PERMUTATIONS, HYPERPLANES AND POLYNOMIALS OVER
FINITE FIELDS

ANDRÁS GÁCS, TAMÁS HÉGER, ZOLTÁN LÓRÁNT NAGY, AND DÖMŐTÖR PÁLVÖLGYI

Abstract. Starting with a result in combinatorial number theory we prove that (apart from a couple of exceptions that can be classified), for any elements $a_1, \ldots, a_n$ of $GF(q)$, there are distinct field elements $b_1, \ldots, b_n$ such that $a_1b_1 + \cdots + a_nb_n = 0$. This implies the classification of hyperplanes lying in the union of the hyperplanes $X_i = X_j$ in a vector space over $GF(q)$, and also the classification of those multisets for which all reduced polynomials of this range are of reduced degree $q - 2$. The proof is based on the polynomial method.

1. Introduction

This paper is devoted to a result formulated in three different terminologies. We start with a result in combinatorial number theory which might resemble Snevily’s conjecture [7]. Then we derive two consequences (which are essentially equivalent to the original result), one about the range of polynomials over a finite field, and one about hyperplanes in a vector space over a finite field fully lying in the union of certain fixed hyperplanes.

Although perhaps the consequence about the range of polynomials solves a more natural question (and raises interesting open problems), our proof is most easily formulated in the additive combinatorial terminology, so we start with this result. It was motivated by a result of Stéphane Vinatier [8].

Theorem 1.1. Suppose $\{a_1, a_2, \ldots, a_p\}$ is a multiset in the finite field $GF(p)$, $p$ prime. Then after a suitable permutation of the indices, either $\sum_i ia_i = 0$, or $a_1 = a_2 = \cdots = a_{p-2} = a$, $a_{p-1} = a + b$, $a_p = a - b$ for field elements $a$ and $b$, $b \neq 0$.

In the paper [8] Vinatier proves a similar result (though with a slightly different terminology) with the extra assumption that $a_1, \ldots, a_p$, when considered as integers, satisfy $a_1 + \cdots + a_p = p$.

Before going further, let us recall that Snevily’s conjecture states that for any abelian group $G$ of odd order (written multiplicatively), and positive integer $n \leq |G|$, for any sets $\{a_1, \ldots, a_n\}$ and $\{b_1, \ldots, b_n\}$ of elements of $G$, there is a permutation $\pi$ of the indices, such that the elements $a_1b_{\pi(1)}$, $a_2b_{\pi(2)}$, $\ldots$, $a_nb_{\pi(n)}$ are different. Alon proved this for groups of prime degree [2] and later Dasgupta, Károlyi, Serra and Szegedy [5] for cyclic groups. Alon’s result is in fact more general: he only assumes that $\{a_1, \ldots, a_n\}$ is a multiset. Let us remark that if this general version was true for cyclic groups (it is obviously not), then there would be no exception in Theorem 1.1, and the proof would easily follow from this general version.

The authors were supported by OTKA grants T 67867, T 049662 and Bolyai scholarship.
Theorem 1.1 will follow from the following more general result, where $p$ is replaced by an arbitrary prime power $q$ and the number of elements is arbitrary.

**Theorem 1.2.** Suppose \( \{a_1, a_2, \ldots, a_n\} \) is a multiset in the finite field \( GF(q) \), with \( n \leq q \). Then one can find distinct field elements \( b_1, b_2, \ldots, b_n \) such that \( \sum_i a_i b_i = 0 \), unless one of the following holds:

(i) \( n = q \) and after permutation of the indices, \( a_1 = a_2 = \cdots = a_{q-2} = a, \ a_{q-1} = a+b, \ a_q = a-b \) for field elements \( a \) and \( b \neq 0 \).

(ii) \( n = q - 1 \), and after permutation of the indices, \( a_1 = a_2 = \cdots = a_{q-2} = a, \ a_{q-1} = 2a \) for a field element \( a \neq 0 \).

(iii) \( n \leq q-1 \) and after permutation of the indices, \( a_1 = a_2 = \cdots = a_{n-2} = 0, \ a_{n-1} = b, \ a_n = -b \) for a field element \( b \neq 0 \).

Note that if we let \( n = q = p \), \( p \) prime in Theorem 1.2, then we get Theorem 1.1 (one should note that a permutation of the indices 1, 2, \ldots, \( p \) and different field elements \( b_1, b_2, \ldots, b_p \) are the same).

In Sections 2 and 3 we derive two consequences of Theorem 1.2. The proof will be given in Section 4, finally, Section 5 is devoted to remarks and open problems.

We end this introduction with recalling Lucas’ theorem and Alon’s Combinatorial Nullstellensatz.

Lucas’ theorem tells how binomial coefficients behave modulo a prime \( p \). Let the \( p \)-adic expansion of \( n \) and \( k \) be \( n = \sum_{i=1}^{r} n_i p^{i-1} \) and \( k = \sum_{i=1}^{r} k_i p^{i-1} \), respectively. Then \( \binom{n}{k} \equiv \binom{n_1}{k_1} \cdots \binom{n_r}{k_r} \) modulo \( p \). For a proof, see [6]. We will use this often without explicitly referring to it.

Alon’s Combinatorial Nullstellensatz [1] states that if a polynomial vanishes for all substitutions from the direct product of certain sets, then it is in a certain ideal. We will only use the following particular case:

**Theorem 1.3.** If a polynomial \( G(Y_1, \ldots, Y_k) \) over the finite field \( GF(q) \) vanishes for all substitutions, then it can be written in the following form:

\[
G(Y_1, \ldots, Y_k) = (Y_1^q - Y_1)f_1 + \cdots + (Y_k^q - Y_k)f_k,
\]

where the \( f_i \)'s are polynomials in \( Y_1, \ldots, Y_k \) of degree at most \( \deg(G) - q \).

*Proof.* See Alon [1]. \( \square \)

Finally, let us recall that for any finite field \( GF(q) \), \( \sum_{x \in GF(q)} x^k = 0 \) when \( 1 \leq k \leq q-2 \), and \( \sum x^{q-1} = -1 \). We will often use this later.

