Institute of Mathematics

Ph.D. thesis

Applications of the Combinatorial Nullstellensatz

Zoltán Lóránt Nagy

Doctoral School: Mathematics

Director: Miklós Laczkovich, D.Sc.

Professor, Member of the Hungarian Academy of Sciences

Doctoral Program: Pure Mathematics

Director: András Szűcs, D.Sc.

Professor, Corresp. Member of the Hungarian Academy of Sciences

Supervisors:

András Gács, Ph.D.

Gyula Károlyi, D.Sc.

Tamás Szőnyi, D.Sc.

Acknowledgments

I am truly grateful to my supervisors, András Gács, Gyula Károlyi and Tamás Szőnyi for all their help and guidance. Their profound knowledge of combinatorics combined with generous and supporting attitude helped me in many ways: in motivation, careful writing, establishing a theory and most of all, learning how to study mathematical problems rather than simply solving interesting exercises and enjoying this kind of research work.

I wish to thank all my co-authors for the inspiring work together. It was a really valuable experience for me to share ideas and study problems with Péter Csikvári, Tamás Héger, Balázs Patkós, Dömötör Pálvölgyi, Fedor Petrov, Ágnes Tóth and Máté Vizer.

I am also thankful for the pleasant atmosphere provided under my PhD years especially for Péter Csikvári, Tamás Héger, György Kiss, Erika Renáta Kovács, Marcella Takáts, Ágnes Tóth and Péter Sziklai. I received a different kind of support too, from OTKA (number 81310).

I am grateful to Kovács Csongorné and Sándor Dobos, my high-school maths teachers, for all their efforts and patience. I was fortunate to participate in the splendid mathematical camps of Lajos Pósa, which were substantial experience in teamwork and in learning to ask good questions.

The encouragement of László Lovász, Gyula Katona, Miklós Simonovits, András Gyárfás and János Barát meant me a lot.

I am indebted to Dávid Kunszenti-Kovács and Tamás Héger for giving many valuable suggestions and thus improving the presentation of the thesis.

I would like to thank my parents, grandparents, my siblings, all my friends and Anna for their constant love and support.

Contents

Chapter 1

List of definitions and notations

$\mathbb{N}$: the set of non-negative integers.

$\mathbb{Z}^+$: the set of positive integers.

$\mathbb{Z}_m$: the cyclic group of order m.

$\mathbb{F}_p$, GF(p) : the finite field of order p, where p is a prime.

$\mathbb{F}_q$, GF(q) the finite field of order q, where q is a prime power.

char($\mathbb{F}$): the characteristics of the field $\mathbb{F}$

G: an abelian group.

(a, b): the greatest common divisor of the integers a and b.

$[a, b]$: The set of integers between a and b inclusive, where a and b are both integers and $a \leq b$. (Sec 5.)

I: an interval of type $[a, b]$. (Sec 5.)

$\overline{A}$: the complement of the set A with respect to the groundset.

${}_qA := {}_q\{a_1, a_2, \ldots a_n\} := \{q^{a_1}, q^{a_2}, \ldots, q^{a_n}\}$, for a set $A = \{a_1, a_2, \ldots a_n\}$.

$|A|$: the cardinality of the (multi)set A.

$m(A)$: the greatest multiplicity in the multiset A.

$m(a), a \in A$: the multiplicity of the element a in the multiset A.

k-set: a set of k elements

$x + A$: the translation of the multiset A of a field $\mathbb{K}$ with an element $x \in \mathbb{K}$, that is, $x + A = \{x + a_i : i \in [1, n]\}$ if $A = \{a_1, \ldots, a_n\}$.

xA: the dilation of the multiset A of a field $\mathbb{K}$ with an element $x \in \mathbb{K}$, that is, $xA = \{x \cdot a_i : i \in [1, n]\}$ if $A = \{a_1, \ldots, a_n\}$.

$A + B$: the sumset of the (multi)sets A and B, $A + B := \{a + b : a \in A, b \in B\}$.

$\times A_i$ $(i \in [1, n])$: the set of n-tuples $(a_1, \ldots, a_n) : a_i \in A_i$.

Sym_n: the symmetric group on $[1, n]$, i.e. the group whose elements are all the permutations of the n symbols, and whose group operation is the composition of such permutations.

$\mathbf{x}$: the vector $\mathbf{x} = (x_1, \ldots, x_n)$.

$\mathbf{1}$: the vector $\mathbf{1} = (1, 1, \ldots, 1)$ (of suitable length).

$\mathbf{B}$: the matrix $\mathbf{B} = ((\beta_{ij}))$.

$P(\underline{\mathbf{x}}, \mathbf{B})$: the Laurent polynomial $P(\underline{\mathbf{x}}, \mathbf{B}) := \prod_{0<i\neq j\leq n} (1 - \frac{x_i}{x_j})^{\beta_{ij}}$.

