APPLICATIONS OF POLYNOMIALS OVER FINITE FIELDS

Péter Sziklai

A doctoral dissertation
submitted to the Hungarian Academy of Sciences
Budapest, 2013

0 Foreword

A most efficient way of investigating combinatorially defined point sets in spaces over finite fields is associating polynomials to them. This *technique* was first used by Rédei, Jamison, Lovász, Schrijver 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 point set, 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 point sets goes back to Segre, recently a bunch of new applications have shown the strength of this method. Finally, dimension arguments on polynomial spaces have become fruitful.

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, flocks, etc.

This work starts with a collection of definitions, methods and results we are going to use later. It is an incomplete overview from the basic facts to some theory of polynomials over finite fields; proofs are only provided when they are either very short or not available in the usual literature, and if they are interesting for our purposes. A reader, being familiar with the topic, may skip Sections 1-8 and possibly return later when the text refers back here. We provide slightly more information than the essential background for the later parts.

After the basic facts (Sections 1-4) we introduce our main tool, the Rédei polynomial associated to point sets (5). There is a brief section on the univariate representation as well (6). The coefficients of Rédei polynomials are elementary symmetric polynomials themselves, what we need to know about them and other invariants of subsets of fields is collected in Section 7. The multivariate polynomials associated to point sets can be considered as algebraic varieties, so we can use some basic facts of algebraic geometry (8). Then, in Section 9 some explanatory background needed for stability results is presented. Already Sections 1-8 contain some new results, some of them are interesting themselves, some others can be understood in the applications in the following sections.

The second (and main) part contains results of finite Galois geometry, where polynomials play a main role. We start with results on intersection numbers of planar point sets (10). Section 10 contains the classification of small and large super-Vandermonde sets, too. A strong result about sets with intersection numbers having a nontrivial common divisor is presented here, this theorem implies the famous result on the non-existence of maximal planar arcs in odd characteristic as well. In Section 11 we show how the method of using algebraic curves for blocking sets (started by Szőnyi) could be developed further, implying a strong characterization result. Then in sections 12, 14 and 15 we deal with different aspects of directions. In Section 12 we examine the linear point sets, which became important because of the linear blocking sets we had dealt with in the previous section. Also here we describe Rédei-type k-blocking sets. Then (13), with a compact stability result on flocks of cones we show the classical way of proving extendibility, which was anticipated in Section 9 already. After it, the contrast can be seen when we present a new method for the stability problem of direction sets in Section 14. Finally, Section 15 contains a difficult extension of the classical direction problem, also a slight improvement (with a new proof) of a nice result of Gács. The dissertation ends with a Glossary of concepts and Notation, and then concludes with the references.

Contents

1 Introduction

In this work we will not give a complete introduction to finite geometries, finite fields nor polynomials. There are very good books of these kinds available, e.g. Ball-Weiner [19] for a smooth and fascinating introduction to the concepts of finite geometries, the three volumes of Hirschfeld and Hirschfeld-Thas [65, 66, 67] as handbooks and Lidl-Niederreiter [79] 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 also help) to enjoy this interdisciplinary field in the overlap of geometry, combinatorics and algebra. To read this work the prerequisits are just linear algebra and geometry.

We would like to use a common terminology.

In 1991, 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 a(n 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 [91] from 1970, which inspired a new series of results on blocking sets and directions in the 1990's. There are a few survey papers on the polynomial methods as well, for instance by Blokhuis [26, 27], Szőnyi [102], Ball [5].

The typical theories in this field have the following character. Define a class of (point)sets (of a geometry) in a combinatorial way (which, typically, 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; finally 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 dissertation:

- an algebraic curve or surface whose points correspond to the "deviant" or "interesting" lines or subspaces meeting a certain point set;
- examination of (lacunary) coefficients of polynomials;
- considering subspaces of the linear space of polynomials.

This work has a large overlap with my book **Polynomials in finite geometry** [SzPpolybk], which is in preparation and available on the webpage `http://www.cs.elte.hu/~sziklai/poly.html` ; most of the topics considered here are described there in a more detailed way.

2 Acknowledgements

Most of my work is strongly connected to 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 form an important part of this topic. Not least, I always enjoyed their warm, joyful, inspirating and supporting company in various situations in the last some years. I am grateful for all the joint work and for all the suggestions they made to improve the quality of this work.

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.

The early version of this work was just started when our close friend and excellent colleague, András Gács died. We all miss his witty and amusing company.

I would like to thank all my coauthors and all my students for the work and time spent together: Leo Storme, Jan De Beule, Sandy Ferret, Jörg Eisfeld, Geertrui Van de Voorde, Michelle Lavrauw, Yves Edel, Szabolcs L. Fancsali, Marcella Takáts, and, working on other topics together: P.L. Erdős, D. Torney, P. Ligeti, G. Kós, G. Bacsó, L. Héthelyi.

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, Potenza, Naples, Caserta, 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. The n-dimensional **vectorspace** over the finite (Galois) field $\mathsf{GF}(q)$ (of q elements) will be denoted by $\mathsf{V}(n,q)$ or simply by $\mathsf{GF}(q)^n$.

The most we work in the Desarguesian **affine space** $\mathsf{AG}(n,q)$ coordinatized by $\mathsf{GF}(q)$ and so imagined as $\mathsf{GF}(q)^n \sim \mathsf{V}(n,q)$; or in the Desarguesian **projective space** $\mathsf{PG}(n,q)$ coordinatized by $\mathsf{GF}(q)$ in homogeneous way, as

$\mathsf{GF}(q)^{n+1} \sim \mathsf{V}(n+1,q)$, and the projective subspaces of (projective) dimension k are identified with the linear subspaces of rank $(k+1)$ of the related $\mathsf{V}(n+1,q)$. In this representation *dimension* will be meant projectively while vector space dimension will be called *rank* (so rank=dim+1). A field, which is not necessarily finite will be denoted by $\mathbb{F}$.

In general capital letters $X, Y, Z, T, ...$ (or $X_1, X_2, ...$) will denote independent variables, while $x, y, z, t, ...$ will typically be elements of a field. 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 $\mathbf{X}$ or $\mathbf{V} = (X, Y, Z, ..., T)$ meaning as many variables as needed; $\mathbf{V}^q = (X^q, Y^q, Z^q, ...)$. As over a finite field of order q for each $x \in \mathsf{GF}(q)$ $x^q = x$ holds, two different polynomials, f and g, in one or more variables, can have coinciding values "everywhere" over $\mathsf{GF}(q)$. But 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; also simply $f = g$ and $f(X) = g(X)$ may denote the same, and we will state it explicitly if two polynomials are equal everywhere over $\mathsf{GF}(q)$, i.e. they define the same function $\mathsf{GF}(q) \to \mathsf{GF}(q)$.

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

For $\mathsf{AG}(n,q)$ we can use the **big field** representation as well: roughly speaking $\mathsf{AG}(n,q) \sim \mathsf{V}(n,q) \sim \mathsf{GF}(q)^n \sim \mathsf{GF}(q^n)$, so the points correspond to elements of $\mathsf{GF}(q^n)$. The geometric structure is defined by the following relation: three distinct points A, B, C are collinear if and only for the corresponding field elements $(a-c)^{q-1} = (b-c)^{q-1}$ holds. This way the ideal points (directions) correspond to (a separate set of) $(q-1)$-th powers, i.e. $\frac{q^n-1}{q-1}$-th roots of unity.

When $\mathsf{PG}(n,q)$ is considered as $\mathsf{AG}(n,q)$ plus the hyperplane at infinity, then we will use the notation H_∞ for that ('ideal') hyperplane. If $n = 2$ then H_∞ is called the line at infinity ℓ_∞. The points of H_∞ or ℓ_∞ are often called *directions* or ideal points.

According to the standard terminology, a line meeting a point set 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). Most of this work 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 work.

4 Finite fields and polynomials

4.1 Some basic facts

Here the basic facts about finite fields are collected. For more see [79].

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

For any $a \in \mathsf{GF}(q)$ $\quad a^q = a$ holds, so the field elements are precisely the roots of $X^q - X$, also if $a \neq 0$ then $a^{q-1} = 1$ and $X^{q-1} - 1$ is the root polynomial of $\mathsf{GF}(q)^*$. (Lucas' theorem implies, see below, that) we have $(a + b)^p = a^p + b^p$ for any $a, b \in \mathsf{GF}(q)$, so $x \mapsto x^p$ is a field automorphism. $\mathsf{GF}(q)$ has a (unique) subfield $\mathsf{GF}(p^t)$ for each $t|h$; $\mathsf{GF}(q)$ is an $\frac{h}{t}$-dimensional vectorspace over its subfield $\mathsf{GF}(p^t)$. The (Frobenius-) automorphisms of $\mathrm{GF}(q)$ are $x \mapsto x^{p^i}$ for $i = 0, 1, ..., h - 1$, forming the complete, cyclic automorphism group of order h. Hence $x \mapsto x^{p^t}$ fixes the subfield $\mathsf{GF}(p^{\gcd(t,h)})$ pointwise (and all the subfields setwise!); equivalently, $(X^{p^t} - X)|(X^q - X)$ iff $t|h$.

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

We often use Lucas' theorem when calculating binomial coefficients $\binom{n}{k}$ in finite characteristic, so "modulo p": let $n = n_0 + n_1 p + n_2 p^2 + ... + n_t p^t$, $k = k_0 + k_1 p + k_2 p^2 + ... + k_t p^t$, with $0 \leq n_i, k_i \leq p - 1$, then $\binom{n}{k} \equiv \binom{n_0}{k_0}\binom{n_1}{k_1}...\binom{n_t}{k_t} \pmod{p}$. In particular, in most cases we are interested in those values of k when $\binom{n}{k}$ is non-zero in $\mathsf{GF}(q)$, so modulo p. By Lucas' theorem, they are precisely the elements of $M_n = \{k = k_0 + k_1 p + k_2 p^2 + ... + k_t p^t : 0 \leq k_i \leq n_i\}$.

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

Result 4.1. *Both* Tr *and* Norm *are in some sense* unique*, i.e. any* $\mathsf{GF}(q)$*-linear function mapping* $\mathsf{GF}(q^n)$ *onto* $\mathsf{GF}(q)$ *can be written in the form* $\mathsf{Tr}_{q^n \to q}(aX)$ *with a suitable* $a \in \mathsf{GF}(q^n)$ *and any multiplicative function mapping* $\mathsf{GF}(q^n)$ *onto* $\mathsf{GF}(q)$ *can be written in the form* $\mathsf{Norm}_{q^n \to q}(X^a)$ *with a suitable integer* a*.*

4.2 Polynomials

Here we summarize some properties of polynomials over finite fields. Given a field $\mathbb{F}$, a polynomial $f(X_1, X_2, ..., X_k)$ is a finite sum of monomial terms $a_{i_1 i_2 ... i_k} X_1^{i_1} X_2^{i_2} \cdots X_k^{i_k}$, where each X_i is a free variable, $a_{i_1 i_2 ... i_k}$, the coefficient of the term, is an element of $\mathbb{F}$. The (total) degree of a monomial is $i_1 + i_2 + ... + i_k$ if the coefficient is nonzero and $-\infty$ otherwise. The (total) degree of f, denoted by $\deg f$ or f°, is the maximum of the degrees of its terms. These polynomials form the ring $\mathbb{F}[X_1, X_2, ..., X_k]$. 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: $Z^{\deg f} \cdot f(\frac{X_1}{Z}, \frac{X_2}{Z}, ..., \frac{X_k}{Z})$, which is a polynomial again (Z is an additional free variable).

Given $f(X_1, ..., X_n) = \sum a_{i_1 ... i_n} X_1^{i_1} \cdots X_n^{i_n} \in \mathbb{F}[X_1, ..., X_n]$, and the elements $x_1, ..., x_n \in \mathbb{F}$ then one may *substitute* them into f: $f(x_1, ..., x_n) = \sum a_{i_1 ... i_n} x_1^{i_1} \cdots x_n^{i_n} \in \mathbb{F}$; $(x_1, ..., x_n)$ 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 $\bar{\mathbb{F}}$, the algebraic closure of $\mathbb{F}$, and it still cannot be written as a product of polynomials over $\bar{\mathbb{F}}$ then f is *absolutely irreducible*. E.g. $X^2+1 \in \mathsf{GF}(3)[X]$ is irreducible but not absolutely irreducible, it splits to $(X+i)(X-i)$ over $\mathsf{GF}(3)$ where $i^2 = -1$. But, for instance, $X^2 + Y^2 + 1 \in \mathsf{GF}(3)[X, Y]$ 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) if $f(X)$ can be written as $f(X) = (X - x)^m \cdot g(X)$ for some polynomial $g(X)$, $m \geq 1$, with $g(x) \neq 0$.

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

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

where

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

is the characteristic function of the set $\{a\}$, this is Lagrange interpolation. 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 $\mathsf{GF}(q) \to \mathsf{GF}(q)$ and polynomials

in $\mathsf{GF}(q)[X]$ of degree $\leq q-1$ is q^q, this representation is unique as they are both a vectorspace of dim $= q$ over $\mathsf{GF}(q)$.

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

Proposition 4.2. *For any (reduced) polynomial* $f(X) = c_{q-1}X^{q-1} + ... + c_0$,

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

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

Result 4.3. *If* f *is bijective (permutation polynomial) then the reduced degree of* f^k *is at most* $q-2$ *for* $k = 1, ..., q-2$.

We note that (i) if $p \nmid |\{t : f(t) = 0\}|$ then the converse is true;
(ii) it is enough to assume it for the values $k \not\equiv 0 \pmod{p}$.

Let's examine $\mathsf{GF}(q)[X]$ as a vector space over $\mathsf{GF}(q)$.

Result 4.4. Gács [61] *For any subspace* V *of* $\mathsf{GF}(q)[X]$, $\dim(V) = |\{\deg(f) : f \in V\}|$.

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 $\mathsf{GF}(q)^n$. We shall refer to $\mathbf{a}$ as a point in the n-dimensional vector space $\mathsf{V}(n,q)$ or affine space $\mathsf{AG}(n,q)$. Consider an f in $\mathsf{GF}(q)[X_1, ..., X_n]$, $f = \sum \alpha_{i_1,i_2,...,i_n} X_1^{i_1} \cdots X_n^{i_n}$.

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.

4.3 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 $i a_i X^{i-1}$ vanishes; in particular

$\deg f' < \deg f - 1$ may occur. Multiple differentiation is denoted by $\partial_X^i f$ or $f^{(i)}$ or f'', 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 $p|m$. Also if $k \leq p$ then a is root of f with multiplicity at least k iff $f^{(i)}(a) = 0$ 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 $\nabla^i_{\mathcal{H}} = (\mathcal{H}^i_X, \mathcal{H}^i_Y, \mathcal{H}^i_Z)$, where $\mathcal{H}^i$ stands for the i-th Hasse-derivation operator (see 5.3). The only properties we need are that $\mathcal{H}^j\ X^k = \binom{k}{j} X^{k-j}$ if $k \geq j$ (otherwise 0); $\mathcal{H}^j$ is a linear operator; $\mathcal{H}^j(fg) = \sum_{i=0}^{j} \mathcal{H}^i f\ \mathcal{H}^{j-i} g$; a is root of f with multiplicity at least k iff $\mathcal{H}^i f(a) = 0$ for $i = 0, 1, ..., k-1$; and finally $\mathcal{H}^i \mathcal{H}^j = \binom{i+j}{i} \mathcal{H}^{i+j}$.

We are going to 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 $\hat{F}(X, Y, Z, \lambda) = F(\lambda X, \lambda Y, \lambda Z) = \lambda^n F(X, Y, Z)$, 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 $(x, y, z) \in \mathsf{GF}(q)^3$, 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 The Rédei polynomial and its derivatives

5.1 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 polynomial*s, 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 point set of $\mathsf{PG}(n, q)$, $S = \{\mathbf{P}_i = (a_i, b_i, ..., d_i) : i = 1, ..., |S|\}$.

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 point set with polynomials,

and if there is no 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 power sum polynomial, which is the $(q-1)$-th power sum of them.

Definition 5.1. *The* **Rédei-polynomial** *of the point set S is defined as follows:*

$$R^S(X,Y,...,T) = R(X,Y,...,T) := \prod_{i=1}^{|S|}(a_iX + b_iY + ... + d_iT) = \prod_{i=1}^{|S|}\mathbf{P}_i \cdot \mathbf{V}.$$

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 point sets S_1 and S_2, for their intersection

$$R^{S_1\cap S_2}(X,Y,...,T) = \gcd\Big(R^{S_1}(X,Y,...,T)\ ,\ R^{S_2}(X,Y,...,T)\Big)$$

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 5.2. *The* **power sum 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 $G(x,y,...,t) = |S| - m$ modulo the characteristic; (in other words, all m-secant hyperplanes will be solutions of $G(X,Y,...,T) - |S| + m = 0$).

The advantage of the power sum 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 point set (S can be reconstructed from it), the power sum polynomial of two different point sets may coincide. This is a hard task in general to classify all the point sets belonging to one given power sum polynomial.

The power sum polynomial of the intersection of two point sets does not seem to be easy to calculate; the power sum polynomial of the union of two point sets is the sum of their power sum polynomials.

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

$$R^{M(S)}(\mathbf{V}) = \prod_{i=1}^{|S|}(M\mathbf{P}_i)\cdot\mathbf{V} = \prod_{i=1}^{|S|}\mathbf{P}_i\cdot(M^\top\mathbf{V}) = R^S(M^\top\mathbf{V}).$$

For a field automorphism σ, $R^{\sigma(S)}(\mathbf{V}) = (R^S)^{(\sigma)}(\mathbf{V})$, which is the polynomial R^S but all coefficients are changed for their image under σ.

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

The following statement establishes a further connection between the Rédei polynomial and the power sum polynomial.

Lemma 5.3. (Gács) *For any set S,*

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

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

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

Definition 5.4. *The* **Rédei-polynomial** *of S is defined as follows:*

$R(X,Y,Z) =$

$\prod_{i=1}^{|S|}(a_iX+b_iY+c_iZ) = \prod_{i=1}^{|S|}\mathbf{P}_i\cdot\mathbf{V} = r_0(Y,Z)X^{|S|} + r_1(Y,Z)X^{|S|-1} + ... + r_{|S|}(Y,Z)$.

For each $j=0,...,|S|$, $r_j(Y,Z)$ is a homogeneous polynomial in two variables, either of total degree j precisely, or (for example when $0\le j\le N_X-1$) 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 5.5. *Note that if $m = 1$, i.e. $[x, y, z]$ is a tangent line at some $(a_t, b_t, c_t) \in S$, 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 $a_tX + b_tY + c_tZ$.*

As an example we mention the following.

Result 5.6. *Let S be the point set of the conic $X^2 - YZ$ in $\mathsf{PG}(2, q)$. Then $G^S(X, Y, Z) = X^{q-1}$ if q is even and $G^S(X, Y, Z) = (X^2 - 4YZ)^{\frac{q-1}{2}}$ if q is odd.* One can read out the geometrical behaviour of the conic with respect to lines, and the difference between the even and the odd case.

I found the following formula amazing.

Result 5.7. *Let S be the point set of the conic $X^2 - YZ$ in $\mathsf{PG}(2, q)$. Then*

$$R^S(X, Y, Z) = Y \prod_{t \in \mathsf{GF}(q)} (tX + t^2Y + Z) = Y(Z^q + Y^{q-1}Z - C_{\frac{q-1}{2}} Y^{\frac{q-1}{2}} Z^{\frac{q+1}{2}} -$$

$$-C_{\frac{q-3}{2}} X^2 Y^{\frac{q-3}{2}} Z^{\frac{q-1}{2}} - C_{\frac{q-5}{2}} X^4 Y^{\frac{q-5}{2}} Z^{\frac{q-3}{2}} - ... - C_1 X^{q-3} Y Z^2 - C_0 X^{q-1} Z),$$

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

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

This is the **affine Rédei polynomial**. Its coefficient-polynomials are $r_j(Y) = \sigma_j(\{b_iY + c_i : i = 1, ..., |S|\})$, elementary symmetric polynomials of the linear terms $b_iY + c_i$, each belonging to an 'affine' point (b_i, c_i). In fact, substituting $y \in \mathsf{GF}(q)$, $b_iy + c_i$ 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) $[0, 1, 0]$.

5.2 "Differentiation" in general

Here we want to introduce some general way of "differentiation". Give each point $\mathbf{P}_i$ the weight $\mu(\mathbf{P}_i) = \mu_i$ for $i = 1, ..., |S|$. Define the curve

$$R'_\mu(X, Y, Z) = \sum_{i=1}^{|S|} \mu_i \frac{R(X, Y, Z)}{a_iX + b_iY + c_iZ}. \qquad (*)$$

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

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

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

(c) Let $[x,y,z]$ be an m-secant with $[x,y,z] \cap [1,0,0] \notin S$. 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 $\sum_{i \notin \{t_1,...,t_m\}} \mu_i \frac{R(X,Y,1)}{a_i X + b_i Y + c_i}$ 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

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

Here $\frac{R(X,Y,1)}{R^{S \cap [0,0,1]}(X,Y,1)}$ is non-zero in $(0,0,1)$. Each term $\frac{R^{S \cap [0,0,1]}(X,Y,1)}{a_{t_j} X + b_{t_j} Y}$ 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.

(b) As $R_\mu^{S \cap [0,0,1]\ \prime}(X,Y,1)$ is a homogeneous polynomial in X and Y, of total degree $(m-1)$, $(0,0,1)$ is of multiplicity exactly $(m-1)$ on $R(X,Y,1)$, unless $R_\mu^{S \cap [0,0,1]\ \prime}(X,Y,Z)$ happens to vanish identically.

Consider the polynomials $\frac{R^{S \cap [0,0,1]}(X,Y,1)}{a_{t_j} X + b_{t_j} Y}$. They are m homogeneous polynomials in X and Y, of total degree $(m-1)$. Form an $m \times m$ matrix M from the coefficients. If we suppose that $a_{t_j} = 1$ for all $\mathbf{P}_{t_j} \in S \cap [0,0,1]$ then the coefficient of $X^{m-1-k} Y^k$ in $\frac{R^{S \cap [0,0,1]}(X,Y,1)}{a_{t_j} X + b_{t_j} Y}$, so m_{jk} is $\sigma_k(\{b_{t_1}, ..., b_{t_m}\} \setminus \{b_{t_j}\})$ for $j = 1, ..., m$ and $k = 0, ..., m-1$. So M is the elementary symmetric matrix (see in Section 7 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 $R_\mu^{S \cap [0,0,1]\ \prime}(X,Y,1) = 0$ 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 $R'_\mu(X,Y,Z)$ at (x,y,z) we have to look at $R'_\mu(X,y,z)$ and find out the multiplicity of the root $X=x$. As before, for each term of $\sum_{i\notin\{t_1,\dots,t_m\}}\mu_i\frac{R(X,y,z)}{a_iX+b_iy+c_iz}$ this multiplicity is m, while for the other terms we have

$$\sum_{i\in\{t_1,\dots,t_m\}}\mu_i\frac{R(X,y,z)}{a_iX+b_iy+c_z}=\frac{R(X,y,z)}{R^{S\cap[x,y,z]}(X,y,z)}\sum_{j=1}^{m}\mu_{t_j}\frac{R^{S\cap[x,y,z]}(X,y,z)}{a_{t_j}X+b_{t_j}y+c_{t_j}z}.$$

Here $\frac{R(X,y,z)}{R^{S\cap[x,y,z]}(X,y,z)}$ is non-zero at $X=x$. Now $R^{S\cap[x,y,z]}(X,y,z)=\prod_{j=1}^{m}a_{t_j}X+b_{t_j}y+c_{t_j}z$.

Each term $\frac{R^{S\cap[x,y,z]}(X,y,z)}{a_{t_j}X+b_{t_j}y+c_{t_j}z}$ is of (X-)degree at most $m-1$. We do know that the degree of $\sum_{j=1}^{m}\mu_{t_j}\frac{R^{S\cap[x,y,z]}(X,y,z)}{a_{t_j}X+b_{t_j}y+c_{t_j}z}$ 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 $\frac{\mu_{t_j}}{a_{t_j}}$ 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 look at the case when all $\mu(\mathbf{P})=1$.
Consider

$$R'_1=\sum_{\mathbf{b}\in B}\frac{R(X,Y,Z)}{b_1X+b_2Y+b_3Z}=\sigma_{|B|-1}(\{b_1X+b_2Y+b_3Z:\mathbf{b}\in B\}).$$

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 $\partial^1_X R=\sum_{\mathbf{b}\in B\setminus L_X}\frac{R(X,Y,Z)}{b_1X+b_2Y+b_3Z}$, 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 tangent line $[x,y,z]$, with $B\cap[x,y,z]=\{\mathbf{a}\}$, into R_1 we get $R_1(x,y,z)=\prod_{\mathbf{b}\in B\setminus\{\mathbf{a}\}}(b_1x+b_2y+b_3z)$, 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 $m-1$.

5.3 Hasse derivatives of the Rédei polynomial

The next theorem is about Hasse derivatives of $R(X,Y,Z)$. (For its properties see Section 4.3.)

Theorem 5.9. *(1) Suppose $[x,y,z]$ is an r-secant line of S with $[x,y,z]\cap S=\{(a_{s_l},b_{s_l},c_{s_l}):l=1,...,r\}$. Then $(\mathcal{H}_X^i\mathcal{H}_Y^j\mathcal{H}_Z^{r-i-j}\ R)(x,y,z)=$*

$$\bar{R}(x,y,z)\cdot\sum_{\substack{m_1<m_2<...<m_i\\ m_{i+1}<...<m_{i+j}\\ m_{i+j+1}<...<m_r\\ \{m_1,...,m_r\}=\{1,2,...,r\}}} a_{s_{m_1}}a_{s_{m_2}}...a_{s_{m_i}}b_{s_{m_{i+1}}}...b_{s_{m_{i+j}}}c_{s_{m_{i+j+1}}}...c_{s_{m_r}},$$

where $\bar{R}(x,y,z)=\prod_{l\notin\{s_1,...,s_r\}}(a_lx+b_ly+c_lz)$, a non-zero element, independent from i and j.

(2) From this we also have

$$\sum_{0\le i+j\le r}(\mathcal{H}_X^i\mathcal{H}_Y^j\mathcal{H}_Z^{r-i-j}\ R)(x,y,z)X^iY^jZ^{r-i-j}=\bar{R}(x,y,z)\prod_{l=1}^{r}(a_{s_l}X+b_{s_l}Y+c_{s_l}Z),$$

constant times the Rédei polynomial belonging to $[x,y,z]\cap S$.

(3) If $[x,y,z]$ is a $(\ge r+1)$-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 $(\ge r+1)$-secant iff for all $i_1,i_2,i_3, 0\le i_1+i_2+i_3\le r$ 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

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

vanishes for each $[x,y,z]$ $(\ge r)$-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

$$(\nabla R)(x,y,z)=(\ (\partial_XR)(x,y,z),\ (\partial_YR)(x,y,z),\ (\partial_ZR)(x,y,z)\ )=(a_t,b_t,c_t).$$

If $[x,y,z]$ is a (≥ 2)-secant, then $(\nabla R)(x,y,z)=\mathbf{0}$. Moreover, $[x,y,z]$ is a (≥ 2)-secant iff $(\nabla R)(x,y,z)=\mathbf{0}$.

Proof: (1) comes from the definition of Hasse derivation and from $a_{s_l}x + b_{s_l}y + c_{s_l}z = 0; l = 1, ..., r$. In general $(\mathcal{H}_X^{i_1}\mathcal{H}_Y^{i_2}\mathcal{H}_Z^{i_3}\ R)(X, Y, Z) =$

$$\sum_{\substack{m_1<m_2<\ldots<m_{i_1}\\ m_{i_1+1}<\ldots<m_{i_1+i_2}\\ m_{i_1+i_2+1}<\ldots<m_{i_1+i_2+i_3}\\ |\{m_1,\ldots,m_{i_1+i_2+i_3}\}|=i_1+i_2+i_3}} a_{m_1}a_{m_2}\ldots a_{m_{i_1}}b_{m_{i_1+1}}\ldots b_{m_{i_1+i_2}}c_{m_{i_1+i_2+1}}\ldots c_{m_{i_1+i_2+i_3}}\prod_{i\notin\{m_1,\ldots,m_{i_1+i_2+i_3}\}} a_iX+b_iY+c_iZ).$$

(2) follows from (1). For (3) observe that after the "r-th derivation" of R still remains a term $a_{s_i}x + b_{s_i}y + c_{s_i}z = 0$ 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 $\prod_{l=1}^{r}(a_{s_l}X + b_{s_l}Y + c_{s_l}Z)$ 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 $\prod_{l=1}^{r}(a_{s_l}x + b_{s_l}y + c_{s_l}z) = 0$.
Or: in the case of a tangent line

$$\nabla R = \sum_{j=1}^{|S|} \nabla(\mathbf{P}_j \cdot \mathbf{V}) \prod_{i\neq j} \mathbf{P}_i \cdot \mathbf{V} = \sum_{j=1}^{|S|} \mathbf{P}_j \prod_{i\neq j} (\mathbf{P}_i \cdot \mathbf{V}).$$ ∎

6 Univariate representations

Here we describe the analogue of the Rédei polynomial for the big field representations.

6.1 The affine polynomial and its derivatives

After the identification $\mathsf{AG}(n, q) \leftrightarrow \mathsf{GF}(q^n)$, described in Section 3, for a subset $S \subset \mathsf{AG}(n, q)$ 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*

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

Here σ_k and $\hat{\sigma}_k$ denote the k-th elementary symmetric polynomial of the set S and $\{(X - s)^{q-1} : s \in S\}$, 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 θ_{n-1}-th roots of unity, moreover, $(x-s_1)^{q-1}=(x-s_2)^{q-1}$ 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 $\mathsf{GF}(q^n)$ are Frobenius-automorphisms $x\mapsto x^{q^m}$ for $i=0,1,...,n-1$, and each of them induces a linear transformation of $\mathsf{AG}(n,q)$. Any linear combination of them, with coefficients from $\mathsf{GF}(q^n)$, can be written as a polynomial over $\mathsf{GF}(q^n)$, 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 $\mathsf{AG}(n,q)$. What's more, the converse is also true: all linear transformations of $\mathsf{AG}(n,q)$ 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 $\mathsf{GF}(q)$ and linearized polynomials of form $c_0X+c_1X^q+c_2X^{q^2}+...+c_{n-1}X^{q^{n-1}}, c_i\in\mathsf{GF}(q^n)$ is $(q^n)^n$.

Proposition 6.1. *(i) The root polynomial of a k-dimensional subspace of $\mathsf{AG}(n,q)$ containing the origin, is a linearized polynomial of degree q^k;*

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

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

$$B(X)=\prod_{s\in S}(1-sX)=\sum_k(-1)^k\sigma_kX^k;$$

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

For the characteristic function χ 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 $BB'\equiv B^2\chi'$.

7 Symmetric polynomials

7.1 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 [111].

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

Definition 7.1. The *k-th elementary symmetric polynomial* of the variables $X_1, ..., X_t$ is defined as

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

σ_0 is defined to be 1 and for $j > t$ $\sigma_j = 0$, identically.

Given a (multi)set $A = \{a_1, a_2, ..., a_t\}$ 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 7.2. The *k-th power sum* of the variables $X_1, ..., X_t$ is defined as

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

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 $\{a_1, ..., a_t\}$. Note also that in the previous formula the binomial coefficient may vanish, and in this case it "hides" π_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.

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

If A is an additive subgroup of $\mathsf{GF}(q)$ of size p^k: $\sigma_j(A) = 0$ whenever $p \not| j < q-1$ holds. Also $\pi_j(A) = 0$ for $j = 1, ..., p^k - 2, p^k$.