2. A result about polynomials of prescribed range

In this section we give another formulation of Theorem 1.2. Although it might seem to be a consequence, it is essentially equivalent to the original result.
Before explaining the problem to be solved, recall that over the finite field \( GF(q) \) any function can be represented by a polynomial of degree at most \( q - 1 \). The degree of such a polynomial is called the reduced degree of the polynomial (function). Before stating our result, let us state a lemma, which can be easily proved using the fact mentioned at the end of the introduction.

**Lemma 2.1.** Suppose \( f(x) = c_{q-1}x^{q-1} + \cdots + c_0 \) is a polynomial over \( GF(q) \). Then \( \sum x f(x) = -c_{q-1} \) and \( \sum x^2 f(x) = -c_{q-2} \).

For a multiset \( M \) of size \( q \) of the field elements we say that \( M \) is the range of the polynomial \( f \) if \( M = \{ f(x) : x \in GF(q) \} \) as a multiset (that is, not only values, but also multiplicities need to be the same). Suppose we have a multiset \( M \) and wish to find a low degree polynomial with range \( M \). By Lemma 2.1, if the sum of elements of \( M \) is not zero, then every reduced polynomial of this range will have reduced degree \( q - 1 \) and vice versa, if the sum is zero, then a reduced polynomial of range \( M \) will automatically have degree at most \( q - 2 \).

**Theorem 2.2.** Let \( M = \{a_1, \ldots, a_q\} \) be a multiset in \( GF(q) \), with \( a_1 + \cdots + a_q = 0 \). There is no polynomial with range \( M \) of reduced degree at most \( q - 3 \) if and only if \( M \) consists of \( q - 2 \) \( a \)-s, one \( a + b \) and one \( a - b \) for field elements \( a \) and \( b \), \( b \neq 0 \).

**Proof.** By Lemma 2.1, polynomials with range \( M \) have reduced degree \( q - 1 \) if and only if \( \sum a_i \neq 0 \). If \( \sum a_i = 0 \), then the second statement of Lemma 2.1 shows that a polynomial \( f \) with range \( M \) has reduced degree at most \( q - 3 \) if and only if \( \sum x^2 f(x) = 0 \).

On the other hand, there is a bijection between polynomials with range \( M \) and the ordered sets \( (b_1, \ldots, b_q) \) (that is, permutations) of \( GF(q) \): a permutation corresponds to the function \( f(b_i) = a_i \). Under this correspondence the condition \( \sum x^2 f(x) = 0 \) translates to \( \sum a_i b_i = 0 \). Hence our claim follows from Theorem 1.2 (with the choice \( n = q \)).

Though the statement of the above theorem looks very innocent, it seems that one needs the whole machinery of Section 4 for the proof. After this result, the natural question is to look for polynomials of degree lower than \( q - 3 \) with prescribed range. This seems to be a very difficult problem.

One might conjecture that the only reason for a multiset (with sum equal to zero) not to be the range of a polynomial of degree less than \( q - k \) is that there is a value of multiplicity at least \( q - k \) (note that a value of mutiplicity \( m \) in the range guarantees that any polynomial of this range has degree at least \( m \)). We will get back to this in Section 5.

### 3. A consequence about hyperplanes of a vector space over \( GF(q) \)

In this section we prove a result about vector spaces over finite fields, which is again essentially equivalent to Theorem 1.2.

Let \( q \) denote a prime power and denote by \( V \) the vector space of dimension \( n \) over the finite field \( GF(q) \) consisting of all \( n \)-tuples \( (X_1, X_2, \ldots, X_n) \). Finally, denote by \( H_{ij} \) the hyperplane with equation \( X_i = X_j \) (\( i \neq j \)). We are interested in hyperplanes fully
Theorem 3.1. Suppose $n \leq q$ and $H \subseteq \cup_{i \neq j} H_{ij}$ is a hyperplane in $V$, $H \neq H_{ij}$ for any $i \neq j$. Then one of the following holds:

(i) $n = q$, $H = \{(X_1, \ldots, X_n) : \sum X_i + c(X_j - X_k) = 0\}$ for a field element $c \neq 0$ and indices $j \neq k$;

(ii) $n = q - 1$, $H = \{(X_1, \ldots, X_n) : \sum X_i + X_j = 0\}$ for an index $j$.

Proof. Let $H = \langle (a_1, \ldots, a_n) \rangle^\perp$. The condition that $H$ is contained in $\cup_{i \neq j} H_{ij}$ translates to the condition that whenever $a_1 x_1 + \cdots + a_n x_n = 0$, necessarily $x_i = x_j$ for an $i \neq j$, or equivalently, there are no distinct elements $x_1, \ldots, x_n$ such that $a_1 x_1 + \cdots + a_n x_n = 0$. Hence we are in (i) or (ii) or (iii) of Theorem 1.2.

It is easy to see that Theorem 1.2 (i) implies (i) of the theorem being proved. If we have (ii) from Theorem 1.2, then (ii) holds here, finally, from 1.2 (iii) we get that $H = H_{ij}$ for an $i$ and $j$, contradiction.

It is not difficult to see that the hyperplanes given in (i) and (ii) are really contained in the union.

Finally we show that affine hyperplanes only give one more example.

Theorem 3.2. All affine hyperplanes contained in $\cup_{i \neq j} H_{ij}$ are linear (for $n \leq q$), except when $n = q$ and the hyperplane is a translate of $\langle (1, \ldots, 1) \rangle^\perp$.

Proof. Suppose the affine hyperplane $\{(X_1, \ldots, X_n) : a_1 X_1 + \cdots + a_n X_n = c\}$ is contained in $\cup_{i \neq j} H_{ij}$. First choose arbitrary distinct field elements $x_1, \ldots, x_n$. Let $d = a_1 x_1 + \cdots + a_n x_n$. By the assumption, $d \neq c$. If $d \neq 0$, then $\left(\frac{d}{a_1} x_1, \ldots, \frac{d}{a_n} x_n\right)$ is in our hyperplane, a contradiction, unless $c = 0$, what we wanted to prove.

If $d = 0$, then interchange the values of two coordinates, $x_i$ and $x_j$ say, to have $a_1 x_1 + \cdots + a_n x_n = (a_i - a_j)(x_j - x_i)$. This is non-zero for well-chosen $i$ and $j$ (unless all the $a_i$s are the same), so we can make the above trick to prove $c = 0$.

