})' \equiv 0$. This holds for which ever indeterminate $Y_i$ we choose to differentiate with respect to and so we conclude that $f\sigma_{kr} \in \text{GF}(q^2)[Y_0, \ldots, Y_{k-3}]$. Hence $f^{p-1}$ divides $\sigma_{kr}$.
If $\kappa \leq p-2$ then $(p-1)(r-1)q + kr(p-1) > kr(q-1)$ and so $\sigma_{kr} \equiv 0$. However the polynomial whose terms are the terms of highest degree in $R(X,Y_0,0,\ldots,0)$ is $(X + Y_0^{q-1})^{(S)}$ which has a term $X^{(r-1)q}Y_0^{kr(q-1)}$ since $(S)_{kr} = 1$. Thus $\sigma_{kr}$ has a term $Y^{kr(q-1)}$ which is a contradiction. Therefore $\kappa \geq p-1$.

**Corollary 26.2.** A code whose weights and length have a common divisor $r$ and whose dual minimum distance is at least 3 has length at least $(r-1)q + (p-1)r$.

### 27 Flocks

**Theorem 27.1.** (Fisher and Thas 1979, Orr 1973) Given an elliptic quadric in $\text{PG}(3,q)$ and a set of $q-1$ pairwise disjoint conics partitioning all but two of its points, then the $q-1$ planes of those conics must contain a common line (that misses the quadric).

**Proof:** Use stereographic projection from one of the uncovered points, mapping all the other points onto the affine plane $\text{AG}(2,q)$ in such a way that the other uncovered point is mapped to the origin. All the conics become pairwise disjoint circles of the affine plane (or the inversive plane over $\text{GF}(q)$). One can imagine them as conics in the plane having two conjugate imaginary points at infinity in common. Now the theorem can be translated saying that a family of $q-1$ disjoint circles covers $\text{AG}(2,q) \setminus \{0\}$ if and only if all circles are centered at the origin.

Now we identify $\text{AG}(2,q) \setminus \{0\}$ and $\text{GF}(q^2) \setminus \{0\}$ as usual; the points are exactly the roots of $Z^{q^2-1} - 1 = 0$.

The $j$-th circle is the set $\{ z : (z - a_j)(z - a_j)^q = r_j \}$, where $a_j \in \text{GF}(q^2), r_j \in \text{GF}(q)^*$. Set $c_j(Z) = (Z - a_j)(Z - a_j)^q - r_j$, then the theorem says $\prod_{j=1}^{q^2-1} c_j(Z) = Z^{q^2-1} - 1$ if and only if all $a_j = 0$.

**Exercise 27.2.** Prove that this “translation” is correct!
Now $\prod_{j=1}^{q-1} c_j(Z) = \prod_{j=1}^{q-1}(Z^{q+1} - a_j Z^q) + \text{terms of degree at most } (q+1)(q-2)+1$. Equating terms of degree greater than $(q+1)(q-2)+1$ one sees that the claim is $\prod_{j=1}^{q-1} Z^q(Z - a_j) = Z^{q^2-1}$ if and only if all $a_j = 0$, i.e. $\prod_{j=1}^{q-1}(Z - a_j) = Z^{q-1}$ if and only if all $a_j = 0$.

**Exercise 27.3.** Generalize the theorem in the following way: If $q - 1$ norm sets 
\[ \{ z \in GF(q^n) : \text{Norm}_{q^n-q}(z - a_j) = r_j \}, \] 
where $a_j \in GF(q^n)$, $r_j \in GF(q)^*$, partition the points of $GF(q^n)^* = AG(n, q) \setminus \{0\}$, then all $a_j$ must be 0.

We are going to use norm sets in Section 29.12.

### 27.1 Partial flocks of the quadratic cone in $\text{PG}(3, q)$

A flock of the quadratic cone of $\text{PG}(3, q)$ is a partition of the points of the cone different from the vertex into $q$ irreducible conics. Associated with flocks are some elation generalised quadrangles of order $(q^2, q)$, line spreads of $\text{PG}(3, q)$ and, when $q$ is even, families of ovals in $\text{PG}(2, q)$, called herds. In [109] Storme and Thas remark that this idea can be applied to partial flocks, obtaining a correspondence between partial flocks of order $k$ and $(k + 2)$-arcs of $\text{PG}(2, q)$, and constructing herds of $(k + 2)$-arcs. Using this correspondence, they can prove that, for $q > 2$ even, a partial flock of size $> q - \sqrt{q} - 1$ if $q$ is a square and $> q - \sqrt{2q}$ if $q$ is a nonsquare, is extendable to a unique flock.

Applying this last result, Storme and Thas could give new and shorter proofs of some known theorems, e.g., they can show directly that if the planes of the flock have a common point, then the flock is linear (this originally was proved by Thas relying on a theorem by D. G. Glynn on inverse planes, and is false if $q$ is odd).

Here we prove the following

**Theorem 27.4.** Assume that the planes $E_i, i = 1, ..., q - \varepsilon$ intersect the quadratic cone $C \subset \text{PG}(3, q)$ in disjoint irreducible conics. If $\varepsilon < \frac{1}{2}(1 - \frac{1}{q+1})\sqrt{q}$ then one can find additional $\varepsilon$ planes (in a unique way), which extend the set $\{E_i\}$ to a flock.

**Proof:** Let $C$ be the quadratic cone $C = \{(1, t, t^2, z) : t, z \in GF(q)\} \cup \{(0, 0, 0, 1)\}$ and $C^* = C \setminus \{(0, 0, 0, 1)\}$. Suppose that the planes $E_i$ intersect $C^*$ in disjoint conics, and $E_i$ has the equation $X_4 = a_i X_1 + b_i X_2 + c_i X_3$, for $i = 1, 2, ..., q - \varepsilon$.

Define $f_i(t) = a_i + b_i t + c_i t^2$, then $E_i \cap C^* = \{(1, t, t^2, f_i(t)) : t \in GF(q)\} \cup \{(0, 0, 1, c_i)\}$. Let $\sigma_k(T) = \sigma_k(f_i(T) : i = 1, ..., q - \varepsilon)$ denote the $i$-th elementary symmetric polynomial of the polynomials $f_i$, then $\text{deg}_T(\sigma_k) \leq 2k$. As for any fixed $T = t \in GF(q)$ the values $f_i(t)$ are all distinct, we would like to find

$$\frac{X^q - X}{\prod_i(X - f_i(t))}.$$
the roots of which are the missing values $GF(q) \setminus \{f_i(t) : i = 1, ..., q - \varepsilon\}$.

We are going to use the technique of Section 11. In order to do so, we define the elementary symmetric polynomials $\sigma_j(t)$ of the “missing elements” with the following formula:

$$X^q - X = (X^{q-\varepsilon}-\sigma_1(t)X^{q-\varepsilon-1}+\sigma_2(t)X^{q-\varepsilon-2}+... \pm \sigma_{q-\varepsilon}(t))(X^{\varepsilon}-\sigma_1^*(t)X^{\varepsilon-1}+\sigma_2^*(t)X^{\varepsilon-2}+... \pm \sigma_\varepsilon^*(t));$$

from which $\sigma_j^*(t)$ can be calculated recursively from the $\sigma_k(t)$-s, as the coefficient of $X^{\varepsilon-j}$, $j = 1, ..., q - 2$ is $0 = \sigma_j^*(t) + \sigma_{j-1}^*(t)\sigma_1(t) + ... + \sigma_1^*(t)\sigma_{j-1}(t) + \sigma_j(t)$; for example

$$\sigma_1^*(t) = -\sigma_1(t); \quad \sigma_2^*(t) = \sigma_1(t)^2 - \sigma_2(t); \quad \sigma_3^*(t) = -\sigma_1(t)^3 + 2\sigma_1(t)\sigma_2(t) - \sigma_3(t);$$

etc. Note that we do not need to use all the coefficients/equations, it is enough to do it for $j = 1, ..., \varepsilon$.

Using the same formulae, obtained from the coefficients of $X^{q-j}, j = 1, ..., \varepsilon$, one can define the polynomials

$$\sigma_1^*(T) = -\sigma_1(T); \quad \sigma_2^*(T) = \sigma_1(T)^2 - \sigma_2(T); \quad \sigma_3^*(T) = -\sigma_1(T)^3 + 2\sigma_1(T)\sigma_2(T) - \sigma_3(T);$$

up to $\sigma_\varepsilon^*$. Note that $\deg_T(\sigma_j^*) \leq 2j$. From the definition

$$(X^{q-\varepsilon}-\sigma_1(T)X^{q-\varepsilon-1}+... \pm \sigma_{q-\varepsilon}(T))(X^{\varepsilon}-\sigma_1^*(T)X^{\varepsilon-1}+\sigma_2^*(T)X^{\varepsilon-2}+... \pm \sigma_\varepsilon^*(T))$$

is a polynomial, which is $X^q - X$ for any substitution $T = t \in GF(q)$, so it is $X^q - X + (T^q - T)(...)$. Now define

$$G(X,T) = X^\varepsilon - \sigma_1^*(T)X^{\varepsilon-1} + \sigma_2^*(T)X^{\varepsilon-2} - ... \pm \sigma_\varepsilon^*(T),$$

from the recursive formulae it is a polynomial in $X$ and $T$, of total degree $\leq 2\varepsilon$ and $X$-degree $\varepsilon$.

For any $T = t \in GF(q)$ the polynomial $G(X,t)$ has $\varepsilon$ roots in $GF(q)$ (i.e. the missing elements $GF(q) \setminus \{f_i(t) : i = 1, ..., q - \varepsilon\}$), so the algebraic curve $G(X,T)$ has at least $N \geq \varepsilon q$ distinct points in $GF(q) \times GF(q)$. Suppose that $G$ has no component (defined over $GF(q)$) of degree $\leq 2$. Let’s apply the Lemma with $d = 2$ and $\alpha < \frac{1}{2}(1 - \frac{1}{q+1})$; (as $2\varepsilon \leq \alpha \sqrt{q}$) we have

$$\varepsilon q \leq N \leq 2\varepsilon(q+1)\alpha,$$

which is false, so $G = G_1G_2$, where $G_1$ is an irreducible factor over $GF(q)$ of degree at most 2. If $\deg_X G_1 = 2$ then $\deg_X G_2 = \varepsilon - 2$, which means that $G_1$ has at most $q + 1$ and $G_2$ has at most $(\varepsilon - 2)q$ distinct points in $GF(q) \times GF(q)$ (at most $\varepsilon - 2$ for each $T = t \in GF(q)$), contradiction (as $G$ has at least $\varepsilon q$).
Both $G_1$ and $G_2$, expanded by the powers of $X$, are of leading coefficient 1. So $G_1$ is of the form $G_1(X, T) = X - f_{q-\varepsilon+1}(T)$, where $f_{q-\varepsilon+1}(T) = a_{q-\varepsilon+1} + b_{q-\varepsilon+1}T + c_{q-\varepsilon+1}T^2$. Let the plane $E_{q-\varepsilon+1}$ be defined by $X_4 = a_{q-\varepsilon+1}X_1 + b_{q-\varepsilon+1}X_2 + c_{q-\varepsilon+1}X_3$.

The plane $E_{q-\varepsilon+1}$ intersects $C^*$ in $\{(1, t, t^2, f_{q-\varepsilon+1}(t)) : t \in \text{GF}(q)\} \cup \{(0, 0, 1, c_{q-\varepsilon+1})\}$. Now we prove that for any $t \in \text{GF}(q)$ the points $\{(1, t, t^2, f_{q-\varepsilon+1}(t)) : i = 1, ..., q - \varepsilon\}$ and $(1, t, t^2, f_{q-\varepsilon+1}(t))$, in other words, the values $f_1(t), ..., f_{q-\varepsilon}(t)$; $f_{q-\varepsilon+1}(t)$ are all distinct. But this is obvious from

\[
(X^{q-\varepsilon} - \sigma_1(t)X^{q-\varepsilon-1} + \sigma_2(t)X^{q-\varepsilon-2} - ... + \sigma_{q-\varepsilon}(t))(X - f_{q-\varepsilon+1}(t)) \mid X^q - X.
\]

Now one can repeat all this above and get $f_{q-\varepsilon+2}, ..., f_q$, so we have

\[
G(X, T) = \prod_{q\varepsilon+1} (X - f_i(T))
\]

and the values $f_i(t), i = 1, ..., q$ are all distinct for any $t \in \text{GF}(q)$. The only remaining case is “$t = \infty$”: we have to check whether the intersection points $E_i \cap C^*$ on the plane at infinity $X_1 = 0$, i.e. the values $c_1, ..., c_{q-\varepsilon}, c_{q-\varepsilon+1}, ..., c_q$ are all distinct (for $\Gamma$ we know it). (Note that if $q$ planes partition the affine part of $C^*$ then this might be false for the infinite part of $C^*$.) From (1), considering the leading coefficients in each defining equality, we have

\[
\sigma_1(\Gamma^*) = -\sigma_1(\Gamma); \quad \sigma_2(\Gamma^*) = \sigma_1(\Gamma)^2 - \sigma_2(\Gamma); \quad \sigma_3(\Gamma^*) = -\sigma_1(\Gamma)^3 + 2\sigma_1(\Gamma)\sigma_2(\Gamma) - \sigma_3(\Gamma);
\]

etc., so

\[
X^q - X = \left(X^{q-\varepsilon} - \sigma_1(\Gamma)X^{q-\varepsilon-1} + \sigma_2(\Gamma)X^{q-\varepsilon-2} - ... + \sigma_{q-\varepsilon}(\Gamma)\right)(X^{q-\varepsilon} - \sigma_1(\Gamma^*)X^{q-\varepsilon-1} + \sigma_2(\Gamma^*)X^{q-\varepsilon-2} - ... + \sigma_{q-\varepsilon}(\Gamma^*)),
\]

which completes the proof.

**Exercise 27.5.** Prove that if $q = p$ is a prime then in Theorem 27.4 the condition $\varepsilon < \frac{1}{2} \sqrt{q}$ can be changed for the weaker $\varepsilon < \frac{1}{4\sqrt{q}} p + 1$ (so the result is much stronger).