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

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

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:

$$k\sigma_k = \pi_1\sigma_{k-1} - \pi_2\sigma_{k-2} + ... + (-1)^{i-1}\pi_i\sigma_{k-i} + ... + (-1)^{k-1}\pi_k\sigma_0 \qquad \text{(N1)}$$

and

$$\pi_{t+k} - \pi_{t+k-1}\sigma_1 + ... + (-1)^i\pi_{t+k-i}\sigma_i + ... + (-1)^t\pi_k\sigma_t = 0. \qquad \text{(N2)}$$

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

$$\sum_{i=0}^{k}(-1)^i\pi_i\sigma_{k-i} = 0. \qquad \text{(N3)}$$

One may 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 $\prod_i(X + a_iY + b_i)$ by X, the coefficient polynomials will be of the form $\sigma_k(\{a_iY + b_i : i\})$.

Result 7.3. *Expanding the Rédei-polynomial*

$$\prod_{a\in \mathsf{GF}(q)} (X - aY - f(a)) = \sum_{k=0}^{q} r_k(Y) X^{q-k},$$

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

* * *

There are some determinant formulae being intimately connected to symmetric polynomials. Given $S = \{x_1, x_2, ..., x_n\}$, the following determinant is called the **Vandermonde-determinant** of S:

$$VdM(x_1, x_2, ..., x_n) = \begin{vmatrix} 1 & 1 & ... & 1 \\ x_1 & x_2 & ... & x_n \\ x_1^2 & x_2^2 & ... & x_n^2 \\ \vdots & & & \\ x_1^{n-1} & x_2^{n-1} & ... & x_n^{n-1} \end{vmatrix} = \prod_{i<j} (x_i - x_j)$$

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

$$MRD_P(x_1, ..., x_n) = \begin{vmatrix} x_1 & x_2 & ... & x_n \\ x_1^P & x_2^P & ... & x_n^P \\ x_1^{P^2} & x_2^{P^2} & ... & x_n^{P^2} \\ \vdots & & & \\ x_1^{P^{n-1}} & x_2^{P^{n-1}} & ... & x_n^{P^{n-1}} \end{vmatrix} = \prod_{(\lambda_1,...,\lambda_n)\in \mathsf{PG}(n-1,P)} \sum_{i=1}^{n} \lambda_i x_i$$

Note that this formula gives the value of the determinant up to a non-zero constant only, but usually we ask whether det = 0 or not.

The **elementary symmetric determinant** of S is

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

One may give a unified proof for the determinant formulae, considering $x_1, ..., x_n$ as free variables. Note that (a) $VdM(x_1, x_2, ..., x_n) \neq 0$ iff $\{x_1, ..., x_n\}$ are pairwise distinct; (b) $MRD_{p^e}(x_1, x_2, ..., x_n) \neq 0$ iff $\{x_1, ..., x_n\}$ are independent over $\mathsf{GF}(p^e)$.

Result 7.4. *The following general form of the elementary symmetric determinant can be defined: Given* $S = \{x_1, x_2, ..., x_n, x_{n+1}, ..., x_m\}$,

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

so somehow the elements $x_{n+1}, ..., x_m$ *"do not count".*

Result 7.5. *We have (folklore, Ball)*

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

$$= \begin{vmatrix} T & X_1 & X_2 & ... & X_{n-1} & 1 \\ T^q & X_1^q & X_2^q & ... & X_{n-1}^q & 1 \\ T^{q^2} & X_1^{q^2} & X_2^{q^2} & ... & X_{n-1}^{q^2} & 1 \\ \vdots & & & & & \\ \vdots & & & & & \\ T^{q^n} & X_1^{q^n} & X_2^{q^n} & ... & X_{n-1}^{q^n} & 1 \end{vmatrix} \Bigg/ \begin{vmatrix} X_1 & X_2 & ... & X_{n-1} & 1 \\ X_1^q & X_2^q & ... & X_{n-1}^q & 1 \\ X_1^{q^2} & X_2^{q^2} & ... & X_{n-1}^{q^2} & 1 \\ \vdots & & & & \\ X_1^{q^{n-1}} & X_2^{q^{n-1}} & ... & X_{n-1}^{q^{n-1}} & 1 \end{vmatrix}.$$

8 Basic facts about algebraic curves

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 8.1. (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* $\bar{\mathbb{F}}$ *always equality holds.* ∎

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

Theorem 8.2. Hasse-Weil, Serre *For an absolutely irreducible non-singular algebraic curve* $f \in \mathsf{GF}(q)[X, Y, Z]$ *of degree* n *we have*

$$|N_q(f) - (q+1)| \le g\lfloor 2\sqrt{q} \rfloor \le (n-1)(n-2)\sqrt{q}.$$

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 $\mathsf{GF}(q) \subset \mathsf{GF}(q_1)$ we have $N_q(f) \leq N_{q_1}(f)$.

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

Result 8.3. *For an absolutely irreducible algebraic curve $f \in \overline{\mathsf{GF}(q)}[X,Y,Z]$ of degree n, that cannot be defined over $\mathsf{GF}(q)$, 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 8.4. Stöhr-Voloch [100] *For an irreducible algebraic curve $f \in \mathsf{GF}(q)[X,Y,Z]$, $q = p^h$, of degree n with N_q rational points over $\mathsf{GF}(q)$ 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 $N_p \leq 2n(n-2) + \frac{2}{5}np$;
(iv) if $q = p$, $3 \leq n \leq \frac{1}{2}p$ and f has s double points then $N_p \leq \frac{2}{5}n(5(n-2) + p) - 4s$.

In (i) the condition is automatically satisfied if $q = p$ is a prime.

As an illustration one can prove the following statement easily.

Result 8.5. *Let $f(X)$ be a polynomial of degree at most $\sqrt[4]{q}$, (q odd), which assumes square elements of $\mathsf{GF}(q)$ only. Then $f = g^2$ for a suitable polynomial $g(X)$.*

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

Result 8.6. Barlotti-bound *If a curve of degree n has no linear factors over $\mathsf{GF}(q)$ then $N_q \leq (n-1)q+n$. In fact, if a point set of $\mathsf{PG}(2,q)$ intersects every line in at most n points then it has at most $(n-1)q+n$ points.*

Proposition 8.7. [SzPnopts] *A curve of degree n defined over $\mathsf{GF}(q)$,* without linear components, *has always $N_q \leq (n-1)q+\frac{n}{2}$ points in $\mathsf{PG}(2,q)$.*

Sketch of the proof: let k be maximal such that every tangent of the curve contains at least k points of the the curve (counting without multiplicity, in $\mathsf{PG}(2,q)$). Easy to see that (i) $N_q \leq (n-1)q+k$; (ii) $N_q \leq (n-1)q+(n-k)$.∎

In [SzPnopts] I conjectured the following, which was later called by Kim and Homma "the Sziklai Conjecture":

~~**Conjecture**~~ **8.8.** [SzPnopts]*: We conjecture that a curve of degree n defined over $\mathsf{GF}(q)$,* without linear components, *has always $N_q \leq (n-1)q+1$ points in $\mathsf{PG}(2,q)$.*

I also mentioned that for $n = 2, \sqrt{q}+1, q-1$ it would be sharp as the curves $X^2 - YZ, X^{\sqrt{q}+1} + Y^{\sqrt{q}+1} + Z^{\sqrt{q}+1}$ 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*, for some histrorical reason.

Note that it is very easy to prove the conjecture in the following cases:

(i) if there exists a line skew to the curve and $(q,n)=1$;

(ii) if $n \leq \sqrt{q}+1$ then $q+1+(n-1)(n-2)\sqrt{q} \leq nq-q+1$ proves it by Weil's bound Theorem 8.2;

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

(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 $C_1 \cup C_2 \cup ... \cup C_k$ with degrees $n_1, ..., n_k$; 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 $n_j q - q + 1$ points. By Result 8.3 C_j can be defined over $\mathsf{GF}(q)$ and Weil does its job again.
For (iii) the Barlotti-bound, recounted looking around from a singular point, will work. ∎

In a series of three papers, recently Homma and Kim proved the conjecture ([72, 73, 74]), except for the case $q=4$, $f = X^4 + Y^4 + Z^4 + X^2Y^2 +$

$Y^2Z^2 + Z^2X^2 + X^2YZ + XY^2Z + XYZ^2 = 0$ for which it is false (i.e. this is the unique counterexample, it has 14 $\mathsf{GF}(4)$-rational points). They also found out, what neither me, nor other experts of the field had known, that Proposition 8.7 had been known by Segre many years before (see [94].).

The following lemma is a generalization of a result by Szőnyi. For $d = 1$ it can be found in Sziklai [SzPdpow], which is a variant of a lemma by Szőnyi [104].

Lemma 8.9. *Let $\mathcal{C}_n$, $1 \leq d < n$ be a curve of order n defined over $\mathsf{GF}(q)$, not containing a component defined over $\mathsf{GF}(q)$ of degree $\leq d$. Denote by N the number of points of $\mathcal{C}_n$ in $\mathsf{PG}(2,q)$. 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 $\alpha > \frac{1}{d+1} + \frac{1+d(d-1)\sqrt{q}}{(d+1)q}$, $n < \alpha\sqrt{q} - d + 2$, $N < \alpha nq$. Here $\alpha = \frac{1}{d}$ can be written (that is often needed) when $d \leq \sqrt[6]{q}$.

Proof: Suppose first that $\mathcal{C}_n$ is absolutely irreducible. Then Weil's theorem ([113], [65]) 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 $\mathcal{C}_n$ is not absolutely irreducible, then it can be written as $\mathcal{C}_n = \mathcal{D}_{i_1} \cup ... \cup \mathcal{D}_{i_s}$, where $\mathcal{D}_{i_j}$ is an absolutely irreducible component of order i_j, so $\sum_{j=1}^{s} i_j = n$. If $\mathcal{D}_{i_j}$ can not be defined over $\mathsf{GF}(q)$, then it has at most $N_{i_j} \leq (i_j)^2 \leq i_j(q+1)\alpha$ points in $\mathsf{PG}(2,q)$ (see Ex. 8.3). If $\mathcal{D}_{i_j}$ is defined over $\mathsf{GF}(q)$, then the Weil-bound implies again that $N_{i_j} \leq i_j(q+1)\alpha$. Hence

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

For applications see Section 9, Theorem 13.1, Theorem 13.2 and Theorem 13.7.

Result 8.10. *If $q = p$ is prime and $\alpha > \frac{2}{5}$ then in the theorem above $n \leq (\frac{1}{2}\alpha - \frac{1}{5})p + 2$ is enough for $N \leq n(p+1)\alpha$.*

9 Finding the missing factors, removing the surplus factors

Here we treat a very general situation, with several applications in future.

Given $A = \{a_1, ..., a_{q-\varepsilon}\} \subset \mathsf{GF}(q)$, 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"

$\{a_{q-\varepsilon+1}, ..., a_q\} = \mathsf{GF}(q) \setminus A$, 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

$$\sigma_j = \sigma_j(A), \quad \sigma_k^* = \sigma_k(\mathsf{GF}(q) \setminus A),$$

we get $X^q - X =$

$(X^{q-\varepsilon} - \sigma_1 X^{q-\varepsilon-1} + \sigma_2 X^{q-\varepsilon-2} - ... \pm \sigma_{q-\varepsilon-1} X \mp \sigma_{q-\varepsilon})(X^\varepsilon - \sigma_1^* X^{\varepsilon-1} + \sigma_2^* X^{\varepsilon-2} - ... \pm \sigma_{\varepsilon-1}^* X \mp \sigma_\varepsilon^*)$,

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

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

Note that we do not need to use all the coefficients/equations, it is enough to do it for $j = 1, ..., \varepsilon$. (The further equations can be used as consequences of the fact that the a_i-s are pairwise distinct, there are results making profit from it.)

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 $B = \{b_1, ..., b_{q+\varepsilon}\} \supset \mathsf{GF}(q)$ be a multiset of elements of $\mathsf{GF}(q)$, and let $F(X) = \prod_{i=1}^{q+\varepsilon}(X - b_i)$ be their root polynomial. We would like to find the "surplus elements" $\{b_{k_1}, ..., b_{k_\varepsilon}\} = B \setminus \mathsf{GF}(q)$, or, equivalently, $\bar{G}(X) = \prod_{i=1}^{\varepsilon}(X - b_{k_i})$. Obviously, $\bar{G}(X) = \frac{F(X)}{X^q - X}$, so $F(X) = (X^q - X)\bar{G}(X)$. Suppose that $\varepsilon \leq q-2$. Expanding this equation and introducing the elementary symmetric polynomials

$$\sigma_j = \sigma_j(B), \quad \bar{\sigma}_k = \sigma_k(B \setminus \mathsf{GF}(q)),$$

we get $X^{q+\varepsilon} - \sigma_1 X^{q+\varepsilon-1} + \sigma_2 X^{q+\varepsilon-2} - ... \pm \sigma_{\varepsilon-1} X^{q+1} \mp \sigma_\varepsilon X^q \pm ...$
$... \pm \sigma_{q+\varepsilon-1} X \mp \sigma_{q+\varepsilon} = (X^q - X)(X^\varepsilon - \bar{\sigma}_1 X^{\varepsilon-1} + \bar{\sigma}_2 X^{\varepsilon-2} - ... \pm \bar{\sigma}_{\varepsilon-1} X \mp \bar{\sigma}_\varepsilon) =$

$= X^{q+\varepsilon} - \bar{\sigma}_1 X^{q+\varepsilon-1} + \bar{\sigma}_2 X^{q+\varepsilon-2} - ... \pm \bar{\sigma}_{\varepsilon-1} X^{q+1} \mp \bar{\sigma}_\varepsilon X^q +$ terms of lower degree.

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

$$\bar{\sigma}_k = \sigma_k \text{ for all } k = 1, ..., \varepsilon. \tag{2}$$

Note that if $\varepsilon \geq q-1$ then it's slightly more complicated.

* * *

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 $S \subseteq \mathsf{GF}(q)$ such that for each $y \in S$ the set $A_y = \{c_iy + d_i : i\}$ consists of pairwise distinct elements of $\mathsf{GF}(q)$, or, similarly, the multiset $B_y = \{c_iy + d_i : i\}$ contains $\mathsf{GF}(q)$. Then the σ_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 ε lines. So first we define $\sigma_k^*(y)$ (or $\bar{\sigma}_k(y)$, resp.), meaning the coefficient of $X^{\varepsilon-k}$ in $\bar{G}_y(X)$ 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 σ_k^*-s or $\bar{\sigma}_k$-s are still valid. So one may define the polynomials analogously to (1):

$\sigma_1^*(Y) \stackrel{\text{def}}{=} -\sigma_1(Y)$; $\sigma_2^*(Y) \stackrel{\text{def}}{=} \sigma_1^2(Y) - \sigma_2(Y)$;
$\sigma_3^*(Y) \stackrel{\text{def}}{=} -\sigma_1^3(Y) + 2\sigma_1(Y)\sigma_2(Y) - \sigma_3(Y)$; etc.
or analogously to (2):

$$\bar{\sigma}_k(Y) \stackrel{\text{def}}{=} \sigma_k(Y) \text{ for all } k = 1, ..., \varepsilon$$

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

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

Now we can define the algebraic curve

$$G^*(X,Y) \stackrel{\text{def}}{=} X^\varepsilon - \sigma_1^*(Y)X^{\varepsilon-1} + \sigma_2^*(Y)X^{\varepsilon-2} - ... \pm \sigma_{\varepsilon-1}^*(Y)X \mp \sigma_\varepsilon^*(Y)$$

or in the other case

$$\bar{G}(X,Y) \stackrel{\text{def}}{=} X^\varepsilon - \bar{\sigma}_1(Y)X^{\varepsilon-1} + \bar{\sigma}_2(Y)X^{\varepsilon-2} - ... \pm \bar{\sigma}_{\varepsilon-1}(Y)X \mp \bar{\sigma}_\varepsilon(Y).$$

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 $\mathsf{GF}(q) \times \mathsf{GF}(q)$: for any $y \in S$ we have ε solutions of $G^*(X, y) = 0$, i.e. the ε 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 ε_i points, counted with intersection multiplicity. So the number of points on G_i is at least $\varepsilon_i|S| - \varepsilon_i(\varepsilon_i - 1)$, where the second term 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 8.9 (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 ε in our case, is small enough, i.e. if $\varepsilon < \sqrt{q}$ and $|S| > \max\{\frac{\varepsilon - 1 + \sqrt[4]{q}}{\sqrt{q}}, \frac{1}{2}\} \cdot (q + 1)$ in the first and $|S| > \max\{\frac{\varepsilon - 1 + \sqrt[4]{q}}{\sqrt{q}}, \frac{1}{2}\} \cdot (q + 1) + \varepsilon - 1$ in the second case.

It means, that one can add ε linear polynomials $\alpha_i Y + \beta_i$ in the first case such that for any $y \in S$, the values $\{c_i y + d_i\} \cup \{\alpha_j y + \beta_j\} = \mathsf{GF}(q)$. In the second case we have a weaker corollary: for any $y \in S$, the values $\{c_i y + d_i\} \setminus \{\alpha_j y + \beta_j\} = \mathsf{GF}(q)$, which means that adding the new lines $\alpha_j Y + \beta_j$ "with multiplicity$= -1$" then $S \times \mathsf{GF}(q)$ 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 $S \times \mathsf{GF}(q)$ usually have some concrete meaning when applying this technique; this work contains some applications, see Theorem 13.4, Section 14, 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.

Result 9.1. *Using the second ("surplus") case above one can prove (Szőnyi) that a blocking set $B \subset \mathsf{PG}(2, q)$ with $|B \cap \mathsf{AG}(2, q)| = q + 1$ affine points always contains a(n affine) point that is unnecessary (i.e. it can be deleted without violating the blocking property).*

Result 9.2. *Let $f_i(T)$, $i = 1, ..., q - \varepsilon$ be polynomials of degree at most d, and suppose that their graphs $\{(t, f_i(t)) : t \in \mathsf{GF}(q)\}$ are pairwise distinct. Easy to prove that if $\varepsilon < c\sqrt{q}$ then one can find $f_{q-\varepsilon+1}(T), ..., f_q(T)$, each of degree at most d such that the graphs of these q polynomials partition the affine plane.*

Result 9.3. *Let $f_i(T)$, $i = 1, ..., q - \varepsilon$ be polynomials, each from a subspace U of $\mathsf{GF}(q)[T]$ with $1 \in U$, and suppose that their graphs $\{(t, f_i(t)) : t \in \mathsf{GF}(q)\}$ are pairwise distinct. One can prove that if ε is small enough then one can find $f_{q-\varepsilon+1}(T), ..., f_q(T)$, each from U, such that the graphs of these q polynomials partition the affine plane.*

10 Prescribing the intersection numbers with lines

Suppose that a function $m : \mathcal{L} \to \mathbb{N}$ is given, where $\mathcal{L}$ is the set of lines of $\mathsf{PG}(2,q)$. The problem is to find conditions, necessary and/or sufficient, under which we can find a point set 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 $\mathsf{PG}(2,q)$, $\mathbf{m} = (m(\ell_1), m(\ell_2), ..., m(\ell_{q^2+q+1}))$ is the weight-vector, then the problem is reduced to finding a ("characteristic vector") $\mathbf{v}$ such that $A\mathbf{v} = \mathbf{m}$. It is quite natural to write A in a symmetric form (i.e. indexing the rows and columns with homogeneous triples from $\mathsf{GF}(q)$ in the same order). As A is non-singular, we have $\mathbf{v} = A^{-1}\mathbf{m}$. Now one can turn the question around: for which $\mathbf{m}$ will $\mathbf{v}$ be of the required type, for example a non-negative, integer or 0-1 vector?

It is easy to compute that

$$A^{-1} = \frac{1}{q}A^T - \frac{1}{q(q+1)}J = \frac{1}{q}A - \frac{1}{q(q+1)}J \text{ and } JA = (q+1)J, \text{ so } A^2 - J - qI = 0.$$

Hence we also know that the eigenvalues of A are $q+1$, $\sqrt{q}$ and $-\sqrt{q}$.

In most cases $\mathbf{m}$ 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 $\mathbf{v}$ satisfying $A\mathbf{v} \in M$.

10.1 Sets with constant intersection numbers mod p

In [25, 31] the following is proved:

Proposition 10.1. *Let S be a point set in $\mathsf{AG}(2,q)$, suppose that every line intersects S in 1 (mod p) points, or is completely disjoint from S. Then $|S| \le q - p + 1$.*

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 $\mathsf{AG}(2,q) \leftrightarrow \mathsf{GF}(q^2)$ 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 $x \in \mathsf{GF}(q^2)$ the value of $(x-s)^{q-1}$ depends on the direction of the line joining x and s. If $x \in S$ then every direction will occur with multiplicity divisible by p, hence all the points of S are roots of f, which is of degree $q-1$. The biggest value $\equiv 1 \bmod p$ 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 $\mathsf{AG}(2,q)$.

Note that in Proposition 10.1 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 point sets in $\mathsf{PG}(2,q)$ with 1 (mod p) -secants only, e.g. the plane itself, or a unital, etc.

Result 10.2. *(Blokhuis) The following generalization is true as well. Let S be a point set in $\mathsf{AG}(n,q)$, $n \geq 1$, and suppose that every hyperplane intersects S in 1 (mod p) points, or is completely disjoint from S. Then $|S| \leq q-p+1$.*

The situation is different if we consider the projective plane.

Theorem 10.3. *Given a point set $S = \{(a_i,b_i,c_i) : i = 1,...,s\} = \{(a_i,b_i,1) : i = 1,...,s_1\} \cup \{(a_j,b_j,0) : j = s_1+1,...,s\} \subseteq \mathsf{PG}(2,q)$, 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 $0 \leq k+l \leq q-1$, $\binom{k+l}{k} \neq 0 \bmod p$, we have $\sum_{i=1}^{|S|} a_i^{q-1-k-l}b_i^k c_i^l = 0$ (here $0^0 = 1$).

(iv) for all $0 \leq k+l \leq q-2$, $\binom{k+l}{k} \neq 0 \bmod p$, we have $\sum_{i=1}^{s_1} a_i^k b_i^l = 0$ and for all $0 \leq m \leq q-1$, $\sum_{i=1}^{s} a_i^{q-1-m}b_i^m = 0$.

Proof: Note that if each line intersects S in r mod p points then $|S| \equiv r$ (mod p). (Count $|S|$ from a point not in S) 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 $(a_ix+b_iy+c_iz)^{q-1}$ will be 1 in $G(x,y,z)$ hence $G(x,y,z) = 0$. As $\deg G \leq q-1$ we have (i)⇒(ii). One can turn it around: if $G(x,y,z) = 0$ then the number of terms $(a_ix+b_iy+c_iz)^{q-1}$ with nonzero (i.e. =1) value should be zero mod p, so (ii)⇒(i).

For the rest consider the coefficient of $X^{q-1-k-l}Y^kZ^l$ in G (for $0 \le k+l \le q-1$), it is

$$\binom{q-1}{k+l}\binom{k+l}{k}\sum_{i=1}^{|S|} a_i^{q-1-k-l}b_i^k c_i^l \;=\; 0$$

if (ii) holds and vice versa. Finally (iii)⇔(iv) is obvious. ∎

Many interesting point sets (small blocking sets, unitals, maximal arcs, even point sets, 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 refer here to Section 10.2, where this property is defined and examined, see Definition 10.4.)

Take the "affine" part of a Vandermonde-set, i.e. points with $c_i \neq 0$ (the rest does not count in the power sum) and suppose that all its points are written as $(a_i, b_i, 1)$. After the $\mathsf{AG}(2,q) \leftrightarrow \mathsf{GF}(q^2)$ identification this point becomes $a_i + b_i\omega$ for some generator ω of $\mathsf{GF}(q^2)$. Substituting $(1, \omega, Z)$ into G we get

$$0 = G(1,\omega,Z) = \sum_{(a_i,b_i,1)\in S} ((a_i+b_i\omega)+Z)^{q-1} + \sum_{(a_j,b_j,0)\in S} (a_j+b_j\omega)^{q-1} =$$

$$\sum_{k=0}^{q-2} \pm Z^{q-1-k} \sum_{(a_i,b_i,1)\in S} (a_i+b_i\omega)^k \quad + \quad \sum_{(a_i,b_i,c_i)\in S} (a_i+b_i\omega)^{q-1}$$

which means that the affine part of a (generalized) Vandermonde set, considered as a set in $\mathsf{GF}(q^2)$, has power sums equal to zero for exponents $1, ..., q-2$. (The last, constant term is just $G(1,\omega,0) = 0$.)

10.2 Vandermonde and super-Vandermonde sets

After Theorem 10.3 it is quite natural to examine sets with many vanishing power sums.

Definition 10.4. *Let $1 < t < q$. We say that $T = \{y_1, ..., y_t\} \subseteq \mathsf{GF}(q)$ is a* Vandermonde-set, *if $\pi_k = \sum_i y_i^k = 0$ for all $1 \le k \le t-2$.*

Vandermonde-sets were first defined and studied in [62]. This part is a generalization from [SzPvdm].

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 $p \not| t$ 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.)

In general, for a multiset S from a field, $w = w_S$ denotes the smallest positive integer k for which the power sum $\pi_k = \sum_{s \in S} s^k \neq 0$ if such k exists, otherwise $w = \infty$. We note that there exist sets for which the value w can be ∞, however in that case the set has to contain multiple elements, in fact we have $w = \infty \Leftrightarrow$ all the multiplicities are divisible by the characteristic p. Hence the Vandermonde (and the forthcoming super-Vandermonde) sets are extremal with respect to the value of w.

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

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ y_1 & y_2 & \dots & y_t \\ y_1^2 & y_2^2 & \dots & y_t^2 \\ \vdots & & & \\ y_1^{t-1} & y_2^{t-1} & \dots & y_t^{t-1} \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix},$$

it cannot result in the zero vector.

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

$$\begin{pmatrix} y_1 & y_2 & \dots & y_t \\ y_1^2 & y_2^2 & \dots & y_t^2 \\ \vdots & & & \\ y_1^{t-1} & y_2^{t-1} & \dots & y_t^{t-1} \\ y_1^t & y_2^t & \dots & y_t^t \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix},$$

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 $k = 1, ..., t-1$, 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 10.5. *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 the Vandermonde-property is characterized.

Proposition 10.6. *Let $T = \{y_1, ..., y_t\} \subseteq \mathsf{GF}(q)$. 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 $0 \leq t' \leq p-1$, $t' \equiv t \bmod p$);

(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 χ are the power sums of the set T, so (i) and (iii) are clearly equivalent. (i) $\Leftrightarrow$(iv) is similar. The equivalence of (i) and (ii) is an easy consequence of the Newton formulae relating power sums and elementary symmetric polynomials. ∎

Note that for the function χ 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 $p|t$ we have $g^p(Y) + Y$.)

And now we characterize the super-Vandermonde-property.

Proposition 10.7. *Let $T = \{y_1, ..., y_t\} \subseteq \mathsf{GF}(q)$. The following are equivalent*

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

(ii) the polynomial $f(Y) = \Pi_{i=1}^{t}(Y - y_i)$ is of the form $Y^{t'}g(Y)^p + c$ (where $0 \leq t' \leq p-1$, $t' \equiv t \bmod p$);

(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, mostly from [62].

Example 10.8. *Let q be a prime power.*

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

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

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

(iv) Let q be odd and consider the points of $\mathsf{AG}(2,q)$ as elements of $\mathsf{GF}(q^2)$ and a $q+1$-set $A = \{a_1, ..., a_{q+1}\}$ 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 $\mathsf{GF}(q^2)$.

Proof: (i) Suppose T is an additive subgroup of size t in $\mathsf{GF}(q)$. We want to prove that Proposition 10.6 (ii) is satisfied, that is $f(Y) = \Pi_{y\in T}(Y-y)$ has only terms of degree divisible by p, except for the term Y. If we prove that f is additive, hence $\mathsf{GF}(p)$-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 $\deg(r_t) \leq t-1$). 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 $\mathsf{GF}(q)$. Then the polynomial $f(Y) = \Pi_{i=1}^{t}(Y-y_i)$ is of the form $Y^t - 1$ so Proposition 10.7 (ii) is satisfied, we are done.
(iii) Let $\{x_1, ..., x_q\} \subseteq \mathsf{GF}(q^2)$ correspond to the affine part of the hyperoval $\mathcal{H}$ and ε_1 and ε_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 $x \notin \{x_1, ..., x_q\}$. There are $q^2 - q$ different choices for such an x, while the degree of χ is at most $q-2$, so $\chi(X) \equiv \varepsilon_1 + \varepsilon_2$ identically (that is, all coefficients of χ are zero except for the constant term), so by Proposition 10.6 (iv), we are done.

(iv) A short proof is that by Segre's theorem such a point set is a conic if q is odd, so affine equivalent to the "unit circle" $\{\alpha \in \mathsf{GF}(q^2) : a^{q+1} = 1\}$, which is a multiplicative subgroup. ∎

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

Note that Proposition 10.6 (iv) implies that if $T \subseteq \mathsf{GF}(q_1) \leq \mathsf{GF}(q_2)$ then T is a Vandermonde-set in $\mathsf{GF}(q_1)$ if and only if it is a Vandermonde-set in $\mathsf{GF}(q_2)$.

Result 10.9. *Let $B \subset \mathsf{PG}(2, q)$ be a point set, $|B| = q + k$, with every intersection number being $1 \mod p$ and suppose that $B \cap \ell_\infty = k$. One can see that $B \setminus \ell_\infty \subset \mathsf{AG}(2, q)$, considered as a subset of $\mathsf{GF}(q^2)$, 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 Rédei type, is always a (translate of a) subspace of $\mathsf{GF}(q^2)$, considered as a vectorspace over a suitable subfield (hence an additive subgroup of $\mathsf{GF}(q^2)$); see Theorem 11.5.

There are other interesting examples as well.

Example 10.10. *Let $q = q_0^{t-1}$, then in $\mathsf{GF}(q)$ $T = \{1\} \cup \{\omega^{q_0^i} : i = 0, ..., t-2\}$ for some element $\omega \in \mathsf{GF}(q)^*$ satisfying $\mathsf{Tr}_{q\to q_0}(\omega^k) = -1$ for all $k = 1, ..., t-1$.*

Proof:

$$\sum_{i=0}^{t-2}(\omega^{q_0^i})^k = \sum_{i=0}^{t-2}(\omega^k)^{q_0^i} = \mathsf{Tr}_{q\to q_0}(\omega^k) = -1.$$

Note that such ω exists for several triples (t, q_0, q), here I enlist some values; "-" means that such ω does *not* exist, while "x" means that the only element with the property above is $1 \in \mathsf{GF}(q_0^{t-1})$:

q_0 t	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
3	x			x			x		-	x	-		x			x
4		x		x		x		x		x		x	?			
5		-	x				-	x	-			?				
7	-	-		-	x		-			?						
8		x		x		x		x		x	?					
9	x		-	x	-		x		-	x	?					

Result 10.11. *Let $T = \{y_1, ..., y_t\}$ be a super-Vandermonde set. Then*

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

Proof: Consider

$$\begin{pmatrix} 1-t & 1 & \dots & 1 \\ y_1 & y_2 & \cdots & y_t \\ y_1^2 & y_2^2 & \dots & y_t^2 \\ \vdots & & & \\ y_1^{t-1} & y_2^{t-1} & \dots & y_t^{t-1} \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

hence the determinant should be zero:
$VdM(y_1, y_2, ..., y_t) - ty_2y_3 \cdots y_t VdM(y_2, y_3, ..., y_t) = 0$. So
$t = \frac{VdM(y_1,y_2,...,y_t)}{y_2y_3\cdots y_t VdM(y_2,y_3,...,y_t)} = \frac{(y_1-y_2)(y_1-y_3)\cdots(y_1-y_t)}{y_2y_3\cdots y_t}$. ∎

Note that it is easy 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.