Finally, if all the $a_i$s are the same, then one can easily find distinct $x_i$s to give $a_1 x_1 + \cdots + a_n x_n \neq 0$ (and make the above trick), unless $n = q$, which was the exceptional case in the claim.

4. Proof of Theorem 1.2

The proof will be carried out in several steps. We will assume $q \geq 11$. Small cases can be handled easily. We will also suppose $q$ is odd. For the proof of the even case (which is relatively easier) see the last subsection of the present section.

In Subsection 1 we make some easy observations (with elementary combinatorial proofs). As we will see, the theorem easily follows from the $n = q$ case (that is why results in Sections 2 and 3 are essentially equivalent to the result being proved).
In Subsection 2, using algebraic methods, we will derive an identity about a polynomial that will reflect the combinatorial properties of a multi-set \( \{a_1, \ldots, a_k\} \) for which one cannot find distinct field elements \( b_1, \ldots, b_k \) such that \( a_1 b_1 + \cdots + a_k b_k = 0 \). The proof will be more or less standard application of the Nullstellensatz.

The essential part of the proof of Theorem 1.2 will be carried out in Subsection 3, where (after supposing that one cannot find distinct field elements \( b_1, \ldots, b_q \) such that \( a_1 b_1 + \cdots + a_q b_q = 0 \)), we will use the information gained in Subsection 2 to deduce first that most of the \( a_i \)s are equal, and later that exactly \( q - 2 \) of them are equal.

Subsection 4 will be devoted to the \( q \) even case.

4.1. Easy combinatorial observations.

Proposition 4.1. In Theorem 1.2 everything follows from the \( n = q \) case.

Proof. If \( n < q \), then extend the set of \( a_i \)s to a set of size \( q \) with \( a_{n+1} = \cdots = a_q = 0 \). After this everything easily follows from the \( n = q \) case. \( \square \)

Hence from now on, we only consider the \( n = q \) case. We are looking for an ordering \( b_1, \ldots, b_q \) of the elements of \( GF(q) \) in such a way that \( \sum_i a_i b_i = 0 \).

Lemma 4.2. If for a multiset \( \{a_1, \ldots, a_q\} \) there is no ordering \( b_1, \ldots, b_q \) of the elements of \( GF(q) \) such that \( \sum_i a_i b_i = 0 \), then the same holds for any translation \( \{a_1 + c, \ldots, a_q + c\} \) and any non-zero multiple \( \{ca_1, \ldots, ca_q\} \).

Proof. Straightforward. \( \square \)

Note that if the \( a_i \)s are different, then it is easy to find a suitable ordering for which \( \sum_i b_i a_i = 0 \) holds (for instance let \( b_i = a_i \)). Hence by the previous lemma, we can suppose that 0 is not among the \( a_i \)s.

Lemma 4.3. Theorem 1.2 is true if \( n = q \) odd and the \( a_i \)s admit at most 3 different values.

Proof. If all the \( a_i \)s are the same, then any ordering results in \( \sum_i a_i b_i = 0 \), so suppose there are at least two values.

After transformation suppose that 0 is the value with largest multiplicity and the remaining two values are 1 and \( a \) (here \( a = 1 \) is possible).

First suppose \( a = 1 \) and that the 1-s are \( a_1 = \cdots = a_m = 1 \). We determine an appropriate ordering recursively. Let \( b_1 \neq 0 \) arbitrary, \( b_2 = -b_1, b_3 \) any non-zero value, which has not been used, \( b_4 = -b_3, \ldots \). If \( m \) is even, then after we determined the first \( m \) \( b_i \)s, the rest of the values is arbitrary. If \( m \) is odd, then \( b_m = 0 \) and the rest is arbitrary.

Next suppose \( a \neq 1 \) and that \( a_1 = \cdots = a_m = 1, a_{m+1} = \cdots = a_{m+l} = a \), and the rest is zero. If at most one of \( m \) and \( l \) is odd, then we can do the same as above. If \( m \) and \( l \) are both odd, then we can get rid of one 1 and one \( a \) by letting \( b_1 = -a \) and \( b_{m+1} = 1 \) and do the same trick as above for the rest of the values (note that \( q \) is large enough and \( m + l < 2q/3 \)).

This does not work if \( a = -1 \). If \( m = l = 1 \), then we have that our set is \( q - 2 \) zeros, a 1 and a \( -1 \), this is the exceptional case of the claim of the theorem. If one of them, \( m \) say,
is at least 3, then $b_1 = A$, $b_2 = B$, $b_3 = C$, $b_{m+1} = A + B + C$ with well-chosen $A$, $B$ and $C$, and the same trick again. \hfill \Box

In subsection 3, using algebraic tools we will be able to prove equations of the form $(a_1 - a_2)(a_2 - a_3)\ldots = 0$ for any permutation of the indices. From this, we will try to deduce that most of the $a_i$s are the same. The following easy observations will be very useful tools for this.

**Lemma 4.4.** Suppose the multiset $\{a_1, \ldots, a_k\}$ contains at least 3 different values and denote by $l$ the maximal multiplicity in the set. Let $m_1$, $m_2$ and $m_3$ be natural numbers with $m_1 + 2m_2 + 3m_3 = k$. Then one can partition the $a_i$s into $m_3$ classes of size 3, $m_2$ classes of size 2 and $m_1$ classes of size 1 in such a way, that elements in the same class are pairwise different, provided we have one of the following cases.

(i) $m_2 = 0$, $m_1 = 1$, $l \leq m_3$;
(ii) $m_2 = 1$, $m_1 = 0$, $l \leq m_3 + 1$;
(iii) $m_3 = 0$, $l \leq m_1 + m_2$;
(iv) $m_3 = 1$, $m_2 = 0$, $l \leq m_1$;
(v) $m_3 = 1$, $m_2 = 1$, $l \leq m_1 + 1$.

**Proof.** First permute the $a_i$s in such a way that equal elements have consecutive indices. This implies that if $|i - j| \geq l$, then $a_i$ and $a_j$ are different.

(i) We have $k = 3m_3 + 1$ and $l \leq m_3$. Let the $i$-th class consist of $a_i$, $a_{i+m_3}$ and $a_{i+2m_3}$ for $i = 1, \ldots, m_3$; and let $a_k$ be the last class (of size 1).