**Exercise 27.6.** Assume that the planes $E_i, i = 1, ..., q + \varepsilon$ intersect the quadratic cone $C \subset \text{PG}(3, q)$ in disjoint irreducible conics that cover the cone minus its vertex. If $\varepsilon < \frac{1}{4\sqrt{q} p + 1}$ then one can find $\varepsilon$ planes (in a unique way), such that if you remove the points of the irreducible conics, in which these $\varepsilon$ planes intersect $C$, from the multiset of the original cover then every point of $C$ (except the vertex) will be covered precisely once.

**Exercise 27.7.** Let $P$ be the parabola $Y = X^2$ in $\text{AG}(2, q)$. Suppose that the secant lines $Y = a_iX + b_i, \ i = 1, ..., \frac{q^2 - 3}{2}$ and the tangent $Y = a_0X + b_0 = 0$ meet $P$ in $q - 2$ distinct points. Find the formula of the missing secant $Y = \alpha X + \beta$ (i.e. express $\alpha, \beta$ with the $a_i, b_i$-s).

* * *
27. Flocks

27.2 Partial flocks of cones of higher degree

Using the method above one can prove a more general theorem on flocks of cylinders with base curve \((1, T, T^d)\). This is from [116].

**Theorem 27.8.** For \(2 \leq d \leq \sqrt[q]{q}\) consider the cone \(\{(1, t, t^d, z) : t, z \in GF(q)\} \cup \{(0, 0, 1, z) : z \in GF(q)\} \cup \{(0, 0, 0, 1)\} = C \subset PG(3, q)\) and let \(C^* = C \setminus \{(0, 0, 0, 1)\}\). Assume that the planes \(E_i, i = 1, ..., q - \varepsilon, E_i \not\in (0, 0, 0, 1)\), intersect \(C^*\) in pairwise disjoint curves. If \(\varepsilon < \left\lfloor \frac{1}{d} \sqrt[q]{q} \right\rfloor\) then one can find additional \(\varepsilon\) planes (in a unique way), which extend the set \(\{E_i\}\) to a flock, (i.e. \(q\) planes partitioning \(C^*\)).

The proof (see below) starts like in the quadratic case. Using elementary symmetric polynomials we find an algebraic curve \(G(X, Y)\), which “contains” the missing planes in some sense. The difficulties are (i) to show that \(G\) splits into \(\varepsilon\) factors, and (ii) to show that each of these factors corresponds to a missing plane. For (i) we use our Lemma 10.15. For (ii) we have to show that most of the possible terms of such a factor do not occur, which needs a linear algebra argument on a determinant with entries being elementary symmetric polynomials; this matrix may be well-known but the author could not find a reference for it.

**Proof of Theorem 27.8.** Suppose that the plane \(E_i\) has the equation \(X = a_iX_1 + b_iX_2 + c_iX_3\), for \(i = 1, 2, ..., q - \varepsilon\).

Define \(f_i(T) = a_i + b_iT + c_iT^d\), then \(E_i \cap C = \{(1, t, t^d, f_i(t)) : t \in GF(q)\} \cup \{(0, 0, 1, c_i)\}\). Let \(\sigma_k(T) = \sigma_k(\{f_i(t) : i = 1, ..., q - \varepsilon\})\) denote the \(k\)-th elementary symmetric polynomial of the polynomials \(f_i\), then \(\deg_T(\sigma_k) \leq dk\).

We proceed as in the quadratic case and so we define the polynomials

\[
\sigma_1^* = -\sigma_1(T); \quad \sigma_2^* = \sigma_1(T)^2 - \sigma_2(T); \quad \sigma_3^* = -\sigma_1(T)^3 + 2\sigma_1(T)\sigma_2(T) - \sigma_3(T); ...
\]

\((1^*)\)

up to \(\sigma_\varepsilon^*\). Note that \(\deg_T(\sigma_\varepsilon^*) \leq dj\). From the definition

\[
\left( X^{q-\varepsilon} - \sigma_1(T) X^{q-\varepsilon-1} + ... + \pm \sigma_{q-\varepsilon}(T) \right) \left( X^{\varepsilon} - \sigma_1^*(T) X^{\varepsilon-1} + \sigma_2^*(T) X^{\varepsilon-2} - ... + \pm \sigma_\varepsilon^*(T) \right)
\]

is a polynomial, which is \(X^q - X\) for any substitution \(T = t \in GF(q)\), so it is of the form \(X^q - X + (T^n - T)(...)\). Now define

\[
G(X, T) = X^{\varepsilon} - \sigma_1^*(T) X^{\varepsilon-1} + \sigma_2^*(T) X^{\varepsilon-2} - ... + \pm \sigma_\varepsilon^*(T),
\]

\((2)\)

from the recursive formulae it is a polynomial in \(X\) and \(T\), of total degree \(\leq d\varepsilon\) and \(X\)-degree \(\varepsilon\).

For any \(T = t \in GF(q)\) the polynomial \(G(X, t)\) has \(\varepsilon\) roots in \(GF(q)\) (i.e. the missing elements \(GF(q) \setminus \{f_i(t) : i = 1, ..., q - \varepsilon\}\)), so the algebraic curve \(G(X, T)\) has at least \(N \geq \varepsilon q\) distinct points in \(GF(q) \times GF(q)\). Suppose that \(G\) has no
component (defined over $\text{GF}(q)$) of degree $\leq d$. Let’s apply the Lemma with a suitable $\frac{1}{d+1} + \frac{1 + d(d - 1)\sqrt{q}}{(d+1)q} \leq \alpha < \frac{1}{d}$, $n = \deg G \leq d\varepsilon \leq \frac{1}{2}\sqrt{q} - d + \frac{3}{2}$, we have

$$\varepsilon q \leq N \leq d\varepsilon \alpha < \varepsilon q,$$

which is false, so $G = H_1G_1$, where $H_1$ is an irreducible factor over $\text{GF}(q)$ of degree at most $d$. If $\deg_X H_1 = d_X \geq 2$ then $\deg_X G_1 = \varepsilon - d_X$, which means that $H_1$ has at most $q + 1 + (d_X - 1)(d_X - 2)\sqrt{q}$ and $G_1$ has at most $(\varepsilon - d_X)q$ distinct points in $\text{GF}(q) \times \text{GF}(q)$ (at most $\varepsilon - d_X$ for each $T \in \text{GF}(q)$), so in total $G$ has

$$\varepsilon q \leq N \leq (\varepsilon - d_X + 1)q + 1 + (d_X - 1)(d_X - 2)\sqrt{q},$$

a contradiction if $2 \leq d_X \leq \sqrt{q} + 1$, so $\deg_X H_1 = 1$.

One can suppose w.l.o.g. that both $H_1$ and $G_1$, expanded by the powers of $X$, are of leading coefficient $1$. So $H_1$ is of the form $H_1(X, T) = X - f_{\varepsilon+1}(T)$, where

$$f_{\varepsilon+1}(T) = a_{\varepsilon+1} + b_{\varepsilon+1}T + c_{\varepsilon+1}T^d + \delta_{\varepsilon+1}(T),$$

where $\delta_{\varepsilon+1}(T)$ is an “error polynomial” with terms of degree between 2 and $d - 1$. At the end of the proof we will show that $\delta_{\varepsilon+1}$ and other error polynomials are zero.

Now one can repeat everything for $G_1$, which has at least $(\varepsilon - 1)q$ distinct points in $\text{GF}(q) \times \text{GF}(q)$ (as $H_1$ has exactly $q$ and $H_1G_1$ has at least $\varepsilon q$). The similar reasoning gives $G_1 = H_2 G_2$, where $H_2(X, T) = X - f_2(T)$ with $f_2(T) = a_2 + b_2T + c_2T^d + \delta_{\varepsilon+1}(T)$. Going on we get $f_q(T)$ (where for $j = q - \varepsilon + 1, \ldots, q$ we have $f_j(T) = a_j + b_jT + c_j T^d + \delta_j(T)$), where $\delta_j(T)$ contains terms of degree between 2 and $(d - 1)$ only). Hence

$$G(X, T) = \prod_{q - \varepsilon + 1}^q (X - f_i(T)).$$

For any $t \in \text{GF}(q)$ the values $f_1(t), \ldots, f_q(t)$ are all distinct, this is obvious from

$$\left(X^{q - \varepsilon} - \sigma_1(t)X^{q - \varepsilon - 1} + \sigma_2(t)X^{q - \varepsilon - 2} - \ldots \pm \sigma_{q - \varepsilon}(t)\right) \left((X - f_{\varepsilon+1}(t)) \ldots (X - f_q(t))\right) = X^q - X.$$

For $j = q - \varepsilon + 1, \ldots, q$ let the plane $E_j$ be defined by $X_4 = a_j X_1 + b_j X_2 + c_j X_3$. We are going to prove that $\{E_j : j = 1, \ldots, q\}$ is a flock.

First we check the case $t = \infty$: we have to check whether the intersection points $E_i \cap C$ on the plane at infinity $X_1 = 0$, i.e. the values $c_1, \ldots, c_{q - \varepsilon}; c_{q - \varepsilon + 1}; \ldots, c_q$ are all distinct (for $\Gamma$ we know it). (Note that even if $q$ planes partition the affine part
Our final and the last missing argument we need is that for each \( j \) on the right hand side. Hence we have a system of homogeneous linear equations that are pairwise disjoint, \( E_1, \ldots, E_q \) is a flock of \( C \).
28 Spreads and ovoids

In this section we show, very briefly, how spreads and ovoids can be handled by polynomials. The first, very basic part is from Ball [7], while the second one is based on [10].

28.1 Spreads

A 1-spread of $\text{PG}(3, q)$ is a collection of $q^2 + 1$ lines that partitions the space. Consider the representation of $\text{PG}(3, q)$ with $(q^3 + q^2 + q + 1)$-th roots of unity (i.e. $(q - 1)$-th powers) in $\text{GF}(q^4)^*$. (Hyper)planes are given by the zeros of equations of the form

$$a^{q^2+q+1} X^{q^2+q+1} + a^{q+1} X^{q+1} + a X + 1 = 0,$$

where $a$ is also a $(q^3 + q^2 + q + 1)$-th root of unity. Lines are given by the zeros of polynomials of the form

$$L_{\alpha\beta}(X) = X^{q+1} - \alpha X + \beta,$$

where $\alpha$ and $\beta$ satisfy certain conditions which we shall calculate. All the points $x$ of $\text{PG}(3, q)$ satisfy

$$x^{q^3+q^2+q+1} - 1 = 0$$

so

$$L_{\alpha\beta}(X) = X^{q+1} - \alpha X + \beta.$$

is identically zero since it is a polynomial of degree at most 1 and has $q+1$ distinct zeros corresponding to the points on the line $L_{\alpha\beta}$. By manipulating the coefficients we have that $L_{\alpha\beta}$ is a line precisely when

$$\beta^{q^2+q^2+q+1} = 1 \quad \text{and} \quad \alpha^{q+1} = \beta^q - \beta^{q^2+q+1}.$$

If $\beta^{q^2+1} = 1$ then $\alpha = 0$, if $\beta^{q^2+1} \neq 1$ then there are $q + 1$ possibilities for $\alpha$. This gives $(q^3 + q)(q + 1) + q^2 + 1 = (q^2 + 1)(q^2 + q + 1)$ lines as needed, so these restrictions are sufficient as well as necessary.

Symplectic spreads

For every point $\lambda$ of $\text{PG}(3, q)$, viewed as a $(q^3 + q^2 + q + 1)$-st root of unity in $\text{GF}(q^4)$, let

$$\omega_\lambda(X) = (-\lambda^{q^2})^{q^2+q+1} X^{q^2+q+1} + (-\lambda^{q^2})^{q+1} X^{q+1} + (-\lambda^{q^2}) X + 1$$

be a polynomial over $\text{GF}(q^4)$ whose zeros correspond to the points of a hyperplane. It is easy to verify that

$$\omega_\lambda(\varepsilon)\lambda^{q+1} = \omega_\varepsilon(\lambda)\varepsilon^{q+1} \quad \text{and} \quad \omega_\lambda(\lambda) = 0.$$
and it follows from this that $\omega$ defines a symplectic polarity on $\text{PG}(3, q)$. The planes $\omega_\lambda(X)$ and $\omega_\varepsilon(X)$ intersect in the line given by the zeros of the equation

$$X^{q+1} + \varepsilon \alpha \left( \frac{\lambda^{q+1} - \varepsilon^{q+1}}{\lambda - \varepsilon} \right) X - \frac{\varepsilon \lambda^{q+1} - \lambda \varepsilon^{q+1}}{\lambda - \varepsilon} = 0.$$ 

The line joining the points $\lambda$ and $\varepsilon$ is given by the zeros of the equation $X^{q+1} - \alpha X + \beta = 0$ where

$$\alpha = \frac{\lambda^{q+1} - \varepsilon^{q+1}}{\lambda - \varepsilon} \quad \text{and} \quad \beta = \frac{\varepsilon \lambda^{q+1} - \lambda \varepsilon^{q+1}}{\lambda - \varepsilon}.$$ 

The two lines coincide whenever $\alpha \beta = -\alpha$ and the lines for which this condition holds are the totally isotropic lines.

A symplectic 1-spread is a spread whose elements are totally isotropic lines.