10.3 Small and large super-Vandermonde sets

If in Proposition 10.7(ii) we write $Y^t f(\frac{1}{Y})$ then we get a polynomial of degree t and its roots are $\{\frac{1}{y} : y \in T\}$. 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 $\{y : y^t = 1\}$, if it exists (so iff $t|q-1$).

If $f(Y) = g^p(Y) + Y^t$ 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 $h(y_1) = \frac{-1}{ty_1^{t-1}} = -\frac{1}{t}y_1^{q-t}$. 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 $t \le \frac{q-1}{2}$.

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 $\mathsf{GF}(q)$ 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 $< p$" and "of size $> q/p$", resp.

Theorem 10.12. [SzPvdm] *Suppose that* $T \subset \mathsf{GF}(q)$ *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. ∎

Theorem 10.13. [SzPvdm] *Suppose that* $T \subset \mathsf{GF}(q)$ *is a super-Vandermonde set of size* $|T| > q/p$. *Then* T *is a (transform of a) multiplicative subgroup.*

Proof: It requires a rather lengthy calculation. Let us write $Y^q - Y = f(Y)h(Y)$, where $f(Y) = Y^t + b_{mp}Y^{mp} + b_{(m-1)p}Y^{(m-1)p} + ... + b_pY^p + b_0$ and $h(Y) = Y^{q-t} + a_{q-t-1}Y^{q-t-1} + ... + a_2Y^2 + a_1Y$.
Consider the coefficient of $Y^1, Y^2, ..., Y^q$ in this equation. We get

$Y^1 : -1 = a_1b_0$

$Y^j : a_j = 0$ if $2 \leq j \leq t$ and $j \neq 1 \pmod p$

$Y^j : a_j = 0$ if $t+1 \leq j \leq 2t$ and $j \neq 1, t+1 \pmod p$

$Y^j : a_j = 0$ if $2t+1 \leq j \leq 3t$ and $j \neq 1, t+1, 2t+1 \pmod p$ and so on, generally

$Y^j : a_j = 0$ if $kt+1 \leq j \leq (k+1)t$ and $j \neq 1, t+1, ..., kt+1 \pmod p$.

$Y^{p+1} : a_{p+1}b_0 + a_1b_p = 0$

$Y^{2p+1} : a_{2p+1}b_0 + a_{p+1}b_p + a_1b_{2p} = 0$

generally

$Y^{kp+1} : a_{kp+1}b_0 + a_{(k-1)p+1}b_p + ... + a_{p+1}b_{(k-1)p} + a_1b_{kp} = 0$, for $k = 1, 2, ..., m$.

$Y^{t+1} : a_1 + b_0a_{t+1} + b_pa_{t-p+1} + b_{2p}a_{t-2p+1} + ... + b_{mp}a_{t-mp+1} = 0$

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

$Y^{t+1} : a_1 + b_0a_{t+1} = 0$.

$Y^{2t+1} : a_{t+1} + b_0a_{2t+1} + b_pa_{2t-p+1} + ... + b_{mp}a_{2t-mp+1} = 0$

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

$Y^{2t+1} : a_{t+1} + b_0a_{2t+1} = 0$ if $p \neq 2$.

Similarly

$Y^{3t+1} : a_{2t+1} + b_0 a_{3t+1} + b_p a_{3t-p+1} + ... + b_{mp} a_{3t-mp+1} = 0.$

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 $t \neq 0 \pmod p$.

$Y^{3t+1} : a_{2t+1} + b_0 a_{3t+1} = 0$ if $p \neq 2, 3$.

Generally

$Y^{lt+1} : a_{(l-1)t+1} + b_0 a_{lt+1} + b_p a_{lt-p+1} + ... + b_{mp} a_{lt-mp+1} = 0$, for $l = 1, 2, ..., n-1$.

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 $lt + 1 \neq 1, t+1, ..., (l-1)t+1 \pmod p$. It gives $(l-1)t$ conditions:

$lt + 1 \neq 1 \pmod p$ so $p \neq l$;

$lt + 1 \neq t + 1 \pmod p$ so $p \neq (l-1)$;

$lt + 1 \neq 2t + 1 \pmod p$ so $p \neq (l-2)$;

and so on

$lt + 1 \neq (l-2)t + 1 \pmod p$ so $p \neq 2$; finally

$lt + 1 \neq (l-1)t + 1 \pmod p$ so $t \neq 0$, which is true.

Hence generally we get

$Y^{lt+1} : a_{(l-1)t+1} + b_0 a_{lt+1} = 0$ if $p \neq 1, 2, ..., l$.

In particular, substituting $l = n-1$ into this equation we get

$Y^{(n-1)t+1} : a_{(n-2)t+1} + b_0 a_{(n-1)t+1} = 0$ if $p \neq 1, 2, ..., n-1$.

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 $p \neq 1, 2, ..., n-1$. We will now prove that it leads to a contradiction.

Substituting $a_{(n-2)t+1} = 0$ into the equation

$Y^{(n-2)t+1} : a_{(n-3)t+1} + b_0 a_{(n-2)t+1} = 0$, we get $a_{(n-3)t+1} = 0$.

We can substitute this again into the equation

$Y^{(n-3)t+1} : a_{(n-4)t+1} + b_0 a_{(n-3)t+1} = 0$, and we get $a_{(n-4)t+1} = 0$.

Substituting this in a decreasing order we get

$Y^{t+1} : a_1 + b_0 a_{t+1} = 0$ so $a_1 = 0$.

Hence $-1 = a_1 b_0$, so $a_1 \neq 0$, **Case 2** implied a contradiction. It means that **Case 1** will occur, so $t = \frac{q-1}{n}$ if $p \neq 1, 2, ..., n-1$. In other words $t|q-1$ if $p \neq 1, 2, ..., n-1$.
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 $a_{(n-2)t+1} = -b_0$.

Substituting this into the equation

$Y^{(n-2)t+1} : a_{(n-3)t+1} + b_0 a_{(n-2)t+1} = 0$, we get

$Y^{(n-2)t+1} : a_{(n-3)t+1} + b_0 b_0 = 0$ 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 $l = n-1, n-2, ..., 1$. Finally

$Y^{t+1} : a_1 = (-b_0)^{n-1}$.

Substituting this into $-1 = a_1 b_0$, 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

$Y^{(n-1)t+p+1} : a_{(n-2)t+p+1} + b_p + b_{2p} a_{(n-1)t+p+1} + ... = 0$

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 $k = 1, 2, ..., m$.

On the other hand

$Y^{lt+p+1} : a_{(l-1)t+p+1} + b_0 a_{lt+p+1} + b_p a_{lt+1} = 0$, for $l = 1, 2, ..., n-1$.

Generally we get

$Y^{lt+kp+1} : a_{(l-1)t+kp+1} + b_0 a_{lt+kp+1} + b_p a_{lt+(k-1)p+1} + ... + b_{kp} a_{lt+1} = 0$ for $l = 1, 2, ..., n-1$ and $k = 1, 2, ..., m$.

In particular, if $l = 1$ the equation is of the form

$Y^{t+kp+1} : a_{kp+1} + b_0 a_{t+kp+1} + b_p a_{t+(k-1)p+1} + ... + b_{kp} a_{t+1} = 0$.

Lemma 10.14. $b_p = b_{2p} = ... = b_{mp} = 0$.

Proof: We prove it by induction.

Step 1. First we prove that $b_p = 0$. Consider the equation

$Y^{(n-2)t+p+1} : a_{(n-3)t+p+1} + b_0 a_{(n-2)t+p+1} + b_p a_{(n-2)t+1} = 0.$ $(*)$

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 $(*)$, we get

$Y^{(n-2)t+p+1} : a_{(n-3)t+p+1} - b_0 b_p - b_0 b_p - b_0 = 0$ so $a_{(n-3)t+p+1} = 2b_0 b_p$.

Generally we can write

$Y^{lt+p+1} : a_{(l-1)t+p+1} + b_0 a_{lt+p+1} + b_p a_{lt+1} = 0$ for $l = n-1, n-2, ..., 1.(**)$
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
$Y^{(l+1)t+1} : a_{lt+1} = (-b_0)^{n-l-1}$ into the equation $(**)$, we get
$Y^{lt+p+1} : a_{(l-1)t+p+1} = (-1)^{n-l}(n-l)b_0^{n-l-1}b_p$ for $l = n-1, n-2, ..., 1$. If $l = 0$ it means
$Y^{p+1} : a_{p+1}b_0 + a_1 b_p = 0.$ $(***)$
Substituting
$Y^{t+p+1} : a_{p+1} = (-1)^{n-1}(n-1)b_0^{n-2}b_p$ and
$Y^{t+1} : a_1 = (-b_0)^{n-1}$ into $(***)$, we get
$Y^{p+1} : (-1)^{n-1} n b_0^{n-1} b_p = 0.$
In this equation $-1 \neq 0 \pmod p$, $n \neq 0 \pmod p$ and $b_0 \neq 0 \pmod p$ (from the equation $a_1 b_0 = -1$). 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
$Y^{(n-2)t+sp+1} : a_{(n-3)t+sp+1} + b_0 a_{(n-2)t+sp+1} + b_{sp} a_{(n-2)t+1} = 0.$ $(\star)$
We have seen that
$Y^{(n-1)t+sp+1} : a_{(n-2)t+sp+1} + b_{sp} = 0$ so $a_{(n-2)t+sp+1} = -b_{sp}$ and
$Y^{(n-1)t+1} : a_{(n-2)t+1} = -b_0$.
Substituting these into the equation $(\star)$, we get
$Y^{(n-2)t+sp+1} : a_{(n-3)t+sp+1} - b_0 b_{sp} - b_0 b_{sp} = 0$ so $a_{(n-3)t+sp+1} = 2b_0 b_{sp}$.
Generally we can write
$Y^{lt+sp+1} : a_{(l-1)t+sp+1} + b_0 a_{lt+sp+1} + b_{sp} a_{lt+1} = 0$ $(\star\star)$
for $l = n-1, n-2, ..., 1$.
Substituting
$Y^{(l+1)t+sp+1} : a_{lt+sp+1} = (-1)^{n-l-1}(n-l-1)b_0^{n-l-2}b_{sp}$ and
$Y^{(l+1)t+1} : a_{lt+1} = (-b_0)^{n-l-1}$ into the equation $(\star\star)$, we get
$Y^{lt+sp+1} : a_{(l-1)t+sp+1} = (-1)^{n-l}(n-l)b_0^{n-l-1}b_{sp}$ for $l = n-1, n-2, ..., 1$.
If $l = 0$ it means
$Y^{sp+1} : a_{sp+1}b_0 + a_1 b_{sp} = 0.$ $(\star\star\star)$
Substituting
$Y^{t+sp+1} : a_{sp+1} = (-1)^{n-1}(n-1)b_0^{n-2}b_{sp}$ and
$Y^{t+1} : a_1 = (-b_0)^{n-1}$ into $(\star\star\star)$, we get
$Y^{sp+1} : (-1)^{n-1} n b_0^{n-1} b_{sp} = 0.$
In this equation $-1 \neq 0 \pmod p$, $n \neq 0 \pmod p$ and $b \neq 0 \pmod p$ (from the equation $a_1 b_0 = -1$). It means that $b_{sp} = 0$. ∎

So we have got $b_p = b_{2p} = ... = b_{mp} = 0$. It means that $f(Y)$ is of the form
$f(Y) = Y^t + b_0$, and that $t | q-1$ so $t = \frac{q-1}{n}$ and $(-b_0)^n = 1$. Hence

$f(Y) = Y^{\frac{q-1}{n}} + b_0$, where $(-b_0)^n = 1$ if $p \neq 1, 2, ..., n-1 \pmod p$. So the roots of $f(Y)$ are the elements of a coset of a multiplicative subgroup of order t. ∎

10.4 Sets with intersection numbers 0 mod r

Here we continue the examination of sets of $\mathsf{PG}(2,q)$ intersecting every line in a constant number of points mod p. This section is based on [SzPcomd]. For the more general k-dimensional case see the paper itself. The proofs are similar (although in higher dimensions it is more complicated) and are streamlined and then generalised versions of the proof in [12].

Theorem 10.15. *Let $1 < r < q = p^h$. A point set $S \subset \mathsf{PG}(2,q)$ which is incident with 0 mod r points of every line has $|S| \geq (r-1)q + (p-1)r$ 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 $|S| = 0 \mod r$. By counting points of S on lines through a point in S we have $|S| = 1 + (-1)(q+1) \mod r$ and combining these two equalities we see that $q = 0 \mod r$.

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 $\mathsf{GF}(q^2) \simeq \mathsf{AG}(2,q)$ 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 $c \in \mathsf{GF}(q^2)$ the corresponding points of $\mathsf{AG}(2,q)$ 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 σ_j is at most $j(q-1)$ and there are q^2 elements in $\mathsf{GF}(q^2)$, hence $\sigma_j \equiv 0$ when $0 < j < q$ and r does not divide j. So

$$R(X,Y) = X^{|S|} + \sigma_r X^{|S|-r} + \sigma_{2r} X^{|S|-2r} + ... + \sigma_q X^{|S|-q} + \sigma_{q+1} X^{|S|-q-1} + ... + \sigma_{|S|}.$$

For all $y \in \mathsf{GF}(q^2)$ 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

$$R(X,y)G_y(X) = (X^{q+1}-1)\frac{\partial R}{\partial Y}(X,y) =$$

$$(X^{q+1}-1)(\sigma'_r X^{|S|-r} + \sigma'_{2r} X^{|S|-2r} + ... + \sigma'_q X^{|S|-q} + \sigma'_{q+1} X^{|S|-q-1} + ...). \quad (*)$$

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 σ'_{q+1}, where $'$ 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 σ'_{q+1}.

For any natural number κ 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 $(*)$ is

$$-\sigma'_{i(q+1)+kr} + \sigma'_{(i+1)(q+1)+\kappa r}$$

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 $\sigma'_{i(q+1)+\kappa r} = 0$ 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 $(*)$ this has coefficient $-\sigma'_{\kappa r}$ (since $\sigma'_{q+1+\kappa r} = 0$). The only term of degree zero mod r in G is the constant term which is σ'_{q+1}. The coefficient of the term of degree $|S| - \kappa r$ in $R(X,y)$ is $\sigma_{\kappa r}$. Hence

$$\sigma_{\kappa r}\sigma'_{q+1} = -\sigma'_{\kappa r} \quad \text{for all } y \notin S. \qquad (**)$$

If $y \in S$ then $\sigma_{q+1}(y) = 1$ and if $y \notin S$ then $\sigma_{q+1}(y) = 0$. Let

$$f(Y) = \prod_{y \in S} (Y - y).$$

Then $f\sigma_{q+1} = (Y^{q^2} - Y)g(Y)$ for some $g \in \mathsf{GF}(q^2)[Y]$ of degree at most $|S| - 1$ (the degree of σ_{q+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 $\sigma'_{q+1} f = f'$.

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 $(X + Y^{q-1})^{|S|}$ which has a term $X^{(r-1)q} Y^{\kappa r(q-1)}$ 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 10.16. *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. 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 [55].

Corollary 10.17. *There are no non-trivial maximal arcs in* $\mathsf{PG}(2, q)$ *when* q *is odd.*

Proof: A maximal arc has $(r-1)q + r$ points, see the Barlotti-bound in Result 8.6. ∎

11 Blocking sets

A blocking set with respect to k-dimensional subspaces is a point set 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 $\mathsf{PG}(2, q)$ there exist minimal blocking sets of size $\sim \frac{3}{2}q$; the

projective triangle of size $3(q+1)/2$ if q is odd and the projective triad (which is a linear point set in fact) of size $3q/2+1$ if q is even. In general, in $\mathsf{PG}(n,q)$ 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 $\frac{q^{n-k+1}-1}{q-1} \sim q^{n-k}$ 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 $\sim \frac{3}{2}q$ then the blocking set will be of size $\sim \frac{3}{2}q^{n-k}$ roughly. A blocking set with respect to k-dimensional subspaces of $\mathsf{PG}(n,q)$ is said to be *small* if it is smaller than $\frac{3}{2}(q^{n-k}+1)$, in particular in the plane it means that $|B| < 3(q+1)/2$.

We remark that there is another terminology as well: a **k-blocking set** is a blocking set with respect to $(n-k)$-dimensional subspaces (so here the smallest and trivial examples are k-dimensional projective subspaces, this is where the name comes from). It may lead to some confusion, but sometimes this is the more natural name, see e.g. Section 12.

A most interesting question of the theory of blocking sets is to classify the small ones. A natural construction (blocking the k-subspaces of $\mathsf{PG}(n,q)$) is a subgeometry $\mathsf{PG}(h(n-k)/e, p^e)$, if it exists (recall $q=p^h$, so $1 \le e \le h$ and $e|h$).

It is one of the earliest results concerning blocking sets, due to Bruen [40], that a nontrivial blocking set of a projective plane of order q is of size $\ge q+\sqrt{q}+1$, 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 $\mathsf{PG}(n,q)$, is again a blocking set, w.r.t. the $(k+r-n)$-dimensional subspaces of $\mathsf{PG}(r,q)$ (where $\dim(V) = n-r-1$ and V is disjoint from the blocking set).

A blocking set of $\mathsf{PG}(r,q)$, which is a projection of a subgeometry of $\mathsf{PG}(n,q)$, 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 [82], [85].

Conjecture 11.1. The Linearity Conjecture. *In $\mathsf{PG}(n,q)$ every small blocking set, with respect to k-dimensional subspaces, is linear.*

There are some cases of the Conjecture that are proved already (this list is not complete).

Theorem 11.2. *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 [24]) $h = 1$ *(i.e. there is no small non-trivial blocking set at all);*

(ii) (Szőnyi [103]) $h = 2$ *(the only non-trivial example is a Baer subplane with* $p^2 + p + 1$ *points);*

(iii) (Polverino [86]) $h = 3$ *(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 [33], Ball [7]) *if* $p > 2$ *and there exists a line* ℓ *intersecting* B *in* $|B \cap \ell| = |B| - q$ *points (so a blocking set of Rédei type);*

(b) for general k*:*

(i) (Szőnyi and Weiner) [109] *if* $h(n-k) \leq n$, $p > 2$ *and* B *is not contained in an* $(h(n-k)-1)$*-dimensional subspace;*

(ii) (Storme-Weiner [99] (*for* $k = n-1$), Bokler and Weiner [114]) $h = 2$, $q \geq 16$*;*

(iii) (Storme-Sziklai [SzPkblock]) *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);*

(iv) (Sziklai-Van de Voorde[SzPVdV]) *if* $k = n-1$, $p \geq 5h - 11$ *and* B *is not contained in an* $(h-2)$*-dimensional subspace.*

There is an even more general version of the Conjecture. A t-fold blocking set w.r.t. k-subspaces is a point set which intersects each k-subspace in at least t points. Multiple points may be allowed as well.

Conjecture 11.3. The Linearity Conjecture for multiple blocking sets: *In* $\mathsf{PG}(n,q)$ *any* t*-fold blocking set* B*, with respect to* k*-dimensional subspaces, is the union of some (not necessarily disjoint) linear point sets* $B_1, ..., B_s$*, 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 $(\sqrt[4]{q}+1)$-fold blocking set in $\mathsf{PG}(2,q)$, constructed by Ball, Blokhuis and Lavrauw [15], which is *not* the union of smaller blocking sets. (This multiple blocking set is a linear point set.)

First we study 1-fold blocking sets of $\mathsf{PG}(2,q)$, with respect to lines.

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 11.4. (Blokhuis [24]) *In* $\mathsf{PG}(2,p)$*,* p *prime, the size of a non-trivial blocking set is at least* $3(p+1)/2$*.*

The following theorem of Blokhuis, Ball, Brouwer, Storme and Szőnyi [33], which was refined and turned to its current beautiful form by Ball [7], classifies the so-called small *blocking sets of Rédei type* (for the definition and further information compare to Theorem 11.2(iv), and see e.g. Section 12):

Theorem 11.5. *Let $|U| = q$ be a pointset in $\mathsf{AG}(2,q)$, $q = p^h$, 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 $\frac{q+3}{2} \leq N \leq q+1$;

(ii) $\mathsf{GF}(s)$ is a subfield of $\mathsf{GF}(q)$ 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 $\mathsf{GF}(s)$-linear pointset.

In other words, it means that (if $p > 2$) a small blocking set of Rédei type is always a linear pointset.

* * *

One can formulate the chase for minimal (nontrivial) blocking sets (in $\mathsf{PG}(2,q)$) in an algebraic way as follows. Consider the polynomial ring $\mathsf{GF}(q)[X,Y,Z]$ and its subset $\mathsf{GF}(q)[X,Y,Z]_{hom}$, the homogeneous polynomials of any degree. The fully reducible polynomials form the multiplicative sub-semigroups $\mathcal{R}$ and $\mathcal{R}_{hom}$ in them. ($\mathcal{R}$ stands for **r**educible and **R**édei as well.) Let $\mathsf{GF}(q)[X,Y,Z]_0$ and $\mathsf{GF}(q)[X,Y,Z]_{hom,0}$ denote the sets (ideals) of polynomials vanishing everywhere in $\mathsf{GF}(q) \times \mathsf{GF}(q) \times \mathsf{GF}(q)$.

Both $\mathsf{GF}(q)[X,Y,Z]_0$ and $\mathsf{GF}(q)[X,Y,Z]_{hom,0}$, as ideals, can be generated by three polynomials from $\mathcal{R}$ (and $\mathcal{R}_{hom}$, resp.), for example $\mathsf{GF}(q)[X,Y,Z]_0 = \langle (X^q - X); (Y^q - Y); (Z^q - Z)\rangle$ and $\mathsf{GF}(q)[X,Y,Z]_{hom,0} = \langle (Y^qZ - YZ^q); (Z^qX - ZX^q); (X^qY - XY^q)\rangle$. Note also that for any $a,b,c \in \mathsf{GF}(q)$ the polynomial $a(Y^qZ - YZ^q) + b(Z^qX - ZX^q) + c(X^qY - XY^q)$ is still totally reducible. (It is the Rédei polynomial of the point set consisting of the points of the line $[a,b,c]$.)

The blocking set problem is now equivalent to finding minimal polynomials, w.r.t. divisibility, as partial order, in

$$(\mathcal{R}_{hom} \cap \mathsf{GF}(q)[X,Y,Z]_{hom,0}).$$

The trivial blocking sets, as we have seen, correspond to the minimal polynomials $a(Y^qZ - YZ^q) + b(Z^qX - ZX^q) + c(X^qY - XY^q)$.

11.1 One curve

So let $|B| = q + k$ be our blocking set. We often suppose that $|B| < 2q$. Recall the Rédei polynomial of B:

$$R(X,Y,Z) = \prod_{(a_i,b_i,c_i)\in B} (a_iX + b_iY + c_iZ) = \sum_{j=0}^{q+k} r_j(Y,Z)X^{q+k-j}.$$

Definition 11.6. ([37], [103]) *Let $\mathcal{C}$ 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 11.7. *If the line $L_X[1,0,0]$ contains the points $\{(0,b_{i_j},c_{i_j}) : j = 1,...,N_X\}$ then*

$$r_{N_X}(Y,Z) = (\prod_{a_s\neq 0} a_s) \prod_{j=1}^{N_X}(b_{i_j}Y + c_{i_j}Z) \quad | \quad R(X,Y,Z);$$

$$r_{N_X}(Y,Z) \quad | \quad f(X,Y,Z);$$

so f can be written in the form $f = r_{N_X}\bar{f}$, where $\bar{f}(X,Y,Z)$ 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 $R(X,Y,Z) = r_{N_X}(Y,Z)\bar{R}(X,Y,Z)$ 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_{N_X}, so $r_{N_X}|r_j\ \forall j$. ∎

Note that the curve r_{N_X} consists of N_X lines on the dual plane, all passing through $[1,0,0]$.
On the other hand if $k < q$ then

$$f = \mathcal{H}_X^q R = \sum_{\{s_1,s_2,...,s_q\}} a_{s_1}a_{s_2}...a_{s_q} \prod_{j\notin\{s_1,s_2,...,s_q\}} (a_jX + b_jY + c_jZ).$$

Obviously it is enough to sum for subsets $\{\mathbf{P}_{s_1},\mathbf{P}_{s_2},...,\mathbf{P}_{s_q}\} \subseteq B \setminus L_X$.

If one coordinatizes B such that each a_i is either 0 or 1, then

$$f = r_{N_X}\bar{f} = r_{N_X} \sum_{\substack{J\subseteq\{1,2,\ldots,q+k\}\\ |J|=k-N_X\\ a_i\neq 0\ \forall i\in J}} \prod_{j\in J}(X + b_jY + c_jZ).$$

Also

$$r_{N_X} = \mathcal{H}_X^{q+k-N_X} R = \mathcal{H}_X^{k-N_X} f.$$

The next proposition summarizes some important properties of the Rédei polynomial and of this curve.

Theorem 11.8. ([103])

(1.1) For a fixed (y, z) (where $(0, -z, y) \notin B$), 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 $\bar{R}(X, y, z)$ if and only if the line with equation $xX + yY + zZ = 0$ intersects B in exactly r points.

(2.1) For a fixed $(0, -z, y) \notin B$ 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 $(0, -z, y) \notin B$; and $f(X, y, z)$ splits into linear factors over $\mathsf{GF}(q)$ for these fixed (y, z)'s.

(2.2) If the line $[0, -z, y]$ (where $(0, -z, y) \notin B$) 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 $\mathsf{GF}(q)$-rational points and helps us to translate geometric properties of B into properties of f.

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 $\prod_{x\in\mathsf{GF}(q)}(X - x) = X^q - X$. 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 11.8 will be used frequently without further reference.

The next lemma shows that the linear components of $\bar{f}$ (or the curve $\bar{\mathcal{C}}$ defined by $\bar{f}=0$) correspond to points of B which are not essential.

Lemma 11.9. ([103])

(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 $(aX+by_0+cz_0)$ divides $\bar{f}(X,y_0,z_0)$. In other words, the line $L: aX+bY+cZ$ and $\bar{\mathcal{C}}$ 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 $\bar{\mathcal{C}}$.

(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 [65], 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 $\mathsf{GF}(q)$-rational points of certain components of f, see Blokhuis, Pellikaan, Szőnyi [37].

Lemma 11.10. ([37]) *(1) The sum of the intersection multiplicities $I(P, f \cap \ell_P)$ over all $\mathsf{GF}(q)$-rational points of f is at least $\deg(f)(q+1) - \deg(\bar{f})N_X$, where ℓ_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 $g_0 = g.c.d.(g, r_{N_X})$ 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 $\mathsf{GF}(q)$-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 $\bar{f}$ 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 $\mathsf{GF}(q)$, 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 [37]); 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 11.10, 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 11.11. ([34]) *There are at most $k^2 - k + 1$ lines that meet B in at least two points.*

Proof: First we prove that there are at least $2q + 1 - |B|$ tangents through any essential point P of any blocking set B. Indeed, if $P \in B$ is essential with t tangents through it then choose the coordinate system so that $P \in \ell_\infty$ and ℓ_∞ is a tangent to B. Putting one point on each tangent except ℓ_∞ results in an affine blocking set of size $|B| - 1 + t - 1$, which is, by the theorem of Jamison, at least $2q - 1$, hence $t \geq 2q + 1 - |B|$.

Now, 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 11.4 in the prime case.

Theorem 11.12. (Blokhuis [24]) *In* $\mathsf{PG}(2,p)$, *p prime, the size of a non-trivial blocking set is at least* $3(p+1)/2$.

Proof: Take a component $g = \bar{g}$ (of degree s) of $\bar{f}$. 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 11.10. On the other hand, again since p is prime, it cannot be non-classical with respect to lines. Therefore, by the Stöhr-Voloch theorem 8.4, it has at most $s(p+s-1)/2$ $\mathsf{GF}(p)$-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 $\bar{f}$ must be (absolutely) irreducible. Now Lemma 11.10 can be applied to f itself and it says that $\bar{f}$ 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 $\mathsf{GF}(p)$. Solving the inequality $pk - k(k-1) \leq k^2-k+1$ implies $k \geq (p+2)/2$. ∎

11.2 Three new curves

In this subsection we introduce three nice curves. We use the notation $\mathbf{V} = (X,Y,Z); \mathbf{V}^q = (X^q, Y^q, Z^q)$ and $\mathbf{\Psi} = \mathbf{V} \times \mathbf{V}^q = ((Y^qZ - YZ^q), (Z^qX - ZX^q), (X^qY - XY^q))$. Let B be a minimal blocking set of $\mathsf{PG}(2,q)$. Since $R(X,Y,Z)$ vanishes for all homogeneous $(x,y,z) \in \mathsf{GF}(q) \times \mathsf{GF}(q) \times \mathsf{GF}(q)$, we can write it as

$$R(X,Y,Z) = \mathbf{\Psi} \cdot \mathbf{g} = \det(\mathbf{V}, \mathbf{V}^q, \mathbf{g}) =$$

$$(Y^qZ - YZ^q)\, g_1(X,Y,Z) + (Z^qX - ZX^q)\, g_2(X,Y,Z) + (X^qY - XY^q)\, g_3(X,Y,Z),$$

where g_1, g_2, g_3 are homogeneous polynomials of degree $k-1$ in three variables and $\mathbf{g} = (g_1, g_2, g_3)$. Note that $\mathbf{g}$ is not determined uniquely, it can be changed by $\mathbf{g}' = \mathbf{g} + g_0\mathbf{V}$ for any homogeneous polynomial $g_0 \in \mathsf{GF}(q)[X,Y,Z]$ of total degree $k-2$, if $k < q$; and for $\mathbf{g}' = \mathbf{g} + g_0\mathbf{V} + g_{00}\mathbf{V}^q$ 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 $R = (a,b,c) \cdot \mathbf{\Psi}$.

Now one can define $\mathbf{f} = \mathbf{V} \times \mathbf{g}$. Then $\mathbf{f} \cdot (\mathbf{V}^q - \mathbf{V}) = f_1(X^q - X) + f_2(Y^q - Y) + f_3(Z^q - Z) = R$, and f_1, f_2, f_3 are homogeneous polynomials of degree k. If $k < q$ then, by this "decomposition" of R, $\mathbf{f}$ is determined uniquely.

Conversely, if for some $\mathbf{g}'$ also $\mathbf{f} = \mathbf{V} \times \mathbf{g}'$ holds then $\mathbf{g}' = \mathbf{g} + g\mathbf{V}$ for some homogeneous polynomial g of degree $k-2$.

We also remark that, as $\mathbf{V} \cdot (\mathbf{V} \times \mathbf{g}) = 0$, we have $\mathbf{V}\mathbf{f} = 0$. For another proof see 11.17.

If $k \geq q$ then $\mathbf{f}$ is not necessarily unique in the decompositon of R. But if we choose $\mathbf{f} = \mathbf{V} \times \mathbf{g}$ for some $\mathbf{g}$ then 11.17 remains valid (otherwise it may happen that $\mathbf{V} \cdot \mathbf{f}$ is not the zero polynomial).

The following lemma summarizes some fundamental properties of $\mathbf{g}$.

Proposition 11.13. *(1.1) If a point $P(a,b,c) \in B$ is not essential, then there exists an equivalent $\mathbf{g}' = \mathbf{g} + g_0\mathbf{V}$ (or $\mathbf{g}' = \mathbf{g} + g_0\mathbf{V} + g_{00}\mathbf{V}^q$) of $\mathbf{g}$ such that $aX + bY + cZ$ 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 $aX + bY + cZ$ 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 $R_0 = \mathbf{g}_0\mathbf{\Psi}$, so $\mathbf{\Psi} \cdot (\mathbf{g}_0(aX+bY+cZ) - \mathbf{g}) = 0$.