(ii) We have $k = 3m_3 + 2$ and $l \leq m_3 + 1$. Let the $i$-th class consist of $a_i$, $a_{i+m_3+1}$ and $a_{i+2m_3+2}$ for $i = 1, \ldots, m_3$; and let $a_{m_3+1}$ and $a_{2m_3+2}$ form the last class (of size 2).

(iii) We have $k = 2m_2 + m_1$ and $l \leq m_1 + m_2$. Let the $i$-th class consist of $a_i$ and $a_{i+m_1+m_2}$ for $i = 1, \ldots, m_2$; and the rest of the classes (of size 1) is arbitrary.

(iv) We know that our multiset has at least three different values, that is all we need for this case.

(v) If $m_1 = 0$, then we can use the already proved case (ii). Otherwise we have at least 6 elements. If we have at least 4 different values, then one of them has multiplicity bigger than 1. It is easy to see that the arrangement is possible. If there are exactly 3 different values, then by $l \leq m_1 + 1$, we know that at least two values occur more than 1 time. Again it is easy to find the desired arrangement. \hfill \Box

4.2. The algebraic tool.

After the above easy observations, we introduce the main tool of the proof.

**Theorem 4.5.** Suppose $a_1, \ldots, a_k$ are non-zero field elements with the property that there are no distinct field elements $b_1, \ldots, b_k$ such that $\sum_i a_i b_i = 0$. Define the following polynomial:

$$G(Y_1, \ldots, Y_k) = \left( (Y_1 + \cdots + Y_k)^{q-1} - 1 \right) D(Y_1, \ldots, Y_k),$$
where $D$ is the following determinant:

$$
\begin{vmatrix}
    a_1^{k-1} & a_1^{k-2}Y_1 & a_1^{k-3}Y_1^2 & \cdots & Y_1^{k-1} \\
    \cdot & \cdot & \cdot & \cdots & \cdot \\
    \cdot & \cdot & \cdot & \cdots & \cdot \\
    a_k^{k-1} & a_k^{k-2}Y_k & a_k^{k-3}Y_k^2 & \cdots & Y_k^{k-1}
\end{vmatrix}
$$

Then

$$G(Y_1, \ldots, Y_k) = \sum_{i=1}^{k} (Y_1^q - Y_i) f_i,$$

where the $f_i$s are polynomials in $Y_1, \ldots, Y_k$ of degree at most the degree of $G$ minus $q$.

Proof. First consider the following polynomial:

$$F(X_1, \ldots, X_k) = \left( (a_1 X_1 + \cdots + a_k X_k)^{q-1} - 1 \right) \prod_{1 \leq i < j \leq k} (X_i - X_j).$$

We wish to prove that $F$ vanishes for all substitutions.

Note that $\prod_{1 \leq i < j \leq k} (X_i - X_j)$ assures that $F$ can only be non-zero if the substituted $X_1, \ldots, X_k$ are different.

On the other hand, $(a_1 X_1 + \cdots + a_k X_k)^{q-1} - 1 = 0$ if and only if $a_1 X_1 + \cdots + a_k X_k \neq 0$. By the assumption, such $X_i$s cannot be all distinct.

Before going further note that $\prod_{1 \leq i < j \leq k} (X_i - X_j)$ is (maybe $-1$ times) the following Vandermonde determinant:

$$\begin{vmatrix}
    1 & X_1 & X_1^2 & \cdots & X_1^{k-1} \\
    \cdot & \cdot & \cdot & \cdots & \cdot \\
    \cdot & \cdot & \cdot & \cdots & \cdot \\
    1 & X_k & X_k^2 & \cdots & X_k^{k-1}
\end{vmatrix}$$

Now replace the variables of $F$ with $Y_i := a_i X_i$ ($i = 1, \ldots, k$). Using that $\prod_{1 \leq i < j \leq k} (X_i - X_j)$ is essentially the Vandermonde determinant, this shows that $F$ is zero everywhere if and only if this is true about

$$\left( (Y_1 + \cdots + Y_k)^{q-1} - 1 \right) D_1(Y_1, \ldots, Y_k),$$

where $D_1$ is the following determinant:

$$\begin{vmatrix}
    1 & (Y_1/a_1) & (Y_1/a_1)^2 & \cdots & (Y_1/a_1)^{k-1} \\
    \cdot & \cdot & \cdot & \cdots & \cdot \\
    \cdot & \cdot & \cdot & \cdots & \cdot \\
    1 & (Y_k/a_k) & (Y_k/a_k)^2 & \cdots & (Y_k/a_k)^{k-1}
\end{vmatrix}$$
Finally note that one can get $G$ from this polynomial by multiplying the $i$-th row of the determinant by $a_i^{k-1} \neq 0$ for $i = 1, \ldots, k$.

Hence $G$ is zero for all substitutions. By Theorem 1.3, $G$ has the claimed form.  

The above theorem shows that in any term of $G$ of maximal degree, at least one of the $Y_i$s has degree at least $q$. The main idea of the proofs of the next subsection is that we determine the coefficient (in terms of the $a_i$s) of well-chosen terms with all degrees at most $q - 1$ to deduce conditions on the $a_i$s.

### 4.3. The essential part of the proof.

Now we are ready to prove that there is a value among the $a_i$s with large multiplicity. We have to deal with the prime case (which is much easier) separately.

**Lemma 4.6.** Suppose $q = p$ prime and there is no ordering $b_1, \ldots, b_p$ of the elements of $GF(p)$ such that $\sum_i a_i b_i = 0$. Then at least $\frac{p+2}{3}$ of the $a_i$s are the same.

**Proof.** After transformation suppose 0 is not among the $a_i$s. Consider the polynomial $G$ from Theorem 4.5 with $k = p$. By 4.5, terms of maximal degree of $G$ have at least one $Y_i$ with degree at least $p$. We distinguish two cases according to whether $p \equiv 1 \pmod{3}$ or $p \equiv 2 \pmod{3}$.