$P(x_0, \underline{\mathbf{x}}, \mathbf{B})$: the Laurent polynomial $P(x_0, \underline{\mathbf{x}}, \mathbf{B}) = \prod_{0\leq i\neq j\leq n} (1 - \frac{x_i}{x_j})^{\beta_{ij}}$.

CT $P(\underline{\mathbf{x}})$ the constant term of the Laurent polynomial $P(\underline{\mathbf{x}})$.

$(t)_k$ denotes the q-Pochhammer symbol, a shorter form of $(t; q)_k$; $(t)_k = (1 - t)(1 - tq) \ldots (1 - tq^{k-1})$, and $(t)_0$ is defined to be 1.

$\chi(x \in \text{Property}) = \begin{cases} 1 & \text{if Property holds for } x \\ 0 & \text{else} \end{cases}$ the characteristic function.

cyclic translate of a sequence $M = \{m_1, \ldots, m_n\}$ is $\{m_{i+1}, m_{i+2}, \ldots, m_i\}$ for some $i \in [1, n]$, where the index is taken $\pmod n$.

Laurent polynomial with coefficients in a field $\mathbb{F}$ is an expression of the form $\sum_k c_k x^k$, $p_k \in \mathbb{F}$, where x is a formal variable, the summation index k is an not necessarily positive integer and only finitely many coefficients c_k are non-zero.

Range of a polynomial P over a finite field $\mathbb{F}_q$ is the multiset $\{P(x), x \in \mathbb{F}_q\}$.

Chapter 2

Introduction

Polynomial techniques became fundamental and powerful tools to reveal structural properties in many fields of combinatorics, including additive combinatorics [6, 65], combinatorial geometry [20], finite geometry [19, 56, 82, 91], graph theory [5, 53] and extremal set theory [3, 36].

Our main work focuses on two different approaches to the so-called Combinatorial Nullstellensatz of Noga Alon. The most common applications of this theorem rely on some non-vanishing argument. In Chapter 3, we provide a solution to a problem concerning range of polynomials over finite fields, with several applications in finite geometry and additive combinatorics. One of the major tools here is the general form of the Combinatorial Nullstellensatz, which is a structural statement about polynomials that fulfill some vanishing conditions on a product set. In contrast with applications of the non-vanishing lemma 2.1.2 which abound, this approach is rare to find in the literature. Chapter 4 is devoted the problem's variation over cyclic groups, which is solved completely. From another point of view, a weaker assertion of the Nullstellensatz can be interpreted as a variation of a theorem concerning interpolations. While a particular non-zero (leading) coefficient implies the existence of a value from a large enough product set, where the polynomial not vanishes, the idea can viewed the other way around. In the articles of Lasoń [73] and Karasev–Petrov [64], the coefficient in view is expressed explicitly in terms of the polynomial function and the set elements where we would like to evaluate the polynomial. This effective version has turned out to be an efficient tool to treat several, partly long-

standing conjectures concerning q-analogue identities. In Chapter 5, we discuss the method and confirm the statement of the so called Forrester-conjecture and the q-analogue version of the Aomoto-identity, as a consequence of the q-analogue common generalization of these two identities.

Chapter 3 and 4 is based on a joint work with András Gács, Tamás Héger and Dömötör Pálvölgyi [39], and on [80], respectively, while Chapter 5 summarizes the results of joint work with Gyula Károlyi [67] and with Gyula Károlyi, Fedor Petrov and Vladislav Volkov [68].

2.1 On the background and context of the Combinatorial Nullstellensatz of Alon

After earlier results (see, e.g. [6]), Noga Alon presented an influential survey [1] on the possible applications of the so called Combinatorial Nullstellensatz. In a general form, it can be formulated similarly to the Nullstellensatz of Hilbert (see, e.g. [54]) as follows.

THEOREM 2.1.1. *[Combinatorial Nullstellensatz, general form] Let $\mathbb{F}$ be an arbitrary field and let $P = P(x_1, \ldots, x_k)$ be a polynomial of k variables over $\mathbb{F}$. Let $A_1, A_2, \ldots, A_k$ be nonempty subsets of $\mathbb{F}$, and define*

$$g_i(x_i) = \prod_{s \in A_i} (x_i - s).$$

If $P(s_1, s_2, \ldots s_k) = 0$ for all k-tuples $(s_1, s_2, \ldots s_k) \in \times A_i$, then the polynomial P is in the ideal generated by the univariate polynomials g_i. More precisely,

$$P = \sum_{i=1}^{k} h_i g_i,$$

where $h_i = h_i(x_1, x_2, \ldots, x_k)$ are multivariate polynomials over $\mathbb{F}$ satisfying

$$\deg(h_i) \leq \deg(P) - \deg(g_i).$$

The proof of this theorem can be found in [1].