(1.2) Now $aX + bY + cZ$ divides R as well, so $(a,b,c) \in B$. Deleting it, the Rédei polynomial of the new point set is $(Y^qZ - YZ^q)\,\frac{g_1(X,Y,Z)}{aX+bY+cZ} + (Z^qX - ZX^q)\,\frac{g_2(X,Y,Z)}{aX+bY+cZ} + (X^qY - XY^q)\,\frac{g_3(X,Y,Z)}{aX+bY+cZ}$, 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

$$\phi(X,Y,Z)\Big|_{[a,b,c]} = \phi(bZ - cY, cX - aZ, aY - bX).$$

In general $f(X,Y,Z)\Big|_{[a,b,c]} = f(-bY - cZ, aY, aZ) = f(bX, -aX - cZ, bZ) = f(cX, cY, -aX - bY)$, where e.g. $f(-bY - cZ, aY, aZ)$ can be used if $a \neq 0$ etc.

Theorem 11.14. *(1)*

$$R\Big|_{[a,b,c]} = \left(ag_1\Big|_{[a,b,c]} + bg_2\Big|_{[a,b,c]} + cg_3\Big|_{[a,b,c]}\right)\left((ZY^q - Z^qY)\Big|_{[a,b,c]}\right)$$

(the last factor should be changed for $(XZ^q - X^qZ)\Big|_{[a,b,c]}$ *if* $a = 0$ *and* $b \neq 0$ *and for* $(YX^q - Y^qX)\Big|_{[a,b,c]}$ *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* $ag_1\Big|_{[a,b,c]} + bg_2\Big|_{[a,b,c]} + cg_3\Big|_{[a,b,c]} = 0$*. 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*

$$\frac{R}{aX + bY + cZ}\Big|_{[a,b,c]} = \frac{\left(a(g_1\Big|_{[a,b,c]} + bg_2\Big|_{[a,b,c]} + cg_3\Big|_{[a,b,c]}\right)}{(aX + bY + cZ)\Big|_{[a,b,c]}}\left((ZY^q - Z^qY)\Big|_{[a,b,c]}\right)$$

(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* $ag_1\Big|_{[a,b,c]} + bg_2\Big|_{[a,b,c]} + cg_3\Big|_{[a,b,c]}$ *with multiplicity* $r - 1$*.*

Proof: Easy calculations. For instance to prove (2) we simply need

$$R\Big|_{[a,b,c]} = ag_1\Big|_{[a,b,c]} + bg_2\Big|_{[a,b,c]} + cg_3\Big|_{[a,b,c]} = 0. \qquad \blacksquare$$

See Example 11.4 for showing the use of (2) above: there we get that the equation of the "canonical" Baer subplane is

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

meaning that the Baer subplane is just $\{(a, b, c) \in \mathsf{PG}(2, q) : G_{a,b,c}(X, Y, Z) \equiv 0\}$.

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 11.15. *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 $\mathbf{g}(x,y,z)=[0,0,0]$ then $[x,y,z]$ is a $\geq$ 2-secant as the $\leq$ 1-st derivatives are 0.

Proof: Recall Theorem 5.9, 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:

$$(a_t,b_t,c_t)\cdot\mathbf{g}(x,y,z)=(\nabla R)(x,y,z)\cdot\mathbf{g}(x,y,z)=((x,y,z)\times\mathbf{g}(x,y,z))\cdot\mathbf{g}(x,y,z)=0.$$

Here $(x,y,z)\neq\mathbf{g}(x,y,z)$ as their cross product is (a_t,b_t,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 5.9) hence

$$\mathbf{0}=(\nabla R)(x,y,z)=(x,y,z)\times\mathbf{g}(x,y,z).$$

∎

or: we can use Theorem 11.14.

We also calculate ∇R for future use: $\nabla R=\mathbf{\Psi}(\nabla\circ\mathbf{g})+\mathbf{V}^q\times\mathbf{g}$.

The following is true as well. We will see (Theorem 11.28, Corollary 11.32) that if B is *small*, then R can be written in the form

$$X^q(Yg_{XY}+Zg_{XZ})+Y^q(Xg_{YX}+Zg_{YZ})+Z^q(Xg_{ZX}+Yg_{ZY}),$$

where the polynomials $g_{XY},...,g_{ZY}$ contain only exponents divisible by p. Surprisingly or not, $g_{XY}=-g_{YX},g_{XZ}=-g_{ZX},g_{ZY}=-g_{YZ}$, as $0=Xf_1+Yf_2+Zf_3=XY(g_{XY}+g_{YX})+YZ(g_{YZ}+g_{ZY})+ZX(g_{ZX}+g_{XZ})$. One can take $\partial_X\partial_Y,\partial_Y\partial_Z,\partial_Z\partial_X$ of both sides.

Now $\mathbf{g}=(g_{YZ},g_{ZX},g_{XY})$, which is a kind of "natural choice" for $\mathbf{g}$.

11.3 Three old curves

In this section we will present the method using three old algebraic curves. As an application we show Szőnyi's result [103] 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 $\mathsf{PG}(2,p)$.

Let now B be a minimal blocking set of $\mathsf{PG}(2,q)$. Since $R(X,Y,Z)$ vanishes for all $(x,y,z)\in\mathsf{GF}(q)\times\mathsf{GF}(q)\times\mathsf{GF}(q)$, we can write it as

$$R(X,Y,Z)=(X^q-X)f_1(X,Y,Z)+(Y^q-Y)f_2(X,Y,Z)+(Z^q-Z)f_3(X,Y,Z)=\mathbf{W}\cdot\mathbf{f},$$

where $\mathbf{f} = (f_1, f_2, f_3)$ 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 11.6 and examined in Section 11.1; while f_2 and f_3 behave very similarly.

Proposition 11.16. (Lovász, Szőnyi) *Let $[x, y, z]$ be a tangent line to B at the point $(a_t, b_t, c_t) \in B$. Then*

$$\mathbf{f}(x, y, z) = (f_1(x, y, z), f_2(x, y, z), f_3(x, y, z)) = (a_t, b_t, c_t)$$

as homogeneous triples.

Proof: Recall Theorem 5.9, 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:

$$(a_t, b_t, c_t) = (\nabla R)(x, y, z) = (\nabla(\mathbf{W}\cdot\mathbf{f}))(x, y, z) = ((\nabla\circ\mathbf{W})\mathbf{f}+(\nabla\circ\mathbf{f})\mathbf{W})(x, y, z) =$$

$$-\mathbf{I}\ \mathbf{f}(x, y, z) + \mathbf{0} = -\mathbf{f}(x, y, z).$$ ∎

Lemma 11.17. *If $k < q - 1$ then $\mathbf{V} \cdot \mathbf{f} = Xf_1 + Yf_2 + Zf_3 = 0$. (Hence $R = \mathbf{V}^q\mathbf{f}$ as well).*

Proof: If $[x, y, z]$ is a tangent then by 11.16 $\mathbf{V} \cdot \mathbf{f}$ vanishes, and by the end of Theorem 5.9 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 5.9 (6) with $r = 1$. ∎

Note also that $\mathbf{f} = \nabla^q_{\mathcal{H}} R$; and $-\mathbf{f} = (\nabla \circ \mathbf{f})\mathbf{V}$.

From Theorem 5.9 (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_{N_X} of Lemma 11.7, so points on factors corresponding to points with $a_i = 0$.

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 $(x, y, z) \in \mathsf{GF}(q) \times \mathsf{GF}(q) \times \mathsf{GF}(q)$ if the line with equation $xX + yY + zZ = 0$ intersects B in at least two points (cf. Proposition 11.8 (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 11.18. ([103]) *The curves f_i have almost the same set of $\mathsf{GF}(q)$-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 $(x,y,z) \in \mathsf{GF}(q) \times \mathsf{GF}(q) \times \mathsf{GF}(q)$ we get $-f_1(x,y,z) = \partial_X R(x,y,z)$ and similarly $-f_2(x,y,z) = \partial_Y R(x,y,z)$. 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 11.19. ([103]) *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 $g = Z$.*

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 11.9 (2) gives ($N = 1$, $k \leq q-2$) that the point (a_i, b_i, c_i) can be deleted, a contradiction.

Suppose that g 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 $\mathsf{GF}(q)$-rational points. Using Bézout's theorem it immediately gives Lemma 11.11 back.

11.4 Examples

In this section we compute the polynomials (curves) for some well-known point sets. The computations are also used to illustrate several results and ideas of this dissertation. In the cases when the point set is a blocking set, we use the notation $\mathbf{f} = (f_1, f_2, f_3)$ and $\mathbf{g} = (g_1, g_2, g_3)$ for the curves defined above. We recall $R = \mathbf{f} \cdot (X,Y,Z) = \mathbf{g} \cdot (Y^qZ - YZ^q, Z^qX - ZX^q, X^qY - XY^q)$.

Example 11.20.

The line $[a,b,c]$. Its Rédei polynomial is $a(Y^qZ - YZ^q) + b(Z^qX - ZX^q) + c(X^qY - XY^q)$.

Example 11.21.

A conic. For the Rédei polynomial of the parabola $X^2 - YZ$ see Result 5.7.

Example 11.22.

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

$$R(X,Y,Z) = XYZ((-Z)^{\frac{q-1}{2}} - X^{\frac{q-1}{2}})(X^{\frac{q-1}{2}} - Y^{\frac{q-1}{2}})((-Y)^{\frac{q-1}{2}} - Z^{\frac{q-1}{2}}) =$$

$$(X^q - X)YZ[Z^{\frac{q-1}{2}} - (-Y)^{\frac{q-1}{2}}] + (Y^q - Y)XZ[(-X)^{\frac{q-1}{2}} - Z^{\frac{q-1}{2}}] +$$

$$(Z^q - Z)XY[(-Y)^{\frac{q-1}{2}} - (-X)^{\frac{q-1}{2}}] =$$

$$(X^qY - XY^q)Z[Z^{\frac{q-1}{2}} - (-Y)^{\frac{q-1}{2}} - (-X)^{\frac{q-1}{2}}] + (Y^qZ - YZ^q)X[(-X)^{\frac{q-1}{2}} - Z^{\frac{q-1}{2}} -$$

$$(-Y)^{\frac{q-1}{2}}] + (Z^qX - ZX^q)Y[(-Y)^{\frac{q-1}{2}} - Z^{\frac{q-1}{2}} - (-X)^{\frac{q-1}{2}}].$$

Note that $\mathbf{g} = \mathbf{0}$ iff $[x,y,z] = [\alpha^2,1,0]$ or $[1,0,-\alpha^2]$ or $[0,-\alpha^2,1]$, so for the 2-secants.

Example 11.23.

The *sporadic almost-Rédei blocking set.* The affine plane of order 3 can be embedded into $\mathsf{PG}(2,7)$ as the points of inflexion of a non-singular cubic. The 12 lines of this plane cover each point of $\mathsf{PG}(2,7)$, 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 [SzPnuc2].

A representation of this blocking set is the following: its affine part is $U = \{(x, -x^6 + 3x^3 + 1, 1) : x \in \mathsf{GF}(7)\} \cup \{(0,-1,1)\}$, the infinite part is $D = \{(1,0,0),(1,1,0),(1,2,0),(1,4,0)\}$. Now

$R(X,Y,Z) = X^{10}Y^2 - X^{10}Z^2 - X^7Y^5 - 2X^7Y^3Z^2 + 3X^7YZ^4 - X^4Y^8 + X^4Z^8 + XY^{11} + XY^9Z^2 + 4XY^7Z^4 + XY^3Z^8$

from which we get $\mathbf{f} =$

$(X^3Y^2 - X^3Z^2 - Y^5 - 2Y^3Z^2 + 3YZ^4,\ -X^4Y + XY^4 + XY^2Z^2 + 4XZ^4,\ X^4Z + XY^3Z)$

and $\mathbf{g} = (XY^2Z,\ X^3Z + 2Y^3Z,\ X^3Y - Y^4 + 3Z^4)$.

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

Example 11.24.

The *Baer-subplane.*

In $\mathsf{PG}(2,q)$ the standard embedding of a Baer subplane is $\{(a,b,1) : a,b \in \mathsf{GF}(\sqrt{q})\} \cup \{(m,1,0) : m \in \mathsf{GF}(\sqrt{q})\} \cup \{(1,0,0)\}$.

Now its Rédei polynomial is

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

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

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 11.25.

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

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

$$\mathbf{f}=(\ X^{q^2}Z+X^{q^2-q}Y^qZ-X^{q^2-q}YZ^q+Y^{q^2}Z-YZ^{q^2},\ X^{q^2}Z+X^{q^2-q+1}Z^q+XZ^{q^2},$$
$$-X^{q^2+1}-X^{q^2}Y-X^{q^2-q+1}Y^q-XY^{q^2}\ )$$

$$\text{and}\qquad \mathbf{g}=(\ -X^{q^2},\ X^{q^2}+X^{q^2-q}Y^q+Y^{q^2},\ X^{q^2-q}Z^q+Z^{q^2}\ ).$$

Example 11.26.

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

Then, after the linear transformation $(1,a^{q-1},0)\mapsto(1-a^{q-1},a^{q-1}-\beta,0)$, where β 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 11.27.

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

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

11.5 Small blocking sets

Lemmas 11.18 and 11.19 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 11.28. ([103]) *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 Lemma 11.10 the number of $\mathsf{GF}(q)$-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 11.19, 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 $q+2 \leq k+N_X+\bar{s}$ and from $N_X+\bar{s} \leq k$ 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 $f_1 \in \mathsf{GF}(q)[X^{p^e},Y,Z]$, $f_2 \in \mathsf{GF}(q)[X,Y^{p^e},Z]$ and $f_3 \in \mathsf{GF}(q)[X,Y,Z^{p^e}]$. By the Theorem $e \geq 1$.

Proposition 11.29. *If $q=p$ is a prime and $|B| < p + \frac{2p+4-N_X}{3}$, 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 11.28 gives $p+2 \leq k+N_X+\deg(g) \leq 3k/2+N_X/2$, that is $\frac{2(p+2)-N_X}{3} \leq k$. ∎

The following corollary, due to Szőnyi, generalizes the similar result of Rédei on blocking sets of *Rédei type*.

Corollary 11.30. ([103]) *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 ℓ 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 $f_1(X,y,z) = r_{N_X}(y,z)\bar{f}_1(X,y,z)$ 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 $\bar{f}_1(X,Y,Z)$ with multiplicity divisible by p (and the same is true for f_1), so by Theorem 11.8 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 11.31. (Blokhuis [24]) *If $q = p$ is a prime, then $|B| \geq 3(q+1)/2$ for the size of a non-trivial blocking set.* ∎

The next corollary is a crucial one.

Corollary 11.32. *If B is a blocking set of size less than $3(q+1)/2$, then the X-exponents in $\bar{f}_1$, the Y-exponents in $\bar{f}_2$ and the Z-exponents in $\bar{f}_3$ are $0 \pmod{p^e}$; 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 $1 \pmod{p^e}$.*

Proof: The first statement is just Theorem 11.28. From this the similar statement follows for f_i: the X-exponents in f_1, the Y-exponents in f_2 and the Z-exponents in f_3 are $0 \pmod{p^e}$.

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 $X^{\alpha p^e+1}Y^{\beta' p^e+1}Z^{\gamma' p^e+1}$, 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 $-aX^{\alpha p^e+1}Y^{\beta' p^e+1}Z^{\gamma}$, 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 form $aX^{\alpha p^e}Y^{\beta' p^e+1}Z^{\gamma' p^e}$.

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 $1 \pmod{p^e}$ and for instance $f_1 = r_{N_X}\bar{f}_1$ and $\deg \bar{f}_1 = \deg_X \bar{f}_1$, 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 $\bar{f}_i$ other exponents can occur as well. Comparing the exponents one can find $Y\partial_Y \bar{f}_1 + Z\partial_Z \bar{f}_1 = X\partial_X \bar{f}_1 + Y\partial_Y \bar{f}_1 + Z\partial_Z \bar{f}_1 = 0$ 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. [30]) that the minimum of the (geometric) exponents of the points in B is equal to e defined above.

Theorem 11.33. [SzPblin] *Let B be a blocking set with exponent e. If for a certain line $|\ell \cap B| = p^e + 1$ then $\mathsf{GF}(p^e)$ is a subfield of $\mathsf{GF}(q)$ and $\ell \cap B$ is $\mathsf{GF}(p^e)$-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 $\alpha Y^{p^e+1} + \beta Y Z^{p^e} + \gamma Y^{p^e} Z + \delta Z^{p^e+1}$. As $r_{N_X}(0,1) = r_{N_X}(1,0) = r_{N_X}(1,-1) = 0$ we have $r_{N_X} = Y^{p^e}Z - YZ^{p^e} = \prod_{(a,b)\in \mathsf{PG}(1,p^e)}(aY+bZ)$. ∎

Now we can disclose one of our main goal: 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 [28].

Proposition 11.34. *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 (point-)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 $sp^{e_P} + 2rp^{e_P} + 1 \leq q+k$. From (1) $s+r \geq (q-k+1)/p^{e_P}+1$, so $q/p^{e_P} - (k-1)/p^{e_P} + r + 1 \leq s+2r \leq q/p^{e_P} + (k-1)/p^{e_P}$ hence $r \leq 2(k-1)/p^{e_P} - 1$ and $s \geq q/p^{e_P} - (k-1)/p^{e_P} + 1 - r \geq q/p^{e_P} - 3(k-1)/p^{e_P} + 2$.

For proving (3) subtract the number of points on $(p^{e_P}+1)$-secants through P from $|B|$, it is $\leq q+k-(q/p^{e_P}-3(k-1)/p^{e_P}+2)p^{e_P}-1 = 4k-2p^{e_P}-4$. 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). ∎

Recall that there are at least $q+1-k$ tangent lines through P, so at most k secants. We also know from Szőnyi [103] that $q/p^e+1 \leq k \leq q/p^e + q/p^{2e} + 2q/p^{3e} + \ldots$ Now "almost all" line-intersections of B are $\mathsf{GF}(p^e)$-linear (in fact they are isomorphic to $\mathsf{PG}(1,p^e)$ in the non-tangent case).

Corollary 11.35. [SzPblin] *For the exponent e of the blocking set, $e|h$ (where $q = p^h$).*

Proof: By Proposition 11.34 B has a lot of short secants. By Theorem 11.33 these intersections are all isomorphic to $\mathsf{PG}(1, p^e)$, so $\mathsf{GF}(p^e)$ is a subfield of $\mathsf{GF}(p^h) = \mathsf{GF}(q)$. ∎

Now we can give a very short proof for Theorem 11.5 in the case when $p^e > 13$.

Corollary 11.36. [SzPblin] *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 $\alpha \in \mathsf{GF}(p^e)$. **Claim:** αP (affine point!) is also in B. If OP is a short secant then it is obvious.

Consider the short secants through P, there are at least $q/p^e - 3(k-1)/p^e + 2$. Most of them, at least $q/p^e - 3(k-1)/p^e + 2 - \frac{4k-2p^e-4}{p^e-1} \geq \frac{q}{p^e} - \frac{7k-3k/p^e}{p^e-1}$, 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 ℓ_i, take $\alpha\ell_i$, it contains αP. If all of $\{\alpha\ell_i : i \in I\}$ were long secants then they would contain at least $2p^e(\frac{q}{p^e} - \frac{7k-3k/p^e}{p^e-1}) > q+k$ 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 $\alpha \in \mathsf{GF}(p^e)$, so it forms a vectorspace over $\mathsf{GF}(p^e)$. 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 11.37. *Let B be a minimal blocking set of $\mathsf{PG}(2, q)$, $q = p^h$, 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

$q + 1 + p^e\lceil\frac{q/p^e+1}{p^e+1}\rceil \leq |B| \leq \frac{1+(p^e+1)(q+1)-\sqrt{(1+(p^e+1)(q+1))^2-4(p^e+1)(q^2+q+1)}}{2}$.

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 point set isomorphic to $\mathsf{PG}(1,p^e)$.

These bounds are due to Blokhuis, Polverino and Szőnyi, see [86, 103], and asymptotically they give $q+\frac{q}{p^e}-\frac{q}{p^{2e}}+\frac{q}{p^{3e}}-\ldots \leq |B| \leq q+\frac{q}{p^e}+\frac{q}{p^{2e}}+2\frac{q}{p^{3e}}+\ldots$. We 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^e property was established by Szőnyi; our Theorem 11.35 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 11.33, on their number see Proposition 11.34.

Let $S(q)$ denote the set of possible sizes of small minimal blocking sets in $\mathsf{PG}(2,q)$.

Corollary 11.38. *Let B be a minimal blocking set of $\mathsf{PG}(n,q)$, $q=p^h$, with respect to k-dimensional subspaces, of size $|B| < \frac{3}{2}(q^{n-k}+1)$, 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^e 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^e+1) points precisely, and each of these (p^e+1)-sets is a collinear point set isomorphic to $\mathsf{PG}(1,p^e)$.

Proof: (Sketch.) Most of this was proved by Szőnyi and Weiner in [109]. Consider the line determined by any two points in a (p^e+1)-secant k-subspace, this line should contain p^e+1 points. Then the technique of [109] 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 $\mathsf{PG}(n,q)$ into $\mathsf{PG}(n,q^{n-k})$ where the original blocking set B becomes a blocking set w.r.t. hyperplanes, then choose an $(n-3)$-dimensional subspace $\Pi \subset \mathsf{PG}(n,q^{n-k})$ not meeting any of the secant lines of B and project B from Π onto a plane $\mathsf{PG}(2,q^{n-k})$ to obtain a planar minimal blocking set, for which Theorem 11.33 and Proposition 11.34 can be applied, implying $e|h(n-k)$.

Now in $\mathsf{PG}(n+1,q) \supseteq \mathsf{PG}(n,q)$ build a cone B^* with base B and vertex $V \in \mathsf{PG}(n+1,q) \setminus \mathsf{PG}(n,q)$; then B^* will be a (small, minimal) blocking set in $\mathsf{PG}(n+1,q)$ w.r.t. k-dimensional subspaces. The argument above gives $e|h(n+1-k)$, so $e \mid \text{g.c.d.}(h(n-k), h(n+1-k)) = h$. ∎

We remark that one may go on with building the theory for multiple blocking set. For instance, when $B \subset \mathsf{PG}(2,q)$ is a double blocking set of size $2q+k$ then

$$R(X,Y,Z) \;=\; \mathbf{W}\ \mathbf{F}(X,Y,Z)\ \mathbf{W}^T,$$

where $\mathbf{F}(X,Y,Z) = (f_{ij}(X,Y,Z))_{3\times 3}$. We will not meet this challenge now, for details see Blokhuis, Lovász, Storme, Szőnyi [28], [SzPmult1], [SzPmult2].

12 Linear point sets and Rédei type k-blocking sets in $\mathsf{PG}(n,q)$

In this section, k-blocking sets in $\mathsf{PG}(n,q)$, being of Rédei type, are investigated. In this section we do not use polynomials, but this provides the geometrical background for the parts about (i) blocking sets; (ii) directions; (iii) linear point sets, so it seemed reasonable to include it here.

A standard method to construct Rédei type k-blocking sets in $\mathsf{PG}(n,q)$ is to construct a cone having as base a Rédei type k'-blocking set in a subspace of $\mathsf{PG}(n,q)$. But also other Rédei type k-blocking sets in $\mathsf{PG}(n,q)$, which are not cones, exist. We give in this section a condition on the parameters of a Rédei type k-blocking set of $\mathsf{PG}(n, q=p^h)$, p a prime power, which guarantees that the Rédei type k-blocking set is a cone. This condition is sharp.

12.1 Introduction

There is a continuously growing theory on Rédei type blocking sets and their applications, also on the set of directions determined by the graph of a function or (as over a finite field every function is) a polynomial; the intimate connection of these two topics is obvious.

Let's recall some notation briefly. As usual, we consider $\mathsf{PG}(n,q)$ as the union of $\mathsf{AG}(n,q)$ and the 'hyperplane at infinity' H_∞. A point set in $\mathsf{PG}(n,q)$ is called *affine* if it lies in $\mathsf{AG}(n,q)$, while a subspace of $\mathsf{PG}(n,q)$ is called *affine* if it is not contained in H_∞. So in this sense an affine line has one infinite point on it. Let $\theta_n = |PG(n,q)| = \frac{q^{n+1}-1}{q-1} = q^n + q^{n-1} + ... + q + 1$.

A *k-blocking set* $B \subset PG(n,q)$ is a set of points intersecting every $(n-k)$-dimensional subspace, it is called *trivial* if it contains a k-dimensional subspace. A point $b \in B$ is *essential* if $B \setminus \{b\}$ is no longer a k-blocking set (so there is an $(n-k)$-subspace L intersecting B in b only, such an $(n-k)$-subspace can be called a *tangent*); B is *minimal* if all its points are essential. Note that for $n = 2$ and $k = 1$ we get the classical planar blocking sets.

Definition 12.1. We say that a set of points $U \subset \mathsf{AG}(n,q)$ *determines the direction* $d \in H_\infty$, if there is an affine line through d meeting U in at least two points. Denote by D the set of determined directions. Finally, let $N = |D|$, the number of determined directions.

We will always suppose that $|U| = q^k$. Now we show the connection between directions and blocking sets:

Proposition 12.2. *If $U \subseteq \mathsf{AG}(n,q)$, $|U| = q^k$, then U together with the infinite points corresponding to directions in D form a k-blocking set in $\mathsf{PG}(n,q)$. If the set D does not form a k-blocking set of H_∞ then all the points of U are essential.*

Proof: Any infinite $(n-k)$-subspace $H_{n-k} \subset H_\infty$ is blocked by D: there are q^{k-1} (disjoint) affine $(n-k+1)$-spaces through H_{n-k}, and in any of them, which has at least two points in U, a determined direction of $D \cap H_{n-k}$ is found.

Let $H_{n-k-1} \subset H_\infty$ and consider the affine $(n-k)$-subspaces through it. If $D \cap H_{n-k-1} \neq \emptyset$ then they are all blocked. If H_{n-k-1} does not contain any point of D, then every affine $(n-k)$-subspace through it must contain exactly one point of U (as if one contained at least two then the direction determined by them would fall into $D \cap H_{n-k-1}$), so they are blocked again. So $U \cup D$ blocks all affine $(n-k)$-subspaces and all the points of U are essential when D does not form a k-blocking set in H_∞. ∎

Unfortunately in general it may happen that some points of D are non-essential. If D is not too big (i.e. $|D| \leq q^k$, similarly to planar blocking sets) then it is never the case.

Proposition 12.3. *If $|D| < \frac{q^{n-1}-1}{q^{n-k-1}-1}$, then all the points of D are essential.*

Proof: Take any point $P \in D$. The number of $(n-k-1)$-subspaces through P in H_∞ is $\frac{\theta_{n-2}\theta_{n-3}\ldots\theta_k}{\theta_{n-k-2}\theta_{n-k-3}\ldots\theta_1\cdot 1}$. Any other $Q \in D \setminus \{P\}$ blocks at most $\frac{\theta_{n-3}\ldots\theta_k}{\theta_{n-k-3}\ldots\theta_1\cdot 1}$ of them. So some affine $(n-k)$-subspace through one of those infinite $(n-k-1)$-subspaces containing P only, will be a tangent at P. ∎

The k-blocking set B arising in this way has the property that it meets a hyperplane in $|B| - q^k$ points. On the other hand, if a minimal k-blocking set of size $\leq 2q^k$ meets a hyperplane in $|B| - q^k$ points then, after deleting this hyperplane, we find a set of points in the affine space determining these $|B| - q^k$ directions, so the following notion is more or less equivalent to a point set plus its directions: a k-blocking set B is of *Rédei type* if it meets a hyperplane in $|B| - q^k$ points. We remark that the theory developed by Rédei in his book [91] is highly related to these blocking sets. Minimal k-blocking sets of Rédei type are in a sense extremal examples, as for any (non-trivial) minimal k-blocking set B and hyperplane H, where H intersects B in a set $H \cap B$ which is not a k-blocking set in H, $|B \setminus H| \geq q^k$ holds.

Since the arising k-blocking set has size $q^k + |D|$, in order to find small k-blocking sets we will have to look for sets determining a small number of directions.

Hence the main problem is to classify sets determining few directions, which is equivalent to classifying small k-blocking sets of Rédei type. A strong motivation for the investigations is, that in the planar case, A. Blokhuis, S. Ball, A. Brouwer, L. Storme and T. Szőnyi classified blocking sets of Rédei type, with size $< q + \frac{q+3}{2}$, see Theorem 11.5

We call a *Rédei* k-blocking set B of $\mathsf{PG}(n,q)$ *small* when $|B| \leq q^k + \frac{q+3}{2}q^{k-1} + q^{k-2} + q^{k-3} + \cdots + q$. These small Rédei k-blocking sets will be studied in detail in the next sections.

It is our goal to study the following problem. A small Rédei k-blocking set in $\mathsf{PG}(n,q)$ can be obtained by constructing a cone with vertex a $(k-2)$-dimensional subspace Π_{k-2} in $\mathsf{PG}(n,q)$ and with base a small Rédei blocking set in a plane Π_2' skew to Π_{k-2}.

However, these are not the only examples of small k-blocking sets in $\mathsf{PG}(n,q)$. For instance, the subgeometry $\mathsf{PG}(2k,q)$ of $\mathsf{PG}(n=2k,q^2)$ is a small k-blocking set of $\mathsf{PG}(2k,q^2)$, and this is not a cone.

We give a condition (Theorem 12.15) on the parameters of the small Rédei k-blocking set in $\mathsf{PG}(n,q)$ which guarantees that this small Rédei k-blocking set is a cone; so that the exact description of this k-blocking set is reduced to that of the base of the cone.

This condition is also sharp since the k-blocking set $\mathsf{PG}(2k,q)$ in $\mathsf{PG}(2k,q^2)$ can be used to show that the conditions imposed on n, k and h in Theorem 12.15 cannot be weakened.

Our results also contribute to the study of *linear k-blocking sets in* $\mathsf{PG}(n,q)$ discussed by Lunardon [82].

Warning: In the remaining part of this section we always suppose that the conditions of the "moreover" part of Theorem 11.5 are fulfilled.

12.2 k-Blocking sets of Rédei type

Proposition 12.4. *Let $U \subset \mathsf{AG}(n,q)$, $|U| = q^k$, and let $D \subseteq H_\infty$ be the set of directions determined by U. Then for any point $d \in D$ one can find an $(n-2)$-dimensional subspace $W \subseteq H_\infty$, $d \in W$, such that $D \cap W$ blocks all the $(n-k-1)$-dimensional subspaces of W.*

The proposition can be formulated equivalently in this way: D is a union of some $B_1, ..., B_t$, each one of them being a $(k-1)$-blocking set of a projective subspace $W_1, ..., W_t$ resp., of dimension $n-2$, all contained in H_∞.

Proof: The proof goes by induction; for any point $d \in D$ we find a series of subspaces $S_1 \subset S_2 \subset ... \subset S_{n-1} \subset \mathsf{AG}(n,q)$, $\dim(S_r) = r$ such that $s_r = |S_r \cap U| \geq q^{k-n+r} + 1$ and d is the direction determined by S_1. Then, using the pigeon hole principle, after the r-th step we know that all the $(n-k-1)$-dimensional subspaces of $S_r \cap H_\infty$ are blocked by the directions determined by points in S_r, as there are q^{k-n+r} disjoint affine $(n-k)$-subspaces through any of them in S_r, so at least one of them contains 2 points of $U \cap S_r$.