### 28.2 Ovoids

**Generalised quadrangles**

A generalised quadrangle is a polar space of rank 2 and consists of points and lines which have the following properties. (Q1) Two points lie on at most one line (Q2) If $L$ is a line, and $p$ a point not on $L$, then there is a unique point of $L$ collinear with $p$. (Q3) No point is collinear with all others. The axioms (Q1)-(Q3) are self-dual; the dual of a generalised quadrangle is a generalised quadrangle. Let $Q$ be a finite generalised quadrangle. Each line is incident with $1 + s$ points and each point is incident with $1 + t$ lines, for some $s$ and $t$, and we say $Q$ is a generalised quadrangle of order $(s; t)$. If $s = t$ then $Q$ is said to have order $s$. An ovoid of a generalised quadrangle is a set of points $O$ such that each line contains exactly one point of $O$. A spread of a generalised quadrangle is a set $S$ of lines such that each point is incident with exactly one line of $S$. An ovoid $O$ and a spread $S$ of $Q$ satisfy

$$|O| = |S| = st + 1.$$ 

The set of lines dual to the ovoid $O$ form a spread in the generalised quadrangle dual to $Q$. The set of points dual to the spread $S$ form an ovoid in the generalised quadrangle dual to $Q$.

Let $q = p^h$ for some prime $p$ and integer $h$. Let $\text{Sp}(4, q)$ denote the symplectic generalised quadrangle of order $q$. The points of $\text{Sp}(4, q)$ are the points of $\text{PG}(3, q)$ and the lines are the totally isotropic lines of a symplectic polarity. Recall that a symplectic polarity is induced by an alternating bilinear form $b$. An alternating bilinear form on a vector space $V$ satisfies $b(v, v) = 0$ for all $v \in V$. This implies $b(v; w) = -b(w; v)$ for all $v, w \in V$. (Expand $b(v + w, v + w) = 0$.) Hence if the characteristic is 2 then any alternating form is symmetric.
Let $O(5, q)$ denote the generalised quadrangle of order $q$ whose points are the points of a non-singular quadric in $\text{PG}(4, q)$ and whose lines are the lines contained in that quadric. Later we will examine ovoids in $O(5, q)$. To define $O(5, q)$ one may choose the quadratic form $Q(x) = x_0x_4 + x_1x_3 + x_2^2$ on $V(5, q)$; in this case note that any ovoid containing $(0; 0; 0; 0; 1)$ may be written in the form

$$O(f) = \{(0; 0; 0; 0; 1)\} \cup \{(1, x, y, f(x, y), y^2 - x f(x, y)) : x, y \in \text{GF}(q)\}.$$  

In fact, due to the following lemma, ovoids in $O(5, q)$ are dual to spreads in $\text{Sp}(4, q)$.

**Lemma 28.1.** $O(5, q)$ is the dual of $\text{Sp}(4, q)$.

**Proof:** Let $O^*(6, q)$ be the Klein quadric of lines of $\text{PG}(3, q)$. The image of the lines of $\text{Sp}(4, q)$ is the intersection of $O^*(6, q)$ with a hyperplane $\text{PG}(4, q)$, which is $O(5, q)$. The lines of $\text{Sp}(4, q)$ incident with a given point form a pencil of lines in a plane and therefore their images on $O(5, q)$ lie on a line. \hfill $\blacksquare$

The geometry $\text{Sp}(4, q)$ in $\text{GF}(q^4)$

We recall the geometry of $\text{PG}(3, q)$ represented in $\text{GF}(q^4)$, see Section 6.1. Condition (**), that we will use, can be found there.

Let $\Gamma$ be an element of $\text{GF}(q^4)$ satisfying $\Gamma^{q^2 - 1} = -1$. Let $b$ be the alternating bilinear form defined by

$$b(X, Y) := \text{Tr}(\Gamma Y^2 X) = \Gamma Y^2 X + \Gamma Y^2 X^q - \Gamma X^2 Y^q - \Gamma Y^2 X^q$$

and note that $b(X, Y) = -b(Y, X)$. The map $y \mapsto b(X, y) = \text{Tr}(\Gamma y^2 X) = 0$ maps $y$ to its symplectic hyperplane and defines a symplectic polarity. Let $x$ and $y$ be two orthogonal elements of $\text{GF}(q^4)$, $b(x, y) = 0$, and let $L(X) = X^2 + c X^q + e X$ be the line that joins them. By elimination from the equations $L(x) = 0$ and $L(y) = 0$ we can deduce that

$$(x^q y - y^q x)c = x^q y^q - y^q x^q \quad \text{and} \quad (x^q y - y^q x)c = -(x^q y - y^q x)$$

and

$$(\Gamma c + \Gamma^2 ec^q)(x^q y - y^q x) = b(x, y) = 0.$$  

The totally isotropic lines of the polarity defined by $b(X, Y)$ have $-\gamma c = ec^q$ where $\gamma = \Gamma^1 - q$, as well as the necessary restrictions. In the case when $c = 0$ there are $q^2 + 1$ lines where each line is given by the set of zeros of an equation of the form $X^2 + e X = 0$ where $e^{q^2 + 1} = 1$. In the case when $c$ is non-zero let $d = c^{-1}$ and we find that $e = -\gamma d^{q - 1}$ and

$$\gamma d^{q - 1} q - \gamma e^{-1} d^{q - 1} + 1 = 0. \quad \text{(†)}$$

For each $d$ satisfying this equation there is a totally isotropic line which is given by the set of zeros of an equation of the form $d X^2 + X^q - \gamma d X = 0$. The points
of $\text{Sp}(4, q)$ are the points of $\text{PG}(3, q)$ and for this reason we take as before the
points to be the $(q^3 + q^2 + q + 1)$-st roots of unity (alternatively the non-zero
$(q - 1)$-st powers) in $\text{GF}(q^4)$. Therefore we replace the indeterminate $X$ by $U$ where
$U = X^{q-1}$. It now follows that the lines of $\text{Sp}(4, q)$ are given by the zeros
(all $(q^3+q^2+q+1)$-st roots of unity) of equations $U^{q+1} + e = 0$ for each $e$ satisfying
$e^{q^2+1} = 1$ and
\[ dU^{q+1} + U - \gamma d^q = 0 \] (++)
for each $d$ satisfying (+).

Remark. The geometry $\text{PG}(1, q^2)$ has as points the subspaces of rank 1 in $V(2, q^2)$. In $\text{GF}(q^4)$ they are the given by sets of zeros of equations of the form
\[ X^{q^2} + eX = 0 \]
where $e^{q^2+1} = 1$. Hence the lines defined by the sets of zeros of equations of the form $U^{q+1} + e = 0$ are skew and together they form a Desarguesian spread $R$
of $\text{Sp}(4, q)$. A Desarguesian spread is equivalent to a regular spread. The set of
points in the generalised quadrangle $O(5, q)$ dual to a regular spread of $\text{Sp}(4, q)$
is an elliptic quadric. Hence we need to prove that a spread of $\text{Sp}(4, q)$ meets the
spread $R$ in 1 modulo $p$ lines.

Remark. The equations (**) and $-\gamma c = ec^q$ imply that
\[ e^2 = \gamma^{-1} e^{q+1}(e^{q^2+1} - 1). \]
When $q$ is even we can take square roots and parameterize the lines using $(q^3+q^2+q+1)$-st roots of unity. Moreover when $q$ is even we can assume that $\gamma = 1$ since
the alternating form is also symmetric. Thus we have that the totally isotropic
lines of $\text{Sp}(4, q)$ are given by the zeros of equations of the form
\[ U^{q+1} + (e^{(q^2+q+2)/2} + e^{(q+1)/2})U + e = 0 \]
and one can check that if the point $x$ lies on the line parameterized by $e$ then $e$
lies on the line parameterized by $x^{2q}$. Hence we see that $\text{Sp}(4, q)$ is self-dual when
$q$ is even, a fact first noted by Tits in 1962.

Ovoids of $O(5, q)$

Theorem 28.2. An ovoid in $O(5, q)$ meets an elliptic quadric in 1 modulo $p$ points.

This result was proved for $q$ even by Bagchi and Sastry in 1987, who proved that
an ovoid meets not only an elliptic quadric but also a Tits ovoid in an odd number
of points.

Recall that $q = p^h$ for some prime $p$ and integer $h$. In this section we prove that
a spread of $\text{Sp}(4, q)$ has 1 modulo $p$ lines in common with the regular spread $R$.
This regular spread is entirely arbitrary.
Proof of the theorem. Let $S$ be a spread of $\text{Sp}(4,q)$ and let the sets $D$ and $E$ be such that for $d \in D$ the line
\[ dU^{q+1} + U - \gamma d^q = 0 \]
is in $S$ and for $e \in E$ the line $U^{q+1} + e = 0$ is in $S$. Clearly $|D| + |E| = q^2 + 1$. The aim will be to show that $|D| = 0$ modulo $p$ and then the result will follow.

The bilinear form $b(X,Y)$ can be rewritten for the points of $\text{PG}(3,q)$ by replacing $X$ by $U$ and $Y$ by $V$. Hence for a fixed point $u$ in $\text{PG}(3,q)$ the zeros of the polynomial
\[ (u,V) := \gamma u^{q+1} - \gamma V^{q+1} + u^{q^2+q+1}V - uV^{q^2+q+1} \]
are the points that are orthogonal to $u$, i.e. lie on the symplectic hyperplane through $u$. Let $v$ be the point of $\text{Sp}(4,q)$ (i.e. $\text{PG}(3,q)$) that is the intersection of the line of $\text{Sp}(4,q)$ of the form
\[ dV^{q+1} + V - \gamma d^q = 0 \]
with the plane $(u,V) = 0$, assuming that the line is not contained in the plane. We can calculate directly or check by substitution that
\[ v^q = -u(du^{q+1} + u - \gamma d^q)^{q-1}. \]

Similarly, if $v$ is the point of intersection of the line of $\text{Sp}(4,q)$ of the form $V^{q+1} + e = 0$ with the plane $(u,V) = 0$ then
\[ v^q = \gamma^{-1}ue(u^{q+1} + e)^{q-1}. \]

The coefficient of $V^{q^2+q}$ in $(u,V)$ is minus the sum of all the points in the plane $(u,V) = 0$ and is zero. Likewise the sum of all the points on any line is minus the coefficient of $V^q$ in the equation of this line which is also zero. Hence the sum of all points lying in an affine plane is also zero. Thus the sum of all the points of intersection of the spread $S$ with the plane $(u,V) = 0$ is zero and we have
\[ 0 = \sum v = \sum v^q = -\sum_{d \in D} u(du^{q+1} + u - \gamma d^q)^{q-1} + \sum_{e \in E} \gamma^{-1}ue(u^{q+1} + e)^{q-1}. \]

Note that of course one of the lines of the spread contains the point $u$ and the term in the sum corresponding to this line will be zero. The polynomial
\[ \sum_{d \in D} U(dU^{q+1} + U - \gamma d^q)^{q-1} - \sum_{e \in E} \gamma^{-1}Ue(U^{q+1} + e)^{q-1} \]
is zero for all points of $\text{PG}(3,q)$ and since it’s degree is only $q^2$ it is identically zero. However the coefficient of $U^q$ is $|D|$ and hence $|D| = 0$ modulo $p$. \qed
29. Non-geometrical applications

There is an extensive number of applications of polynomials throughout mathematics, here I show some which are close to my combinatorial-algebraic taste. E.g. the (unfortunately still unpublished) book of Babai and Frankl [4] contains a chapter devoted to spaces of polynomials. I learned some of the following applications from Tamás Szőnyi’s paper [127], some others from Alon’s paper [1]. I am also grateful for the advice of Gy. Károlyi.

29.1 Normal factorizations of Abelian groups

Let $G = \mathbb{Z}_p \times \mathbb{Z}_p$ (we are going to use the additive notation) and suppose that $G = A + B$ with $A, B \subseteq G$, $(0, 0) \in A, B$ and for each $g \in G$ there is a unique way to write it as $g = a + b, a \in A, b \in B$. Then we say that $G = A + B$ is a normal factorization of $G$.

Theorem 29.1. In every normal factorization of $G = \mathbb{Z}_p \times \mathbb{Z}_p$, either $A$ or $B$ is a subgroup.

Proof: [91] One can identify $G$ and $AG(2, p)$ in the obvious way; then the subgroups of order $p$ correspond to lines through the origin. The key idea is to show that no direction is determined by both $A$ and $B$.

Suppose to the contrary that some direction (suppose without loss of generality that the horizontal direction, i.e. $(0)$) is determined by both $A$ and $B$. Let $\alpha(g)$ be the first coordinate of $g \in G$, and $\omega$ a primitive $p$-th root of unity. Then

$$
\left( \sum_{a \in A} \omega^{\alpha(a)} \right) \left( \sum_{b \in B} \omega^{\alpha(b)} \right) = \sum_{a \in A, b \in B} \omega^{\alpha(a+b)} = p \sum_{i=0}^{p-1} \omega^i = 0,
$$

as each element of $G$ occurs precisely once in the form $a + b$. So one of the two factors of the product above must be zero, suppose this is the first one (corresponding to $A$). It means that the set of numbers $\{\alpha(a) : a \in A\}$ contain all the residues modulo $p$, hence $A$ does not determine the horizontal direction. In general it means that for any direction $(m)$, at least one of $A$ and $B$ does not determine $(m)$. So either $A$ or $B$ determines at most $\frac{p+1}{2}$ directions, hence, by Theorem 18.1, it is a line. As they contain the origin, that line is a subgroup.

The “stability version” of this result is the following: let $G = \mathbb{Z}_p \times \mathbb{Z}_p$ and $A, B \subseteq G$, $(0, 0) \in A, B$, $|A| > p - \varepsilon, |B| > p - \varepsilon$, where $\varepsilon \leq cp$ for a small constant $c$. Suppose that if for some $g \in G, g = a_1 + b_1 = a_2 + b_2, a_i \in A, b_i \in B$ then $a_1 = a_2$ and $b_1 = b_2$. (We may say that $A + B \subseteq G$ is a partial normal factorization of $G$.)
Exercise 29.2. In every partial normal factorization of $G = \mathbb{Z}_p \times \mathbb{Z}_p$, either $A$ or $B$ can be extended to a subgroup of order $p$, if $\varepsilon \leq \ldots$ (determine!).

Exercise 29.3. (Rédéi) Let $G = \mathbb{Z}_p \times \mathbb{Z}_p$ and let $A \subset G$, $|A| = p$. Assume that $A$ is not a subgroup. Then there are at most $\frac{p-1}{2}$ subsets $B$ for which $|B| = p$, $0 \in B$ and $G = A + B$ holds.