First suppose $3 \mid p - 1$ and let us find the coefficient of the following term:

$$Y_1^{p-1}Y_2^{p-1}Y_3^{p-1}Y_4^{p-4}Y_5^{p-4}Y_6^{p-4} \cdots Y_{p-3}^{3}Y_{p-2}^{3}Y_{p-1}^{3}.$$ 

First of all note that the degree of this term equals the degree of $G$, which is $\frac{(p-1)(p+2)}{2}$. By the sentence after Theorem 4.5, the coefficient (depending on the $a_i$s) has to be zero.

We claim that apart from a nonzero scalar (depending on the $a_i$s), this coefficient is

$$(a_1-a_2)(a_2-a_3)(a_3-a_1)(a_4-a_5)(a_5-a_6)(a_6-a_4) \cdots (a_{p-3}-a_{p-2})(a_{p-2}-a_{p-1})(a_{p-1}-a_{p-3}).$$

To see this note that all terms of $D$ are of the form $Y_{\pi(1)}^{p-1}Y_{\pi(2)}^{p-2} \cdots Y_{\pi(p)}^{0}$, where $\pi$ is a permutation of the indices $\{1, \ldots, p\}$. To get the term above, we need 1, 2 and 3 for $\pi(1)$, $\pi(2)$, $\pi(3)$ (any order), then 4, 5 and 6 for $\pi(4)$, $\pi(5)$, $\pi(6)$ (any order),... For any such $\pi$, we need the term $Y_{\pi(1)}^{0}Y_{\pi(2)}^{1}Y_{\pi(3)}^{2}Y_{\pi(4)}^{0}Y_{\pi(5)}^{1}Y_{\pi(6)}^{2} \cdots$ from $(Y_1 + \cdots + Y_p)^{p-1}$ to have the desired product. All such terms come from $(Y_1 + \cdots + Y_p)^{p-1}$ with the same non-zero coefficient.

Finally, note that the terms we need from $D$ are exactly the ones coming from the following part of the determinant:
Now suppose the maximal multiplicity in the multiset \( \{a_i \} \) of the indices, which is exactly what we claimed.

Before we write up \( G \), we can permute the \( a_i \)'s, hence we get that for any permutation \( \pi \) of the indices,

\[
(a_{\pi(1)} - a_{\pi(2)})(a_{\pi(2)} - a_{\pi(3)})(a_{\pi(3)} - a_{\pi(1)})(a_{\pi(4)} - a_{\pi(5)})(a_{\pi(5)} - a_{\pi(6)})(a_{\pi(6)} - a_{\pi(4)}) \cdots \\
\cdots (a_{\pi(p-3)} - a_{\pi(p-2)})(a_{\pi(p-2)} - a_{\pi(p-1)})(a_{\pi(p-1)} - a_{\pi(p-3)}) = 0. \tag{1}
\]

Now suppose the maximal multiplicity in the multiset \( \{a_1, \ldots, a_p\} \) is \( l \leq \frac{p-1}{3} \). By Lemma 4.4 (i), this implies that we can find a permutation of the indices such that the first 3 elements are different, the second 3 are different, \ldots, the last 3 are different. This contradicts (1), so the proof of the \( 3|p - 1 \) case is done.

Now suppose \( 3|p + 1 \) and let us find the coefficient of the following term:

\[
Y_1^{p-1}Y_2^{p-1}Y_3^{p-1}Y_4^{p-4}Y_5^{p-4}Y_6^{p-4} \cdots Y_{p-4}^{4}Y_{p-3}^{4}Y_{p-2}^{4}Y_{p-1}^{4}Y_p.
\]

We claim that apart from a nonzero scalar (depending on the \( a_i \)’s), this coefficient is

\[
(a_1 - a_2)(a_2 - a_3)(a_3 - a_1)(a_4 - a_5)(a_5 - a_6)(a_6 - a_4) \cdots \\
\cdots (a_{p-4} - a_{p-3})(a_{p-3} - a_{p-2})(a_{p-2} - a_{p-4})(a_{p-1} - a_p).
\]

The rest is similar to the proof of the previous case. Here we need to use Lemma 4.4 (ii) at the end.

\begin{lemma}
Suppose \( q = p^h > 9 \) for an odd prime \( p \) and \( h > 1 \), and that there is no ordering \( b_1, \ldots, b_q \) of the elements of \( GF(q) \) such that \( \sum_i a_ib_i = 0 \). Then at least \( \frac{q^3 - 3}{2} \) of the \( a_i \)'s are the same.
\end{lemma}

\begin{proof}
The proof is similar to the previous one, but it will be much more difficult to determine the coefficient of the appropriate term in \( G \).
\end{proof}
After transformation suppose 0 is not among the \(a_i\)s. Consider the polynomial \(G\) from Theorem 4.5 with \(k = q\). By 4.5, terms of maximal degree of \(G\) have at least one \(Y_i\) with degree at least \(q\).

The term to give information about the \(a_i\)s this time is the following:

\[
\prod_{i=1}^{q} Y_i^{q_i-1} \cdot (Y_1Y_3Y_5 \cdots Y_{2p-3})(Y_{2p-1}Y_{2p} \cdots Y_{3p-3})^{p}(Y_{p^2+1}Y_{p^2+2} \cdots Y_{p^2+p-1})^{p^2} \cdots \\
\cdots Y_{p^{h-1}+1}Y_{p^{h-1}+2} \cdots \ Y_{p^{h-1}+p-1})^{p^{h-1}}
\]

The degree of this term is \(1 + 2 + \cdots + (q-1) + (p-1)(1+p+p^2+\cdots+p^{h-1}) = (q) + q - 1\), this is the degree of \(G\). A little calculation shows that all \(Y_i\)s have degree at most \(q - 1\) in this term.

It is easy to see that one way to get this term in \(G\) is to take \(\prod_{i=1}^{q} Y_i^{q_i-1}\) from the Vandermonde part and the rest from \((Y_1 + \cdots + Y_q)^{q-1}\). We will prove that besides this, the only way to get this term with a non-zero coefficient is to interchange the role of some pairs of variables with the same degree. These pairs are: \(Y_1, Y_2\) (both of degree 1), \(Y_3, Y_4\) (both of degree 3), \(Y_{2p-3}, Y_{2p-2}\) (both of degree \(2p-3\)); \(Y_{2p-1}, Y_{3p-1}\) (both of degree \(3p-2\)), \(Y_{2p}, Y_{3p}\) (both of degree \(3p-1\)); \(Y_{4p-3}, Y_{4p-2}\) (both of degree \(4p-4\)); \(Y_{p^2+1}, Y_{p^2+2}\) (both of degree \(2p^2\)); \(Y_{p^2+2}, Y_{2p^2+2}\) (both of degree \(p^2+1\)); \(\cdots\), \(Y_{p^{h-1}+1}Y_{p^{h-1}+2}\) (both of degree \(2p^{h-1}\)).