For $r = 1$ it is obvious as d is determined by at least $2 = q^0+1 \geq q^{k-n+1}+1$ points of some line S_1. Then for $r+1$ consider the $\frac{q^{n-r}-1}{q-1}$ subspaces of dimension $r+1$ through S_r, then at least one of them contains at least

$$s_r + \frac{q^k - s_r}{\frac{q^{n-r}-1}{q-1}} = q^{k+1-n+r} + \frac{(s_r - q^{k-n+r})(q^{n-r}-q)}{q^{n-r}-1} > q^{k+1-n+r}$$

points of U. ∎

Corollary 12.5. *For $k = n-1$ it follows that D is the union of some $(n-2)$-dimensional subspaces of H_∞.* ∎

This corollary became important in the applications. E.g. in the nice paper Alderson-Gács[1], this became a key lemma for proving that if a linear code is extendible then it is extendible in a linear way as well.

Observation 12.6. A *projective triangle* in $\mathsf{PG}(2,q)$, q odd, is a blocking set of size $3(q+1)/2$ projectively equivalent to the set of points $\{(1,0,0),(0,1,0),(0,0,1),(0,1,a_0),(1,0,a_1),(-a_2,1,0)\}$, where a_0, a_1, a_2 are non-zero squares [65, Lemma 13.6]. The sides of the triangle defined by $(1,0,0),(0,1,0),(0,0,1)$ all contain $(q+3)/2$ points of the projective triangle, so it is a Rédei blocking set.

A cone, with a $(k-2)$-dimensional vertex at H_∞ and with the q points of a planar projective triangle, not lying on one of those sides of the triangle, as

a base, has q^k affine points and it determines $\frac{q+3}{2}q^{k-1}+q^{k-2}+q^{k-3}+...+q+1$ directions.

Lemma 12.7. *Let $U \subset \mathsf{AG}(n,q)$, $|U| = q^{n-1}$, and let $D \subseteq H_\infty$ be the set of directions determined by U. If $H_k \subseteq H_\infty$ is a k-dimensional subspace not completely contained in D then each of the affine $(k+1)$-dimensional subspaces through it intersects U in exactly q^k points.*

Proof: There are q^{n-1-k} mutually disjoint affine $(k+1)$-dimensional subspaces through H_k. If one contained less than q^k points from U then some other would contain more than q^k points (as the average is just q^k), which would imply by the pigeon hole principle that $H_k \subseteq D$, contradiction. ∎

Theorem 12.8. *Let $U \subset \mathsf{AG}(n,q)$, $|U| = q^{n-1}$, and let $D \subseteq H_\infty$ be the set of directions determined by U. Suppose $|D| \leq \frac{q+3}{2}q^{n-2}+q^{n-3}+q^{n-4}+...+q^2+q$. Then for any affine line ℓ either (i) $|U \cap \ell| = 1$ (iff $\ell \cap H_\infty \notin D$), or (ii) $|U \cap \ell| \equiv 0 \pmod{p^e}$ for some $e = e_\ell | h$.*

(iii) Moreover, in the second case the point set $U \cap \ell$ is $\mathsf{GF}(p^e)$-linear, so if we consider the point at infinity p_∞ of ℓ; two other affine points p_0 and p_1 of $U \cap \ell$, with $p_1 = p_0 + p_\infty$, then all points $p_0 + xp_\infty$, with $x \in GF(p^e)$, belong to $U \cap \ell$.

Proof: (i) A direction is not determined iff each affine line through it contains exactly one point of U. (ii) Let $|U \cap \ell| \geq 2$, $d = \ell \cap H_\infty$. Then, from Corollary 12.5, there exists an $(n-2)$-dimensional subspace $H \subset D$, $d \in H$. There are q^{n-2} lines through d in $H_\infty \setminus H$, so at least one of them has at most

$$\leq \frac{|D|-|H|}{q^{n-2}} \leq \frac{\frac{q+1}{2}q^{n-2}-1}{q^{n-2}} = \frac{q+1}{2} - \frac{1}{q^{n-2}}$$

points of D, different from d. In the plane spanned by this line and ℓ we have exactly q points of U, determining less than $\frac{q+3}{2}$ directions. So we can use Theorem 11.5 for (ii) and (iii). ∎

Corollary 12.9. *Under the hypothesis of the previous theorem, U is a $\mathsf{GF}(p^e)$-linear set for some $e|h$.*

Proof: Take the greatest common divisor of the values e_ℓ appearing in the theorem for each affine line ℓ with more than one point in U. ∎

The preceding result also means that for any set of affine points ('vectors') $\{a_1, a_2, ..., a_t\}$ in U, and $c_1, c_2, ..., c_t \in GF(p^e)$, $\sum_{i=1}^{t} c_i = 1$, we have $\sum_{i=1}^{t} c_i a_i \in U$ as well. This is true for $t = 2$ by the corollary, and for $t > 2$ we can combine them two by two, using induction, like

$$c_1a_1 + ... + c_ta_t =$$

$$(c_1 + \cdots + c_{t-1}) \left(\frac{c_1}{c_1 + \cdots + c_{t-1}} a_1 + \cdots + \frac{c_{t-1}}{c_1 + \cdots + c_{t-1}} a_{t-1} \right) + c_t a_t,$$

where $c_1 + ... + c_t = 1$.

Theorem 12.10. *Let $U \subset \mathsf{AG}(n, q)$, $|U| = q^k$, and let $D \subseteq H_\infty$ be the set of directions determined by U. If $|D| \leq \frac{q+3}{2} q^{k-1} + q^{k-2} + ... + q^2 + q$, then any line ℓ intersects U either in one point, or $|U \cap \ell| \equiv 0 \pmod{p^e}$, for some $e = e_\ell | h$. Moreover, the set $U \cap \ell$ is $\mathsf{GF}(p^e)$-linear.*

Proof: If $k = n - 1$, then the previous theorem does the job, so suppose $k \leq n-2$. Take a line ℓ intersecting U in at least 2 points. There are at most $q^k - 2$ planes joining ℓ to the other points of U not on ℓ; and their infinite points together with D cover at most $q^{k+1} + \frac{1}{2} q^k + ...$ points of H_∞, so they do not form a $(k+1)$-blocking set in H_∞. Take any $(n-k-2)$-dimensional space H_{n-k-2} not meeting any of them, then the projection π of $U \cup D$ from H_{n-k-2} to any 'affine' $(k+1)$-subspace S_{k+1} is one-to-one between U and $\pi(U)$; $\pi(D)$ is the set of directions determined by $\pi(U)$, and the line $\pi(\ell)$ contains the images of $U \cap \ell$ only (as H_{n-k-2} is disjoint from the planes spanned by ℓ and the other points of U not on ℓ). The projection is a small Rédei k-blocking set in S_{k+1}, so, using the previous theorem, $\pi(U \cap \ell)$ is $\mathsf{GF}(p^e)$-linear for some $e|h$. But then, as the projection preserves the cross-ratios of quadruples of points, the same is true for $U \cap \ell$. ∎

Corollary 12.11. *Under the hypothesis of the previous theorem, U is a $\mathsf{GF}(p^e)$-linear set for some $e|h$.*

Proof: Let e be the greatest common divisor of the values e_ℓ appearing in the preceding theorem for each affine line with more than one point in U. ∎

12.3 Linear point sets in $\mathsf{AG}(n, q)$

First we generalize Lemma 12.7.

Proposition 12.12. *Let $U \subset \mathsf{AG}(n,q)$, $|U| = q^k$, and let $D \subseteq H_\infty$ be the set of directions determined by U. If $H_r \subseteq H_\infty$ is an r-dimensional subspace, and $H_r \cap D$ does not block every $(n-k-1)$-subspace of H_r then each of the affine $(r+1)$-dimensional subspaces through H_r intersects U in exactly $q^{r+k+1-n}$ points.*

Proof: There are q^{n-1-r} mutually disjoint affine $(r+1)$-dimensional subspaces through H_r. If one contained less than $q^{r+k+1-n}$ points from U then some other would contain more than $q^{r+k+1-n}$ points (as the average is just $q^{r+k+1-n}$), which would imply by the pigeon hole principle that $H_r \cap D$ would block all the $(n-k-1)$-dimensional subspaces of H_r, contradiction. ∎

Lemma 12.13. *Let $U \subseteq \mathsf{AG}(n,p^h)$, $p > 2$, be a $\mathsf{GF}(p)$-linear set of points. If U contains a complete affine line ℓ with infinite point v, then U is the union of complete affine lines through v (so it is a cone with infinite vertex, hence a cylinder).*

Proof: Take any line ℓ' joining v and a point $Q' \in U \setminus \ell$, we prove that any $R' \in \ell'$ is in U. Take any point $Q \in \ell$, let m be the line $Q'Q$, and take a point $Q_0 \in U \cap m$ (any affine combination of Q and Q' over $\mathsf{GF}(p)$; see paragraph after the proof of Corollary 12.9). Now the cross-ratio of Q_0, Q', Q (and the infinite point of m) is in $\mathsf{GF}(p)$. Let $R := \ell \cap Q_0R'$, so $R \in U$. As the cross-ratio of Q_0, R', R, and the point at infinity of the line $R'R$, is still in $\mathsf{GF}(p)$, it follows that $R' \in U$. Hence $\ell' \subset U$. ∎

Lemma 12.14. *Let $U \subseteq \mathsf{AG}(n,p^h)$ be a $\mathsf{GF}(p)$-linear set of points. If $|U| > p^{n(h-1)}$ then U contains a line.*

Proof: The proof goes by double induction (the 'outer' for n, the 'inner' for r). The statement is true for $n = 1$. First we prove that for every $0 \le r \le n-1$, there exists an affine subspace S_r, $\dim S_r = r$, such that it contains at least $|S_r \cap U| = s_r \ge p^{hr-n+2}$ points. For $r = 0$, let S_0 be any point of U. For any $r \ge 1$, suppose that each r-dimensional affine subspace through S_{r-1} contains at most p^{hr-n+1} points of U, then

$$p^{hn-n+1} \le |U| \le \frac{p^{hn}-p^{h(r-1)}}{p^{hr}-p^{h(r-1)}}(p^{hr-n+1}-s_{r-1})+s_{r-1} \le$$

$$\le \frac{p^{hn}-p^{h(r-1)}}{p^{hr}-p^{h(r-1)}}(p^{hr-n+1}-p^{h(r-1)-n+2})+p^{h(r-1)-n+2}.$$

But this is false, contradiction.

So in particular for $r = n-1$, there exists an affine subspace S_r containing at least $|S_r \cap U| \geq p^{h(n-1)-n+2}$ points of U. But then, from the $(n-1)$-st ('outer') case we know that $S_{n-1} \cap U$ contains a line. ∎

Now we state the main theorem of this section. We assume $p > 3$ to be sure that Theorem 11.5 can be applied.

Theorem 12.15. *Let $U \subset \mathsf{AG}(n,q)$, $n \geq 3$, $|U| = q^k$. Suppose U determines $|D| \leq \frac{q+3}{2}q^{k-1} + q^{k-2} + q^{k-3} + ... + q^2 + q$ directions and suppose that U is a $\mathsf{GF}(p)$-linear set of points, where $q = p^h$, $p > 3$.*

If $n-1 \geq (n-k)h$, then U is a cone with an $(n-1-h(n-k))$-dimensional vertex at H_∞ and with base a $\mathsf{GF}(p)$-linear point set $U_{(n-k)h}$ of size $q^{(n-k)(h-1)}$, contained in some affine $(n-k)h$-dimensional subspace of $\mathsf{AG}(n,q)$.

Proof: It follows from the previous lemma (as in this case $|U| = p^{hk} \geq p^{n(h-1)+1}$) that $U = U_n$ is a cone with some vertex $V_0 = v_0 \in H_\infty$. The base U_{n-1} of the cone, which is the intersection with any hyperplane disjoint from the vertex V_0, is also a $\mathsf{GF}(p)$-linear set, of size q^{k-1}. Since U is a cone with vertex $V_0 \in H_\infty$, the set of directions determined by U is also a cone with vertex V_0 in H_∞. Thus, if U determines N directions, then U_{n-1} determines at most $(N-1)/q \leq \frac{q+3}{2}q^{k-2} + q^{k-3} + q^{k-4} + ... + q^2 + q$ directions. So if $h \leq \frac{(n-1)-1}{(n-1)-(k-1)}$ then U_{n-1} is also a cone with some vertex $v_1 \in H_\infty$ and with some $\mathsf{GF}(p)$-linear base U_{n-2}, so in fact U is a cone with a one-dimensional vertex $V_1 = \langle v_0, v_1 \rangle \subset H_\infty$ and an $(n-2)$-dimensional base U_{n-2}, and so on; before the r-th step we have V_{r-1} as vertex and U_{n-r}, a base in an $(n-r)$-dimensional space, of the current cone (we started "with the 0-th step"). Then if $h \leq \frac{(n-r)-1}{(n-r)-(k-r)}$, then we can find a line in U_{n-r} and its infinite point with V_{r-1} will generate V_r and a U_{n-1-r} can be chosen as well. When there is equality in $h \leq \frac{(n-r)-1}{(n-r)-(k-r)}$, so when $r = n-(n-k)h-1$, then the final step results in $U_{(n-k)h}$ and $V_{n-1-h(n-k)}$. ∎

The previous result is sharp as the following proposition shows.

Proposition 12.16. *In $\mathsf{AG}(n, q = p^h)$, for $n \leq (n-k)h$, there exist $\mathsf{GF}(p)$-linear sets U of size q^k containing no affine line.*

Proof: For instance, $\mathsf{AG}(2k,p)$ in $\mathsf{AG}(2k,p^2)$ for which $n = 2k = (n-k)h = (2k-k)2$.

More generally, write $hk = d_1 + d_2 + ... + d_n$, $1 \leq d_i \leq h-1$ $(i = 1, ..., n)$ in any way. Let U_i be a $\mathsf{GF}(p)$-linear set contained in the i-th coordinate

axis, $O \in U_i, |U_i| = p^{d_i}$ $(i = 1, ..., n)$. Then $U = U_1 \times U_2 \times ... \times U_n$ is a proper choice for U. ∎

13 Stability

We start with a result of [SzPdpow], which is a generalization of the main result of [104]. Let D be a set of directions in $\mathsf{AG}(2, q)$. A set $U \subset \mathsf{AG}(2, q)$ is called a *D-set* if U determines precisely the directions belonging to D.

Theorem 13.1. *Let U be a D-set of $\mathsf{AG}(2, q)$ 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 $|Y| = q$.*

The proof is based on Lemma 8.9, we omit the details here.

Comparing this to Theorem 11.5 one can see that if $U \subset \mathsf{AG}(2, q)$ determines $N \leq \frac{q+1}{2}$ directions and U is of size $q - \varepsilon$, with ε small then still we know the structure of U.

The analogue of Theorem 13.1 is the following version of the results of [SzPnuc2, 37]:

Theorem 13.2. *Let $U \subset \mathsf{AG}(2, q)$ be a point set of size $|U| = q + \varepsilon$, where $\varepsilon \leq \alpha\sqrt{q} - 1$ and $\frac{1}{2} + \frac{1}{4\sqrt{q}} \leq \alpha \leq 1$. Suppose that there are more than $\alpha(q+1)$ points on ℓ_∞, through which every affine line contains at least one point of U (kind of "nuclei" at infinity); let the complement of this point set on ℓ_∞ be called D. Then one can find ε 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 $U = \{(a_i, b_i) : i = 1, ..., q + \varepsilon\}$, 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 $\mathsf{GF}(q) \subset A(y) = \{-a_i y + b_i : i = 1, ..., q + \varepsilon\}$ for the multiset $A(y)$, that is, when $(y) \notin D$. Similarly, let $A(Y) = \{-a_i Y + b_i : i = 1, ..., q + \varepsilon\}$, 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 $\bar{\sigma}_j = \bar{\sigma}_j(A(y)) = \sigma_j(A(y) \setminus \mathsf{GF}(q))$ be the j-th elementary symmetric polynomial of the "extra" elements.

Note that $\sigma_j = (-1)^j r_j$, and like in Section 9, we have $\bar{\sigma}_j = \sigma_j$, and we can define

$$\bar{\sigma}_j(Y) \stackrel{\text{def}}{=} \sigma_j(Y) = (-1)^j r_j(Y).$$

Define the polynomial $f(X,Y) = X^\varepsilon - \bar{\sigma}_1 X^{\varepsilon-1} + \bar{\sigma}_2 X^{\varepsilon-2} - +... + (-1)^\varepsilon \bar{\sigma}_\varepsilon$. Here f is of total degree ε 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

$$f(X,y_0) = \prod_{\beta \in A_{y_0} \setminus \mathsf{GF}(q)} (X-\beta),$$

so the curve $\mathcal{F}$ defined by $f(X,Y)=0$ has precisely ε 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 $\mathsf{PG}(2,q)$.

Now, using Lemma 8.9 with the same α, we have that $\mathcal{F}$ has a linear component $X+aY-b$ over $\mathsf{GF}(q)$. 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.

* * *

We finish this subsection with a general statement on the stability of point sets. (Compare this to the beginning of Section 10.)

Result 13.3. *If $S_1, S_2 \subseteq \mathsf{PG}(2,q)$ are two point sets, with characteristic vectors $\mathbf{v}_{S_1}, \mathbf{v}_{S_2}$ and weight (or line-intersection) vectors $\mathbf{m}_{S_1} = A\mathbf{v}_{S_1}, \mathbf{m}_{S_2} = A\mathbf{v}_{S_2}$, (where A is the incidence matrix of the plane) then*

$$||\mathbf{m}_{S_1} - \mathbf{m}_{S_2}||^2 = (|S_1| - |S_2|)^2 + q \cdot |S_1 \triangle S_2|$$

where $||\mathbf{x}|| = \sqrt{\sum x_i^2}$ and $\triangle$ denotes symmetric difference.

Note that it means that the (Euclidean) distance of the line-intersection vectors of any two point sets is at least $\sqrt{q}$, so in this sense every point set is "stable".

13.1 Partial flocks of the quadratic cone in $\mathsf{PG}(3,q)$

A flock of the quadratic cone of $\mathsf{PG}(3,q)$ 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 $\mathrm{PG}(3,q)$ and, when q is even, families of ovals in $\mathrm{PG}(2,q)$, called herds. In [98] 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 $\mathsf{PG}(2,q)$, 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 $>q-\sqrt{2}\sqrt{q}$ 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 inversive planes, and is false if q is odd).

Here we prove the following

Theorem 13.4. [SzPflock] *Assume that the planes $E_i, i=1,...,q-\varepsilon$ intersect the quadratic cone $C\subset\mathsf{PG}(3,q)$ in disjoint irreducible conics. If $\varepsilon<\frac{1}{4}(1-\frac{1}{q+1})\sqrt{q}$ then one can find additional ε planes (in a unique way), which extend the set $\{E_i\}$ to a flock.*

Proof: Let C be the quadratic cone $C=\{(1,t,t^2,z):t,z\in\mathsf{GF}(q)\}\cup\{(0,0,1,z):z\in\mathsf{GF}(q)\}\cup\{(0,0,0,1)\}$ 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 $X_4=a_iX_1+b_iX_2+c_iX_3$, for $i=1,2,...,q-\varepsilon$.

Define $f_i(T)=a_i+b_iT+c_iT^2$, then $E_i\cap C^*=\{(1,t,t^2,f_i(t)):t\in\mathsf{GF}(q)\}\cup\{(0,0,1,c_i)\}$. 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 $\deg_T(\sigma_k)\le 2k$. As for any fixed $T=t\in\mathsf{GF}(q)$ 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 $\mathsf{GF}(q)\setminus\{f_i(t):i=1,...,q-\varepsilon\}$.

We are going to use the technique of Section 9. In order to do so, we define the elementary symmetric polynomials $\sigma_j^*(t)$ of the "missing elements" with the following formula:

$X^q-X=$

$$\left(X^{q-\varepsilon}-\sigma_1(t)X^{q-\varepsilon-1}+\sigma_2(t)X^{q-\varepsilon-2}-...\pm\sigma_{q-\varepsilon}(t)\right)\left(X^{\varepsilon}-\sigma_1^*(t)X^{\varepsilon-1}+\sigma_2^*(t)X^{\varepsilon-2}-...\pm\sigma_{\varepsilon}^*(t)\right);$$

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

$$\sigma_1^*(t) = -\sigma_1(t);\ \ \sigma_2^*(t) = \sigma_1(t)^2 - \sigma_2(t);\ \ \sigma_3^*(t) = -\sigma_1(t)^3 + 2\sigma_1(t)\sigma_2(t) - \sigma_3(t);$$

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

$$\sigma_1^*(T) = -\sigma_1(T); \sigma_2^*(T) = \sigma_1(T)^2 - \sigma_2(T); \sigma_3^*(T) = -\sigma_1(T)^3 + 2\sigma_1(T)\sigma_2(T) - \sigma_3(T); \tag{1}$$

up to σ_ε^*. Note that $\deg_T(\sigma_j^*) \leq 2j$. 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 $T = t \in \mathsf{GF}(q)$, so it is $X^q - X + (T^q - T)(...)$. Now define

$$G(X, T) = X^\varepsilon - \sigma_1^*(T)X^{\varepsilon-1} + \sigma_2^*(T)X^{\varepsilon-2} - ... \pm \sigma_\varepsilon^*(T), \tag{2}$$

from the recursive formulae it is a polynomial in X and T, of total degree $\leq 2\varepsilon$ and X-degree ε.

For any $T = t \in \mathsf{GF}(q)$ the polynomial $G(X, t)$ has ε roots in $\mathsf{GF}(q)$ (i.e. the missing elements $\mathsf{GF}(q) \setminus \{f_i(t) : i = 1, ..., q - \varepsilon\}$), so the algebraic curve $G(X, T)$ has at least $N \geq \varepsilon q$ distinct points in $\mathsf{GF}(q) \times \mathsf{GF}(q)$. Suppose that G has no component (defined over $\mathsf{GF}(q)$) of degree ≤ 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 $\mathsf{GF}(q)$ 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 $\mathsf{GF}(q) \times \mathsf{GF}(q)$ (at most $\varepsilon - 2$ for each $T = t \in \mathsf{GF}(q)$), contradiction (as G has at least εq).

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 $\{(1, t, t^2, f_{q-\varepsilon+1}(t)) : t \in \mathsf{GF}(q)\} \cup \{(0, 0, 1, c_{q-\varepsilon+1})\}$. Now we prove that for any $t \in \mathsf{GF}(q)$ the points

$\{(1,t,t^2,f_i(t)) : i=1,...,q-\varepsilon\}$ 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 $\Big(X^{q-\varepsilon}-\sigma_1(t)X^{q-\varepsilon-1}+\sigma_2(t)X^{q-\varepsilon-2}-...\pm\sigma_{q-\varepsilon}(t)\Big)\Big(X-f_{q-\varepsilon+1}(t)\Big) \mid X^q-X$.

Now one can repeat all this above and get $f_{q-\varepsilon+2},...,f_q$, so we have

$$G(X,T)=\prod_{q\varepsilon+1}^{q}(X-f_i(T))$$

and the values $f_i(t), i=1,...,q$ are all distinct for any $t\in\mathsf{GF}(q)$. 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 $\underbrace{c_1,...,c_{q-\varepsilon}}_{\Gamma};\ \underbrace{c_{q-\varepsilon+1},...,c_q}_{\Gamma^*}$ are all distinct (for Γ 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

$$\sigma_1(\Gamma^*)=-\sigma_1(\Gamma);\ \ \sigma_2(\Gamma^*)=\sigma_1(\Gamma)^2-\sigma_2(\Gamma);\ \ \sigma_3(\Gamma^*)=-\sigma_1(\Gamma)^3+2\sigma_1(\Gamma)\sigma_2(\Gamma)-\sigma_3(\Gamma);$$

etc., so

$X^q-X=\Big(X^{q-\varepsilon}-\sigma_1(\Gamma)X^{q-\varepsilon-1}+\sigma_2(\Gamma)X^{q-\varepsilon-2}-...\sigma_{q-\varepsilon}(\Gamma)\Big)\Big(X^{q-\varepsilon}-\sigma_1(\Gamma^*)X^{q-\varepsilon-1}+\sigma_2(\Gamma^*)X^{q-\varepsilon-2}-...\sigma_{q-\varepsilon}(\Gamma^*)\Big)$, which completes the proof. ∎

In the prime case one can prove a better bound:

Result 13.5. *If $q=p$ is a prime then in Theorem 13.4 the condition $\varepsilon<\frac{1}{4}\sqrt{q}$ can be changed for the weaker $\varepsilon<\frac{1}{40}p+1$ (so the result is much stronger).*

Using a similar method one can prove an "upper stability" result:

Result 13.6. *Assume that the planes $E_i, i=1,...,q+\varepsilon$ intersect the quadratic cone $C\subset\mathsf{PG}(3,q)$ in disjoint irreducible conics that cover the cone minus its vertex. If $\varepsilon<\frac{1}{4}(1-\frac{1}{q+1})\sqrt{q}$ then one can find ε planes (in a unique way), such that if you remove the points of the irreducible conics, in which these ε planes intersect C, from the multiset of the original cover then every point of C (except the vertex) will be covered precisely once.*

13.2 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 [SzPflhigh].

Theorem 13.7. *For $2 \le d \le \sqrt[6]{q}$ consider the cone $\{(1,t,t^d,z) : t,z \in \mathsf{GF}(q)\} \cup \{(0,0,1,z) : z \in \mathsf{GF}(q)\} \cup \{(0,0,0,1)\} = C \subset \mathsf{PG}(3,q)$ and let $C^* = C \setminus \{(0,0,0,1)\}$. Assume that the planes E_i, $i = 1,...,q-\varepsilon$, $E_i \not\ni (0,0,0,1)$, intersect C^* in pairwise disjoint curves. If $\varepsilon < \lfloor \frac{1}{d^2}\sqrt{q} \rfloor$ then one can find additional ε 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. *We could have indicated the modifications only; then the text would be one or two pages shorter but possibly more complicated. We did not want to omit the original (quadratic) proof either because of its compactness; we ask for the reader's understanding and mercy.* 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 ε factors, and (ii) to show that each of these factors corresponds to a missing plane. For (i) we use our Lemma 8.9. 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 13.7. Suppose that the plane E_i has the equation $X_4 = a_iX_1 + b_iX_2 + c_iX_3$, for $i = 1,2,...,q-\varepsilon$.

Define $f_i(T) = a_i + b_iT + c_iT^d$, then $E_i \cap C = \{(1,t,t^d,f_i(t)) : t \in \mathsf{GF}(q)\} \cup \{(0,0,1,c_i)\}$. 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 $\deg_T(\sigma_k) \le dk$.

We proceed as in the quadratic case and so we define the polynomials

$$\sigma_1^*(T) = -\sigma_1(T);\ \sigma_2^*(T) = \sigma_1(T)^2 - \sigma_2(T);\ \sigma_3^*(T) = -\sigma_1(T)^3 + 2\sigma_1(T)\sigma_2(T) - \sigma_3(T);\ ... \tag{1*}$$

up to σ_ε^*. Note that $\deg_T(\sigma_j^*) \le dj$. From the definition

$$\Big(X^{q-\varepsilon} - \sigma_1(T)X^{q-\varepsilon-1} + ... \pm \sigma_{q-\varepsilon}(T)\Big)\Big(X^\varepsilon - \sigma_1^*(T)X^{\varepsilon-1} + \sigma_2^*(T)X^{\varepsilon-2} - ... \pm \sigma_\varepsilon^*(T)\Big)$$

is a polynomial, which is $X^q - X$ for any substitution $T = t \in \mathsf{GF}(q)$, so it is of the form $X^q - X + (T^q - T)(...)$. Now define

$$G(X,T) = X^\varepsilon - \sigma_1^*(T)X^{\varepsilon-1} + \sigma_2^*(T)X^{\varepsilon-2} - ... \pm \sigma_\varepsilon^*(T), \tag{2}$$

from the recursive formulae it is a polynomial in X and T, of total degree $\le d\varepsilon$ and X-degree ε.

For any $T = t \in \mathsf{GF}(q)$ the polynomial $G(X,t)$ has ε roots in $\mathsf{GF}(q)$ (i.e. the missing elements $\mathsf{GF}(q) \setminus \{f_i(t) : i = 1,...,q-\varepsilon\}$), so the algebraic curve $G(X,T)$ has at least $N \ge \varepsilon q$ distinct points in $\mathsf{GF}(q) \times \mathsf{GF}(q)$. Suppose that G

has no component (defined over $\mathsf{GF}(q)$) of degree $\leq d$. Let's apply the Lemma with a suitable $\frac{1}{d+1} + \frac{1+d(d-1)\sqrt{q}}{(d+1)q} \leq \alpha < \frac{1}{d}$, $n = \deg G \leq d\varepsilon \leq \frac{1}{d}\sqrt{q} - d + \frac{3}{2}$, we have

$$\varepsilon q \leq N \leq d\varepsilon q\alpha < \varepsilon q,$$

which is false, so $G = H_1G_1$, where H_1 is an irreducible factor over $\mathsf{GF}(q)$ 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 $\mathsf{GF}(q) \times \mathsf{GF}(q)$ (at most $\varepsilon - d_X$ for each $T = t \in \mathsf{GF}(q)$), 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 $H_1(X,T) = X - f_{q-\varepsilon+1}(T)$, where

$$f_{q-\varepsilon+1}(T) = a_{q-\varepsilon+1} + b_{q-\varepsilon+1}T + c_{q-\varepsilon+1}T^d + \delta_{q-\varepsilon+1}(T),$$

where $\delta_{q-\varepsilon+1}(T)$ is an "error polynomial" with terms of degree between 2 and $d-1$. At the end of the proof we will show that $\delta_{q-\varepsilon+1}$ and other error polynomials are zero.

Now one can repeat everything for G_1, which has at least $(\varepsilon-1)q$ distinct points in $\mathsf{GF}(q) \times \mathsf{GF}(q)$ (as H_1 has exactly q and H_1G_1 has at least εq). The similar reasoning gives $G_1 = H_2G_2$, where $H_2(X,T) = X - f_{q-\varepsilon+2}(T)$ with $f_{q-\varepsilon+2}(T) = a_{q-\varepsilon+2} + b_{q-\varepsilon+2}T + c_{q-\varepsilon+2}T^d + \delta_{q-\varepsilon+2}(T)$. Going on we get $f_{q-\varepsilon+3}, ..., f_q$ (where for $j = q-\varepsilon+1, ..., q$ we have $f_j(T) = a_j + b_jT + c_jT^d + \delta_j(T)$, 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 $t \in \mathsf{GF}(q)$ the values $f_1(t), ..., f_q(t)$ are all distinct, this is obvious from

$$\Big(X^{q-\varepsilon} - \sigma_1(t)X^{q-\varepsilon-1} + \sigma_2(t)X^{q-\varepsilon-2} - ... \pm \sigma_{q-\varepsilon}(t)\Big)\Big((X - f_{q-\varepsilon+1}(t))...(X - f_q(t))\Big) = X^q - X.$$

For $j = q-\varepsilon+1, ..., q$ let the plane E_j be defined by $X_4 = a_jX_1 + b_jX_2 + c_jX_3$. We are going to prove that $\{E_j : j = 1, ..., q\}$ 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

$\underbrace{c_1, ..., c_{q-\varepsilon}}_{\Gamma}$; $\underbrace{c_{q-\varepsilon+1}, ..., c_q}_{\Gamma^*}$ are all distinct (for Γ we know it). (Note that even 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

$\sigma_1(\Gamma^*) = -\sigma_1(\Gamma)$; $\sigma_2(\Gamma^*) = \sigma_1(\Gamma)^2 - \sigma_2(\Gamma)$; $\sigma_3(\Gamma^*) = -\sigma_1(\Gamma)^3 + 2\sigma_1(\Gamma)\sigma_2(\Gamma) - \sigma_3(\Gamma)$;

etc., so

$$X^q - X = \Big(X^{q-\varepsilon} - \sigma_1(\Gamma)X^{q-\varepsilon-1} + \sigma_2(\Gamma)X^{q-\varepsilon-2} - ... \pm \sigma_{q-\varepsilon}(\Gamma)\Big)\Big(X^\varepsilon - \sigma_1(\Gamma^*)X^{\varepsilon-1} + \sigma_2(\Gamma^*)X^{\varepsilon-2} - ... \pm \sigma_{q-\varepsilon}(\Gamma^*)\Big),$$

which we wanted to prove.