The most standard variant, an easy consequence of Theorem 2.1.1 asserts that the zero locus of a polynomial $P(x_1, \ldots x_k)$ cannot contain a large Cartesian product $A_1 \times \ldots \times A_k$ if a certain monomial coefficient of P is non-zero. Many authors refer to this version as 'the Combinatorial Nullstellensatz' as well, even though it does not imply the full content of Theorem 2.1.1.

THEOREM 2.1.2 (Combinatorial Nullstellensatz, non-vanishing form). *Let $\mathbb{F}$ be an arbitrary field and let $P = P(x_1, \ldots, x_k)$ be a polynomial of k variables over $\mathbb{F}$. Suppose that there exists a monomial $\prod_{i=1}^{k} x_i^{d_i}$, such that the sum $\sum_{i=1}^{k} d_i$ equals the total degree of P, and the coefficient of $\prod_{i=1}^{k} x_i^{d_i}$ is nonzero. Then for any set of subsets $A_1, \ldots A_k \in \mathbb{F}$ such that $\mid A_i \mid > d_i$, there exists a k-tuple $(s_1, s_2, \ldots s_k) \in \times A_i$ for which $P(s_1, s_2, \ldots s_k) \neq 0$.*

For the sake of completeness we include a short proof.

Proof. Suppose the result is false. We may assume that $\mid A_i \mid = d_i + 1$. Define the polynomials $g_i(x_i) := \prod_{s \in A_i}(x_i - s)$. Theorem 2.1.1 implies that $P = \sum_{i=1}^{k} h_i g_i$, where $\deg(h_i) \leq \sum_{i=1}^{k} d_i - \deg(g_i)$ holds for all indices i. Consider the coefficient of the monomial $\prod_{i=1}^{k} x_i^{d_i}$, whose degree equals the total degree of P. On the one hand, it is nonzero. On the other hand, if the degree of a summand $h_i g_i = h_i \prod_{s \in A_i}(x_i - s)$ is equal to the degree of P, it should be divisible by $x_i^{d_i+1}$, which leads to a contradiction. □

REMARK 2.1.3. *[68, 73] The non-vanishing lemma can be stated in a slightly stronger form, as follows. We may also consider any monomial $\prod_{i=1}^{k} x_i^{d_i}$ of the polynomial $P = P(x_1, \ldots, x_k)$ with nonzero coefficient, if there is no monomial $\prod_{i=1}^{k} x_i^{\delta_i}$ of $P = P(x_1, \ldots, x_k)$ such that $\delta_i \geq d_i$ for all i, aside from $\prod x_i^{d_i}$. That is, instead of taking a monomial of maximum degree, we may consider any maximal monomial with respect to the natural partial order associated to the exponent sequence of the ordered variables $x_1, x_2, \ldots, x_k$.*

In ordinary cases, this variant is used to show lower bounds on the size of some combinatorial objects, or at least an existence of a combinatorial object. Usually the application of the method does not provide a suitable structure, only shows the existence. To describe the phenomenon, we point out the key steps in order to

apply the theorem, and prove the Erdős-Ginzburg-Ziv theorem (prime case) using this technique, which will be a reference point later on. The Erdős-Ginzburg-Ziv theorem can be interpreted as a starting point of zero-sum theory, and many more general research. For more details, we refer to [17, 23, 40].

THEOREM 2.1.4 (Erdős-Ginzburg-Ziv). *Let $(a_1, a_2, \ldots, a_{2p-1})$ be a sequence of $2p-1$ elements of $\mathbb{Z}_p$, where p is a prime. Then there exists a subsequence of length p, in which the sum of the elements equals zero.*

Proof. **Step 1.** *To the contrary, assume that some set, associated to the problem, is small.* In this case, the set in view is the set S of element of $\mathbb{F}_p$ admitted by the sum of a subsequence of p elements. That is, S is the set of possible sum values, and we suppose that 0 is not admitted.

Step 2. *Associate variables to the problem, and find a polynomial which is vanishing on the set described in Step 1.* Let variable y_i take value 1 if a_i appears among the summands of the sum, and take value 0 if a_i does not appear. Hence, the polynomials

$$f_1(y_1, \ldots, y_{2p-1}) := \sum_{i=1}^{2p-1} y_i \text{ and } f_2(y_1, \ldots, y_{2p-1}) := \sum_{i=1}^{2p-1} a_i y_i$$

takes value zero, if and only if the number of summands is divisible by p, and if the sum is divisible by p, respectively. Since $x^{p-1} = 1$ for each $x \in \mathbb{F}_p \setminus 0$, the polynomial

$$\left(1 - f_1^{p-1}(y_1, \ldots, y_{2p-1})\right)\left(1 - f_2^{p-1}(y_1, \ldots, y_{2p-1})\right) - \prod_{i=1}^{2p-1}(1 - y_i)$$

takes value zero, if and only if the number of summands is p and the sum is zero (mod p).