Let us look for the term in question. From the Vandermonde part, all terms are of the form \(Y_{\pi(1)}^{\pi(1)} \cdots Y_{\pi(q)}^{\pi(q)}\) for a permutation \(\pi\) of the indices. In the term in question, we have only two \(Y_i\)s of degree less than 2: \(Y_1, Y_2\), hence \(\{\pi(1), \pi(2)\} = \{1, 2\}\). Similarly we get that \(\{\pi(2k-1), \pi(2k)\} = \{2k-1, 2k\}\) for \(k \leq p - 1\). This shows that the part coming from \((Y_1 + \cdots + Y_q)^{q-1}\) starts with \(Y_{\pi(1)}^{\pi(1)} Y_{\pi(3)}^{\pi(3)} \cdots Y_{\pi(2p-3)}^{\pi(2p-3)}\). The coefficient of such a term in \((Y_1 + \cdots + Y_q)^{q-1}\) starts with \((q - 1)(q - 2) \cdots (q - p + 1)\) (times something depending on the degrees of the rest of the \(Y_i\)s). If the degree of any of the rest of the \(Y_i\)s is not divisible by \(p\), then (by Lucas’ theorem) the coefficient is zero, since it is divisible by \((q - 1)(q - 2) \cdots (q - p + 1)(q-p)\) with a \(k\) not divisible by \(p\). Hence we only have to consider those possibilities, when the term coming from \((Y_1 + \cdots + Y_q)^{q-1}\) starts with \(Y_{\pi(1)}^{\pi(1)} Y_{\pi(3)}^{\pi(3)} \cdots Y_{\pi(2p-3)}^{\pi(2p-3)}\) and continues with all the \(Y_i\)s having degree divisible by \(p\).

So far we have identified all \(Y_i\)s coming from the Vandermonde part of degree at most \(2p-3\). After this, in the term in question we have \((Y_{2p-1}Y_{3p-1})^{3p-2}(Y_{2p}Y_{3p})^{3p-1} \cdots (Y_{3p-3}Y_{4p-3})^{4p-4}\). These should come from the Vandermonde part from the terms of degrees between \(2p-2\) and \(4p-4\). Since we know that the corresponding terms of the part coming from \((Y_1 + \cdots + Y_q)^{q-1}\) all need to have degree divisible by \(p\), the only possibility is that we have \(\{\pi(2p-1), \pi(3p-1)\} = \{2p-1, 3p-1\}\). The only possibility is that we have \(\{\pi(2p), \pi(3p)\} = \{2p, 3p\}, \{\pi(3p-3), \pi(4p-3)\} = \{3p-3, 4p-3\}\).

After this there are terms with unique degrees, hence the Vandermonde part has to have this part: \(Y_{4p-2}^{4p-2}Y_{4p-1}^{4p-2} \cdots Y_{p^2-1}^{p^2-1}\).
Hence we already know that the part coming from \((Y_1 + \cdots + Y_q)^{q-1}\) starts with \(p - 1\) terms of degree 1, then \(p - 1\) terms of degree \(p\). This means that the rest of the \(Y_i\)'s have to have degree divisible by \(p^2\), since otherwise we would get a coefficient starting with 

\[
(q - 1)(q - 2) \cdots (q - p + 1) \frac{q - p}{p} \frac{q - 2p}{p} \cdots \frac{q - (p - 1)p}{p} \frac{q - p^2}{k},
\]

where \(k\) is not divisible by \(p^2\), but this is zero.

One can continue by induction on \(i\) to show that the part coming from the Vandermonde determinant has to have the following form:

\[
\prod_{i=1}^{q} Y_{\pi(i)}^{i-1},
\]

where (as we promised above) \(\pi\) is a permutation of the indices such that \(\pi(i) = i\), except for a couple of values: \(\{\pi(1), \pi(2)\} = \{1, 2\}, \{\pi(3), \pi(4)\} = \{3, 4\}, \ldots, \{\pi(2p - 3), \pi(2p - 2)\} = \{2p - 3, 2p - 2\};

\(\{\pi(2p - 1), \pi(3p - 1)\} = \{2p - 1, 3p - 1\}; \{\pi(2p), \pi(3p)\} = \{2p, 3p\}, \ldots, \{\pi(3p - 3), \pi(4p - 3)\} = \{3p - 3, 4p - 3\};

\(\{\pi(p^2 + 1), \pi(2p^2 + 1)\} = \{p^2 + 1, 2p^2 + 1\}, \{\pi(p^2 + 2), \pi(2p^2 + 2)\} = \{p^2 + 2, 2p^2 + 2\}, \ldots, \{\pi(p^2 + p - 1), \pi(2p^2 + p - 1)\} = \{p^2 + p - 1, 2p^2 + p - 1\};

\[\vdots\]

\(\{\pi(p^{h-1} + 1), \pi(2p^{h-1} + 1)\} = \{p^{h-1} + 1, 2p^{h-1} + 1\}, \{\pi(p^{h-1} + 2), \pi(2p^{h-1} + 2)\} = \{p^{h-1} + 2, 2p^{h-1} + 2\}, \ldots, \{\pi(p^{h-1} + p - 1), \pi(2p^{h-1} + p - 1)\} = \{p^{h-1} + p - 1, 2p^{h-1} + p - 1\}.