Note that the factorizations of Abelian groups has a rather complicated theory; neither this statement above can be extended to groups of order $p^n$, $n > 2$.

A motivating problem for Lovász and Schrijver [91] was the following application.

It was conjectured by van Lint (and proved in the prime case by van Lint and Williams) that if $X \subset GF(q^2)$, $0, 1 \in X$, $|X| = q$ and the difference of any two elements of $X$ is a square element of $GF(q^2)$, then $X = GF(q)$.

Exercise 29.4. Prove this conjecture in the case $q = p$ prime, using the representation $AG(2, p) \sim GF(p^2)$ and Theorem 18.1.

The conjecture for general $q$ was proved by Blokhuis [29] with polynomials. His proof and his method was generalized for the analogous statement concerning $d$-th powers instead of squares of $GF(q^2)$ in [113]:

Theorem 29.5. If $1 < d \mid (q + 1)$, $X \subset GF(q^2)$, $0, 1 \in X$, $|X| = q$ and the difference of any two elements of $X$ is always a $d$-th power of $GF(q^2)$, then $X = GF(q)$.

Exercise 29.6. Prove either of these results using Theorem 18.14.

Again, the $q$-subsets of $GF(q^2)$ above (or the $q$-cliques of the Paley graph $P_{q^2, d}$, see below) are quite “stable”:

Exercise 29.7. [113] If $1 < d \mid (q + 1)$, $X \subset GF(q^2)$, $0, 1 \in X$, $|X| = q - \varepsilon$, where $\varepsilon < \left(1 - \frac{1}{3}\right)\sqrt{q}$. Suppose that the difference of any two elements of $X$ is always a $d$-th power of $GF(q^2)$, then $X \subseteq GF(q) \subset GF(q^2)$.

29.2 The Paley graph

The Paley graph $P_q$ has $GF(q)$ as vertex set, and $(a, b)$ is an edge if and only if $b - a$ is a square element of $GF(q)$. It is undirected iff $1$ is a square, i.e. $q = 4k + 1$.

Let’s examine the automorphisms of $P_q$. Note that the maps $x \mapsto a^2x + b$, $a, b \in GF(q)$, $a \neq 0$ are always automorphisms.

Let $f : GF(q) \rightarrow GF(q)$ be an automorphism and consider the difference quotients $\frac{f(y) - f(x)}{y - x}$. If $(x, y)$ was an edge then both the denominator and the numerator are squares, while if $(x, y)$ was not an edge then both the denominator and the
numerator are nonsquares; in both cases the difference quotient, i.e. the direction determined by \((x, f(x))\) and \((y, f(y))\) is a square. In fact we have proved that \(f\) is an automorphism if and only if \(f\) is bijective and the directions it determines are all squares in \(GF(q)\).

Hence \(f\) determines at most \(q^2 - 1\) directions and Theorems 18.1 and 18.14 can be applied.

So for example if \(q = p\) we immediately have that \(f\) is linear, so of form \(x \mapsto a^2x + b\). The non-prime case is more difficult.

Exercise 29.8. Prove that the automorphism group of the Paley graph \(P_{q^2}\) \((q = p^h)\) is \(\{f(X) = a^2X^{p^j} + b : a \in GF(q)^*, b \in GF(q), j = 0, ..., h - 1\}\)

Exercise 29.9. Prove that the Paley graph \(P_{q^2}\) has clique number \(\omega(P_{q^2}) = q\).

Exercise 29.10. Generalize the notion of Paley graph, using \(d\)-th powers instead of squares.

Exercise 29.11. Formulate Theorem 29.5 in the language of Paley graphs.

29.3 Representing systems

Another application in Rédei’s book [103] (Section 37) is about common representing systems of subgroups. Let \(G\) be a group, \(H\) a subgroup of it, then \(R \subset G\) is a representing system of \(H\) if \(R\) intersects each coset of \(H\) in precisely one element.

Let \(G = \mathbb{Z}_p \times \mathbb{Z}_p\) again, and let \(H_1, ..., H_k\) be its subgroups of order \(p\). We want to find a common representing system \(R\), so for which \((0, 0) \in R\) (it can be achieved w.l.o.g.), \(|R| = p\) (this is obvious) and \(R + H_i = G\) (by definition). Note that any further subgroup (different from \(H_1, ..., H_k\)) will do, so we require that \(R\) is not a subgroup. In the usual representation (as above), every \(H_i\) is a line through the origin; and \(R\) is a representing system for \(H_i\) if \(\forall r_1 \neq r_2 \in R \ (r_1 - r_2) \notin H_i\), in other words when the directions determined by \(R\) are different from the slopes of the given lines \(H_i\). Hence, by 18.1, there is no such common representing system if \(k > \frac{p^2 - 1}{2}\), and if \(k = \frac{p^2 - 1}{2}\) then \(R\) can be described:

Theorem 29.12. Suppose that the subgroups \(H_1, ..., H_k \leq G = \mathbb{Z}_p \times \mathbb{Z}_p\) have a common representing system \(R\), \((0, 0) \in R\), which is not a subgroup. Then \(k \leq \frac{p^2 - 1}{2}\), and if \(k = \frac{p^2 - 1}{2}\) then, after a suitable change of the two factors \(\mathbb{Z}_p\), \(R\) is the set described in Theorem 19.1, and the subgroups \(H_i\) are lines of form \(\{(x, mx) : x \in GF(p)\}\), where each \((m)\) is a direction not determined by \(R\).

Note that it does not mean that for any set of \((\frac{p^2 - 1}{2} \text{ or less})\) subgroups there is a common representing system.
29.4 Wielandt’s visibility theorem

The following theorem was proved first by Wielandt using very complicated methods; later Blokhuis and Seidel [38] has pointed out that it was an easy consequence of Rédei’s theorem.

**Theorem 29.13.** (Wielandt) Let $G$ be a permutation group acting on the points of $\text{AG}(2,p)$, $p$ prime, containing all the translations. Let $G_0$ denote the stabilizer of the origin. Let $S$ be the set of $k$ lines through the origin, $1 \leq k \leq \frac{p-1}{2}$. If $G_0$ maps the union of the lines in $S$, as a pointset, onto itself, then any $g \in G_0$ maps the lines of $S$ to lines (of $S$).

**Proof:** [38] Let $g \in G_0$ and let’s denote by $\tau(v)$ the translation by the vector $v \in \text{GF}(p) \times \text{GF}(p)$; ($g$ is also a map $\text{GF}(p)^2 \rightarrow \text{GF}(p)^2$). Let $x$ and $y$ be points on a line $\ell$ of $S$. The vector $(x - y)$ shows the slope of $\ell$. Translate the point $(x - y)$ by $y$, then let $g$ act on it, finally translate it by $-g(y)$: we get

$$
\left(\tau(-g(y)) \ g \tau(y)\right)(x-y) = \left(\tau(-g(y)) \ g\right)(x) = \left(\tau(-g(y))\right)(g(x)) = g(x) - g(y).
$$

Note that the two translations do not change the directions, and $g$ turned the direction of $x - y$ to the direction of a(nother) line of $S$.

It means that for any line $\ell$ in $S$, the direction determined by any two points on $g(\ell)$, coincides with the slope of one of the lines in $S$. Hence $g(\ell)$ determines at most $\frac{p-1}{2}$ directions, so by Theorem 18.1 it is a line.

Note that the permutations of $G$ do not necessarily preserve the lines. Naturally, as $G = G_0T$ (where $T$ is the group of translations), all the elements of $G$ map the lines in $S$ into lines. To make the theorem above (which sounds somewhat peculiar) more “motivated”, we remark that the translations form a regular, but (in general) not normal subgroup $T$ of order $p^2$, and the lines through the origin are subgroups of $T$, each of order $p$.

29.5 Burnside’s theorem

Dress, Klin and Muzichuk [60] and, independently, Ott [96] has realized that a famous theorem of Burnside can be proved in an elementary way, using Rédei’s result (in fact the prime case was re-proved independently by Muzichuk and also by others a few times). Here, for historical reason, we just quote the theorem, without proof, for the details see [60].

**Theorem 29.14.** (Burnside) Let $G$ be a transitive permutation group of degree $p$ ($p$ prime). Then either $G$ is doubly transitive or it is isomorphic to a subgroup of the affine transformation group $\{x \mapsto ax + b : a, b \in \text{GF}(p), a \neq 0\}$. 

29. Non-geometrical applications

We also mention an application of Blokhuis’ Theorem 21.4, given by Á. Bereczky. His result is about the existence of fixed-point free $p$-elements of a permutation group (a $p$-element is a permutation whose order is a power of $p$).

**Theorem 29.15.** (Á. Bereczky [25]) Let $p$ be an odd prime, $a \geq 1$. If $p + 1 \leq b < \frac{3}{2}(p + 1)$ then every transitive permutation group of degree $p^a b$ contains a fixed-point free $p$-element.

29.6 Jaeger’s conjecture

In [2] Alon and Tarsi use Rédei polynomials to prove Jaeger’s conjecture for $q$ non prime. Jaeger’s conjecture states that when $q \geq 5$, for all matrices $M \in \text{GL}(n, q)$ there exists a vector $y \in \text{GF}(q)^n$ with the property that neither $y$ nor $M y$ have any zero coordinate. (Jaeger conjectured this for $q = 5$ only.)

This problem can be formulated in many equivalent ways:

- the points of the vectorspace $V(n, q)$ cannot be covered by two sets of $n$ independent linear hyperplanes;
- given two bases of $V(n, q)$, $\{v_i : i = 1, ..., n\}$ and $\{w_i : i = 1, ..., n\}$ then there exists a vector $u \in V(n, q)$, $u = \sum \alpha_i v_i = \sum \beta_i w_i$, with each $\alpha_i, \beta_j$ being nonzero coordinates;
- $\text{PG}(n - 1, q)$ cannot be covered by (the union of the faces of) two simplices.

Note that for $q = 2$ the matrix $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, while for $q = 3$ the matrix $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ are counterexamples. Also if the conjecture is false for some $(q, n_0)$ then it is false for any $(q, n), n \geq n_0$.

Let us see how Rédei polynomials can be used to tackle this problem. If the conjecture is not true then there is a matrix $M \in \text{GL}(n, q)$ with the property that $M y$ has a zero component, for all $y \in \text{GF}(q)^n$ with no zero component. The set of $n$ points $A$ that is made up of the rows of $M$ that spans the whole space and has the property that the hyperplane $y_1 X_1 + y_2 X_2 + ... + y_n X_n = 0$ is incident with a point of $A$ for all $y \in \text{GF}(q)^n$ with no zero component. In other words, if we define a Rédei polynomial

$$R(Y_1, Y_2, ..., Y_n) := \prod_{(x_1, x_2, ..., x_n) \in A} (x_1 Y_1 + x_2 Y_2 + ... + x_n Y_n)$$

then for all vectors $y$ which have no zero component $R(y_1, y_2, ..., y_n) = 0$. This algebraic property of $R$ implies that we can write

$$R(Y_1, Y_2, ..., Y_n) = (Y_1^{q-1} - 1)f_1 + (Y_2^{q-1} - 1)f_2 + ... + (Y_n^{q-1} - 1)f_n, \quad (*)$$
where \( f_1, f_2, \ldots, f_n \in \text{GF}(q)[Y_1, Y_2, \ldots, Y_n] \) are polynomials of degree at most \( n - (q - 1) \). The matrix \( M \) is non-singular and so has an inverse \( M^{-1} = (a_{ij}) \). If we make the substitution \( Y_i = \sum_{j=1}^{n} a_{ij} Z_j \) we have

\[
Z_1 Z_2 \ldots Z_n = \sum_{i=1}^{n} \left( \left( \sum_{j=1}^{n} a_{ij} Z_j \right)^{q-1} - 1 \right) f_i.
\]

Now on the right-hand side when we try to find a term \( Z_{j_1} Z_{j_2} \ldots Z_{j_{q-1}} \) from one of the \( \left( \sum a_{ij} Z_j \right)^{q-1} \) terms, as we must since the left-hand side is \( Z_1 Z_2 \ldots Z_n \), the coefficient is a multiple of \( (q - 1)! \). If \( q \) is not prime then this is always zero and we have a contradiction.

We can explore this situation a little bit. First note that if \( q \) is a prime we have

\[
Z_1 Z_2 \ldots Z_n = -\sum_{i=1}^{n} \left( \sum_{j<i} a_{ij} a_{ij2} \ldots a_{ijq-1} Z_{j1} Z_{j2} \ldots Z_{j_{q-1}} \right) f_i = -\sum_{j<i} Z_{j1} Z_{j2} \ldots Z_{j_{q-1}} \sum_{i=1}^{n} \left( a_{ij} a_{ij2} \ldots a_{ijq-1} \right) f_i.
\]

A typical term of \( f_i \) is

\[
Y_{i_1} Y_{i_2} \ldots Y_{i_{n-q+1}} = \left( \sum_{j=1}^{n} a_{i1j} Z_j \right) \left( \sum_{j=1}^{n} a_{i2j} Z_j \right) \ldots \left( \sum_{j=1}^{n} a_{i_{n-q+1}j} Z_j \right).
\]

where \( i_1, \ldots, i_{n-q+1} \) are not necessarily pairwise distinct. What is the coefficient of \( Z_1 Z_2 \cdot Z_{n-q+1} \) for instance on the right hand side? It is

\[
\sum_{\pi \in \text{Sym}(1,2, \ldots, n-q+1)} a_{i_1 \pi(1)} a_{i_2 \pi(2)} \ldots a_{i_{n-q+1} \pi(n-q+1)}.
\]

Let’s examine the Rédei polynomial of the counterexamples in the \( q = 2 \) and \( q = 3 \) cases above! They are

\[
R(Y_1, Y_2) = (Y_1 + Y_2) Y_1 = (Y_1^2 - 1) Y_1 + (Y_2^2 - 1) Y_1 = Y_1^3 \cdot Y_1 + Y_1^2 \cdot Y_1
\]

and

\[
R(Y_1, Y_2) = (Y_1 + Y_2) (Y_1 - Y_2) = (Y_1^2 - 1) 1 + (Y_2^2 - 1) (-1) = Y_1^2 \cdot 1 + Y_2^2 \cdot (-1).
\]

In (*) consider the terms of degree \( \leq n-q+1 \). They are \( f_1 + f_2 + \ldots + f_n \), hence \( f_1 + f_2 + \ldots + f_n \equiv 0 \) and \( R(Y_1, Y_2, \ldots, Y_n) = Y_1^{q-1} f_1 + Y_2^{q-1} f_2 + \ldots + Y_n^{q-1} f_n \), (***)
where \( f_1, \ldots, f_n \) are homogeneous polynomials of degree \( n - q + 1 \). We claim that if \((y_1, \ldots, y_n)\) is a zero-free point which is orthogonal to at least two rows of the matrix \( M \) then \( f_j(y_1, \ldots, y_n) = 0 \) for each \( j = 1, \ldots, n \). Let e.g. \( j = 1 \) and consider \( \hat{R}(Y_1) = R(Y_1, y_2, \ldots, y_n) = (Y_1^{q-1} - 1)f_1(Y_1, y_2, \ldots, y_n) \). Since \( \hat{R} \) splits into linear factors, so does \( f_1(Y_1, y_2, \ldots, y_n) \) as well; and as \( Y_1 = y_1 \) is a multiple root of \( \hat{R} \), it is a root of \( f_1(Y_1, y_2, \ldots, y_n) \) (with multiplicity decreased by one). Consequently each \( f_i \) vanishes on the same set of points \( S \subseteq (\mathbb{GF}(q))^n \).