Step 3. *Determine the total degree, and a suitable monomial whose degree equals the total degree.* Note that the degree of our polynomial is $2p - 1$. Clearly, the monomial $\prod_{i=1}^{2p-1} y_i$ has coefficient different from zero.

Step 4. *Set a suitable set system A_i and apply Theorem 2.1.2 to the polynomial.* The condition on any set A_i is to contain more than 1 element, hence the choice $A_i = \{0, 1\}$ suits the requirements. Then Theorem 2.1.2 implies that the polynomial cannot vanish on the Cartesian product $\{0, 1\}^{2p-1}$. This is a contradiction, which means that there must be a subsequence of p elements and of sum zero. □

To emphasize the efficiency of this method, we note that it recently helped to solve the well known Erdős-Heilbronn conjecture (see [27]), one of Snevily's conjectures (see [2]) and the finite field Kakeya conjecture (see [28]).

Another easy, yet a bit more delicate consequence of Theorem 2.1.1 is the following

COROLLARY 2.1.5. *If a polynomial $P = P(Y_1, \dots, Y_k)$ over a finite field $\mathbb{F}_q$ vanishes for all substitutions, then it can be written in the following form:*

$$P(Y_1, \dots, Y_k) = h_1(Y_1^q - Y_1) + \cdots + h_k(Y_k^q - Y_k),$$

where the h_i are polynomials in $Y_1, \dots, Y_k$ of total degree at most $\deg(P) - q$.

Proof. Applying Theorem 2.1.1 with $A_i := \mathbb{F}_q$ and $g_i(Y_i) := \prod_{s \in \mathbb{F}_q}(Y - s) = Y^n - Y$ implies the statement. □

The general form of the Nullstellensatz is rather rarely used. It was first applied in a paper of Károlyi [65]. In Section 3., we contribute to the applications of Theorem 2.1.5.

As it was pointed out in several papers and surveys [1, 72, 92], Theorem 2.1.1 may be considered as some generalization of the Lagrange interpolation. Indeed, the following facts are well known.

PROPOSITION 2.1.6. *If a polynomial $P \in \mathbb{F}[x]$ is a non-zero polynomial with $deg(P) \leq d$ ($d \geq 1$ is an integer), then P vanishes at at most d elements of $\mathbb{F}$ (has at most d roots in $\mathbb{F}$). Conversely, for any given set A of cardinality at most d, there exists a polynomial of degree at most d that vanishes on the whole set A.*

That is, to obtain an upper bound on the size of a one-dimensional set A, it would suffice to exhibit a non-zero low-degree polynomial that vanishes on A. On the other hand, to bound the size of a set A from below, one would have to show that the only low-degree polynomial that vanishes on A is the zero polynomial.

PROPOSITION 2.1.7. *[Lagrange interpolation] Suppose P is a polynomial of one variable over $\mathbb{F}$, and $\deg(P) \leq d$. If one knows its values $P(s)$ at $d + 1$ distinct points*

$s_1, s_2, \ldots, s_{d+1}$, *then* $P(x)$ *is determined by the formula*

$$P(x) = \sum_{i=1}^{d+1} P(s_i) \prod_{\substack{j=1 \\ j \neq i}}^{d+1} \frac{x - s_j}{s_i - s_j}.$$

Clearly, the former proposition's first assertion is a consequence of that of the latter. The non-vanishing polynomial lemma (Theorem 2.1.2) may be considered as a generalization of Proposition 2.1.6 for multivariate polynomials. Our next aim is to introduce another lemma for multivariate polynomials, which can be considered as an analogue of the Lagrange interpolation technique, and was first observed independently by Lasoń [73]; and Karasev and Petrov [64]. This form easily implies the non-vanishing form of the Nullstellensatz (Theorem 2.1.2) and will play a fundamental part in the proofs of constant term identities in Section 5.

LEMMA 2.1.8 (Quantitative Nullstellensatz). *Let* $\mathbb{F}$ *be a field, and let* $P \in \mathbb{F}[x_1, x_2, \ldots, x_m]$, *be a multivariate polynomial for which* $\deg(P) \leq d_1 + d_2 + \ldots + d_m$. *Take an arbitrary set system* $A_1, A_2, \ldots, A_m$ *such that* $A_i \subseteq \mathbb{F}$ *and* $|A_i| = d_i + 1$. *Then the coefficient of* $\prod x_i^{d_i}$ *is*

$$\sum_{z_1 \in A_1} \sum_{z_2 \in A_2} \sum_{z_m \in A_m} \frac{P(z_1, z_2, \ldots z_m)}{\phi_1'(z_1)\phi_2'(z_2)\cdots\phi_m'(z_m)},$$

where $\phi_i(x) = \prod_{a \in A_i}(x - a)$.