This means that apart from a non-zero constant (including powers of those \(a_i\) for which we did not have a choice for \(\pi(i)\)), the term coming from the Vandermonde part is the product of \(2 \times 2\) determinants of the form

\[
\begin{vmatrix}
    a_i^{q-1-k} Y_i^k & a_i^{q-1-k-p^n} Y_i^{k+p^n} \\
    a_j^{q-1-k} Y_j^k & a_j^{q-1-k-p^n} Y_j^{k+p^n}
\end{vmatrix}.
\]

Dividing such a term with the non-zero \((a_ia_j)^{q-1-k-p^n}\) and using that \(x \to x^p^n\) is an automorphism of the field, we end up in a situation similar to the prime case:

\[
(a_1 - a_2)(a_3 - a_4) \cdots (a_{2p-3} - a_{2p-2}),
\]

\[
(a_{2p-1} - a_{3p-1})(a_{2p} - a_{3p}) \cdots (a_{3p-3} - a_{4p-3}),
\]

\[
(a_{p^2+1} - a_{2p^2+1})(a_{p^2+2} - a_{2p^2+2}) \cdots (a_{p^2+p-1} - a_{2p^2+p-1}),
\]

\[\vdots\]

\[
(a_{p^{h-1}+1} - a_{2p^{h-1}+1})(a_{p^{h-1}+2} - a_{2p^{h-1}+2}) \cdots (a_{p^{h-1}+p-1} - a_{2p^{h-1}+p-1}) = 0.
\]

Similarly to the prime case, this is true after any permutation of the indices. The number of brackets here is \(h(p - 1)\), so by Lemma 4.4 (iii), we only need \(q - p(h - 1) \geq \frac{q+1}{2}\), this is true for \(q > 9\) odd.
Let $N$ denote the maximal multiplicity in the multiset $\{a_1, \ldots, a_q\}$. By the previous two claims $N$ is large. After translation, suppose the value in question is zero. We need to show that if there is no ordering $b_i$ of the field elements achieving $\sum_i a_i b_i = 0$, then $n = q - 2$. The plan is to use the same machinery for the remaining non-zero $a_i$s.

**Lemma 4.8.** Suppose $a_1, \ldots, a_k$ are non-zero elements of $GF(q)$ with $k < 2q/3$ if $q = p$ prime and $k \leq \frac{q-3}{2}$ if $q = p^h$, $h \geq 2$, admitting at least 3 different values and with the property that no value occurs more than $q - k$ times. Either there are different elements $b_1, \ldots, b_k$ such that $\sum a_i b_i = 0$ or $k = 3$.

**Proof.** Consider the polynomial $G$ from Theorem 4.5. By 4.5, terms of maximal degree of $G$ have at least one $Y_i$ with degree at least $q$.

Just like previously, we look for appropriate terms in $G$ to gain information about the $a_i$s.

If $4 \leq k \leq \frac{q+3}{2}$ holds, then consider the following term (of maximal degree):

$$Y_1^{(q-5)/2+k}Y_2^{(q-5)/2+k}Y_3^{k-3}Y_4^{k-3}Y_5^{k-5}Y_6^{k-6} \cdots Y_k^0.$$  

It is easy to see that there are only four terms coming from $(Y_1 + \cdots + Y_q)^{q-1}$ that (multiplied by the appropriate term coming from the Vandermonde part) can contribute to this term. These four terms are $Y_i Y_j^{q-1} Y_k^{q-3}$, where $i = 3$ or 4 and $\{j, k\} = \{1, 2\}$. Each of them comes with coefficient $(q-1)(q-2)/(q-1)/2 \neq 0$. Hence we have $(a_1 - a_2)(a_3 - a_4) = 0$.

Just like previously, this is true for any permutation of the indices. By Lemma 4.4, this implies that there is a value among the $a_i$s with multiplicity at least $k - 1$ contradicting the assumption that the $a_i$s admit at least 3 values.

Now consider the $k > \frac{q+3}{2}$ case, and note that this case can occur only if $q = p$ prime. We have to distinguish between two cases according to whether $p \equiv 1$ or 2 (mod 3).

If $3|p - 1$, then consider the following term (of maximal degree):

$$Y_1^{k+(p-7)/3}Y_2^{k+(p-7)/3}Y_3^{k+(p-7)/3}Y_4^{k-4}Y_5^{k-5} \cdots Y_k^0.$$  

It is easy to see that the coefficient is a non-zero term times

$$(a_1 - a_2)(a_2 - a_3)(a_3 - a_1),$$  

implying (by Lemma 4.4) that there is a value among the $a_i$s with multiplicity at least $k - 2$. This contradicts the assumption that no value has multiplicity more than $q - k$.

If $3|p + 1$, then one should consider the following term (of maximal degree):

$$Y_1^{k+(p-8)/3}Y_2^{k+(p-8)/3}Y_3^{k+(p-8)/3}Y_4^{k-4}Y_5^{k-4}Y_6^{k-6}Y_7^{k-7} \cdots Y_{k-1}^{1}Y_k^0.$$  

Here the coefficient is essentially

$$(a_1 - a_2)(a_2 - a_3)(a_3 - a_1)(a_4 - a_5).$$  

It is not difficult to see that similarly to the previous case, this leads to contradiction.
Proof. (of Theorem 1.2) By Proposition 4.1, we can suppose \( k = q \) and by Lemma 4.3 that there are at least 4 different values among the \( a_i \)'s. Suppose there is no ordering \( b_1, \ldots, b_q \) of the elements of \( GF(q) \) giving \( \sum_i a_i b_i = 0 \). We have to find a contradiction. After transformation (by Lemma 4.2 and the sentence after its proof) suppose 0 is not among the \( a_i \)'s and apply Lemma 4.6 or 4.10 to find a lot of identical among the \( a_i \)'s. Apply a transformation to make this value zero and apply Lemma 4.8 for the rest of the \( a_i \)'s. We cannot have different \( b_i \)'s for these indices such that \( \sum a_i b_i = 0 \) (here the sum is only for those \( i \)-s, for which \( a_i \neq 0 \)), because otherwise the \( b_i \)'s could be easily extended to an ordering of the field such that \( \sum_i a_i b_i = 0 \). Hence we have \( k = 3 \), that is, the multiset \( \{a_1, \ldots, a_q\} \) contains \( q - 3 \) zeros and 3 distinct non-zero elements, \( a, b \) and \( c \) say.

Suppose \( a + b \neq 0 \). Then \( ba + (-a)b + 0c = 0 \), a contradiction.

\[ \square \]

4.4. Proof for \( q \) even.

The proof is similar for \( q \) even. We can use Lemma 4.2 and 4.1 (the proof presented works for \( q \) even). Lemma 4.3 should be replaced by the following.