29.7 Graphs containing \( p \)-regular subgraphs

Theorem 29.16. Alon-Friedland-Kalai [1] For any prime \( p \), any loopless graph \( G(V, E) \) with average degree bigger than \( 2p - 2 \) and maximum degree at most \( 2p - 1 \) contains a \( p \)-regular subgraph.

The most interesting case is \( p = 3 \), see [1] for the details.

Proof: Let \((a_{v,e})_{v \in V, e \in E}\) be the incidence matrix of \( G \), i.e. \( a_{v,e} = 1 \) or \( 0 \) as \( v \in e \) or not. Associate a variable \( X_e \) to each edge \( e \), and define the polynomial

\[
F = \prod_{v \in V} \left( 1 - \left( \sum_{e \in E} a_{v,e} X_e \right)^p \right) - \prod_{e \in E} (1 - X_e)
\]

over \( \mathbb{GF}(p) \). \( \deg F = |E| \) as \( (p - 1)|V| < |E| \) by assumption. The coefficient of \( \prod_{e \in E} X_e \) is \( (-1)^{|E|+1} \neq 0 \). Hence, by Theorem 5.17, there is a vector \( x \) with coordinates \( x_e \in \{0, 1\} \) such that \( F(x_e : e \in E) \neq 0 \). This \( x \) is not the zero vector as \( F(0) = 0 \). Also for each \( v \in V \), \( \sum_{e \in E} a_{v,e} x_e = 0 \mod p \) since otherwise \( F \) would vanish at \( x \). So in the subgraph consisting of the edges with \( x_e = 1 \) every degree is precisely \( p \) (as the maximum degree is \( \leq 2p - 1 \)).

29.8 Blokhuis’ proof of Bollobás’ theorem

Theorem 29.17. Let \( A_1, \ldots, A_h \) and \( B_1, \ldots, B_h \) be collections of sets with \( \forall i : |A_i| = r, |B_i| = s \) and \( A_i \cap B_j = \emptyset \) if and only if \( i = j \). Then \( h \leq \binom{r+s}{s} \).

Proof: [30] W.l.o.g. we can assume that every set is a subset of \( \mathbb{R} \). Define the polynomials

\[
a_i(X) = \prod_{\alpha \in A_i} (X - \alpha), \quad i = 1, \ldots, h; \quad b_j(X) = \prod_{\beta \in B_j} (X - \beta), \quad j = 1, \ldots, h.
\]

By the properties of resultants, see Section 9.5, and the conditions on the sets \( A_i \) and \( B_j \), we get that \( R(a_i, b_j) \neq 0 \) if and only if \( i = j \). Let \( c(X) = c_s X^s + \ldots + c_1 X + c_0 \)
be an arbitrary polynomial of degree $s$, then for a fixed $i$ we have that $R(a_i, c)$ is a homogeneous polynomial of degree $s$ in the coefficients (considered as variables) $c_0, ..., c_s$ of $c$. We claim that the polynomials $R(a_i, c), i = 1, ..., h$ are independent in the $(r+s^+)$-dimensional vectorspace of homogeneous polynomials of degree $r$ in the variables $c_0, ..., c_s$ (and hence $h \leq (r+s^+)h$). To prove this independence, suppose that $\sum_i \lambda_i R(a_i, c) = 0$. Then substituting $b_j$ for the polynomial $c$ we get $\lambda_j = 0$.

29.9 Alon-F{"u}redi

**Theorem 29.18.** Let $\mathbb{F}$ be a field. Suppose that in $\mathbb{F}^d$ the union of the hyperplanes $H_i, i = 1, ..., m$ cover the vertices of the hypercube $\{0, 1\}^d$ except the origin. Then $m \geq d$.

**Proof:** Let the equation of $H_i$ be $\sum_{j=1}^d a_{ij} X_j - 1 = 0$. Then

$$F(X_1, ..., X_d) = \prod_{i=1}^m \left( \sum_{j=1}^d a_{ij} X_j - 1 \right)$$

vanishes in every $x = (x_1, ..., x_d), x_j \in \{0, 1\}, x \neq (0, 0, ..., 0)$, but $F(0, 0, ..., 0) \neq 0$. Now

$$G(X_1, ..., X_d) = \prod_{i=1}^m \left( \sum_{j=1}^d a_{ij} X_j - 1 \right) - (-1)^{d+m} \prod_{j=1}^d (X_j - 1)$$

vanishes on $\{0, 1\}^d$. Theorem 5.17 states that if $X_1 X_2 \cdots X_d$ is a leading term then $G$ cannot vanish on a set of form $S_1 \times S_2 \times ... \times S_d$, with each $|S_i| > 1$. Hence $X_1 X_2 \cdots X_d$ is not a leading term and $m \geq d$.

Note that in case of the equality $m = d$ the coefficient of $X_1 X_2 \cdots X_d$ must be zero in

$$G(X_1, ..., X_d) = \prod_{i=1}^d \left( \sum_{j=1}^d a_{ij} X_j - 1 \right) - \prod_{j=1}^d (X_j - 1)$$

hence $\text{Per}(a_{ij}) = 1$.

29.10 Chevalley-Warning

This theorem of Chevalley and Warning holds for any finite field; for simplicity we prove it over $\mathbb{GF}(p)$ only.

**Theorem 29.19.** Let $f_1, ..., f_m$ be polynomials from $\mathbb{GF}(p)[X_1, ..., X_n]$. If $n > \sum_{i=1}^m \deg(f_i)$ and the polynomials have a common zero $c = (c_1, ..., c_n)$ then they have another common zero.
Proof: Suppose that the statement is false and define

\[ f(X_1, \ldots, X_n) = \prod_{i=1}^{m} \left( (1 - f_i(X_1, \ldots, X_n))^p - 1 \right) - \delta \prod_{j=1}^{n} \prod_{\alpha \in \text{GF}(p) \setminus \{c_j\}} (X_j - \alpha), \]

where \( \delta \neq 0 \) is chosen such that \( f(c) = 0 \).

Observe that \( f(x) = 0 \) for any \( x \in \text{GF}(p)^n \). It holds for \( x = c \); by assumption there exists some \( f_j \) for which \( f_j(x) \neq 0 \) hence \( 1 - f_j(x)^p = 0 \). Similarly, as for some \( i \), \( x_i \neq c_i \), so we have \( \prod_{\alpha \in \text{GF}(p) \setminus \{c_j\}} (X_i - \alpha) = 0 \) and then \( f(x) = 0 \).

Let \( t_i = p - 1 \) for \( i = 1, \ldots, n \); then the coefficient of \( \prod_{i=1}^{n} X_i^{t_i} \) in \( f \) is \( -\delta \neq 0 \). Hence by Theorem 5.17 with \( S_i = \text{GF}(p) \) for all \( i \), we have that there exists an \( s \in \text{GF}(p)^n \) for which \( f(s) \neq 0 \), a contradiction.

A Chevalley-Warning type application of the punctured Nullstellensatz

This nice result of Ball-Serra [22] can be now posed as an exercise.

Exercise 29.20. Let \( f_1, f_2, \ldots, f_m \) be polynomials of \( \text{GF}(q)[X_1, X_2, \ldots, X_n] \) and let \( d = |D_1| + \ldots + |D_m| \), where \( D_i \) is the set of elements \( c \) of \( \text{GF}(q) \) where there exists a common zero of \( f_1, f_2, \ldots, f_m \) with \( i \)-th coordinate \( c \). If \( d \neq 0 \), in other words if the polynomials \( f_1, f_2, \ldots, f_m \) have a common zero, then

\[ \sum_{i=1}^{m} \deg(f_i) \geq \frac{nq - d}{q - 1}. \]

29.11 Cauchy-Davenport

Theorem 29.21. Let \( A, B \subseteq (\mathbb{Z}_p, +) \) be two subsets of size \( |A| = k, |B| = l \). Then \( |A + B| \geq \min\{k + l - 1, p\} \).

Proof: Let \( \mathbb{Z}_p = (\text{GF}(p), +) \). If \( k + l > p \) then everything is obvious: for any \( g \in G \) the sets \( A \) and \( g - B \) will intersect, so \( g \in A + B \). Suppose that \( |A + B| \leq k + l - 2 \) and choose \( C \subseteq G \) such that \( A + B \subseteq C \) and \( |C| = k + l - 2 \). Define \( F(X, Y) = \prod_{c \in C} (X + Y - c) \), it vanishes on \( A \times B \). Here \( \deg F = (k - 1) + (l - 1) \) and the coefficient of \( X^{k-1}Y^{l-1} \) is \( \binom{k+l-2}{k-1} \neq 0 \) (as \( k + l - 2 < k + l - 1 \leq p \)). It contradicts Theorem 5.17.

The very similar proof of the Eliahou-Kervaire-Bollobás-Leader theorem is
**Exercise 29.22.** Alon [1] Let $\beta_p(r, s)$ denote the smallest $n$ for which the triple $(r, s, n)$ satisfies the Hopf-Stiefel condition, i.e. $\binom{n}{k} \equiv 0 \pmod{p}$ for every $n - r < k < s$.

If $A$ and $B$ are nonempty subsets of the vectorspace $V(d, p)$, $|A| = r, |B| = s$, then $|A + B| \geq \beta_p(r, s)$.

Dias da Silva and Hamidoune proved that for $A \subset \mathbb{Z}_p$, $|A| = k$, $p$ a prime, $|A + A| = |\{a_1 + a_2 : a_1 \neq a_2 \in A\}| \geq \min\{2|A| - 3, p\}$, settling a problem of Erdős and Heilbronn. The proof below contains a slight simplification by Károlyi.

Suppose to the contrary that a set $GF(p) \supset C \supseteq A + A$, with $|C| = 2k - 4$. Consider

$$f(X, Y) = (X - Y)^2 \prod_{c \in C} (X + Y - c) = (X - Y)^2(X + Y)^{2k - 4} + \text{terms of lower degree.}$$

Then $f(a_1, a_2) = 0$ for all $a_1, a_2 \in A$. $\deg f = 2k - 2$, the coefficient of $X^{k-1}Y^{k-1}$ is $(2k-4) - 2(2k-4) + \binom{2k-4}{k-1} = \frac{-2(2k-4)!}{(k-1)!(k-1)!}$, which is nonzero if $0 < 2k - 4 < p$ (otherwise we are done). Thus, by Theorem 5.17 we can find $a_1, a_2 \in A$ such that $f(a_1, a_2) = 0$, contradiction. 

### 29.12 Another application

Let $H$ be a fixed graph. The classical problem from which extremal graph theory has originated is to determine the maximum number of edges a graph on $n$ vertices can have without containing a copy of $H$. This maximum value is the Turán number of $H$ and is customarily denoted by $\text{ex}(n, H)$.

It is particularly interesting to determine the Turán numbers when $H$ is bipartite, as in most cases even the order of magnitude is open. The Zarankiewicz problem concerns the complete bipartite graph, so $\text{ex}(n, K_{t,s})$, where $t \leq s$.

Kővári, T. Sós and Turán gave the upper bound for arbitrary fixed $t$:

$$\text{ex}(n, K_{t,s}) \leq c_{t,s}n^{2 - \frac{t}{s}},$$

where $c_{t,s} > 0$ is a constant depending on $t$ and $s$. The right hand side is conjectured to give the correct order of magnitude. However the best general lower bound, obtained by the probabilistic method, is

$$c'n^{2 - \frac{s+t-2}{st-1}} \leq \text{ex}(n, K_{t,s}),$$

where $c' > 0$ is an absolute constant, but for all $2 \leq t \leq s \frac{s+t-2}{st-1} > \frac{1}{t}$ holds; so the lower bound is always of lower order of magnitude.

The optimality of the upper bound (up to a constant factor) is proved for $t = 2, 3$ and all $s \geq t$. The incidence graphs of projective planes demonstrate this order of
magnitude for \( t = 2 \). In this case, however, even the asymptotic order of magnitude is known: \( \text{ex}(n, K_{2,s}) = \frac{\sqrt{3} - 1}{2} n^{3/2} + O(n^{4/3}) \) (Füredi [65]).

The optimality for \( t = 3 \) was established by Brown [50]. Later Füredi proved that Brown’s construction is asymptotically optimal: \( \text{ex}(n, K_{3,3}) = \Theta(n^{5/3}) \).