Now we want to get rid of the δ_j's, i.e. we are going to prove that $\delta_{q-\varepsilon+1}, ..., \delta_q = 0$. Let s be the maximal T-exponent appearing in any of $\delta_{q-\varepsilon+1}, ..., \delta_q$, so each $\delta_j(T) = d_j T^s + ...$ (for $j = q-\varepsilon+1, ..., q$; also $2 \leq s \leq d-1$ and there exists a $d_j \neq 0$). In the equation
$G(X,T) = X^\varepsilon - \sigma_1^*(T)X^{\varepsilon-1} + \sigma_2^*(T)X^{\varepsilon-2} - ... \pm \sigma_\varepsilon^*(T) =$

$$\prod_{i=1}^{\varepsilon}(X - a_{q-\varepsilon+i} - b_{q-\varepsilon+i}T - c_{q-\varepsilon+i}T^d - \delta_{q-\varepsilon+i}(T)),$$

the coefficient of $X^{\varepsilon-j}T^{d(j-1)+s}$, $j = 1, ..., \varepsilon$ is zero on the left hand side (i.e. the coefficient of $T^{d(j-1)+s}$ in σ_j^*, it can be seen by induction from (1^*) for instance), and it is

$$\sigma_{j-1}(\Gamma^* \backslash \{c_{q-\varepsilon+1}\})d_{q-\varepsilon+1} + \sigma_{j-1}(\Gamma^* \backslash \{c_{q-\varepsilon+2}\})d_{q-\varepsilon+2} + ... + \sigma_{j-1}(\Gamma^* \backslash \{c_q\})d_q$$

on the right hand side. Hence we have a system of homogeneous linear equations for $d_{q-\varepsilon+1}, ..., d_q$ with the elementary symmetric determinant

$$\begin{vmatrix} 1 & 1 & ... & 1 \\ \sigma_1(\Gamma^* \setminus \{c_{q-\varepsilon+1}\}) & \sigma_1(\Gamma^* \setminus \{c_{q-\varepsilon+2}\}) & ... & \sigma_1(\Gamma^* \setminus \{c_q\}) \\ \sigma_2(\Gamma^* \setminus \{c_{q-\varepsilon+1}\}) & \sigma_2(\Gamma^* \setminus \{c_{q-\varepsilon+2}\}) & ... & \sigma_2(\Gamma^* \setminus \{c_q\}) \\ \vdots & & & \\ \sigma_{\varepsilon-1}(\Gamma^* \setminus \{c_{q-\varepsilon+1}\}) & \sigma_{\varepsilon-1}(\Gamma^* \setminus \{c_{q-\varepsilon+2}\}) & ... & \sigma_{\varepsilon-1}(\Gamma^* \setminus \{c_q\}) \end{vmatrix} =$$

$\prod_{1 \leq i < j \leq \varepsilon}(c_{q-\varepsilon+i} - c_{q-\varepsilon+j})$, which is non-zero as the c_i's are pairwise distinct. Hence the unique solution is $d_{q-\varepsilon+1}, ..., d_q = 0$ and $f_j(T) = a_j + b_j T + c_j T^d$ for each $j = 1, ..., q$.

Our final and the last missing argument we need is that for $j = 1, ..., q$ the plane E_j intersects C in $\{(1, t, t^d, f_j(t)) : t \in \mathsf{GF}(q)\} \cup \{(0, 0, 1, c_j)\}$, so these intersections are pairwise disjoint, $E_1, ..., E_q$ is a flock of C. ∎

14 On the structure of non-determined directions

14.1 Introduction

This section is based on [SzPdirec]. Recall that given a point set $U \subset \mathsf{AG}(n,q) \subset \mathsf{PG}(n,q)$, a direction, i.e. a point $t \in H_\infty = \mathsf{PG}(n,q) \setminus \mathsf{AG}(n,q)$ is *determined* by U if there is an affine line through t which contains at least 2 points of U. Note that if $|U| > q^{n-1}$ then every direction is determined.

Especially in the planar case, many results on extendability of affine point sets not determining a given set of directions are known. Let's recall the following theorem from [104].

Theorem 14.1. *Let $U \subseteq \mathsf{AG}(2,q)$ be a set of affine points of size $q-\varepsilon$ with $\varepsilon < \sqrt{q}/2$, which does not determine a set D of more than $(q+1)/2$ directions. Then U can be extended to a set of size q, not determining the set D of directions.*

An extendability result known for general dimension is the following. Originally, it was proved in [50] for $n = 3$. A proof for general n can be found in [9].

Theorem 14.2. *Let $q = p^h$, p an odd prime and $h > 1$, and let $U \subseteq \mathsf{AG}(n,q)$, $n \geq 3$, be a set of affine points of size $q^{n-1} - 2$, which does not determine a set D of at least $p+2$ directions. Then U can be extended to a set of size q, not determining the set D of directions.*

The natural question is whether Theorem 14.2 can be improved in the sense that extendability of sets of size $q^{n-1} - \varepsilon$ is investigated, for $\varepsilon > 2$, possibly with stronger assumptions on the number of non-determined directions. This general question seems to be hard for $n \geq 3$, and up to our knowledge, no other result different from Theorem 14.2 is known for $n \geq 3$.

In this section, we investigate affine point sets of size $q^{n-1} - \varepsilon$, for arbitrary ε, where the strongest results are obtained when ε is small. Instead of formulating an extendability result in terms of the number of non-determined directions, we formulate it in terms of the structure of the set of non-determined directions. Finally, we add a section with an application of the obtained theorem.

14.2 The main result

As usual, a point of $\mathsf{PG}(n,q)$ is represented by a homogenous $(n+1)$-tuple $(a_0, a_1, ..., a_n) \neq (0, 0, \ldots, 0)$. A hyperplane is the set of points whose coor-

dinates satisfy a linear equation

$$a_0X_0 + a_1X_1 + \cdots + a_nX_n = 0$$

and so hyperplanes are represented by homogeneous $(n+1)$-tuples $[a_0, a_1, ..., a_n] \neq [0, 0, \ldots, 0]$. Embed the affine space $\mathsf{AG}(n,q)$ in $\mathsf{PG}(n,q)$ such that the hyperplane $X_0 = 0$, i.e. the hyperplane with coordinates $[1, 0, \ldots, 0]$ is H_∞, the hyperplane at infinity of $\mathsf{AG}(n,q)$. Then the points of $\mathsf{AG}(n,q)$ will be coordinatized as $(1, a_1, a_2, ..., a_n)$.

The map δ from the points of $\mathsf{PG}(n,q)$ to its hyperplanes, mapping a point $(a_0, a_1, a_2, ..., a_n)$ to a hyperplane $[a_0, a_1, \ldots, a_n]$ is the *standard duality* of $\mathsf{PG}(n,q)$.

Let $U \subseteq \mathsf{AG}(n,q)$ be an affine point set, $|U| = q^{n-1} - \varepsilon$. Let $D \subseteq H_\infty$ be the set of directions determined by U and put $N = H_\infty \setminus D$ the set of non-determined directions.

Lemma 14.3. *Let $0 \leq r \leq n-2$. Let $\alpha = (0, \alpha_1, \alpha_2, \alpha_3, ..., \alpha_n) \in N$ be a non-determined direction. Then each of the affine subspaces of dimension $r+1$ through α contain at most q^r points of U.*

Proof: We prove it by the pigeon hole principle. An affine subspace of dimension $r+1$ through α contains q^r affine (disjoint) lines through α, and each line contains at most one point of U as α is a non-determined direction. ∎

Definition 14.4. *If an affine subspace of dimension $r+1 \leq n-1$ through $\alpha \in N$ contains less than q^r points of U, then it is called a* deficient subspace. *If it contains $q^r - t$ points of U, then its* deficiency *is t.*

Corollary 14.5. *Let $T \subseteq H_\infty$ be a subspace of dimension $r \leq n-2$ containing $\alpha \in N$. Then there are precisely ε deficient subspaces of dimension $r+1$ (counted possibly with multiplicity) through T (a subspace with deficiency t is counted with multiplicity t).*

In particular:

Corollary 14.6. *There are precisely ε affine* lines *through α not containing any point of U (and $q^{n-1} - \varepsilon$ lines with 1 point of U each).*

Now consider the set $U = \{(1, a_1^i, a_2^i, a_3^i, \ldots, a_n^i) : i = 1, ..., q^{n-1} - \varepsilon\}$. We define its Rédei polynomial as follows:

$$R(X_0, X_1, X_2, ..., X_n) = \prod_{i=1}^{q^{n-1}-\varepsilon} (X_0 + a_1^i X_1 + a_2^i X_2 + ... + a_n^i X_n).$$

The intersection properties of the set U with hyperplanes of $\mathsf{PG}(n,q)$ are translated into algebraic properties of the polynomial R as follows. Consider $x_1, x_2, \ldots, x_n \in \mathsf{GF}(q)$, then $x \in \mathsf{GF}(q)$ is a root with multiplicity m of the equation $R(X_0, x_1, x_2, \ldots, x_n) = 0$ if and only if the hyperplane $[x, x_1, x_2, \ldots, x_n]$ contains m points of U.

Define the set $S(X_1, X_2, ..., X_n) = \{a_1^i X_1 + a_2^i X_2 + ... + a_n^i X_n : i = 1, ..., q^{n-1} - \varepsilon\}$, then R can be written as

$$R(X_0, X_1, X_2, ..., X_n) = \sum_{j=0}^{q^{n-1}-\varepsilon} \sigma_{q^{n-1}-\varepsilon-j}(X_1, X_2, ..., X_n) X_0^j,$$

where $\sigma_j(X_1, X_2, ..., X_n)$ is the j-th elementary symmetric polynomial of the set $S(X_1, X_2, ..., X_n)$.

Consider the subspace $s_{x_1,x_2,...,x_n} \subset H_\infty = [1, 0, ..., 0]$ of dimension $n-2$ which is the intersection of the hyperplanes $[x_0, x_1, x_2, ..., x_n], x_0 \in \mathsf{GF}(q)$. Suppose that $s_{x_1,x_2,...,x_n}$ contains an undetermined direction then, by Lemma 14.3, each of the hyperplanes different from H_∞ through $s_{x_1,x_2,...,x_n}$, contains at most q^{n-2} points of U. This implies that there are precisely ε such hyperplanes (counted with multiplicity) through $s_{x_1,x_2,...,x_n}$ containing less than q^{n-2} points of U (a hyperplane with deficiency t is counted with multiplicity t). Algebraically, this means that for the $(n-2)$-dimensional subspace $s_{x_1,x_2,...,x_n}$,

$$R(X_0, x_1, x_2, ..., x_n) f(X_0) = (X_0^q - X_0)^{q^{n-2}} \tag{1}$$

where $f(X_0) = X_0^\varepsilon + \sum_{k=1}^{\varepsilon} f_k X_0^{\varepsilon-k}$ is a fully reducible polynomial of degree ε. Comparing the two sides of equation (1), one gets linear equations for the coefficients f_k of f in terms of the $\sigma_j(x_1, \ldots, x_n)$, and it is easy to see that the solution for each f_k is a polynomial expression in terms of the $\sigma_j(x_1, \ldots, x_n)$, $j = 1, \ldots, k$, use e.g. Cramer's rule to solve the system of equations, and notice that the determinant in the denominator equals 1. The polynomial expression is independent from the elements $x_1, x_2, \ldots, x_n$ (still under the assumption that $s_{x_1,x_2,...,x_n}$ does contain an undetermined direction), so we can change them for the variables $X_1, X_2, \ldots, X_n$ which makes the coefficients f_k polynomials in these variables; then the total degree of each $f_k(\sigma_j(X_1, \ldots, X_n) : j = 1, \ldots, n)$ is k.

Hence, using the polynomial expressions $f_k(\sigma_j : j)$, we can define the polynomial

$$f(X_0, X_1, \ldots, X_n) = X_0^\varepsilon + \sum_{k=1}^{\varepsilon} f_k(\sigma_1, \ldots, \sigma_k) X_0^{\varepsilon-k} \tag{2}$$

Clearly, $f(X_0, X_1, \ldots, X_n)$ is a polynomial of total degree ε, and, substituting $X_i = x_i$, $i = 1, \ldots, n$ for which $s_{x_1,\ldots,x_n}$ contains an undetermined direction, yields the polynomial $f(X_0, x_1, \ldots, x_n)$ that splits completely into ε linear factors. Also, since f contains the term X_0^ε, the point $(1, 0, 0, \ldots, 0)$ is not a point of the hypersurface.

Suppose now that $f = \prod_i \phi_i$, where the polynomials $\phi_i(X_1, \ldots, X_n)$ are irreducible of degree ε_i, $\sum_i \varepsilon_i = \varepsilon$. Then each factor inherits the properties that (i) whenever the subspace $s_{x_1,x_2,\ldots,x_n} \subset H_\infty$ of dimension $n-2$ contains an undetermined direction, then $\phi_i(X_0, x_1, x_2, ..., x_n)$ splits into ε_i linear factors; and (ii) $(1, 0, ..., 0)$ is not a point of ϕ_i. So from now on we will think of f as an irreducible polynomial satisfying (i) and (ii).

$f(X_0, X_1, \ldots, X_n) = 0$ is an algebraic hypersurface in the dual space $\mathsf{PG}(n, q)$. Our aim is to prove that it splits into ε hyperplanes, or (equivalently) that it contains a linear factor (i.e. a hyperplane; then we can decrease ε by one, etc.). Therefore, we state and prove a series of technical lemmas.

Lemma 14.7. *Let $T \neq H_\infty$ be a deficient hyperplane through $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_n) \in N$ (so T contains less than q^{n-2} points of U). Then in the dual space $\mathsf{PG}(n, q)$, T corresponds to an intersection point t of f and the hyperplane $[\alpha_0, \alpha_1, \ldots, \alpha_n]$.*

Proof: If $T = [x_0, x_1, \ldots, x_n]$ is a deficient hyperplane, then x_0 is a solution of the equation $f(X_0, x_1, x_2, \ldots, x_n) = 0$, hence, in the dual space $\mathsf{PG}(n, q)$, $t = (x_0, x_1, \ldots, x_n)$ is a point of f. If T contains $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_n) \in N$, then t is contained in the hyperplane $[\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_n]$. ∎

Lemma 14.8. *Let $(\alpha) \in N$ be a non-determined direction. Then in the dual space $\mathsf{PG}(n, q)$ the intersection of the hyperplane $[\alpha]$ and f is precisely the union of ε different subspaces of dimension $n - 2$.*

Proof: First notice that

> If $(0, \alpha_1, \alpha_2, ..., \alpha_n) \in H_\infty = [1, 0, ..., 0]$ is an undetermined direction, then for all the subspaces $s_{x_1,x_2,\ldots,x_n} \subset H_\infty$ of dimension $n-2$ through $(0, \alpha_1, \alpha_2, \alpha_3, ..., \alpha_n)$ the polynomial $f(X_0, x_1, x_2, ..., x_n)$ has precisely ε roots, counted with multiplicity.

translates to

> In the hyperplane $[0, \alpha_1, \alpha_2, ..., \alpha_n] \ni (1, 0, ..., 0)$, all the lines through $(1, 0, ..., 0)$ intersect the surface $f(X_0, x_1, x_2, ..., x_n) = 0$ in precisely ε points, counted with intersection multiplicity.

Define $\bar{f}$ as the surface of degree $\bar{\varepsilon} \leq \varepsilon$, which is the intersection of f and the hyperplane $[0, \alpha_1, \alpha_2, ..., \alpha_n]$. We know that all the lines through $(1, 0, ..., 0)$ intersect $\bar{f}$ in precisely ε points (counted with intersection multiplicity). So if $\bar{f} = \prod_i \bar{\phi}_i$, where $\bar{\phi}_i$ is irreducible of degree $\bar{\varepsilon}_i$ and $\sum_i \bar{\varepsilon}_i = \bar{\varepsilon}$, then we have that all the lines through $(1, 0, ..., 0)$ intersect $\bar{\phi}_i$ in precisely $\bar{\varepsilon}_i$ points (counted with intersection multiplicity).

By Corollary 14.6 we know that there are precisely ε different affine lines through the non-determined direction (α) not containing any point of U. In the dual space $\mathsf{PG}(n, q)$ these lines correspond to ε different subspaces of dimension $n-2$ contained in the hyperplane $[\alpha]$. The deficient hyperplanes through these ε original lines correspond to the points of the subspaces in the dual. Hence by Lemma 14.7, all points of these subspaces are in f, which means that in $[\alpha]$ there are ε different subspaces of dimension $n-2$ totally contained in f. ∎

Now we prove a lemma, which is interesting for its own sake as well.

Lemma 14.9. *Let $f(X_0, ..., X_n)$ be a homogeneous polynomial of degree $d < q$. Suppose that there are $n-1$ independent concurrent lines $\ell_1, ..., \ell_{n-1}$ through the point P in $\mathsf{PG}(n, q)$ totally contained in the hypersurface $f = 0$. Then the hyperplane spanned by $\ell_1, ..., \ell_{n-1}$ is a tangent hyperplane of f.*

Proof: Without loss of generality, let $P = (1, 0, 0, ..., 0)$ and ℓ_i be the "axis" $\langle P, \overset{0}{(1}, \overset{1}{0}, 0, ..., 0, \overset{i}{1}, 0, \ldots, \overset{n}{0})\rangle$, $i = 1, ..., n-1$. We want to prove that the hyperplane $x_n = 0$, i.e. $[0, ..., 0, 1]$ is tangent to f at P.

Firstly, observe that $\partial_{X_0} f(P) = 0$ as f has no term of type X_0^d since $f(P) = 0$.

Now we prove that $\partial_{X_i} f(P) = 0$ for all $i = 1, ..., n-1$. As f vanishes on ℓ_i we have $f(sX_i, 0, ..., 0, X_i, 0, ..., 0) = 0$ for all substitutions to s and X_i. As $f(sX_i, 0, ..., 0, X_i, 0, ..., 0) = X_i^d f_0(s)$ for some f_0 with $\deg f_0 \leq d < q$, we have $f_0 \equiv 0$. In particular, f_0 has no term of degree $d-1$, so f has no term of type $X_0^{d-1} X_i$. Hence $\partial_{X_i} f(1, 0, 0, ..., 0) = 0$. ∎

Corollary 14.10. *Let $f(X_0, ..., X_n)$ be a homogeneous polynomial of degree $d < q$. Suppose that in $\mathsf{PG}(n, q)$ the intersection of a hyperplane H and the hypersurface $f = 0$ contains two complete subspaces of dimension $n-2$. Then H is a tangent hyperplane of f.*

Proof: Choose a point P in the intersection of the two subspaces of dimension $n-2$, the lines $\ell_1, ..., \ell_{n-2}$ through P in one of the subspaces and

ℓ_{n-1} through P in the other such that $\ell_1, ..., \ell_{n-1}$ be independent and apply Lemma 14.9. ∎

Corollary 14.11. *If $(\alpha) = (0, \alpha_1, \alpha_2, ..., \alpha_n) \in N \subset H_\infty$ is a non-determined direction, then (in the dual space) the hyperplane $[\alpha]$ is a tangent hyperplane of f. Note that $[\alpha]$ contains $(1, 0, ..., 0)$.*

Now we generalize Theorem 14.2.

Theorem 14.12. *Let $n \geq 3$. Let $U \subset \mathsf{AG}(n, q) \subset \mathsf{PG}(n, q)$, $|U| = q^{n-1} - 2$. Let $D \subseteq H_\infty$ be the set of directions determined by U and put $N = H_\infty \backslash D$ the set of non-determined directions. Then U can be extended to a set $\bar{U} \supseteq U$, $|\bar{U}| = q^{n-1}$ determining the same directions only, or the points of N are collinear and $|N| \leq \lfloor \frac{q+3}{2} \rfloor$, or the points of N are on a (planar) conic curve.*

Proof: Let $n \geq 3$. The hypersurface $f = 0$ is a quadric in the projective space $\mathsf{PG}(n, q)$. We will investigate the hyperplanes through the point $(1, 0, \ldots, 0)$ that meet $f = 0$ in exactly two $(n-2)$-dimensional subspaces. If the quadric $f = 0$ contains $(n-2)$-dimensional subspaces, then either $n = 3$ and the quadric is hyperbolic, or the quadric must be singular, since $\lfloor (n-1)/2 \rfloor$ is an upper bound for the dimension of the generators. If $f = 0$ contains 2 hyperplanes, then $f = 0$ is the product of two linear factors, counted with multiplicity. But then, by our remark before Lemma 14.7, the set U can be extended. Hence, if we suppose that the set U cannot be extended, the quadric $f = 0$ contains $(n-2)$-dimensional subspaces, so it is a cone with vertex an $(n-3)$-dimensional subspace and base a (planar) conic, or it is a cone with vertex an $(n-4)$-dimensional subspace and base a hyperbolic quadric in a 3-space. (Note that the second one contains the case when $n = 3$ and f is a hyperbolic quadric itself.) Denote in both cases the vertex by V.

Firstly suppose that $f = 0$ has an $(n-3)$-dimensional subspace V as vertex. A hyperplane $[\alpha]$ through $(1, 0, \ldots, 0)$ containing two $(n-2)$-dimensional subspaces must contain V and meets the base conic in two points (counted with multiplicity). Hence $[\alpha]$ is one of the $(q+1)$ hyperplanes through the span of $\langle (1, 0, \ldots, 0),\ V \rangle$, so dually, the undetermined direction (α) is a point of the line, which is the intersection of the dual (plane) of V and H_∞. When q is odd, there are $\frac{q+1}{2}$, respectively $\frac{q+3}{2}$ such hyperplanes meeting the base conic, depending on whether the vertex V is projected from the point $(1, 0, \ldots, 0)$ onto an internal point, respectively, an external point of the base conic. When q is even, there are $\frac{q}{2}$ such hyperplanes.

Secondly suppose that $f = 0$ has an $(n-4)$-dimensional subspace V as vertex. Now a hyperplane $[\alpha]$ through $(1,0,\ldots,0)$ contains V and it meets the base quadric in two lines, i.e. a tangent plane to this hyperbolic quadric. Hence, $[\alpha]$ is one of the q^2+q+1 hyperplanes through the span of $\langle(1,0,\ldots,0),\ V\rangle$, so dually, the undetermined direction (α) is a point of the plane, which is the intersection of the dual (3-space) of V and H_∞.

Among these hyperplanes only those count, which meet the base hyperbolic quadric in two lines, i.e. those which intersect the base 3-space in such a tangent plane of the hyperbolic quadric, which goes through the projection of V from the point $(1,0,\ldots,0)$. Dually these hyperplanes form a conic, so (α) is a point of this conic. ∎

We consider the case when U is extendible as the typical one: otherwise N has a very restricted (strong) structure; although note that there exist examples of maximal point sets U, of size q^2-2, $q \in \{3,5,7,11\}$, not determining the points of a conic at infinity. These examples occur in the theory of maximal partial ovoids of generalized quadrangles, and were studied in [56], [47], and [49]. Non-existence of such examples for $q = p^h$, p an odd prime, $h > 1$, was shown in [50].

Now we prove a general extendability theorem in the 3-space if $\varepsilon < p$.

Theorem 14.13. *Let $U \subset \mathsf{AG}(3,q) \subset \mathsf{PG}(3,q)$, $|U| = q^2-\varepsilon$, where $\varepsilon < p$. Let $D \subseteq H_\infty$ be the set of directions determined by U and put $N = H_\infty \setminus D$ the set of non-determined directions. Then N is contained in a plane curve of degree $\varepsilon^4 - 2\varepsilon^3 + \varepsilon$ or U can be extended to a set $\bar{U} \supseteq U$, $|\bar{U}| = q^2$.*

Proof: We proceed as before: we define the Rédei polynomial of U, then we calculate $f(X_0,X_1,X_2,X_3)$ of degree ε.

Finally we realize that for each triple (α,β,γ), if $(0,\alpha,\beta,\gamma) \in N \subset H_\infty$ is an undetermined direction then the plane $[0,\alpha,\beta,\gamma]$, which apparently goes through the point $(1,0,0,0)$, is a tangent plane of f.

The tangent planes of f are of the form

$$[\partial_{X_0}f(a,b,c,d), \partial_{X_1}f(a,b,c,d), \partial_{X_2}f(a,b,c,d), \partial_{X_3}f(a,b,c,d)]$$

where (a,b,c,d) is a smooth point of f, and there are some others going through points of f where $\partial_{X_0}f = \partial_{X_1}f = \partial_{X_2}f = \partial_{X_3}f = 0$. For planes of both type containing $(1,0,0,0)$ we have $\partial_{X_0}f(a,b,c,d) = 0$, so we get that the triples (α,β,γ), with $(0,\alpha,\beta,\gamma) \in H_\infty$ being an undetermined direction, correspond to tangent planes $[0,\alpha,\beta,\gamma]$ of f in points (a,b,c,d) which belong to the intersection of f and $\partial_{X_0}f$, which is a space curve $\mathcal{C}$ of degree $\varepsilon(\varepsilon-1)$. Projecting these tangent planes from $(1,0,0,0)$ (which all they contain) onto

a (fixed) plane we get that in that plane the projected images $[\alpha, \beta, \gamma]$ are tangent lines of the projected image $\hat{\mathcal{C}}$, which is a plane curve of degree $\varepsilon(\varepsilon-1)$. So we get that the undetermined directions are contained in a plane curve of degree $\varepsilon(\varepsilon-1)\Big(\varepsilon(\varepsilon-1)-1\Big) = \varepsilon^4 - 2\varepsilon^3 + \varepsilon$. ∎

To reach the total strength of this theory, we would like to use an argument stating that it is a "very rare" situation that in $\mathsf{PG}(n,q)$ a hypersurface $f=0$ with $d=\deg f>2$ admits a hyperplane H such that the intersection of H and the hypersurface splits into d linear factors, i.e. $(n-2)$-dimensional subspaces (Totally Reducible Intersection, TRI hyperplane). We conjecture the following.

Conjecture 14.14. *Let $f(X_0, X_1, ..., X_n)$ be a homogeneous irreducible polynomial of degree $d>2$ and let F be the hypersurface in $\mathsf{PG}(n,q)$ determined by $f=0$. Then the number of TRI hyperplanes to F is "small" or F is a cone with a low dimensional base.*

By small we mean the existence of a function (upper bound) $r(d,n)$, which is independent from q; although we would not be surprised if even a constant upper bound, for instance $r(d,n)=45$ would hold in general. By a low dimensional base of a cone we mean an at most 3-dimensional base.

We remark finally that such a result would immediately imply extendability of direction sets U under very general conditions.

14.3 An application

A (finite) *partial geometry*, introduced by Bose [38], is an incidence structure $\mathcal{S}=(\mathcal{P},\mathcal{B},\mathrm{I})$ in which $\mathcal{P}$ and $\mathcal{B}$ are disjoint non-empty sets of objects called points and lines (respectively), and for which $\mathrm{I}\subseteq(\mathcal{P}\times\mathcal{B})\cup(\mathcal{B}\times\mathcal{P})$ is a symmetric point-line incidence relation satisfying the following axioms:

(i) Each point is incident with $1+t$ lines ($t\geqslant 1$) and two distinct points are incident with at most one line.

(ii) Each line is incident with $1+s$ points ($s\geqslant 1$) and two distinct lines are incident with at most one point.

(iii) There exists a fixed integer $\alpha>0$, such that if x is a point and L is a line not incident with x, then there are exactly α pairs $(y_i, M_i)\in\mathcal{P}\times\mathcal{B}$ for which $x\ \mathrm{I}\ M_i\ \mathrm{I}\ y_i\ \mathrm{I}\ L$.

The integers s, t and α are the parameters of $\mathcal{S}$. The *dual* $\mathcal{S}^D$ of a partial geometry $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ is the incidence structure $(\mathcal{B}, \mathcal{P}, \mathrm{I})$. It is a partial geometry with parameters $s^D = t$, $t^D = s$, $\alpha^D = \alpha$.

If $\mathcal{S}$ is a partial geometry with parameters s, t and α, then $|\mathcal{P}| = (s+1)\frac{(st+\alpha)}{\alpha}$ and $|\mathcal{B}| = (t+1)\frac{(st+\alpha)}{\alpha}$. (see e.g. [54]). A partial geometry with parameters s, t, and $\alpha = 1$, is a *generalized quadrangle* of order (s, t), [89].

To describe a class of partial geometries of our interest, we need special pointsets in $\mathsf{PG}(2, q)$. An *arc of degree* d of a projective plane Π of order s is a set $\mathcal{K}$ of points such that every line of Π meets $\mathcal{K}$ in at most d points. If $\mathcal{K}$ contains k points, than it is also called a $\{k, d\}$-arc. The size of an arc of degree d can not exceed $ds - s + d$. A $\{k, d\}$-arc $\mathcal{K}$ for which $k = ds - s + d$, or equivalently, such that every line that meets $\mathcal{K}$, meets $\mathcal{K}$ in exactly d points, is called *maximal*. We call a $\{1, 1\}$-arc and a $\{s^2, s\}$-arc *trivial*. The latter is necessarily the set of s^2 points of Π not on a chosen line.

A typical example, in $\mathsf{PG}(2, q)$, is a conic, which is a $\{q+1, 2\}$-arc, which is not maximal, and it is well known that if q is even, a conic, together with its nucleus, is a $\{q+2, 2\}$-arc, which is maximal. We mention that a $\{q+1, 2\}$-arc in $\mathsf{PG}(2, q)$ is also called an *oval*, and a $\{q+2, 2\}$-arc in $\mathsf{PG}(2, q)$ is also called a *hyperoval*. When q is odd, all ovals are conics, and no $\{q+2, 2\}$-arcs exist ([93]). When q is even, every oval has a nucleus, and so can be extended to a hyperoval. Much more examples of hyperovals, different from a conic and its nucleus, are known, see e.g. [53]. We mention the following two general theorems on $\{k, d\}$-arcs.

Theorem 14.15 ([48]). *Let $\mathcal{K}$ be a $\{ds - s + d, d\}$-arc in a projective plane of order s. Then the set of lines external to $\mathcal{K}$ is a $\{s(s - d + 1)/d, s/d\}$-arc in the dual plane.*

As a consequence, $d \mid s$ is a necessary condition for the existence of maximal $\{k, d\}$-arcs in a projective plane of order s. The results for the Desarguesian plane $\mathsf{PG}(2, q)$ are much stronger. Denniston [55] showed that this condition is sufficient for the existence of maximal $\{k, d\}$-arcs in $\mathsf{PG}(2, q)$, q even. Blokhuis, Ball and Mazzocca [11] showed that non-trivial maximal $\{k, d\}$-arcs in $\mathsf{PG}(2, q)$ do not exist when q is odd. Hence, the existence of maximal arcs in $\mathsf{PG}(2, q)$ can be summarized in the following theorem.

Theorem 14.16. *Non-trivial maximal $\{k, d\}$-arcs in $\mathsf{PG}(2, q)$ exist if and only if q is even.*

Several infinite families and constructions of maximal $\{k, d\}$-arcs of $\mathsf{PG}(2, q)$, $q = 2^h$, and $d = 2^e$, $1 \leq e \leq h$, are known. We refer to [53] for an overview.