**Lemma 4.9.** If our multiset has only 1 or 2 different values and \( n = q \) is even, then Theorem 1.2 is true.

**Proof.** If our set has only one value (of multiplicity \( q \)) then any ordering of \( GF(q) \) is good, so suppose we have two values.

After transformation we can achieve that 0 is the value with multiplicity \( \geq q/2 \) and 1 is the other value with multiplicity \( \leq q/2 \). Hence all we need is that for any \( m \leq q/2 \), there are distinct field elements \( b_1, \ldots, b_m \) such that \( b_1 + \cdots + b_m = 0 \). Denote by \( G \) an additive subgroup of \( GF(q) \) of index 2. Let \( b_1, \ldots, b_{m-1} \) be arbitrary distinct elements of \( G \). If \( b_1 + \cdots + b_{m-1} \) is distinct from all the \( b_i \)'s, then let \( b_m = b_1 + \cdots + b_{m-1} \) and we have the \( m \) elements we were looking for.

If \( b_1 + \cdots + b_{m-1} \) equals one of the \( b_i \)'s, \( b_{m-1} \) say, then we have \( b_1 + \cdots + b_{m-2} = 0 \). Let \( a \in GF(q) \setminus G \). Replace \( b_{m-2} \) with \( b_{m-2} + a \), keep \( b_{m-1} \), and let \( b_m = b_{m-1} + a \). It is easy to see that the \( b_i \)'s are distinct and their sum is zero.

\[ \square \]

Lemma 4.4 and Theorem 4.5 are true for \( q \) even (the proofs presented did not assume \( q \) is odd). Lemma 4.10 should be replaced by the following.

**Lemma 4.10.** Suppose \( q = 2^h > 8 \), and that there is no ordering \( b_1, \ldots, b_q \) of the elements of \( GF(q) \) such that \( \sum a_i b_i = 0 \). Then at least \( q/2 + 1 \) of the \( a_i \)'s are the same.

**Proof.** After transformation suppose 0 is not among the \( a_i \)'s. Consider the polynomial \( G \) from Theorem 4.5 with \( k = q \). By 4.5, terms of maximal degree of \( G \) have at least one \( Y_i \) with degree at least \( q \).

Consider the following term:
\[
Y_1 \prod_{i=1}^{h-1} Y_{i+i+2}^{2^{h-1}} \prod_{i=1}^{q} Y_i^{r-1}
\]

Similarly to Lemma 4.10, one can use Lucas’ theorem to find the coefficient of this term. One can prove that to have the above term with non-zero coefficient, then from the \((Y_1 + \cdots + Y_k)^{q-1} - 1\) part we need \(h\) variables on powers 1, 2, 4, \ldots, \(2^{h-1}\). Using similar observations as before, we can conclude that this implies that the coefficient of our term (apart from the usual non-zero constant) is

\[
(a_1 - a_2) \prod_{i=1}^{h-1} (a_{i+2} - a_{i+2+2^{h-1}}).
\]

Thus this number must equal zero for any permutation of the indices which implies that there is a value in our multiset with multiplicity \(\ge q - h + 1\) because of Lemma 4.4 (iii).

\[\square\]

Instead of Lemma 4.8, one can immediately prove the following.

**Lemma 4.11.** Suppose \(a_1, \ldots, a_k\) are non-zero elements of \(GF(q)\), \(q\) even with \(1 < k < q/2\). Either there are different elements \(b_1, \ldots, b_k\) such that \(\sum a_i b_i = 0\) or all the \(a_i\)s are the same.

**Proof.** Consider the polynomial \(G\) from Theorem 4.5. By 4.5, terms of maximal degree of \(G\) have at least one \(Y_i\) with degree at least \(q\).

Consider the following term:

\[
(Y_k Y_{k-1})^{q/2 + k-2} \cdot Y_{k-2}^{k-3} \cdots Y_2^1 Y_1^0.
\]

It is easy to see that there are only two possibilities to get this term and the coefficient we have (apart from a non-zero constant) is \(a_k - a_{k-1}\). This implies \(a_{k-1} = a_k\) and, since we can permute the indices at the beginning, that all the \(a_i\)s are the same.

\[\square\]

After these lemmas, the proof is easy.

5. **Final remarks**

We would like to remark that for the prime case, that is Theorem 1.1, Péter Csikvári found a relatively short elementary proof [4]. It very much seems however that for general prime powers there is no proof without algebraic techniques.

The result presented in this paper raises natural problems, that seem to be very hard. Instead of the problem considered in Theorem 1.2, one can ask for distinct elements \(b_1, \ldots, b_k\) such that \(\sum_i b_i a_i = 0\) for \(l = 1, \ldots, L\), where \(L\) is a prescribed integer (we get back our result if we let \(L = 1\)). This corresponds to looking for polynomials of prescribed range of degree at most \(q - 2 - L\), a problem already mentioned in Section 2. Let us formulate a conjecture about this.
Conjecture 5.1. Suppose $M = \{a_1, \ldots, a_q\}$ is a multiset of $GF(q)$ with $a_1 + \cdots + a_q = 0$, where $q = p^h$, $p$ prime. Let $k < \sqrt{p}$. If there is no polynomial with range $M$ of degree less than $q - k$, then $M$ contains an element of multiplicity at least $q - k$.

To explain why one needs an upper bound on $k$ in the above conjecture, let us suppose that $q = p$ is prime and define the multiset as 1 with multiplicity $m$, $-m$ with multiplicity 1 and 0 with multiplicity $p - m - 1$. By a result of Biró [3], all polynomials of this range have degree at least roughly $3p/4$, unless $m = \frac{p-1}{2}$ or $\frac{p-1}{3}$ or $2\frac{p-1}{3}$. This shows that for $q = p$ prime, we need $k < p/4$.

The problem considered in Theorem 1.1 could also be generalized to finite (abelian) groups (written multiplicatively) by taking any elements $a_1, \ldots, a_n$ of the group and looking for different degrees $b_1, \ldots, b_n$ from $[1, |G|]$ such that $a_1^{b_1} \cdots a_n^{b_n} = 1$. (Here, to avoid trivial cases, for every $i$ one should not allow those $b_i$s for which $a_i^{b_i} = 1$ holds.)

References