Proof. Assume that P is a monomial. This implies the lemma for arbitrary P, as the coefficient, and the formula as well is linear. Indeed,

$$\sum_{\mathbf{z} \in \times A_i} \frac{(P_1 + P_2)(z_1, z_2, \ldots z_m)}{\phi_1'(z_1)\cdots\phi_m'(z_m)} = \sum_{\mathbf{z} \in \times A_i} \frac{P_1(z_1, z_2, \ldots z_m)}{\phi_1'(z_1)\cdots\phi_m'(z_m)} + \sum_{\mathbf{z} \in \times A_i} \frac{P_2(z_1, z_2, \ldots z_m)}{\phi_1'(z_1)\cdots\phi_m'(z_m)}.$$

Observe that if $n = 1$, and $|A| := d + 1 = \deg(P) + 1$, then

$$P(x) = \sum_{s_i \in A} P(s_i) \prod_{j=1, j \neq i}^{d+1} \frac{x - s_j}{s_i - s_j} = \sum_{s_i \in A} \frac{P(s_i)}{\phi'(s_i)} \cdot \frac{\phi(x)}{(x - s_i)}$$

according to the Lagrange interpolation formula (Proposition 2.1.7), thus the coefficient of x^d is clearly

$$\sum_{s_i \in A} \frac{P(s_i)}{\phi'(s_i)}.$$

If we choose P to be an m-variate monomial $\prod x_i^{d_i}$, and set system $A_1, A_2, \ldots, A_m$ such that $A_i \subseteq \mathbb{F}$ and $|A_i| = d_i + 1$, we obtain

$$\sum_{\mathbf{z} \in \times A_i} \frac{P(z_1, z_2, \ldots z_m)}{\phi_1'(z_1)\phi_2'(z_2)\cdots\phi_m'(z_m)} = \sum_{\mathbf{z} \in \times A_i} \frac{z_1^{d_1} z_2^{d_2} \cdots z_m^{d_m}}{\phi_1'(z_1)\phi_2'(z_2)\cdots\phi_m'(z_m)} =$$

$$= \prod_{i=1}^{m} \sum_{z_i \in A_i} \frac{z_i^{d_i}}{\phi_i'(z_i)}.$$

Apply the $n = 1$ case, and we get that this is exactly the coefficient of the product $x_1^{d_1} \cdot x_2^{d_2} \cdot \ldots \cdot x_m^{d_m}$. □

REMARK 2.1.9. *This lemma implies the statement of Theorem 2.1.2.*

Indeed, if a polynomial P of degree $d = d_1 + d_2 + \ldots + d_m$ vanishes on a Cartesian product $\times A_i$, $|A_i| = d_i + 1$, then each summand is zero in the expression of the coefficient of $\prod x_i^{d_i}$, a contradiction.

Lemma 2.1.8 seems somewhat weaker in higher dimension than the (multivariate version of the) Lagrange interpolation (see e.g. in [83]), as it provides only the leading coefficient. However, it assures a straightforward way to determine the leading coefficient of arbitrary n-variate polynomial, with no particular restriction on the interpolation subsets A_i - except their cardinality. Finally, we end this section by another generalization of Theorem 2.1.2 and Lemma 2.1.8. The main idea is the following. So far, we associated subsets A_i of $\mathbb{F}$ to each variable x_i, to express that the zero locus of a polynomial can (or can not) contain the corresponding Cartesian product $\times A_i$. Instead of subsets, we may consider here multisets as well, that is, multiplicities for each common zero. Although the original non-vanishing lemma can not deal with it, recent papers of Kós, Rónyai, and Kós, Mészáros, Rónyai [70, 71] extend the result. Before we state it, we introduce some notions.

For each $s \in A_i$, $m_i(s)$ will denote its multiplicity in A_i. (Hence, the sum of the multiplicities equals the cardinality of the multiset.)

It is well known that for an arbitrary $\mathbf{s} \in \mathbb{F}^n$, we can express any polynomial $P(\mathbf{x}) \in \mathbb{F}[x_1, \ldots, x_n]$ as

$$P(\mathbf{x}) = \sum_{\mathbf{u}\in\mathbb{N}^n} C_{\mathbf{u},\mathbf{s}} \prod_{i=1}^{n} (x_i - s_i)^{u_i},$$

where the coefficients $C_{\mathbf{u},\mathbf{s}}$ are uniquely determined by $P, \mathbf{u}$ and $\mathbf{s}$. Note that if $\sum_{i=1}^{n} u_i > \deg(P)$ holds then $C_{\mathbf{u},\mathbf{s}}$ is zero, while in case of equality, that is, $\sum_{i=1}^{n} u_i = \deg(P)$, then $C_{\mathbf{u},\mathbf{s}}$ denotes the coefficient of $\prod_{i=1}^{n} {x_i}^{u_i}$ in P which is independent of $\mathbf{s}$. Furthermore, observe that $C_{\mathbf{0},\mathbf{s}} = P(\mathbf{s})$ for $\mathbf{u} = \mathbf{0}$.