The construction of Brown is the following “unit distance graph” in a 3-dimensional affine space: the vertices of our graph will be the points of \( AG(3, q) \). Let \( k_1, k_2 \) be such that \( E : X^2 + k_1 Y^2 + k_2 Z^2 = 1 \) is an elliptic quadric in \( AG(3, q) \). Then the vertices \((x, y, z)\) and \((u, v, w)\) are connected by an edge iff \((x - u)^2 + k_1(y - v)^2 + k_2(z - w)^2 = 1\).

**Proposition 29.23.** This graph has \( \approx n^{5/3} \) edges and does not contain a \( K_{3,3} \).

**Proof:** \( E \) intersects the ideal plane in the conic \( X^2 + k_1 Y^2 + k_2 Z^2 = 0 \), so it has \( q^2 + 1 - (q + 1) = q^2 - q \) affine points and the same is true for all its translates. The neighbours of the vertex are on a translate of \( E \), so the number of edges is \( \frac{1}{2} q^3(q^2 - q) \approx (q^3)^{5/3} \).

Let \( U(u_1, u_2, u_3), V(v_1, v_2, v_3) \) and \( W(w_1, w_2, w_3) \) be three points and \( E_U, E_V, E_W \) the corresponding quadrics, i.e. the (equations of the) neighbours of \( U, V \) and \( W \) resp., so \((X - u_1)^2 + \ldots = 1\), \((X - v_1)^2 + \ldots = 1\) and \((X - w_1)^2 + \ldots = 1\). Subtract the first one from the second and the third, we get two linear equations which do not coincide, so they define either a line or an empty set. As \( E_U \) does not contain a line, this line (if exists), intersects it in at most two points, so \( U, V \) and \( W \) has at most 2 common neighbours.

The idea of this construction is that we define a “surface” “around” each point of the space, such that (i) they are translates of each other (so it is easy to handle them); (ii) they have “many” points (so the graph will contain many edges); and (iii) any three translates intersect in a bounded number of points (so any triple of vertices has a bounded number of common neighbours). The next result, due to Kollár, Rónyai and Szabó [87] generalizes the same idea.

Let the set of vertices of our graph be the elements of \( GF(q^t) \), and recall that \( \text{Norm}_{q^t} a = a \cdot a^q \cdot \ldots \cdot a^{q^{t-1}} = a(q^t - 1)/(q - 1) \). Now two vertices \( a \) and \( b \) are adjacent iff \( \text{Norm}_{q^t} a + b = 1 \). The number of solutions of \( \text{Norm}_{q^t} x = 1 \) is \( q^t - 1 \) in \( GF(q^t) \) so the number of edges is at least \( \frac{1}{2} q^t(q^t - 1) - 1 \approx \frac{1}{2} (q^t)^{2-t} \).

**Theorem 29.24.** This graph \( G_{q,t} \) contains no subgraph isomorphic to \( K_{t,t+1} \).

**Corollary 29.25.** For \( t \geq 2 \) and \( s \geq t! + 1 \) we have \( \text{ex}(n, K_{t,s}) \geq c_t n^{2-t} \), where \( c_t > 0 \) depends on \( t \) only, we may choose \( c_t = 2^{-t} \). For every \( t \) and \( s \geq t \), the inequality holds with \( c = 1/2 \) for infinitely many values of \( n \).
The Corollary follows from the Theorem and from the fact that there is a prime power between $\frac{1}{2}n^{1/t}$ and $n^{1/t}$. The union of $\left\lceil \frac{n}{q} \right\rceil$ disjoint copies of $G_{q,t}$ will have the appropriate number of edges.

The Theorem is a direct consequence of the following: if $d_1, d_2, \ldots, d_t$ are distinct elements of $\mathbb{GF}(q^t)$ then the system of equations

$$\text{Norm}_{q^t \rightarrow q}(X + d_1) = (X + d_1)(X^q + d_1^q)\ldots(X^{q^{t-1}} + d_1^{q^{t-1}}) = 1$$

$$\text{Norm}_{q^t \rightarrow q}(X + d_2) = (X + d_2)(X^q + d_2^q)\ldots(X^{q^{t-1}} + d_2^{q^{t-1}}) = 1$$

$$\vdots$$

$$\text{Norm}_{q^t \rightarrow q}(X + d_t) = (X + d_t)(X^q + d_t^q)\ldots(X^{q^{t-1}} + d_t^{q^{t-1}}) = 1$$

has at most $t!$ solutions $x \in \mathbb{GF}(q^t)$. They prove it by considering a more general system of equations:

**Lemma 29.26.** Let $K$ be a field and $a_{ij}, b_i \in K$ for $1 \leq i, j \leq t$ such that $a_{ij} \neq a_{i'j'}$ if $j \neq j'$. Then the system of equations

$$(X_1 - a_{11})(X_2 - a_{21})\ldots(X_t - a_{t1}) = b_1$$

$$(X_1 - a_{12})(X_2 - a_{22})\ldots(X_t - a_{t2}) = b_2$$

$$\vdots$$

$$(X_1 - a_{1t})(X_2 - a_{2t})\ldots(X_t - a_{tt}) = b_t$$

has at most $t!$ solutions $(x_1, x_2, \ldots, x_t) \in K^t$.

In the proof of the Lemma first polynomials $f_j = (X_1 - a_{1j})(X_2 - a_{2j})\ldots(X_t - a_{tj})$ are defined, then the regular map $F : K^t \rightarrow K^t$ by $F(X_1, X_2, \ldots, X_t) := (f_1, f_2, \ldots, f_t)$. Then the Lemma states that $|F^{-1}(b)| \leq t!$ holds for every $b \in K^t$.

It is obvious for $b = 0$. The rest of the proof involves some commutative algebra and we omit it.

**Remark 29.27.** One gets Theorem 29.24 by putting

$$K = \mathbb{GF}(q^t), a_{ij} = -a_{ij}^{q^{t-1}}, b_j = 1.$$
Chapter 3

Hints and short solutions to the exercises

1 Of Chapter I

Exercise 5.1
In the polynomial ring \( \mathbb{GF}(q)[X] \) the equality 
\[
(1 + X)^n = \prod_{i=0}^{\infty} (1 + X^{n_i})^{p_i} = \prod_{i=0}^{\infty} (1 + X^{p_i})^{n_i}
\]
holds. In other words 
\[
\sum_{k=0}^{\infty} \binom{n}{k} X^k = \prod_{i=0}^{\infty} \sum_{k_i=0}^{p_i-1} \binom{n_i}{k_i} X^{k_0 + k_1 + k_2 + \ldots}
\]
and the result follows from comparison of coefficients.

Exercise 5.2
If \( \omega \) is a generator element of \( \mathbb{GF}(q^n) \) then \( \omega^{\frac{q^n-1}{q-1}} \) generates \( \mathbb{GF}(q) \). Now let \( N : \mathbb{GF}(q^n) \to \mathbb{GF}(q) \) be a multiplicative map with \( N(\omega) = \alpha \in \mathbb{GF}(q) \), then \( N(\omega^k) = \alpha^k \). If \( \alpha = \omega^{\frac{q^n-1}{q-1}} \) then \( N(\omega^k) = \text{Norm}(\omega^k)^{\alpha} \).

Exercise 5.5
\[
- \sum_{x \in \mathbb{GF}(q)} f(x)^k \text{ is on the one hand the coefficient of } X^{q-1}, \text{ on the other hand it is } \sum_{a \in \mathbb{GF}(q)} a^k.
\]

Exercise 5.6
If \( b = 0 \) then the equation is solvable as \( x \mapsto x^2 \) is an automorphism. Multiplying through by \( a/b^2 \) and introducing \( Y = aX/b \) we get \( Y^2 + Y + ac/b^2 = 0 \). As \( \text{Tr} \) is additive we have \( \text{Tr}(Y^2) + \text{Tr}(Y) + \text{Tr}(ac/b^2) = 0 \). As, by definition, \( \text{Tr}(Y^2) = \text{Tr}(Y) \), if the equation is solvable then \( \text{Tr}(ac/b^2) = 0 \).
Conversely, if $\text{Tr}(ac/b^2) = 0$ then the equation is solvable: the sets $\{y^2 + y : y \in GF(2^n)\}$ and $\{z : \text{Tr}_{2^h-2}(z) = 0\}$ are identical; $\subseteq$ is obvious and either of them is the image space of a linear mapping with one-dimensional kernel.

**Exercise 5.7**

Let $\{\deg(f) : f \in V\} = \{d_1, d_2, \ldots, d_n\}$, where $d_1 > d_2 > \ldots > d_n$. Choose a monic $f_i$ with $\deg(f_i) = d_i$, $i = 1, \ldots, n$. We prove that $\{f_1, \ldots, f_n\}$ is a base of $V$. Let $g \in V$, then define $g_0 = g$, and for $k = 1, \ldots, n$ let $a_k$ be the coefficient of $X^{d_k}$ in $g_k$, finally let $g_k = g_{k-1} - a_k f_k$. Observe that $\deg(g_k) < d_k$ and $g_k \in V$. Now $g_n = 0$, so $g = \sum a_i f_i \in \langle f_1, \ldots, f_n \rangle$.

**Exercise 5.8**

$(X - a)^\lambda = \sum_{r=0}^{\lambda} \binom{\lambda}{r} (-a)^{\lambda-r} X^r$; use Lucas' theorem (Exercise 5.1).

For the converse prove that $\sum_{a \in GF(q)} a^{q-1+r-\lambda} (X - a)^\lambda = (-1)^{\lambda-r-1} \binom{\lambda}{r} X^r$ unless $\lambda = q - 1$ and $r = 0$ or $q - 1$.

**Exercise 5.9**

If $f(aY + b, Y) = 0$ then $f(X, Y) = 0$ modulo $X - aY - b$, and hence $X - aY - b \mid f(X, Y)$. It follows that $\prod_{(a, b) \in S} (X - aY - b) \mid f(X, Y)$. Since the degree of the left hand side is $|S|$, the result follows.

**Exercise 5.13**

Let $A = \{\mathbf{P}_i : i = 1, \ldots, n+t-1\}$ be an arc in $\text{PG}(n-1, q)$. Then $f_i(\mathbf{X}) = \mathbf{P}_i \cdot \mathbf{X} = 0$ is the equation of a hyperplane $H_i$ through the origin in $\text{AG}(n, q)$. Any point of $\text{AG}(n, q) \setminus \mathbf{0}$ is covered at most $(n - 1)$ times by these hyperplanes, because of the arc property.

Now $f_i(\mathbf{X})^{q-1} - 1$ vanishes precisely in the points of $\text{AG}(n, q) \setminus H_i$; hence for $\prod_{i=1}^{n+t-1} (f_i(\mathbf{X})^{q-1} - 1)$, at any point of $\text{AG}(n, q) \setminus \mathbf{0}$ at least $(n+t-1) - (n - 1) = t$ factors will be zero. This is a polynomial of degree $(n + t - 1)(q - 1)$.

**Exercise 5.14**

Let $C_i$ be defined by the polynomial $f_i(X, Y)$, then consider $\prod_i f_i$ and use 5.12.

**Exercise 5.21**

Let $g_i(X_i) = \prod_{s_i \in S_i} (X_i - s_i)$, and $l_i(X_i) = \prod_{d_i \in D_i} (X_i - d_i)$. By Theorem 5.20 we can write $f = \sum_{i=1}^{n} h_i g_i + w$, and $w = u \prod_{i=1}^{n} \frac{g_i}{h_i}$ for some non-zero polynomial $u$, and the degree in $X_i$ of $w$ is less than $|S_i|$. 

**Exercise 5.23**

Suppose that $f$ has a zero of degree at least $t$ at all elements of $S_1 \times S_2 \times \ldots \times S_n$. By Theorem 5.22 there are polynomials $h_\tau \in \mathbb{F}[X_1, X_2, \ldots, X_n]$ with the property that $f = \sum_{\tau \in T} g_{\tau(1)} \cdots g_{\tau(t)} h_\tau$, and $\deg h_\tau \leq \deg(f) - \sum_{i \in \tau} \deg(g_i)$. On the right
hand side of this equality the terms of highest degree are divisible by $\prod_{i \in \tau} X_i | S_i |$ for some $\tau$. So there is a $\tau$ for which $r_i \geq \sum_{i \in \tau} | S_i |$ for all $i \in \tau$, a contradiction.

**Exercise 5.26**

$f$ is singular if $f(X) = 0$ has more than one solution. For any solution $x \in \text{GF}(q)$ one can consider the $p^k$-th power $0 = f(x)^{p^k}$. Using $x^{p^k} = x$ and re-ordering, one gets the row of the matrix corresponding to this exponent. Hence for any solution $x$, the vector $(x, x^p, x^{p^2}, \ldots, x^{p^h-1})^T$ is a solution of the homogeneous matrix equation. The other direction is similar.

**Exercise 5.27**

As in the proof of Theorem 5.25, the “if” part is obvious. Consider $\text{GF}(q)$ as an $h$-dimensional vectorspace over $\text{GF}(p^e)$, then $f$ is a $\text{GF}(p^e)$-linear map. The number of such maps is $(p^e)^h$. The polynomials of form $\text{Tr}_{q \rightarrow p^e}(aX)$ are among these maps, the number of these polynomials is $q = (p^e)^h$.

**Exercise 5.32**

Multiply the sum by $\chi(4a^2) = 1$, we get $\chi(a) \sum_x \chi((2ax + b)^2 - (b^2 - 4ac))$. Replacing $2ax + b$ by $y$ and $b^2 - 4ac$ by $d$ yields $\chi(a) \sum_y \chi(y^2 - d)$. The case $d = 0$ is clear, for $d \neq 0$ we have to count the solutions of $Y^2 - d = Z^2$. It defines a hyperbola with $q - 1$ affine points. If $d$ is a nonsquare then for $\frac{q - 1}{2}$ values $y$ we have $\chi(y^2 - d) = 1$ and for the other $\frac{q - 1}{2}$ it is $-1$. If $d$ is a square then for $y = \pm \sqrt{d}$ we have $\chi(y^2 - d) = 0$; for $\frac{q - 3}{2}$ values $y$ we have $\chi(y^2 - d) = 1$ and for the other $\frac{q - 1}{2}$ it is $-1$.