Let q be even and let $\mathcal{K}$ be a maximal $\{k,d\}$-arc of $\mathsf{PG}(2,q)$. We define the incidence structure $T_2^*(\mathcal{K})$ as follows. Embed $\mathsf{PG}(2,q)$ as a hyperplane H_∞ in $\mathsf{PG}(3,q)$. The points of $\mathcal{S}$ are the points of $\mathsf{PG}(3,q)\setminus H_\infty$. The lines of $\mathcal{S}$ are the lines of $\mathsf{PG}(3,q)$ not contained in H_∞, and meeting H_∞ in a point of $\mathcal{K}$. The incidence is the natural incidence of $\mathsf{PG}(3,q)$. One can check easily, using that $\mathcal{K}$ is a maximal $\{k,d\}$-arc, that $T_2^*(\mathcal{K})$ is a partial geometry with parameters $s=q-1$, $t=k-1=(d-1)(q+1)$, and $\alpha=d-1$.

An *ovoid* of a partial geometry $\mathcal{S}=(\mathcal{P},\mathcal{B},\mathrm{I})$ is a set $\mathcal{O}$ of points of $\mathcal{S}$, such that every line of $\mathcal{S}$ meets $\mathcal{O}$ in exactly one point. Necessarily, an ovoid contains $\frac{st}{\alpha}+1$ points. Different examples of partial geometries exist, and some of them have no ovoids, see e.g. [52]. The partial geometry $T_2^*(\mathcal{K})$ has always an ovoid. Consider any plane $\pi\neq H_\infty$ meeting H_∞ in a line skew to $\mathcal{K}$. The plane π then contains $\frac{st}{\alpha}+1=q^2$ points of $\mathcal{S}$, and clearly every line of $\mathcal{S}$ meets π in exactly one point.

It is a natural stability question to investigate *extendability* of point sets of size slightly smaller than the size of an ovoid. In this case, the question is whether a set of points $\mathcal{B}$, with the property that every line meets $\mathcal{B}$ in at most one point, can be extended to an ovoid if $|\mathcal{B}|=q^2-\varepsilon$, and ε is *not too big*. Such a point set $\mathcal{B}$ is called a *partial ovoid* of deficiency ε, and it is called *maximal* if it cannot be extended. The following theorem is from [89] and deals with this question in general for GQs, i.e. for $\alpha=1$.

Theorem 14.17. *Consider a GQ of order (s,t). Any partial ovoid of size $(st-\rho)$, with $0\leq\rho<t/s$ is contained in a uniquely defined ovoid.*

For some particular GQs, extendability beyond the given bound is known. For other GQs, no better bound is known, or examples of maximal partial ovoids reaching the upper bound, are known. For an overview, we refer to [51].

Applied to the GQ $T_2^*(\mathcal{H})$, $\mathcal{H}$ a hyperoval of $\mathsf{PG}(2,q)$, Theorem 14.17 yields that a partial ovoid of $T_2^*(\mathcal{H})$ of size q^2-2 can always be extended. The proof of Theorem 14.17 is of combinatorial nature, and can be generalized to study partial ovoids of partial geometries. However, for the partial geometries $T_2^*(\mathcal{K})$ with $\alpha\geq 2$, such an approach only yields extendability of partial ovoids with deficiency one. In the context of this section, we can study extendability of partial ovoids of the partial geometry $T_2^*(\mathcal{K})$ as a direction problem. Indeed, if a set of points $\mathcal{B}$ is a (partial) ovoid, then no two points of $\mathcal{B}$ determine a line of the partial geometry $T_2^*(\mathcal{K})$. Hence the projective line determined by two points of $\mathcal{B}$, must not contain a point of $\mathcal{K}$, in other words, the set of points $\mathcal{B}$ is a set of affine points, not determining the points of $\mathcal{K}$ at infinity.

Considering a partial ovoid $\mathcal{B}$ of size q^2-2, we can apply Theorem 14.12. Clearly, the non-determined directions, which contain the points of $\mathcal{K}$, do not satisfy the conditions when $\mathcal{B}$ is not extendable. Hence, we immediately have the following corollary.

Corollary 14.18. *Let $\mathcal{B}$ be a partial ovoid of size q^2-2 of the partial geometry $T_2^*(\mathcal{K})$, then $\mathcal{B}$ is always extendable to an ovoid.*

This result is the same as Theorem 14.17 for the GQ $T_2^*(\mathcal{H})$, $\mathcal{H}$ a hyperoval of $\mathsf{PG}(2,q)$, $q>2$.

15 On the number of directions determined by a pair of functions over a prime field

15.1 Introduction

Now we continue our investigations concerning directions in various contexts. This section is based on [SzP2func]. Let $q=p^h$ denote a prime power and consider a set $U=\{(a_i,b_i) : i=1,\ldots,q\}$ of q points in the affine plane $\mathrm{AG}(2,q)$. The *classical direction problem* looks for the size of the direction set of U, defined as

$$D=\{\frac{a_i-a_j}{b_i-b_j} : i\neq j\}\subseteq \mathbb{F}_q\cup\{\infty\}.$$

In the last twenty years or so this problem has received a lot of attention mainly due to its connections with a variety of fields, for example, blocking sets in $\mathrm{PG}(2,q)$ [33], permutation polynomials over a finite field [80] and the factorisation of abelian groups [91].

Based on the initial work of Rédei [91] in 1970, the problem was completely solved, whenever the number of directions is at most $\frac{q+1}{2}$, by Ball, Blokhuis, Brouwer, Storme and Szőnyi [33] and [7] (for small characteristics and a shorter proof). The theorem also characterises the sets of points that have a small number of directions.

The most natural way to formulate an analogous problem for higher dimensions is to take a set U of q^{n-1} points in $\mathrm{AG}(n,q)$ and define D to be the set of determined directions, that is, the set of infinite points which are collinear with two points of U. As in the planar case the non-determined directions are those infinite points through which every line contains exactly 1 point of U. This is what we did in the previous section, see also [8], [16] and [SzPkblock].

In this section we propose another analogue for the three-dimensional case. This analogue can be formulated for any dimension, but the problem turns out to be significantly harder in three dimensions so it is enough to occupy us here. Apart from trivially applying the results for two and three dimensions, the higher dimensional cases would appear to be, for the moment, inaccessible.

Let U be a set of q points in $\mathrm{AG}(3,q)$ and say that an infinite line ℓ is not determined, if every affine plane through ℓ has exactly one point in common with U.

Before stating the main result of the present section, we reformulate the aforementioned problems in terms of functions over finite fields. Consider first the planar case. Whenever the size of D is less than $q+1$ one can apply an affine transformation so that U is the graph of a function. So we can assume that $U = \{(x, f(x)) : x \in \mathbb{F}_q\}$ and

$$D = \{\frac{f(y)-f(x)}{y-x} \mid x, y \in \mathbb{F}_q,\ x \neq y\}.$$

An element c is not in D if and only if $x \to f(x) - cx$ is a bijective map of $\mathbb{F}_q$ to itself. A function which induces a bijective map on $\mathbb{F}_q$ is often called a *permutation polynomial*. (Note that over a finite field any function can be written as a polynomial.)

Let $M(f)$ be the number of elements of $\mathbb{F}_q$ that are not elements of D.

The first analogue to the direction problem in higher dimensions mentioned before, in this terminology, considers the graph of a function from $\mathbb{F}_q^n$ to itself.

The analogue which we will consider in this section, in this terminology, considers the graph of a pair of functions f and g over $\mathbb{F}_q$. A line not determined by the graph $\{(x, f(x), g(x)) \mid x \in \mathbb{F}_q\}$ corresponds to a pair (c, d) for which $f(x) + cg(x) + dx$ is a permutation polynomial. We will denote the number of these pairs by $M(f, g)$.

From now on we will only consider the $q = p$ prime case and use the permutation polynomial terminology.

In [91] Rédei and Megyesi proved that if $q = p$ prime and $M(f) \geq (p-1)/2$, then $f(x) = cx + d$ for some $c, d \in \mathbb{F}_p$. In other words, the set U is a line.

This result can be used to prove that the only way to factorise the elementary abelian group with p^2 elements is to use a coset. This was Rédei's motivation to look at the direction problem for $\mathbb{F}_p$. For more applications of this result to other combinatorial problems, see [80].

In [91] Megyesi provided an example with $M(f) = d-1$, for each divisor d of $p-1$, which, when $d = (p-1)/2$, shows this bound to be best possible.

Namely, let H be a multiplicative subgroup of $\mathbb{F}_p$, let χ_H be the characteristic function of H and let $f(x) = \chi_H(x)x$. If $d \neq 1, p-1$ then $M(f) = d-1$.

In [80] Lovász and Schrijver proved that if $M(f) = (p-1)/2$ then f is affinely equivalent to the example of Megyesi.

In [61] it is proved that if $M(f) \geq 2\lceil\frac{p-1}{6}\rceil+1$, then $(f(x)-(cx+d))(f(x)-(bx+e)) = 0$ for some $b, c, d, e \in \mathbb{F}_p$; in other words, the graph of f is contained in the union of two lines.

In [101] Szőnyi 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 H can be replaced by a union of cosets of a multiplicative subgroup of $\mathbb{F}_p$. 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 $M(f) \leq 2\lceil\frac{p-1}{6}\rceil$, f is affinely equivalent to $x^{\frac{p+1}{2}}$ or f is linear.

In [112] Wan, Mullen and Shiue obtain upper bounds on $M(f)$ in terms of the degree of the polynomial f.

Here we shall prove that if there are more than $(2\lceil\frac{p-1}{6}\rceil + 1)(p + 2\lceil\frac{p-1}{6}\rceil)/2 \approx 2p^2/9$ pairs $(c, d) \in \mathbb{F}_p^2$ with the property that $x \mapsto f(x) + cg(x) + dx$ is a permutation of $\mathbb{F}_p$ then there are elements $a, b, e \in \mathbb{F}_p$ such that $f(x) + ag(x) + bx + e = 0$, for all $x \in \mathbb{F}_p$; in other words the graph of (f, g), $\{(x, f(x), g(x)) \mid x \in \mathbb{F}_p\}$, is contained in a plane. At the end of the section we construct an example showing that for p congruent to 1 modulo 3 this is asymptotically sharp.

15.2 A slight improvement on the earlier result

For a polynomial f over $\mathbb{F}_p$, p prime, define

$$I(f) = \min\{k + l \mid \sum_{x\in\mathbb{F}_p} x^k f(x)^l \neq 0\}.$$

In [61] it was proved that if $M(f) > (p-1)/4$ and $I(f) \geq 2\lceil\frac{p-1}{6}\rceil + 2$ then the graph of f is contained in the union of two lines.

Let

$$\pi_k(Y) = \sum_{x\in\mathbb{F}_p} (f(x) + xY)^k.$$

It's a simple matter to check, see [79, Lemma 7.3], 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 $\sum_{x\in\mathbb{F}_p} x^k = 0$) 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 $I(f) - 1 \geq M(f)$.

Thus in [61] it was proved that if $M(f) \geq 2\lceil \frac{p-1}{6} \rceil + 1$, then the graph of f is contained in the union of two lines.

To be able to prove the main result of this section we need something a little stronger than [61]. We use the same method and essentially follow the proof there but we have to modify the first part of the proof (Lemma 4.1), we manage to avoid the step involving Lemma 4.2, *Step 1* and *Step 2* are the same, we use a slightly different subspace to be able to reduce *Step 3* and *Step 4* a little and *Step 5* we use in the same way.

In this section we shall prove the following theorem.

Theorem 15.1. *If $M(f) \geq (p-1)/6$ and $I(f) \geq 2\lceil \frac{p-1}{6} \rceil + 2$ then the graph of f is contained in the union of two lines.*

The values $I(f)$ 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, $\{(x, f(x)) \mid x \in \mathbb{F}_p\}$, 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

$$-\sum_{x \in \mathbb{F}_p} g(x)$$

is equal to the coefficient of x^{p-1} of g.

Lemma 15.2. *If $3 \leq f^\circ \leq (p-1)/2$ then $I(f) \leq (p+1)/3$.*

Proof: Write $p - 1 = af^\circ + b$ with $0 \leq b < f^\circ$. The degree of $f(x)^a x^b$ is $p-1$, so we have $I(f) \leq a + b$.

If $f^\circ = 3$ then $a + b \leq (p-2)/3 + 1 = (p+1)/3$.

If $(p+1)/3 \leq f^\circ \leq (p-1)/2$ then $a + b = 2 + p - 1 - 2f^\circ \leq (p+1)/3$.

If $(p+1)/4 \leq f^\circ \leq (p-1)/3$ then $a + b = 3 + p - 1 - 3f^\circ \leq 3 + p - 1 - 3(p+1)/4 = (p+1)/4 + 1 \leq (p+1)/3$ for $p \geq 11$.

If $4 \leq f^\circ \leq (p+1)/4$ then $a + b \leq (p - b - 1)/f^\circ + b \leq p/f^\circ + (bf^\circ - b - 1)/f^\circ \leq p/f^\circ + f^\circ - 2$. This is at most $(p+1)/3$ if and only if the quadratic inequality $3(f^\circ)^2 - (p+7)f^\circ + 3p \leq 0$ is satisfied. For $p \geq 20$, the inequality is satisfied for both $f^\circ = 4$ and $f^\circ = (p+1)/4$, 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 $f^\circ = 2$ we have $I(f) = (p-1)/2$ and $M(f) = 0$ and for $f^\circ = 1$ we have $I(f) = p-1$ and $M(f) = p-1$.

Lemma 15.3. *If $f^\circ = (p+1)/2$ then either $I(f) \leq (p+5)/4$ or f is affinely equivalent to $x^{\frac{p+1}{2}}$.*

Proof: After applying a suitable affine transformation we can suppose that $f(x) = x^{\frac{p+1}{2}} + g(x)$ where $g^\circ \leq (p-3)/2$.

If $g^\circ \leq 1$ then by applying another linear transformation we can subtract g from f and hence f is affinely equivalent to $x^{\frac{p+1}{2}}$.

Suppose $g^\circ \geq 2$. Write $(p-3)/2 = ag^\circ + b$ with $0 \leq b < g^\circ$ 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 $g(x)^a x^{\frac{p+1}{2}+b}$. Let $r(x) = g(x)^{a+1-i}x^{i\frac{p+1}{2}+b}$ (modulo x^p-x), a typical term in the sum (note that all the binomial coefficients are non-zero). If i is even then $r(x) = g(x)^{a+1-i}x^{b+i}$, which has degree $(a+1-i)g^\circ + b + i = (p-3)/2 + g^\circ - (g^\circ - 1)i < p-1$. If $i \neq 1$ is odd then $r(x) = g(x)^{a+1-i}x^{\frac{p-1}{2}+i+b}$, which has degree $(a+1-i)g^\circ + (p-1)/2 + i + b = p - 2 + g^\circ - (g^\circ - 1)i < p-1$.

Hence $f(x)^{a+1}x^b$ has degree $p-1$ which implies $I(f) \leq a+1+b$.

Finally, note that $a+b \leq (p-3)/(2g^\circ) + g^\circ - 1$, which is at most $(p+1)/4$ if $2 \leq g^\circ \leq (p-3)/4$. If $g^\circ > (p-3)/4$ then $a = 1$ and $b = (p-3)/2 - g^\circ < (p-3)/4$ and so $a+b < (p+1)/4$. ∎

Let $s = \lceil (p-1)/6 \rceil$.

We will assume from now on that $I(f) \geq 2s+2$. By the definition of $I(f)$ the sum

$$\sum_{x \in \mathbb{F}_p} x^k f(x)$$

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 15.2 and Lemma 15.3 the degree of f is at least $(p+3)/2$.

Lemma 15.4. *There is polynomial in $h \in E(f)$ with one of the following properties. Either*

(i) for all i such that $1 \le i \le 2s$, $(h^i)^\circ \le h^\circ + i - 1$ and $(h^2)^\circ = h^\circ + 1$, or

(ii) for all i such that $1 \le i \le 2s$, $(h^i)^\circ \le (h^2)^\circ + i - 2$ and $(h^3)^\circ = (h^2)^\circ + 1$,

and h has no root in $\mathbb{F}_p$.

Proof:

Let

$$d(f) = \max\{(f^i)^\circ - i \mid 1 \le i \le 2s\}$$

and let $d = d(f_1)$ be maximal over all polynomials in $E(f)$. The fact that $f^\circ \ge (p+3)/2$ implies that $d \ge (p+1)/2$.

Let $\pi(Y) = \pi_{p-1-d}(Y)$. The coefficient of $Y^{p-1-d-j}$ in $\pi(Y)$ is $\binom{p-1-d}{j} \sum_{x \in \mathbb{F}_p} x^{p-1-d-j} f^j$ which, by the definition of d, is non-zero for at least one j where $1 \le j \le 2s$. Hence $\pi(Y) \not\equiv 0$.

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 $M(f) \ge (p-1)/6$ the degree of π, $\pi^\circ = p - 1 - d \ge 3M(f) \ge (p-1)/2$ which isn't the case.

Since $0 < p-1-d < p-1$ we have already seen that $\pi(a) = 0$, so either $\pi'(a) \ne 0$ or $\pi''(a) \ne 0$ for some a.

Let f_2 be the inverse of the function $f(x) + ax$.

If

$$0 \ne \pi'(a) = -(d+1) \sum_{x \in \mathbb{F}_p} x(f + ax)^{p-2-d}$$

then $\sum_{z \in \mathbb{F}_p} f_2(z) z^{p-2-d} \ne 0$ and so $f_2^\circ \ge d+1$. By the maximality of d, $f_2^\circ = d+1$ and so $(f_2^i)^\circ - i \le f_2^\circ - 1$. If $(f_2^2)^\circ \le f_2^\circ$ then let $f_3 = f_2 + cx$ where c is chosen so that $(f_3^2)^\circ \ge f_3^\circ + 1$ and f_3 is not a permutation polynomial. Note that $f_3^2 = f_2^2 + 2cx f_2 + c^2 x^2$.

If

$$0 \ne \pi''(a) = (d+1)(d+2) \sum_{x \in \mathbb{F}_p} x^2 (f + ax)^{p-3-d}$$

then $\sum_{z \in \mathbb{F}_p} (f_2(z))^2 z^{p-3-d} \ne 0$ and so $(f_2^2)^\circ \ge d+2$. By the maximality of d, $(f_2^2)^\circ = d+2$ and so $(f_2^i)^\circ - i \le (f_2^2)^\circ - 2$. If $(f_2^3)^\circ \le (f_2^2)^\circ$ then let $f_3 = f_2 + cx$ where c is chosen so that $(f_3^3)^\circ \ge (f_3^2)^\circ + 1$ 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 $\mathbb{F}_p$. ∎

The dimension of a subspace of a finite dimensional vector space of polynomials is equal to the number of degrees occurring amongst the elements

of a subspace, see Result 4.4. This is easily seen if we take the canonical basis $\{1, x, x^2, \ldots, x^t\}$. The matrix whose rows form a basis for the subspace can be reduced to a matrix in row echelon form whose rows span the same subspace and correspond to polynomials of different degrees.

Lemma 15.5. *There is a polynomial in $h \in E(f)$ for which there exist polynomials F, G and H, where $H^\circ - 2 = F^\circ - 1 = G^\circ = r \leq s-2$, $(F,G) = 1$ and*

$$Fh + Gh^2 = H.$$

Note that this implies that h satisfies the conditions of Lemma 15.4 (i).

Proof: Let h be a polynomial satisfying the conditions of Lemma 15.4. Since $I(h) \geq 2s+2$ we have $(h^i)^\circ \leq p - 2s - 3 + i$.

Define subspaces of the vector space of polynomials of maximum degree $p-1$

$$\psi_j = \{Fh + Gh^2 \mid F^\circ \leq j,\ G^\circ \leq j-1\},$$

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 $(hG)^\circ$ is at least $3s$ and at most $5s - 3 < p - 1$. Thus the dimension of ψ_j is $2j+1$.

Since $I(h) \geq 2s+1$ and $2(j+1) \leq 2s$, the sum over $\mathbb{F}_p$ of the evaluation of the product of any two elements of ψ_j is zero, hence the sum of the degrees of any two elements of ψ_{s-1} is not equal to $p-1$. The maximum degree of any element of ψ_{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 ψ_{s-1}.

Let H be of minimal degree, so $(F,G) = 1$.

If h satisfies case (i) of Lemma 15.4 then $(h^2)^\circ = h^\circ + 1$ and $r = G^\circ = F^\circ - 1$. Moreover $Fh^2 + Gh^3 = Hh$ and $(h^3)^\circ \leq h^\circ + 2$ implies $H^\circ \leq r+2$.

If h satisfies case (ii) of Lemma 15.4 then $(h^3)^\circ = (h^2)^\circ + 1 \geq h^\circ + 2$ and $(h^4)^\circ \leq (h^2)^\circ + 2$. Let $F^\circ = r+1$ and so $G^\circ \leq r$. The equation $Fh^3 + Gh^4 = Hh^2$ implies $H^\circ \leq r+2$. If $G^\circ \leq r-1$ then $Fh^2 + Gh^3 = Hh$ implies $r + 2 + h^\circ \geq H^\circ + h^\circ = r + 1 + (h^2)^\circ$ and so $(h^2)^\circ = h^\circ + 1$. But then $Fh + Gh^2 = H$ implies $G^\circ = r$.

Either way we have $r = G^\circ = F^\circ - 1 \geq H^\circ - 2$.

Let $h_1 = h + ax$ and $F_1 = F - 2axG$, $G_1 = G$ and $H_1 = H - a^2x^2G + axF$. Then $F_1h_1 + G_1h_1^2 = H_1$ and we can choose a so that H_1 has degree $r+2$. Now when we look at ψ_{r+1} for h_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 $i = s$ 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 15.6. *There is a polynomial $h \in E(f)$ and a polynomial G, where $G^\circ = r \leq s - 2$, such that for all $j = 2, \ldots, i$, there is an F_j and an H_j with the property that $(F_j, G) = 1$,*

$$F_j h + G^{j-1} h^j = H_j,$$

$F_j^\circ \leq (j-1)(r+1)$, $H_j^\circ \leq (j-1)r + j$ and $H_i^\circ = (i-1)r + i$.

Proof: Let h_1 satisfy the conditions of Lemma 15.5. We start by proving that there is an $h \in E(f)$ for which $(h^{i-1})^\circ \geq h^\circ + i - 2$.

If $(h_1^{i-1})^\circ \leq h_1^\circ + i - 3$ then let $h = h_1 + ax$. Choose a so that $h^{i-1} = \sum_{j=0}^{i-1} \binom{i-1}{j} (ax)^{i-j-1} h_1^j$ has degree at least $h^\circ + i - 2$ 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 15.5 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

$$F_j h + G^{j-1} h^j = H_j.$$

The degrees satisfy $F_j^\circ \leq (j-1)(r+1)$ and $H_j^\circ \leq (j-1)r + j$ and $(F_j, G) = 1$, since $(F, G) = 1$ by Lemma 15.5 and $(F_{j-1}, G) = 1$ by induction.

Now $(h^{i-1})^\circ \geq h^\circ + i - 2$ and the equation $F_{i-1}h + G^{i-2}h^{i-1} = H_{i-1}$ implies that $F_{i-1}^\circ \geq (i-2)(r+1)$ and so $F_{i-1}^\circ = (i-2)(r+1)$. Finally $H_i = -HF_{i-1}$ implies $H_i^\circ = (i-1)r + i$. ∎

Let h satisfy the conditions of Lemma 15.6. Note that this implies that h satisfies the conditions of Lemma 15.5 and Lemma 15.4 (i). Define

$$\phi_j = \{Ah + Bh^i \mid A^\circ \leq j,\ B^\circ \leq j + 1 - i\}.$$

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 15.7. *For $j \leq 2s - 1$ all polynomials of ϕ_j have degree at least H_i° and those of degree at most $p - 2 - h^\circ$ are multiples of H_i.*

Proof: If $Ah + Bh^i = 0$ then, since h has no root in $\mathbb{F}_p$, $A + Bh^{i-1} = 0$. 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 ϕ_j is $2j + 3 - i$.

Suppose that ϕ_j contains a polynomial C of degree n but no polynomial of degree $n+1$. Then ϕ_{j+1} contains a polynomial of degree $n+1$, xC for example, and a polynomial of degree one more than the maximum degree of an element of ϕ_j. However $\dim\phi_{j+1} = \dim\phi_j + 2$, so n is unique. Moreover, the polynomials of degree $n+1$ in ϕ_{j+1} are multiples of a polynomial of degree n in ϕ_j.

Since $j \leq 2s-1$, ϕ_j contains no element of degree $p-1-h^\circ$. Now $H_i \in \phi_{(i-1)r+i-1}$ and is a polynomial of degree less than $p-1-h^\circ$. It is not a multiple of any polynomial in ϕ_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 $(KA)^\circ \leq (i-1)r+i-1$ and $(KB)^\circ \leq (i-1)r$, which would be a constant multiple of H_i. This is not possible since $(F_i, G) = 1$. Thus all polynomials in ϕ_j of degree at most $p-2-h^\circ$ are multiples of H_i and in particular have degree at least H_i°.

∎

The following lemma contradicts the previous one which implies that our assumption that $r \geq 1$ was incorrect.

Lemma 15.8. *There is a non-zero polynomial of degree less than H_i° in ϕ_j for some $j \leq 2s-2$.*

Proof: Suppose $r \geq 2$ and so $i \leq s$. Let

$$\Delta = \{Ah + B_2h^2 + \ldots + B_{i-1}h^{i-1} + Ch^i \mid A^\circ \leq s-1,\ B_j^\circ \leq r-1,\ C^\circ \leq s-i\}.$$

Since $I(h) \geq 2s+1$ the sum of the degrees of any two elements of Δ is not equal to $p-1$. The maximum degree of any element of Δ 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 Δ 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_j, C zero where $E^\circ \leq s-(i-2)r+i-1$.

Substituting $G^{j-1}h^j = H_j - hF_j$ we have

$$G^{i-2}E = G^{i-2}Ah + CG^{i-2}h^i + \sum_{j=2}^{i-1} B_jG^{i-1-j}(H_j - hF_j)$$

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 ϕ_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 $H_i^\circ = (i-1)r+i$.

If $r=1$ then take $i=s$ and define Δ as above. There is a polynomial E in Δ 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 15.7 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 $s-1$.

∎

We can now prove Theorem 15.1.

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. ∎

15.3 Linear combinations of three permutation polynomials

First let's recall Theorem 8.4(i) for our further purposes:

Theorem 15.9. *Let $\pi(Y,Z)$ be an absolutely irreducible polynomial of degree d with coefficients in $\mathbb{F}_p$ such that $1 < d < p$. The number of solutions N to the equation $\pi(y,z) = 0$ in $\mathbb{F}_p^2$ satisfies*

$$N \leq d(d+p-1)/2.$$

Let $M(f,g)$ be the number of pairs $(a,b) \in \mathbb{F}_p^2$ for which $f(x)+ag(x)+bx$ is a permutation polynomial. Let

$$I(f,g) = \min\{k+l+m \mid \sum_{x\in\mathbb{F}_p} x^k f(x)^l g(x)^m \neq 0\}.$$

Recall $s = \lceil \frac{p-1}{6} \rceil$. Before we prove the main result of this section we need the following lemma.

Lemma 15.10. *If $M(f,g) > (2s+1)(p+2s)/2$ then $I(f,g) \geq 2s+2$ or there are elements $c,d,e \in \mathbb{F}_p$ such that $f(x)+cg(x)+dx+e = 0$ for all $x \in \mathbb{F}_p$.*

Proof: Let $\pi_k(Y,Z) = \sum_{x\in\mathbb{F}_p}(f(x)+g(x)Y+xZ)^k$.

By [79, Lemma 7.3], 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 σ_j is absolutely irreducible. Then $\sum \sigma_j^\circ = \pi_k^\circ \leq k$.

Let N_j be the number of solutions of $\sigma_j(a,b) = 0$ in $\mathbb{F}_p$ for which $f(x)+ag(x)+bx$ is a permutation polynomial.

If $\lambda\sigma_j \in \mathbb{F}_p[Y,Z]$, for some λ in an extension of $\mathbb{F}_p$, and $\sigma_j^\circ \geq 2$ then by Theorem 15.9 $N_j \leq \sigma_j^\circ(p+\sigma_j^\circ-1)/2$.

Suppose $\sigma_j^\circ = 1$ 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 $b \in \mathbb{F}_p$ with the property that $\alpha f(x)-(\beta b+\gamma)g(x)+b\alpha x = \alpha f(x)-\gamma g(x)+b(\alpha x-\beta)$ 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 $c,d,e \in \mathbb{F}_p$ such that $f(x)+cg(x)+dx+e = 0$ for all $x \in \mathbb{F}_p$. If $\alpha = 0$ then there are $(p+1)/2$ elements $a \in \mathbb{F}_p$ with the property that $\beta f(x)-\gamma x+a\beta g(x)$ is a permutation polynomial. The set of p points $\{(\beta f(x)-\gamma x, \beta g(x)) \mid x \in \mathbb{F}_p\}$ 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 Rédei and Megyesi's theorem, it is a line. Hence, there are elements c, d and e with the property that $c(\beta f(x)-\gamma x)+d\beta g(x)+e = 0$ for all $x \in \mathbb{F}_p$. Thus, either there are elements $c,d,e \in \mathbb{F}_p$ such that $f(x)+cg(x)+dx+e = 0$ for all $x \in \mathbb{F}_p$ or $N_j \leq (p-1)/2$.

Suppose $\lambda\sigma_j \notin \mathbb{F}_p[Y,Z]$ for any λ in any extension of $\mathbb{F}_p$. The polynomials $\sigma_j = \sum \alpha_{nm}Y^nZ^m$ and $\hat{\sigma}_j = \sum \alpha_{nm}^p Y^nZ^m$ have at most $(\sigma_j^\circ)^2$ zeros in

common by Bezout's theorem. However if $(y,z) \in \mathbb{F}_p^2$ and $\sigma_j(y,z) = 0$ then $\hat{\sigma}_j(y,z) = 0$. Hence

$$N_j \leq (\sigma_j^\circ)^2 \leq \sigma_j^\circ(p + \sigma_j^\circ - 1)/2,$$

whenever $\sigma_j^\circ \leq (p-1)/2$.

Thus if $\pi_k \not\equiv 0$ and $k \leq (p-1)/2$ then $N(\pi_k)$, the number of solutions of $\pi_k(y,z) = 0$ in $\mathbb{F}_p$ for which $f(x) + ag(x) + bx$ is a permutation polynomial, satisfies

$$N(\pi_k) \leq \sum N_j \leq \sum \sigma_j^\circ(p + \sigma_j^\circ - 1)/2 \leq k(p-1)/2 + \frac{1}{2}\sum(\sigma_j^\circ)^2$$

$$\leq k(p-1)/2 + \frac{1}{2}(\sum \sigma_j^\circ)^2 = (k(p-1) + k^2)/2.$$

By hypothesis $\pi_k \equiv 0$ or

$$(2s+1)(p+2s)/2 < N_k \leq (k(p-1) + k^2)/2,$$

which gives $k \geq 2s+2$. Now

$$\pi_k(Y,Z) = \sum_{l=0}^{k}\sum_{m=0}^{k-l}\binom{k}{l}\binom{k-l}{m}\left(\sum_{x\in\mathbb{F}_p} x^{k-l-m}f(x)^l g(x)^m\right) Y^m Z^{k-l-m},$$

and so $I(f,g) \geq 2s+2$.

∎

Theorem 15.11. *If $M(f,g) > (2s+1)(p+2s)/2$ then there are elements $c,d,e \in \mathbb{F}_p$ 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 $b \in \mathbb{F}_p$, which can only occur if there is a constant e such that $f(x) + cg(x) + e = 0$.

So suppose $p \geq 5$ and that there are no elements $c,d,e \in \mathbb{F}_p$ with the property that $f(x) + cg(x) + dx + e = 0$.

Clearly $I(f + ag) \geq I(f,g)$ for all $a \in \mathbb{F}_p$ and $I(f,g) \geq 2s+2$ by Lemma 15.10.