THEOREM 2.1.10. *[70] Let $\mathbb{F}$ be a field, $P = P(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ be a polynomial of degree $\sum_{i=1}^{n} d_i$, where each d_i is a nonnegative integer. Assume that the coefficient of the monomial $\prod_{i=1}^{n} x_i^{d_i}$ is nonzero in P. Suppose further that $A_1, A_2, \ldots A_n$ are multisets of $\mathbb{F}$ such that for the size $|A_i| > d_i$ $(i = 1, \ldots, n)$. Then there exists a point $\boldsymbol{s} = (s_1, \ldots, s_n) \in \times A_i$ and an exponent vector $\boldsymbol{u} = (u_1, \ldots, u_n) \in \mathbb{N}^n$ with $u_i < m_i(s_i)$ for each i, such that $C_{\boldsymbol{u},\boldsymbol{s}} \neq 0$.*

REMARK 2.1.11. *If each multiplicity is 1, the theorem gives back the non-vanishing theorem 2.1.2. Indeed, that would mean there exists a point $\boldsymbol{s} = (s_1, \ldots, s_n) \in \times A_i$ such that $C_{\boldsymbol{u},\boldsymbol{s}} = P(\boldsymbol{s}) \neq 0$.*

Theorem 2.1.10 can be generalized in the spirit of Lemma 2.1.8.

THEOREM 2.1.12 (Multiplicity version of the Quantitative Nullstellensatz). *[68] Let $P \in \mathbb{F}[x_1, \ldots, x_n]$ be a multivariate polynomial such that no monomial majorizes the term $\prod x_i^{d_i}$ in P. Let $A_1, \ldots, A_n$ be arbitrary multisets in $\mathcal{F}$ with corresponding multiplicity functions $m_1, \ldots, m_n$ such that $|A_i| = d_i + 1$ for every i. Assume that either $\operatorname{char}(\mathbb{F}) = 0$ or $\operatorname{char}(\mathbb{F}) \geq \max m_i(c)$ $(i \leq n, c \in \mathbb{F})$. Then the coefficient of $\prod x_i^{d_i}$ in P can be evaluated as*

$$\sum_{s_1\in A_1} \sum_{u_1<m_1(s_1)} \cdots \sum_{s_n\in A_n} \sum_{u_n<m_n(s_n)} \prod_{i=1}^{n} \kappa(A_i, s_i, u_i) \frac{\partial^{u_1+\cdots+u_n} P}{\partial x_1^{u_1} \ldots \partial x_n^{u_n}}(s_1, \ldots, s_n),$$

where

$$\kappa(A_i, s_i, u_i) = \frac{1}{u_i! \cdot (m_i(s_i) - 1 - u_i)!} \cdot \left(\frac{1}{\prod_{c\in A_i\setminus\{s_i\}} (x - c)^{u_i(c)}} \right)^{(m_i(s_i)-1-u_i)} \Bigg|_{x=s_i}.$$

Consequently, if the coefficient of $\prod_{i=1}^{n} x_i^{d_i}$ *in* P *is not zero, then there exists a system of representatives* $s_i \in A_i$ *and multiplicities* $u_i < u_i(s_i)$ *such that*

$$\frac{\partial^{m_1+\cdots+m_n} F}{\partial x_1^{m_1} \dots \partial x_n^{m_n}}(s_1, \dots, s_n) \neq 0.$$

□

The latter two theorems can be considered as the generalization of the non-vanishing lemma built on Hermite interpolation.

For more details and applications of the Combinatorial Nullstellensatz, we refer to [1, 72, 92]. We also mention further generalizations of the Nullstellensatz, see [14].

2.2 Preliminary theorems

Here we introduce some basic facts and theorems, that will be needed later.

LEMMA 2.2.1 (Lucas). *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*

$$\binom{n}{k} \equiv \binom{n_1}{k_1} \cdots \binom{n_r}{k_r} \pmod{p}.$$

For a proof, see [74]. We will use this often without explicitly referring to it.

LEMMA 2.2.2 (About the power sums of the elements of GF(q)). *For arbitrary finite field* GF(q), $\sum_{x \in \mathrm{GF}(q)} x^k = 0$ *when* $1 \leq k \leq q-2$*, and* $\sum_{x \in \mathrm{GF}(q)} x^{q-1} = -1$.