**Exercise 6.1**

The number of $k$-dimensional (linear) subspaces in $V(n, q)$ is $\left[\begin{array}{c} n \\ k \end{array}\right]_q$.

The number of $k$-dimensional (affine) subspaces in $\text{AG}(n, q)$ is $q^{n-k} \left[\begin{array}{c} n \\ k \end{array}\right]_q$.

The number of $k$-dimensional projective subspaces in $\text{PG}(n, q)$ is $\left[\begin{array}{c} n+1 \\ k+1 \end{array}\right]_q$.

**Exercise 7.6**

$X^{q-1}$ means that $(1, 0, 0)$ is the nucleus in the even case, every line except those through the nucleus, intersects the parabola in 0 mod 2 points. Adding $(1, 0, 0)$ to $S$ the *-polynomial becomes zero. In the odd case the tangents of the conic are the solutions $[x, y, z]$ of $X^2 - 4YZ$.

**Exercise 9.5**

Each factor of the right hand side should divide the determinant. The degree of the two sides is equal.

**Exercise 9.7**
Similar to Exercise 9.5. The ‘variables’ are \(x_1, \ldots, x_n\) only.

**Exercise 9.13**

Let \(F(T) = \prod_x (T - f(x))\). The Newton-Waring-Girard formulae (Ex. 9.3, N1-3) imply that all the coefficients, i.e. the elementary symmetric polynomials \(\sigma_i\) are zero if \(i \leq q - 2\) and \(p \neq i\). Hence \(F(T) = G(T)^p + cT\), where \(c = \sum f(x)^q - 1\). Here \(c = 0\) means case (ii), while \(c \neq 0\) implies \(F'(T) = -c \neq 0\), so \(F\) has no multiple root, \(f\) is a permutation polynomial, \(F(T) = T^q - T\), \(c = -1\).

**Exercise 9.14**

Let \(V(f) = \{a_1, \ldots, a_K\}\) and \(m_i = |f^{-1}(a_i)|\) the “multiplicity” of \(a_i\). If \(w_f < \infty\) then

\[
\begin{align*}
m_1 + m_2 + \ldots + m_K &= 0 \\
a_1 m_1 + a_2 m_2 + \ldots + a_K m_K &= 0 \\
^2 m_1 + a_2^2 m_2 + \ldots + a_K^2 m_K &= 0 \\
\vdots \\
a_1^{w_f} m_1 + a_2^{w_f} m_2 + \ldots + a_K^{w_f} m_K &= \beta,
\end{align*}
\]

where \(\beta \neq 0\). If \(K < w_f + 1\) then the first \(K\) equations has the trivial solution \(m_1 = \ldots = m_K = 0\) only, contradicting the last one.

**Exercise 9.22**

Use Exercise 9.8!

**Exercise 9.25**

Consider

\[
\begin{pmatrix}
1 - t & 1 & \ldots & 1 \\
v_1 & v_2 & \ldots & v_t \\
\vdots & \vdots & \ddots & \vdots \\
v_1^{t-1} & v_2^{t-1} & \ldots & v_t^{t-1}
\end{pmatrix}
\begin{pmatrix}
1 \\
1 \\
\vdots \\
1
\end{pmatrix}
= \begin{pmatrix}
0 \\
0 \\
\vdots \\
0
\end{pmatrix},
\]

hence the determinant should be zero:

\[
VdM(v_1, y_2, \ldots, y_t) - ty_2 y_3 \cdots y_t VdM(y_2, y_3, \ldots, y_t) = 0.
\]

So

\[
t = \frac{VdM(v_1, y_2, \ldots, y_t)}{y_2 y_3 \cdots y_t VdM(y_2, y_3, \ldots, y_t)} = \frac{(y_1 - y_2)(y_1 - y_3) \cdots (y_1 - y_t)}{y_2 y_3 \cdots y_t}.
\]

**Exercise 10.1**

The number of coefficients is \(\binom{n+2}{2}\). So the “coefficient vectors” form the points of an \(\binom{n+2}{2} - 1\) dimensional projective space over \(\mathbb{GF}(q)\).

**Exercise 10.2**

Each point \((u, v) \in S\) gives a linear equation for the coefficients of the desired polynomial \(f\). Hence we have a homogeneous system of \(|S|\) such equations. When \(\deg f \geq \sqrt{2|S|} - 1\) then the number of coefficients is larger than \(|S|\).
Exercise 10.8
Consider \( f \cap f^{(q)} \), where \( f^{(q)} \) denotes \( \sum_{ijk}(\alpha_{ijk})X^iY^jZ^k \) when \( f(X,Y,Z) = \sum \alpha_{ijk}X^iY^jZ^k \); then use Bézout’s theorem.

Exercise 10.10
Consider the curve \( F(X,Y) = f(X) - Y^2 \), it has roughly \( 2q \) points (a bit less in fact). By Weil it cannot be irreducible. Write it as the product of two factors, it is not too difficult to see that it must be of form \( f(X) - Y^2 = (g(X) - Y)(h(X) + Y) \), and then \( g = h \) and \( f = g^2 \).

Exercise 10.11
Stand in a point \( P \) of the curve and look around! If \( P \) has multiplicity \( m \geq 1 \) and there is no linear component then on each line we can see at most \( n - m \) points, counted with intersection multiplicities, plus the one we are standing in. It gives \( \leq m + (q + 1)(n - m) = qn + n - qm \leq q(n - 1) + n \).

Exercise 10.12
Note that \( 1 \leq k \leq n - 1 \). (i) If we have a \( k \)-secant line \( \ell \) and \( P \in \ell \cap C \) then looking around from \( P \) we get the bound \( N_q \leq (n - 1)q + k \). (ii) We say that a point \( P \) can see the tangency at \( Q \) if \( Q \) is on the curve and (one of) the tangent line(s) at \( Q \) goes through \( P \). \( P = Q \) is allowed.) Now the points of the curve can see at least \( N_qk \) tangency, so there is at least one point \( P \) of the curve seeing at least \( k \) tangencies. Counting the points of the curve looking around from \( P \) we “lose” at least one (from the total number) at each tangency that \( P \) can see, which gives \( (n - 1)q + n - k \) as an upper bound. Finally \( \min\{(n - 1)q + k, (n - 1)q + n - k\} \leq (n - 1)q + \frac{n}{2} \).

Exercise 10.16
Use Theorem 10.9 by Stöhr and Voloch!

Exercise 10.18
Suppose that \( f \) is irreducible. By a coordinate transformation, which only permutes the elements of \( I \), one can achieve \( f(X',Y',Z') = X'^2 - Y'Z' \). But now \( f^{p+1} \not\in I \), contradiction.

2 Of Chapter II

Exercise 12.3
Let \( \{(a_i,b_i) : i = 1, \ldots, k\} \) be an affine blocking set and suppose that \( (a_1,b_1) = (0,0) \). Consider \( F(X,Y) = \prod_{i=2}^k(a_iX+b_iY+1) \). As \( \{(a_i,b_i) : i = 2, \ldots, k\} \) blocks all the lines not through the origin, \( F(x,y) = 0 \) for all \( (x,y) \neq (0,0) \). Now \( G(X,Y) = \)}
\[ \prod_{i=2}^{k}(a_iX + b_iY + 1) - (X^{q-1} - 1)(Y^{q-1} - 1) \] vanishes on \( \mathbb{GF}(q) \times \mathbb{GF}(q) \), hence \( X^{q-1}Y^{q-1} \) cannot be (one of) its leading term(s) by Theorem 5.17. Hence \( k - 1 \geq 2q - 2 \).

**Exercise 12.5**

If \( P \in B \) is essential with \( t \) tangents through it then choose the coordinate system so that \( P \in \ell_\infty \) and \( \ell_\infty \) is a tangent to \( B \). Putting one point on each tangent except \( \ell_\infty \) results in an affine blocking set of size \(|B| - 1 + t - 1\), which is, by Theorem 12.2, at least \( 2q - 1 \), hence \( t \geq 2q + 1 - |B| \).

**Exercise 13.2**

If \( x \in S \) is of multiplicity \( m \) then from \( x \) in each direction one can see \( 1 - m \mod p \) further points. Hence (1) the number of points (with multiplicity) is \( m + (1 - m)(q - 1) \equiv 1 \mod p \); (2) \( \sum_{s \in S}(x - s)^{q-1} = (1 - m) \sum_{a \in S} 1 \equiv 0 \), so again \( x \) is a root of \( \sum_{s \in S}(X - s)^{q-1} \) of degree \( q - 1 \).

**Exercise 13.3**

\( n = 1 \) is obvious, \( n = 2 \) is Proposition 13.1. Suppose that the statement is proved for \( n - 1 \geq 2 \) and consider a (multi)set \( S \) in \( \mathbb{AG}(n,q) \). Let \( P \in H_\infty \) be a point at infinity (in other words, a direction) not determined by \( S \). Then the quotient geometry at \( P \) is \( \simeq \mathbb{PG}(n-1,q) \), the points of \( S \) go into points of a multiset \( S' \subset \mathbb{PG}(n-1,q) \) in a natural way without any further coincidence; there is a hyperplane (i.e. the quotient of \( H_\infty \)) disjoint from \( S' \), so \( S' \subset \mathbb{AG}(n-1,q) \); finally every hyperplane of \( \mathbb{AG}(n-1,q) \) intersects \( S' \) in either 0 or 1 mod \( p \) points, so by the (induction) hypothesis we are done.

**Exercise 13.4**

Counting the points of \( S \) on the lines through some fixed point \( s \in S \) we have \(|S| \equiv r \mod p \). After the \( \mathbb{AG}(2,q) \leftrightarrow \mathbb{GF}(q^2) \) identification define
\[
 f(X) = \sum_{s \in S}(X - s)^{q-1},
\]

it is not identically zero as the coefficient of \( X^{q-1} \) is \( r \). If \( x \in S \) then every direction will occur with the same multiplicity \( r - 1 \mod p \), hence for each point \( s \in S \), \( f(s) = (r - 1)\sum_{a \in S} 1 \alpha = 0 \), so they are roots of \( f \), which is of degree \( q - 1 \). The biggest value \( \equiv r \mod p \) below \( q \) is \( q - p + r \). However, a set of size \( \leq q + 1 \) always has a 1-secant, so the corollary is that \( r = 1 \).

**Exercise 14.1**

See the proof of Exercise 10.11.

**Exercise 14.2**

Let \( \ell_i \) be the axis \( X_i = 0 \) and \( m_j \) the line \( X_2 = a_jX_1 + b_j \). So for the intersections with the axes we have \( \mathbb{GF}(q)^* = \{a_j : j = 1, ..., q - 1\} = \{b_j : j = 1, ..., q - 1\} = \ldots \)
\( \{ \frac{a_j}{b_j} : j = 1, ..., q - 1 \} \). By Wilson’s theorem (Section 9), we get 
\[-1 = \prod_j a_j = \prod_j \frac{a_j}{b_j} = \frac{\prod_j a_j}{\prod_j b_j} = 1.\]

If \( q \) is even then the lines \( \{ X_2 = aX_1 + a^2 : a \in \mathbb{GF}(q)^* \} \) suffice. In fact, if \( \{ \ell_i \} \cup \{ m_j \} \) is a dual hyperoval then it works. Another solution is the following: let \( P \) be a point not on the triangle. Then the \( q - 2 \) lines through \( P \), not containing the vertices of the triangle, plus the line joining the three missing non-vertex points on \( \ell_1, \ell_2 \) and \( \ell_3 \) form such a set.

**Exercise 14.7**

Let \( Q = L_1 \cap L_2 \) and let \( F \) and \( G \) two curves through the given points. As neither \( F \) nor \( G \) contains \( Q \), a suitable linear combination \( H \) of them does, hence \( H \) contains the given points and \( Q \) as well. Then \( L_1 \) is a component of \( H \), so \( H \) intersects each of the other lines \( L_i \) also in at least \( n + 1 \) points, so \( \prod_{i=1}^k L_i \) divides \( H \). As \( \deg H = n < k \), it follows that \( H = 0 \) and \( F = \lambda G \).

**Exercise 15.1**

The condition is equivalent to saying that there is no collinear triple of points on the graph of \( f \).

**Exercise 15.2**

As \( f(X) \) is a permutation polynomial, \( \deg f \leq q - 2 \). Calculate \( F_s(0) = f'(s) \), it vanishes for every \( s \in \mathbb{GF}(q) \) by Exercise 15.1.

**Exercise 15.3**

\( X^r \) is a permutation polynomial iff \( (r, q - 1) = 1 \). \( F_0(X) = X^{r-1} \) gives \( (r - 1, q - 1) = 1 \) similarly. For \( s \neq 0 \) \( F_s(X) = \frac{(X+1)^{r-1} - s^r}{X^s} = \frac{1}{s^r} \frac{(X/s+1)^{r-1} - 1}{X/s} \), which is a permutation polynomial if and only if \( \frac{(Y+1)^{r-1}}{Y} \) is.

**Exercise 15.4**

Use Exercise 15.3.

**Exercise 15.11**

Its size is \( 1 + (n - 1)(q + 1) \), 1 for \( F_0 \) and \( q + 1 \) for the others. The lines through \( (0, 0, 1) \) intersect each \( F_\lambda \) in one point. For the other affine lines of equation \( aX + Y + bZ, b \neq 0 \), calculate the intersections and use that \( H \) is an additive subgroup.

**Exercise 17.13**

Let us count now the weighted index of points, that is let \( i(P) = \sum kt_{n+k}(P) \), where \( t_{n+k}(P) \) denotes the number of \( (n + i) \)-secants through \( P \). If \( t_0(P) = q/n \), then the index of \( P \) is just \( \varepsilon \). In general, \( 0 \leq i(P) \equiv \varepsilon \pmod{n} \). In particular, for \( \varepsilon < n \), the indices are always at least \( \varepsilon \). On the other hand, adding up indices along a 0-secant gives the total (weighted number) of lines longer than \( n \). For a
point of $S$, the index is $\varepsilon$, hence the total (weighted) number of long lines is at most $\varepsilon |S|/(n+1) < \varepsilon(q+1)$. This is a contradiction.