There is an $a_1 \in \mathbb{F}_p$ with the property that

$$M(f + a_1 g) \geq M(f,g)/p \geq (p-1)/6.$$

By Theorem 15.1 there are constants $c,d,c',d' \in \mathbb{F}_p$ with the property that

$$(f + a_1 g + cx + d)(f + a_1 g + c'x + d') = 0$$

so the graph of (f, g), the set of points $\{(x, f(x), g(x)) \mid x \in \mathbb{F}_p\}$, is contained in the union of two planes.

By Rédei and Megyesi's theorem, since we have assumed that the graph of $f + a_1 g$ is not a line, $M(f + a_1 g) \leq (p-1)/2$ and so there is an $a_2 \neq a_1$ with the property that

$$M(f + a_2 g) \geq (M(f, g) - (p-1)/2)/(p-1) \geq (p-1)/6.$$

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 $(M(f, g) - (p-1))/(p-2) \geq (p-1)/6$ and $(M(f, g) - 3(p-1)/2)/(p-3) \geq (p-1)/6$, there is an a_3 and an a_4 with the property that $M(f + a_3 g) \geq (p-1)/6$ and $M(f + a_4 g) \geq (p-1)/6$ 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. ∎

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 $E = \{e \in \mathbb{F}_q \mid e^{(q-1)/3} = 1\} \cup \{0\}$. Then the set $S = \{(e, 0, 0),\ (0, e, 0),\ (0, 0, e) \mid e \in E\}$ is a set of q points. If π, the plane defined by

$$X_1 + aX_2 + bX_3 = c,$$

is incident with $(e, 0, 0)$ for some $e \in E$ then $c \in E$. 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 π 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 π and all the planes parallel to π 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 $\{X_1 = x \mid x \in \mathbb{F}_q\}$ is one such set of parallel planes then there are functions f and g for which $S = \{(x, f(x), g(x)) \mid x \in \mathbb{F}_q\}$. Each other set of parallel lines with the above property corresponds to a pair (a, b) such that $f(x) + ag(x) + bx$ is a permutation polynomial. Thus $M(f, g) = 2(q-1)^2/9 - 1$. Explicitly the functions f and g can be defined by $f(x) = \chi_H(x)x$ and $g(x) = \chi_{\epsilon H}(x)x$, where χ_H is the characteristic function of $H = \{t^3 \mid t \in \mathbb{F}_p\}$ and ϵ is a primitive third root of unity.

16 Glossary of concepts

Here one can find the most important definitions.

An algebraic **(hyper)surface** in $\mathsf{PG}(n,q)$ is a set of homogeneous polynomials $\{\lambda f(X_1,...,X_{n+1}) : \lambda \in \mathsf{GF}(q)\}$, where f is a polynomial with coefficients from $\mathsf{GF}(q)$. Geometrically, one may think about the points $(x_1,...,x_{n+1}) \in \mathsf{PG}(n,q)$ for which $f(x_1,...,x_{n+1}) = 0$. For more on the *multiplicity* of a point of a surface, see Section 8.

When $n = 2$ then we use the name plane curve instead of surface. If the polynomial f splits into factors over $\mathsf{GF}(q)$ then we call it *reducible* (otherwise irreducible) and the factors are called *components*. If this does not happen even over the algebraic closure $\bar{\mathsf{GF}}(q)$ then f is *absolutely irreducible*.

A (k,n)-**arc** of $\mathsf{PG}(2,q)$ 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 (k,n)-arc is **maximal** if every line intersects it in either 0 or n points.

A **blocking set** (with respect to lines) is a pointset meeting every line. In general, a blocking set in $\mathsf{PG}(n,q)$ w.r.t. k-dimensional subspaces (sometimes it is called an $(n-k)$-blocking set) is a point set meeting every k-subspace. **Do not be confused,** a **k-blocking set** is a blocking set meeting every k-codimensional subspace.

A point P of the blocking set 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 $\mathsf{PG}(2,q)$ is **small** if $|B| < \frac{3}{2}(q+1)$, in general, a blocking set B in $\mathsf{PG}(n,q)$ w.r.t. k-dimensional subspaces is small if $|B| < \frac{3}{2}q^{n-k} + 1$.

A t-fold blocking set meets every k-subspace in at least t points.

A blocking set $B \subset \mathsf{PG}(n,q)$, with respect to k-dimensional subspaces, is of **Rédei type**, if it has precisely q^{n-k} points in the affine part $\mathsf{AG}(n,q) = \mathsf{PG}(n,q) \setminus H_\infty$.

A **subgeometry** of $\Pi = \mathsf{PG}(n,q)$ is a copy of some $\Pi' = \mathsf{PG}(n',q')$ embedded in it, so the points of Π' are points of Π and the k-dimensional subspaces of Π' are just the intersections of some k-subspaces of Π with the pointset of Π'. It follows that $\mathsf{GF}(q')$ must be a subfield of $\mathsf{GF}(q)$.

The **type** of a pointset of $\mathsf{PG}(2,q)$ 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 **cone** $\mathcal{C}$ has a base B in some subspace $\Pi \subset \mathsf{PG}(n,q)$ and a vertex V; the vertex is a subspace disjoint from Π. The cone is the union of all the lines connecting points of B to V. In $\mathsf{PG}(3,q)$, a **flock** of the cone is the partition of $\mathcal{C} \setminus V$ into q disjoint plane sections, with planes not through V. A flock is *linear*, if its planes all contain one fixed line (which does not meet $\mathcal{C}$).

17 Notation

$\mathsf{V}(n,\mathbb{F})$ denotes the n-dimensional vector space with coordinates from the field $\mathbb{F}$. If $\mathbb{F} = \mathsf{GF}(q)$ then we write $\mathsf{V}(n,q)$ instead.

$\mathsf{AG}(n,\mathbb{F})$ denotes the n-dimensional affine space with coordinates from the field $\mathbb{F}$. If $\mathbb{F} = \mathsf{GF}(q)$ then we write $\mathsf{AG}(n,q)$ instead.

$\mathsf{PG}(n,\mathbb{F})$ denotes the n-dimensional projective space with coordinates from the field $\mathbb{F}$. If $\mathbb{F} = \mathsf{GF}(q)$ then we write $\mathsf{PG}(n,q)$ instead.

$\begin{bmatrix} a \\ b \end{bmatrix}_q = \frac{(q^a-1)(q^{a-1}-1)\ldots(q^{a-b+1}-1)}{(q^b-1)(q^{b-1}-1)\ldots(q-1)}$ (the q-binomials or Gaussian binomials, the number of b-dimensional linear subspaces of $\mathsf{V}(a,q)$).

If the order q of a plane or space is fixed we write
$\theta_i = \begin{bmatrix} i+1 \\ 1 \end{bmatrix}_q = \frac{q^{i+1}-1}{q-1} = q^i + q^{i-1} + \ldots + q + 1$.

$\mathsf{Tr}_{q^n \to q}(X) = X + X^q + X^{q^2} + \ldots + X^{q^{n-1}}$ is the trace function from $\mathsf{GF}(q^n)$ to $\mathsf{GF}(q)$.

$\mathsf{Norm}_{q^n \to q}(X) = X X^q X^{q^2} X^{q^{n-1}}$ is the norm function from $\mathsf{GF}(q^n)$ to $\mathsf{GF}(q)$.

J_t is the ideal $\langle (X_1^q - X_1)^{i_1} (X_2^q - X_2)^{i_2} \ldots (X_n^q - X_n)^{i_n} \; : \; 0 \le i_1 + i_2 + \ldots + i_n = t \rangle$ in $\mathsf{GF}(q)[X_1, \ldots, X_n]$ of polynomials vanishing everywhere with multiplicity at least t.

H_∞ is the hyperplane at infinity in the projective space $\mathsf{PG}(n,q)$ when an "affine part" is fixed, i.e. $H_\infty = \mathsf{PG}(n,q) \setminus \mathsf{AG}(n,q)$. When $n = 2$, it is called the "line at infinity" ℓ_∞.

M_f: given the polynomial $f \in \mathsf{GF}(q)[X]$, the number of elements $a \in \mathsf{GF}(q)$ for which $f(X) + aX$ is a permutation polynomial.

D_f: given the polynomial $f \in \mathsf{GF}(q)[X]$, $D_f = \{ \frac{f(x)-f(y)}{x-y} \; : \; x \ne y \in \mathsf{GF}(q) \}$, the set of directions determined by the graph of f.

$N_f = |D_f|$.

w_f: for a polynomial $f \in \mathsf{GF}(q)[X]$, $w_f = \min\{k : \sum_{x \in \mathsf{GF}(q)} f(x)^k \ne 0\}$.

Bibliography

[This dissertation is based on the following papers:]

[SzP2func] S. Ball, A. Gács, P. Sziklai, On the number of directions determined by a pair of functions over a prime field, *J. Combin. Theory Ser. A* **115** (2008), 505-516.

[SzPflock] P. Sziklai, Partial flocks of the quadratic cone, *J. Combin. Th. Ser. A*, **113** (2006), 698-702.

[SzPflhigh] P. Sziklai, Flocks of cones of higher degree, *J. Algebraic Combin.*, **25** (2007), 233–238.

[SzPnopts] P. Sziklai, A conjecture and a bound on the number of points of a plane curve, *Finite Fieds Appl.*, **14** (2008), 41–43.

[SzPblin] P. Sziklai, On small blocking sets and their linearity, *J. Combin. Th. Ser. A*, **115** (2008), 1167-1182.

[SzPvdm] P. Sziklai and M. Takáts, Vandermonde and super-Vandermonde sets, *Finite Fields Appl.*, **14** (2008), 1056-1067.

[SzPdirec] J. De Beule, P. Sziklai and M. Takáts, On the structure of the directions not determined by a large affine point set, *J. Algebr. Combin.*, DOI 10.1007/s10801-013-0430-4.

[SzPkblock] L. Storme and P. Sziklai, Linear point sets and Rédei type k-blocking sets in $\mathsf{PG}(n,q)$, *J. Alg. Comb.* **14** (2001), 221–228.

[SzPcomd] S. Ball, A. Blokhuis, A. Gács, P. Sziklai, Zs. Weiner, On linear codes whose weights and length have a common divisor, *Advances in Mathematics* **211** (2007), 94–104.

[Other papers of the author, mentioned in this dissertation: [

[SzPnuc] P. Sziklai, Nuclei of point sets in $\mathsf{PG}(n,q)$, *Disc. Math.*, **174** (1997), 323-327.

[SzPdpow] P. Sziklai, Subsets of $\mathsf{GF}(q^2)$ with d-th power differences, *Disc. Math.*, **208-209** (1999), 547-555.

[SzPrand] P. Sziklai, A lemma on the randomness of d-th powers in $\mathsf{GF}(q)$, *Bull. Belg. Math. Soc.* **8** (2001), 95-98.

[SzPnuc2] A. Gács, P. Sziklai and T. Szőnyi, Two remarks on blocking sets and nuclei in planes of prime order, *Designs, Codes and Cryptography*, **10** (1997), 29-39.

[SzPszt] P. Sziklai and T. Szőnyi, Blocking sets and algebraic curves, *Rend. Circ. Mat. Palermo* **51** (1998), 71–86.

[SzPmult1] S. Ferret, L. Storme, P. Sziklai, Zs. Weiner, A t mod p result on weighted multiple $(n-k)$-blocking sets in $\mathsf{PG}(n,q)$, *Innovations in Incidence Geometry*, **6-7** (2009), 169-188.

[SzPmult2] S. Ferret, L. Storme, P. Sziklai, Zs. Weiner, A characterization of multiple $(n-k)$-blocking sets in projective spaces of square order, *Advances Geom.*, **14** (2012), 739-756.

[SzPfewpt] Sz. Fancsali, P. Sziklai, M.Takáts The number of directions determined by less than q points, *J. Algebr. Combin.* **37** (2013), 27-37.

[SzPVdV] P. Sziklai, G. Van de Voorde, A small minimal blocking set in $\mathsf{PG}(n,p^t)$, spanning a $(t-1)$-space, is linear, *Designs, Codes, Crypt.*, DOI 10.1007/s10623-012-9751-x.

[SzPpolybk] P. Sziklai, Polynomials in finite geometry, `http://www.cs.elte.hu/~sziklai/poly.html` , in preparation.

[**References:** [

[1] T.L. Alderson, A. Gács, On the maximality of linear codes, *Des. Codes Cryptogr.* **53** (2009), 59–68.

[2] E. F. Assmus, Jr, J. D. Key, *Designs and codes*, Cambridge University Press, 1992.

[3] L. Babai, A. Gál and A. Wigderson, Superpolynomial lower bounds for monotone span programs, *Combinatorica* **19** (1999), 301–319.

[4] S. Ball, Partial unitals and related structures in Desarguesian planes, *Designs, Codes and Cryptography*, **15** (1998), 231–236.

[5] S. Ball , Polynomials in finite geometries, in *Surveys in Combinatorics, 1999, LMS Lecture Note Series* **267** Cambridge University Press 1999, pp. 17–35.

[6] S. Ball, Intersection sets in Desarguesian affine spaces, *European J. Combin.*, **21** (2000), 441–446.

[7] S. Ball , The number of directions determined by a function over a finite field, *J. Combin. Th. Ser. A*, **104** (2003), 341–350.

[8] S. Ball, On the graph of a function in many variables over a finite field, *Des. Codes Cryptogr.* **47** (2008) 159–164.

[9] S. Ball, The polynomial method in Galois geometries, J. De Beule and L. Storme, editors, *Current research topics in Galois geometry*, Mathematics Research Developments, chapter 5, pages 105–130. Nova Sci. Publ., New York, 2012.

[10] S. Ball, A. Blokhuis, On the incompleteness of (k, n)-arcs in Desarguesian planes of order q where n divides q, *Geom. Dedicata*, **74**, (1999), 325–332.

[11] S. Ball, A. Blokhuis, F. Mazzocca, Maximal arcs in Desarguesian planes of odd order do not exist, *Combinatorica* **17** (1997), 31–41.

[12] S. Ball, A. Blokhuis An easier proof of the maximal arc conjecture, *Proc. Amer. Math. Soc.*, **126** (1998), no. 11, 3377–3380.

[13] S. Ball, A. Gács, On the graph of a function over a prime field whose small powers have bounded degree, *European J. Combin.*, *30* (2009) 1575–1584.

[14] S. Ball, P. Govaerts and L. Storme, On ovoids of parabolic quadrics, *Designs, Codes and Cryptography* **38** (2006), 131–145.

[15] S. Ball, A. Blokhuis and M. Lavrauw, Linear $(q+1)$-fold blocking sets in $\mathsf{PG}(2,q^4)$, *Finite Fields Appl.* **6** (2000), 294-301.

[16] S. Ball and M. Lavrauw, On the graph of a function in two variables over a finite field, *J. Algebraic Combin.*, **23** (2006) 243–253.

[17] S. Ball, M. Lavrauw, On the graph of a function in two variables over a finite field, *J. Algebraic Combin.* **23** (2006), 243–253.

[18] S. Ball, M. Lavrauw, How to use Rédei polynomials in higher dimensional spaces, *Le Matematiche* (Catania) **59** (2004), 39–52 (2006).

[19] S. Ball, Zs. Weiner, An introduction to finite geometry, `http://www-ma4.upc.es/~simeon/IFG.pdf`

[20] A. Barlotti, Sui $\{k,n\}$-archi di un piano lineare finito, *Boll. Un. Mat. Ital.* **11** (1956), 553–556.

[21] A. Biró, On polynomials over prime fields taking only two values on the multiplicative group, *Finite Fields and Their Appl.* **6** (2000), 302-308.

[22] A. Blokhuis, On multiple nuclei and a conjecture of Lunelli and Sce, *Bull. Bel. Math. Soc. Simon Stevin* **3** (1994), 349-353.

[23] A. Blokhuis, *Blocking sets in Desarguesian Planes*, in: Paul Erdős is Eighty, vol. **2**, (1996) 133–155. eds.: D. Miklós, V.T. Sós, T. Szőnyi, Bolyai Soc. Math. Studies.

[24] A. Blokhuis, On the size of a blocking set in $\mathrm{PG}(2,p)$, *Combinatorica* **14** (1994), 273–276.

[25] A. Blokhuis, Characterization of seminuclear sets in a finite projective plane, *J. Geom.* **40** (1991), 15–19.

[26] A. Blokhuis, Extremal problems in finite geometries, *Bolyai Society Mathematical Studies* **3** (1991), 111–135.

[27] A. Blokhuis, Polynomials in finite geometries and combinatorics, in *Surveys in Combinatorics, LMS Lecture Notes Series* **187** Cambridge University Press 1993, pp. 35–52.

[28] A. Blokhuis, L. Lovász, L. Storme and T. Szőnyi, On multiple blocking sets in Galois planes, *Adv. Geom.* **7** (2007), 39-53.

[29] A. Blokhuis and J.J. Seidel, Remark on Wielandt's visibility theorem, *Lin. Alg. and its Appl.*, **71** (1985), 29-30.

[30] A. Blokhuis, L. Storme and T. Szőnyi, Lacunary polynomials, multiple blocking sets and Baer subplanes, *J. London Math. Soc.* (2) **60** (1999), 321–332.

[31] A. Blokhuis and T. Szőnyi, Note on the structure of semiovals in finite projective planes, *Discr. Math.* **106/107** (1992), 61–65.

[32] A. Blokhuis, Á. Seress, H. A. Wilbrink, On sets of points without tangents, *Mitt. Math. Sem. Univ. Giessen* **201** (1991), 39–44.

[33] A. Blokhuis, S. Ball, A. Brouwer, L. Storme and T. Szőnyi, On the number of slopes determined by a function on a finite field, *J. Comb. Theory Ser. (A)* **86** (1999), 187–196.

[34] A. Blokhuis and A. E. Brouwer, Blocking sets in Desarguesian projective planes, *Bull. London Math. Soc.* **18** (1986), 132–134.

[35] A. Blokhuis, A.A. Bruen, The minimal number of lines intersected by a set of $q+2$ points, blocking sets and intersecting circles, *J.Comb. Theory (A)*, **50** (1989), 308–315.

[36] A. Blokhuis, K. Metsch, Large minimal blocking sets, strong representative systems and partial unitals, in: *Finite Geometries*, (F. De Clerck et al., eds), Cambridge Univ. Press, Cambridge, 1993, 37–52.

[37] A. Blokhuis, R. Pellikaan, T. Szőnyi, Blocking sets of almost Rédei type, *J. Comb. Theory Ser. A* **78** (1997), 141–150.

[38] R. C. Bose, Strongly regular graphs, partial geometries and partially balanced designs, *Pacific J. Math.*, 13:389–419, 1963.

[39] A. E. Brouwer and A. Schrijver, The blocking number of an affine space, *J. Combin. Theory Ser. A* **24** (1978), 251–253.

[40] A. A. Bruen, Baer subplanes and blocking sets, *Bull. Amer. Math. Soc.* **76** (1970), 342–344.

[41] A. A. Bruen, Blocking sets in finite projective planes, *SIAM J. Appl. Math.* **21** (1971), 380–392.

[42] A.A. Bruen, Polynomial multiplicities over finite fields and intersection numbers, *J. Combin. Th. Ser. A* **60** (1992), 19–33.

[43] A. A. Bruen and M. J. de Resmini, Blocking sets in affine planes, In *Combinatorics '81*, **18** of *Ann. Discrete Math.*, North-Holland, Amsterdam-New York (1983), 169–175. (Rome, 1981)

[44] A.A. Bruen and J.C. Fisher, The Jamison method in Galois geometries, *Designs, Codes and Cryptography* **1** (1991), 199–205.

[45] A.A. Bruen and B. Levinger, A theorem on permutations of a finite field, *Can. J. Math.* **XXV.** (1973), 1060-1065.

[46] A. A. Bruen and J. A. Thas, Blocking Sets, *Geom. Dedicata* **6** (1977), 193–203.

[47] K. Coolsaet, J. De Beule, and A. Siciliano. The known maximal partial ovoids of size $q^2 - 1$ of $\mathrm{Q}(4, q)$. *J. Combin. Des.*, DOI: 10.1002/jcd.21307, 2012.

[48] A. Cossu. Su alcune proprietà dei $\{k, n\}$-archi di un piano proiettivo sopra un corpo finito. *Rend. Mat. e Appl. (5)*, 20:271–277, 1961.

[49] J. De Beule. On large maximal partial ovoids of the parabolic quadric $\mathrm{Q}(4, q)$. *Des. Codes Cryptogr.*, DOI 10.1007/s10623-012-9629-y, 2012.

[50] J. De Beule and A. Gács. Complete arcs on the parabolic quadric $\mathrm{Q}(4, q)$. *Finite Fields Appl.*, 14(1):14–21, 2008.

[51] J. De Beule, A. Klein, and K. Metsch. Substructures of finite classical polar spaces. In J. De Beule and L. Storme, editors, *Current research topics in Galois geometry*, Mathematics Research Developments, chapter 2, pages 35–61. Nova Sci. Publ., New York, 2012.

[52] F. De Clerck, A. Del Fra, and D. Ghinelli. Pointsets in partial geometries. In *Advances in finite geometries and designs (Chelwood Gate, 1990)*, Oxford Sci. Publ., pages 93–110. Oxford Univ. Press, New York, 1991.

[53] F. De Clerck and N. Durante. Constructions and characterizations of classical sets in $\mathrm{PG}(n, q)$. In *Current research topics in Galois geometry*, chapter 1, pages 1–32. Nova Sci. Publ., New York, 2011.

[54] F. De Clerck and H. Van Maldeghem. Some classes of rank 2 geometries. In *Handbook of incidence geometry*, pages 433–475. North-Holland, Amsterdam, 1995.

[55] R. H. F. Denniston, Some maximal arcs in finite projective planes, *J. Combinatorial Theory* **6** (1969), 317–319.

[56] S. De Winter and K. Thas. Bounds on partial ovoids and spreads in classical generalized quadrangles. *Innov. Incidence Geom.*, 11:19–33, 2010.

[57] A.W.M. Dress, M.H. Klin and M.E. Muzichuk, On p-configurations with few slopes in the affine plane over $\mathbb{F}_p$ and a theorem of W. Burnside, *Bayreuther Math. Schriften* **40** (1992), 7-19.

[58] P. Erdős, L. Lovász, Problems and results on 3-chromatic hypergraphs and some related questions, *Infinite and finite sets* (Colloq., Keszthely, 1973; dedicated to P. Erdős on his 60th birthday), Vol. II, pp. 609-627, Colloq. Math. Soc. János Bolyai, Vol. 10, North-Holland, Amsterdam, 1975.

[59] W. Fulton, *Algebraic Curves: An Introduction to Algebraic Geometry*, reprint, Addison Wesley, 1989.

[60] A. Gács, On the size of the smallest non-classical blocking set of Rédei type in $\mathsf{PG}(2, p)$, *J. Combin. Th. Ser. A.* **89** (2000), 43-54.

[61] A. Gács, On a generalization of Rédei's theorem, *Combinatorica* **23** (2003), no. 4, 585–598.

[62] A. Gács, Zs. Weiner, On $(q+t,t)$-arcs of type $(0,2,t)$, *Designs, Codes and Cryptography* **29** (2003), 131–139.

[63] U. Heim, Proper blocking sets in projective spaces, *Discrete Math.* **174** (1997), 167–176.

[64] U. Heim, Blockierende Mengen in endliche projektiven Räumen, *Mitt. Math. Semin. Giessen* **226** (1996), 4-82.

[65] J. W. P. Hirschfeld, Projective geometries over finite fields, *Clarendon Press, Oxford*, 1979, 2nd edition, 1998, 555 pp.

[66] J. W. P. Hirschfeld, Finite projective spaces of three dimensions, Oxford University Press, Oxford, 1985, 316 pp.

[67] J. W. P. Hirschfeld, J. A. Thas, General Galois geometries, Oxford University Press, Oxford, 1991, 407 pp.

[68] J. W. P. Hirschfeld and G. Korchmáros, Arcs and curves over a finite field, *Finite Fields Appl.* **5** (1999), 393-408.

[69] J. W. P. Hirschfeld, G. Korchmáros and F. Torres, *Algebraic Curves over a Finite Field*, Princeton University Press.

[70] J.W.P. Hirschfeld and L. Storme, The packing problem in statistics, coding theory and finite projective spaces: update 2001. *Developments in Mathematics* **3**, Kluwer Academic Publishers. Finite Geometries, Proc. 4th Isle of Thorns Conference (2000), 201-246.

[71] J. W. P. Hirschfeld, T. Szőnyi, Constructions of large arcs and blocking sets in finite planes, *European J. Comb.* **12** (1991), 499-511.

[72] M. Homma, S.J. Kim, Around Sziklai's conjecture on the number of points of a plane curve over a finite field, *Finite Fields Appl.* **15** (2009), 468–474.

[73] M. Homma, S.J. Kim, Sziklai's conjecture on the number of points of a plane curve over a finite field II, *Finite fields: theory and applications*, 225–234, Contemp. Math., **518**, Amer. Math. Soc., Providence, RI, 2010.

[74] M. Homma, S.J. Kim, Sziklai's conjecture on the number of points of a plane curve over a finite field III, *Finite Fields Appl.* **16** (2010), 315–319.

[75] R.E. Jamison, Covering finite fields with cosets of subspaces, *J. of Comb. Th. Ser. A* **22** (1977), 253–266.

[76] B. C. Kestenband, A family of complete arcs in finite projective planes, *Colloq. Math.*, **LVII** (1987), 59–67.

[77] J. Kollár, L. Rónyai, T. Szabó, Norm-graphs and bipartite Turán numbers, *Combinatorica* **16** (1996), 399–406.

[78] G. Korchmáros and F. Mazzocca, On $(q+t)$-arcs of type $(0,2,t)$ in a desarguesian plane of order q, *Math. Proc. Camb. Phil. Soc.* **108** (1990), 445-459.

[79] R. Lidl and H. Niederreiter, Finite fields. Addison-Wesley, Reading, Mass., 1983. (Cambridge University Press, 1988). (Second Edition, Cambridge University Press, 1997.)

[80] L. Lovász and A. Schrijver: Remarks on a theorem of Rédei, *Studia Scient. Math. Hungar* **16** (1981), 449-454.

[81] G. Lunardon, Normal spreads, *Geom. Dedicata* **75** (1999), 245–261.

[82] G. Lunardon, Linear k-blocking sets, *Combinatorica* **21** (2001), 571–581.

[83] L. Lunelli, M. Sce, Considerazioni aritmetiche e risultati sperimentali sui $\{K,n\}_q$-archi, *Ist. Lombardo Accad. Sci. Rend. A* **98** (1964), 3–52.

[84] K. Metsch, Blocking sets in projective spaces and polar spaces, *Combinatorics 2002, Topics in Combinatorics: Geometry, Graph Theory and Designs* (2002), 204–219.

[85] P. Polito, O. Polverino, On small blocking sets, *Combinatorica* **18** (1998), 133–137.

[86] O. Polverino, Small minimal blocking sets and complete k-arcs in $\mathsf{PG}(2,p^3)$, *Discrete Math.* **208/9** (1999), 469–476.

[87] O. Polverino, Small blocking sets in $\mathrm{PG}(2, p^3)$, *Designs, Codes and Cryptography* **20** (2000), 319–324.

[88] O. Polverino, L. Storme, Small minimal blocking sets in $\mathsf{PG}(2, q^3)$, *Eur. J. Comb.* **23** (2002), 83–92.

[89] S. E. Payne and J. A. Thas. *Finite generalized quadrangles*. EMS Series of Lectures in Mathematics. European Mathematical Society (EMS), Zürich, second edition, 2009.

[90] O. Polverino, T. Szőnyi, Zs. Weiner, Blocking sets in Galois planes of square order, Acta Sci. Math. (Szeged) **65** (1999), 737–748.

[91] L. Rédei, *Lückenhafte Polynome über endlichen Körpern*, Akadémiai Kiadó, Budapest, and Birkhäuser Verlag, Basel, 1970 (English translation: *Lacunary polynomials over finite fields*, Akadémiai Kiadó, Budapest, and North Holland, Amsterdam, 1973).

[92] H. Sachar, The $\mathbb{F}_p$-span of the incidence matrix of a finite projective plane, *Geometriae Dedicata* **8** (1979), 407–415.

[93] B. Segre. Ovals in a finite projective plane. *Canad. J. Math.*, 7:414–416, 1955.

[94] B. Segre, Le geometrie di Galois, *Ann. Mat. Pura Appl.* (4) **48** (1959) 1–96.

[95] B. Segre, *Lectures on modern geometry,* Edizioni Cremonese, Rome, Italy, 1961.

[96] B. Segre, Introduction to Galois geometries (ed. J.W.P. Hirschfeld), *Atti Accad. Naz. Lincei Mem. Cl. Sci. Fis. Mat. Natur I* **8** (1967), 133-236.

[97] A. Seidenberg, *Elements of the theory of algebraic curves*, Addison-Wesley, Reading, Mass., 1968.

[98] L. Storme, J. A. Thas, k-arcs and partial flocks, *Linear Algebra Appl.* **226/228** (1995), 33–45.

[99] L. Storme and Zs. Weiner, On 1-blocking sets in $\mathsf{PG}(n, q)$, $n \geq 3$. *Des. Codes Cryptogr.* **21** (2000), 235–251.

[100] K-O. Stöhr and J. F. Voloch, Weierstrass points and curves over finite fields, *Proc. London Math. Soc.*, **52** (1986) 1–19.

[101] T. Szőnyi, Combinatorial problems for Abelian groups arising from geometry, *Periodica Polytechnica*, **19** (1991) 197–212.

[102] T. Szőnyi, Some applications of algebraic curves in finite geometry and combinatorics, in: *Surveys in Combinatorics* (R. A. Bailey, ed.), Cambridge Univ. Press, Cambridge, 1997, 198–236.

[103] T. Szőnyi, Blocking sets in Desarguesian affine and projective planes, *Finite Fields and Appl.* **3** (1997), 187-202.

[104] T. Szőnyi, On the number of directions determined by a set of points in an affine Galois plane, *J. Combin. Th. Ser. A* **74** (1996), 141–146.

[105] T. Szőnyi, On the embeddability of (k, p)-arcs, *Designs, Codes and Cryptography* **18** (1999), 235–246.

[106] T. Szőnyi, Note on the existence of large minimal blocking sets in Galois planes, *Combinatorica* **12** (1992), 227-235.

[107] T. Szőnyi, Some recent applications of Rédei's theory of lacunary polynomials (in Hungarian), *Polygon* **5** (1995), 2, 49–78.

[108] T. Szőnyi, On some applications of curves in finite geometry, *Socrates lecture notes*, Potenza, 2001.

[109] T. Szőnyi, Zs. Weiner, Small blocking sets in higher dimensions, *J. Combin. Th. Ser. A* **95** (2001), 88-101.

[110] T. Szőnyi, Zs. Weiner, On stability theorems in finite geometry, manuscript 2006.

[111] G. Turnwald, A new criterion for permutation polynomials, *Finite Fields and Appl.* **1** (1995), 64–82.

[112] D. Wan, G. L. Mullen and P. J.-S. Shiue, The number of permutation polynomials of the form $f(x) + c(x)$ over a finite field, *Proc. Edinburgh Math. Soc*, **38** (1995) 133–149.

[113] A. Weil, Sur les Courbes Algébrique et les varietés qui s'en déduisent, *Actualités Scientifiques et Industrielles* **1041**, Herman & Cie, Paris, 1948.

[114] Zs. Weiner, Small point sets of $\mathsf{PG}(n,q)$ intersecting each k-space in 1 modulo $\sqrt{q}$ points, *Innovations in Incidence Geometry*, **1**, (2005), 171–180.

[115] F. Wettl, On the nuclei of a finite projective plane, *J. of Geometry* **30** (1987), 157–163.