Polynomials over a finite field may be considered as polynomials with a bounded degree. Indeed, if $P(x) \in \mathbb{F}_q[x]$ has the form $P(x) = c_n x^n + c_{n-1} x^{n-1} + \ldots + c_1 x + c_0$ and $n \geq q$, then $P(x)$ and $P(x) - c_n(x^q - x)x^{n-q}$ are identical as functions, since $x^q - x = 0$ for all $x \in \mathbb{F}_q$. Thus any polynomial over the field GF(q) can be represented by a polynomial of degree at most $q-1$. In fact, any function over GF(q) can be represented by a polynomial of degree at most $q-1$ and this representation is unique. The number of functions over GF(q) is q^q, which is equal to the number of polynomials of degree at most $q-1$. It is clear that these polynomials cannot represent the same function, which confirms the statement.

For any function $f \in \mathbb{F}_q[x]$, the corresponding polynomial is called the *reduced polynomial*, and its degree is called the *reduced degree* of f.

LEMMA 2.2.3. *Suppose that* $f(x) = c_{q-1}x^{q-1} + \cdots + c_0$ *is a polynomial over* $\mathrm{GF}(q)$. *Then* $\sum_{x\in\mathrm{GF}(q)} f(x) = -c_{q-1}$ *and* $\sum_{x\in\mathrm{GF}(q)} xf(x) = -c_{q-2}$.

Proof. Apply Lemma 2.2.2 to $\sum_{x\in\mathrm{GF}(q)} f(x) = \sum_{i\le q-1} \sum_{x\in\mathrm{GF}(q)} c_i x^i$ and to $\sum_{x\in\mathrm{GF}(q)} xf(x) = \sum_{i\le q-1} \sum_{x\in\mathrm{GF}(q)} c_i x^{i+1}$. □

Chapter 3

Range of polynomials over finite fields and related problems

3.1 Introduction and combinatorial number theory point of view

This section 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 [85]. 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, 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 [93].

THEOREM 3.1.1. *Let $\{a_1, a_2, \ldots, a_p\}$ be a multiset in the finite field* $\mathrm{GF}(p)$*, p prime. Then after a suitable permutation of the indices, either $\sum_i ia_i = 0$, or the multiset consists of a ($p-2$ times), $a+b$ and $a-b$ (each once) for some field elements a and b, $b \neq 0$.*

In the paper [93] 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 π of the indices such that the elements $a_1 b_{\pi(1)}$, $a_2 b_{\pi(2)}$, $\ldots$,$a_n b_{\pi(n)}$ are different. Alon proved this for groups of prime degree [2] and later Dasgupta, Károlyi, Serra and Szegedy [26] 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 were true for cyclic groups (it is obviously not), then there would be no exception in Theorem 3.1.1, and the proof would easily follow from this general version.

Theorem 3.1.1 will follow from the following more general result, where p is replaced by an arbitrary prime power q.

THEOREM 3.1.2. *Let $\{a_1, a_2, \ldots, a_q\}$ be a multiset in the finite field* $\mathrm{GF}(q)$*. There are no distinct field elements $b_1, b_2, \ldots, b_q$ such that $\sum_i a_i b_i = 0$ if and only if after a suitable permutation of the indices, $a_1 = a_2 = \cdots = a_{q-2} = a$, $a_{q-1} = a + b$, $a_q = a - b$ for some field elements a and b, $b \neq 0$.*

Note that if we let $q = p$, p prime in Theorem 3.1.2, then we get Theorem 3.1.1 (since q different elements are in fact all the elements in some permutation).

We may formulate it in a more general form which follows easily from the $n = q$ case.

COROLLARY 3.1.3. *Let $\{a_1, a_2, \ldots, a_n\}$ be a multiset in the finite field* $\mathrm{GF}(q)$*, 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 a suitable permutation of the indices, $a_1 = a_2 = \cdots = a_{q-2} = a$, $a_{q-1} = a + b$, $a_q = a - b$ for some field elements a and b, $b \neq 0$.

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

(iiii) $n = q-2$, q *is even, and after a suitable permutation of the indices,* $a_1 = a_2 = \cdots = a_{n-2} = a$ *for a field element* $a \neq 0$.

Proof. If $n < q$, then extend the set of a_is to a set of size q with $a_{n+1} = \cdots = a_q = 0$, then apply the theorem. □

In Subsections 2 and 3 we derive two consequences of Theorem 3.1.2. The proof of the theorem will be given in Section 4. Finally, Section 5 is devoted to remarks and open problems.

Finally, let us recall the version of the Combinatorial Nullstellensatz that will be a key ingredient in this section, namely, the formerly introduced Theorem 2.1.5.

THEOREM 3.1.4. *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* $\deg(G) - q$.