**Exercise 18.3**

Stand into a point $P \in \ell \setminus B$ and look around, you have to see at least one (affine) point of $B$ on each line $\neq \ell$.

In case of equality, if a direction $P \in \ell$ is determined by two affine points of $B \setminus \ell$ then, as there are $q$ affine lines through $P$ and at least one of them contains at least two of the $q$ affine points of $B$, there exists an affine line through $P$ which is not blocked by the affine points of $B$ hence $P$ should be added. A non-determined point means precisely one point per affine line through it, hence it is unnecessary to put it to $B$.

**Exercise 18.6**

A $3/2$-transitive group is either primitive or a Frobenius group. As $D \subseteq \text{GF}(p^e)$, we have that $\text{GF}(p^e)$ is a block of $F_D$, hence $F_D$ is not primitive. As $F_D^{\text{lin}} \subseteq F_D$, it follows that $F_D^{\text{lin}} = F_D$.

**Exercise 18.8**

Use Exercise 18.5.

**Exercise 18.12**

(i) If $b_i = b_j$ then the parabolas meet at $X = 0$. (ii) The equation $\frac{a_i - a_j}{b_i - b_j} = -1/x^2$ must not have a solution $x \in \text{GF}(q)$. (iii) $f$ defines $\leq \frac{p+1}{2}$ directions, hence its graph is a line. If it is non-horizontal then it intersect the horizontal axis.

**Exercise 23.3**

Use that the eigenvalues of the incidence matrix are $q + 1$ and $\pm \sqrt{q}$.

**Exercise 24.6**

Assume that $\mathbf{0}$ is in the blocking set, and $\pi$ is the dual translation plane with respect to $\mathbf{0}$. The dual $\bar{\pi}$ is a translation plane of order $q^2$ with kernel of order $q$. Each line of $\bar{\pi}$ can be regarded as a plane of $\text{AG}(4, q)$ and by Jamison or Theorem 24.5 with $n = 4, k = 2, t = 1$ we are done.

**Exercise 24.8**

Let $l_1, l_2, ..., l_n$ be $n$ lines of $\text{PG}(n, q)$ incident with the same point $x$ of $A$ and spanning $\text{PG}(n, q)$. Let $H$ be the hyperplane which is incident with no point of $A$ and set $S_i = l_i \setminus \{x\}$ and $D_i = l_i \cap H$. Theorem 24.7 implies $|A| - 1 \geq (t-1)(q-1) + n(q-1)$.

**Exercise 24.13**

The binomial coefficient in Corollary 24.12 with $n = 2$ and $j = k = t - (t, q)$ is $(1-t(q, q))$, which is non-zero by Lucas Theorem.
Exercise 27.5
Use the Stöhr-Voloch bound (Exercise 10.16).

Exercise 27.6
Use \( \bar{\sigma}_k(T) \) instead of \( \sigma_k^*(T) \) for \( k = 1, \ldots, \varepsilon \) in the proof; everything remains the same, like in Section 11.

Exercise 27.7
The secant joining \( (c, c^2) \) and \( (d, d^2) \) is \( Y = (c + d)X - cd \). If the missing points are \( (\gamma, \gamma^2) \) and \( (\delta, \delta^2) \) then we need \( \alpha = \gamma + \delta \) and \( \beta = -\gamma \delta \). As \( \sum_{z \in \text{GF}(q)} z = 0 \) and \( \prod_{z \in \text{GF}(q)}^{-1} = -1 \), we have \( \alpha = -\sum a_i \) and \( \beta = \pm \left( \prod_{i=1}^{q-3} b_i \right)^{-1} \).

Exercise 29.3
By the preceding, every such set \( B \) must be a subgroup, hence a line through the origin. \( G = A + B \) implies that every line parallel to \( B \) must intersect \( A \), hence the direction of \( B \) is not determined by \( A \). By Theorem 18.1, there are at most \( p / 2 \) such directions.

Exercise 29.4
For \( x \neq y \in \text{GF}(p^2) \), observe that \( x - y \) is a square in \( \text{GF}(p^2)^* \) iff \( (x - y)^{q-1} \) is a square in the multiplicative subgroup of the \( (p+1) \)-th roots of unity \( \subset \text{GF}(p^2)^* \). So after the \( \text{GF}(p^2) \leftrightarrow \text{AG}(2, p) \) identification, \( X \subset \text{AG}(2, p) \) determines at most \( p+1 \) directions, hence, by Theorem 18.1, it is a line containing 0 and 1.

Exercise 29.8
Use Theorem 18.7.

Exercise 29.20
Define \( f = \prod_{i=1}^{m} (1 - f_i(X_1, X_2, \ldots, X_n)^{q-1}) \) and note that \( f \) is non-zero only precisely at the common zeros of \( f_1, f_2, \ldots, f_m \). If there is a common zero then Theorem 5.20 implies that \( \deg f = (q - 1) \sum_{i=1}^{m} \deg(f_i) \geq nq - \sum_{i=1}^{n} |D_i| \).

Exercise 29.22
Let’s identify \( V(d, p) \) with \( \text{GF}(p^d) \). Let \( C = A + B \), suppose \( |C| = n < \beta_p(r, s) \). Define \( f(X, Y) = \prod_{c \in C}(X + Y - c) \), then \( f \) vanishes on \( A \times B \). By the definition of \( \beta_p(r, s) \) there exists some \( n - r < k < s \) such that \( \binom{s}{k} \neq 0 \) (mod \( p \)). So the coefficient of \( X^{n-k}Y^k \) in \( f \) is nonzero, and \( |A| = r + n - k, |B| = s > k \), by Theorem 5.17 it is a contradiction.
Chapter 4

Glossary of concepts

Here one can find the most important definitions, in alphabetical order.

A \((k, n)\)-arc of \(\text{PG}(2, q)\) is a pointset of size \(k\), meeting every line in at most \(n\) points. An arc is a \((k, 2)\)-arc. A \((k, n)\)-arc is complete if it is not contained in a \((k + 1, n)\)-arc.

A blocking set (w.r.t. lines) is a pointset meeting every line. In general, a blocking set in \(\text{PG}(n, q)\) w.r.t. \(k\)-dimensional subspaces (sometimes it is called an \((n - k)\)-blocking set) is a pointset meeting every \(k\)-subspace. A \(t\)-fold blocking set meets every \(k\)-subspace in at least \(t\) points. A point \(P\) of \(B\) is essential if \(B \setminus \{P\}\) is no longer a blocking set, i.e. there is a 1-secant \(k\)-space through \(P\). \(B\) is minimal if every point of it is essential. A blocking set \(B\) of \(\text{PG}(2, q)\) is small if \(|B| < \frac{3}{2}(q + 1)\), in general, a blocking set \(B\) in \(\text{PG}(n, q)\) w.r.t. \(k\)-dimensional subspaces is small if \(|B| < \frac{3}{2}q^{n-k} + 1\).

Given \(B \subset \text{PG}(2, q)\), the point \(P \notin B\) is a \(t\)-fold nucleus of \(B\) if all the lines through \(P\) intersect \(B\) in at least \(t\) points. \(P \notin B\) is a \(t\)-fold lower nucleus of \(B\) if all the lines through \(P\) intersect \(B\) in at most \(t\) points. So from a nucleus \(B\) seems to be a \(t\)-fold blocking set while from a lower nucleus \(B\) seems to be a \(|B|, t\)-arc. If \(P\) is a point of \(B\) then the similar notions are called internal nuclei.

A blocking set \(B \subset \text{PG}(n, q)\), with respect to \(k\)-dimensional subspaces, is of Rédéi type, if it has precisely \(q^{n-k}\) points in the affine part \(\text{AG}(n, q) = \text{PG}(n, q) \setminus H_\infty\).

A semiola is a pointset of \(\text{PG}(2, q)\) with the property that there is a unique tangent line at each point of it. It is regular, if it is a pointset of type \((0, 1, a)\), i.e. all the secants are of the same length \(a\).

A \(k\)-spread of \(\text{PG}(n, q)\) is a partition of the space into \(k\)-dimensional subspaces.
A subgeometry of $\Pi = \text{PG}(n, q)$ is a copy of some $\Pi' = \text{PG}(n', q')$ embedded in it, so the points of $\Pi'$ are points of $\Pi$ and the $k$-dimensional subspaces of $\Pi'$ are just the intersections of some $k$-subspaces of $\Pi$ with the pointset of $\Pi'$. It follows that $\text{GF}(q')$ must be a subfield of $\text{GF}(q)$.

The type of a pointset of $\text{PG}(2, q)$ is the set of its possible intersection numbers with lines. In particular, an arc is a set of type $(0, 1, 2)$, a set of even type is a pointset with each intersection numbers being even, etc.

A unital is a pointset of $\text{PG}(2, q^2)$ of size $q^3 + 1$ intersecting each line in either 1 or $q + 1$ points. It has a unique 1-secant through each point of it so it is a minimal blocking set.

An untouchable set is a set without tangents.
Chapter 5

Notation

\( \mathbf{V}(n, F) \) denotes the \( n \)-dimensional vector space with coordinates from the field \( F \). If \( F = \mathbb{F}(q) \) then we write \( \mathbf{V}(n, q) \) instead.

\( \mathbf{A}(n, F) \) denotes the \( n \)-dimensional affine space with coordinates from the field \( F \). If \( F = \mathbb{F}(q) \) then we write \( \mathbf{A}(n, q) \) instead.

\( \mathbf{P}(n, F) \) denotes the \( n \)-dimensional projective space with coordinates from the field \( F \). If \( F = \mathbb{F}(q) \) then we write \( \mathbf{P}(n, q) \) instead.

\[ [a \ b]_q = \frac{(q^a-1)(q^{a+1}-1)...(q^{a+b-1}-1)}{(q^b-1)(q^{b+1}-1)...(q-1)} \] (the \( q \)-binomials or Gaussian binomials, the number of \( b \)-dimensional linear subspaces of \( \mathbf{V}(a, q) \)).

If the order \( q \) of a plane or space is fixed we write \( \theta_i = \frac{[i+1]}{1} = q^i + q^{i-1} + ... + q + 1. \)

\( \mathbb{Tr}_{q^n}^q(X) = X + X^q + X^{q^2} + ... + X^{q^n-1} \) is the trace function from \( \mathbb{F}(q^n) \) to \( \mathbb{F}(q) \).

\( \mathbb{Norm}_{q^n}^q(X) = X X^q X^{q^2} X^{q^n-1} \) is the norm function from \( \mathbb{F}(q^n) \) to \( \mathbb{F}(q) \).

In some cases \( \omega \) will denote a primitive element of \( \mathbb{F}(q^n) \) (and sometimes it is nice to assume that \( (\omega, \omega^q, \omega^{q^2}, ..., \omega^{q^{n-1}}) \) form a trace-orthogonal base over \( \mathbb{F}(q) \) if possible, see 5.2).

\( J_t \) is the ideal \( \langle (X_1^t - X_1)^{i_1} (X_2^t - X_2)^{i_2} ...(X_n^t - X_n)^{i_n} : 0 \leq i_1 + i_2 + ... + i_n = t \rangle \) in \( \mathbb{F}(q)[X_1, ..., X_n] \) of polynomials vanishing everywhere with multiplicity at least \( t \).

\( H_\infty \) is the hyperplane at infinity in the projective space \( \mathbf{P}(n, q) \) when an “affine part” is fixed, i.e. \( H_\infty = \mathbf{P}(n, q) \setminus \mathbf{A}(n, q) \). When \( n = 2 \), it is called the “line at infinity” \( \ell_\infty \).
\( M_f \): given the polynomial \( f \in \text{GF}(q)[X] \), the number of elements \( a \in \text{GF}(q) \) for which \( f(X) + aX \) is a permutation polynomial.

\( D_f \): given the polynomial \( f \in \text{GF}(q)[X] \), \( D_f = \{ \frac{f(x) - f(y)}{x - y} : x \neq y \in \text{GF}(q) \} \), the set of directions determined by the graph of \( f \).

\( N_f = |D_f| \).

\( w_f \): given the polynomial \( f \in \text{GF}(q)[X] \), \( w_f = \min\{k : \sum_{x \in \text{GF}(q)} f(x)^k \neq 0 \} \).

\( W_f \): given the polynomial \( f \in \text{GF}(q)[X] \), \( W_f = \min\{k + l : \sum_{x \in \text{GF}(q)} x^k f(x)^l \neq 0 \} \).

\( N(B) \) denotes the set of (external) nuclei of the pointset \( B \).

\( IN(B) \) denotes the set of internal nuclei of the pointset \( B \).
Bibliography


[16] S. Ball, A. Gács, On the graph of a function over a prime field whose small powers have bounded degree, preprint.


A. Blokhuis, On subsets of GF(q^2) with square differences, Indag. Math. 46 (1984), 369-372.

A. Blokhuis, Solution of an extremal problem for sets using resultants of polynomials, Combinatorica 10 (1990), 393–396.


S. Ferret, L. Storme, P. Sziklai, Zs. Weiner, A $t \mod p$ result on weighted multiple $(n-k)$-blocking sets in $\mathrm{PG}(n,q)$, *Innovations in Incidence Geometry*, to appear.


A. Gács, On a generalization of Rédei’s theorem, *Combinatorica* 23 (2003), no. 4, 585–598.


A. Gács, Zs. Weiner, On $(q + t,t)$-arcs of type $(0,2,t)$, *Designs, Codes and Cryptography* 29 (2003), 131–139.


Bibliography


[138] Zs. Weiner, Small point sets of \(\text{PG}(n,q)\) intersecting each \(k\)-space in \(1 \mod \sqrt{q}\) points, *Innovations in Incidence Geometry*, 1, (2005), 171–180.