3.2 A result about polynomials of prescribed range

In this section we give another formulation of Theorem 3.1.2. Although it might seem to be a consequence, it is essentially equivalent to the original result.

For a multiset M of size q of field elements we say that M is the *range* of the polynomial f if $M = \{f(x) : x \in \mathrm{GF}(q)\}$ 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 2.2.3, 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 3.2.1. *Let $M = \{a_1, \ldots, a_q\}$ be a multiset in* $\mathrm{GF}(q)$*, 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 some field elements a and b, $b \neq 0$.*

Proof. By Lemma 2.2.3, polynomials with range M have reduced degree $q-1$ if and only if $\sum a_i \neq 0$. Since $\sum a_i = 0$, the second statement of Lemma 2.2.3 shows that a polynomial f with range M has reduced degree at most $q-3$ if and only if $\sum_x xf(x) = 0$.

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 $\mathrm{GF}(q)$: a permutation corresponds to the function $f(b_i) = a_i$. Under this correspondence the condition $\sum_x xf(x) = 0$ translates to $\sum a_i b_i = 0$. Hence our claim follows from Theorem 3.1.2. □

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.

One might conjecture that the only reason for a multiset (with sum equal to zero) not to be the range 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 multiplicity $m \leq q-1$ in the range guarantees that any polynomial of this range has degree at least m, since the corresponding reduced polynomial f is such that $f-a$ has m roots in $\mathrm{GF}(q)$). We will get back to this at the end of the Chapter.

3.3 A consequence about hyperplanes of a vector space over $\mathrm{GF}(q)$

In this section we prove a result about vector spaces over finite fields, which is again essentially equivalent to Theorem 3.1.2

Let q denote a prime power and denote by V the vector space of dimension n over the finite field $\mathrm{GF}(q)$ 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 contained in $\cup_{i\neq j} H_{ij}$. Note that if $n > q$, then by the pigeon-hole principle the whole space is contained in this union, so the problem is non-trivial only for $n \leq q$. Our main result is the following.

THEOREM 3.3.1. *Suppose that $n \leq q$ 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) $n = q$, $H = \{(x_1, \ldots, x_n) : c(x_j - x_k) + \sum_i x_i = 0\}$ *for a field element* $c \neq 0$ *and indices* $j \neq k$;

(ii) $n = q - 1$, $H = \{(x_1, \ldots, x_n) : x_j + \sum_i x_i = 0\}$ *for an index* j.

Proof. Let $H =< (a_1, \ldots, a_n) >^{\perp}$. The condition that H is contained in $\cup_{i\neq j} H_{ij}$ translates to the condition that whenever $a_1x_1 + \cdots + a_nx_n = 0$, necessarily $x_i = x_j$ for an $i \neq j$, or equivalently, there are no distinct elements $x_1, \ldots, x_n$ such that $a_1x_1 + \cdots + a_nx_n = 0$. Hence we are in (i) or (ii) or (iii) of Corollary 3.1.3.

It is easy to see that Corollary 3.1.3 (i) implies (i) of the theorem being proved. If we have (ii) from Corollary 3.1.3, then (ii) holds here, finally, from 3.1.3 (iii) we get that $H = H_{ij}$ for an i and j, a 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 3.3.2. *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 $(1, \ldots, 1)^{\perp}$.*

Proof. Suppose the affine hyperplane $\{(x_1, \ldots, x_n) : a_1x_1 + \cdots + a_nx_n = c\}$ is contained in $\cup_{i\neq j} H_{ij}$. First choose arbitrary distinct field elements $x_1, \ldots, x_n$. Let $d = a_1x_1 + \cdots + a_nx_n$. By the assumption, $d \neq c$. If $d \neq 0$, then $(\frac{c}{d}x_1, \ldots, \frac{c}{d}x_n)$ is in our hyperplane, a contradiction, unless $c = 0$, which is what we wanted to prove.

If $d = 0$, then interchange the values of two coordinates, x_i and x_j say, to obtain $a_1x_1 + \cdots + a_nx_n = (a_i - a_j)(x_j - x_i)$. This is non-zero for well-chosen i and j (unless all the a_is are the same), so we can use the above trick to prove $c = 0$.

Finally, if all the a_is are the same, say $a_1 = \cdots = a_n = 1$, then one can easily find distinct x_is to obtain $a_1x_1 + \cdots + a_nx_n \neq 0$ (and use the above trick), unless $n = q$, which was the exceptional case in the claim. □

3.4 Proof of Theorem 3.1.2

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 in general, though our combinatorial observations in the first section hold also for q even, except Lemma 3.4.2. For the proof of the even case (which is relatively easier) see the last part 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 multiset $\{a_1, \ldots, a_k\}$ for which one cannot find distinct field elements $b_1, \ldots, b_k$ such that $a_1b_1 + \cdots + a_kb_k = 0$. The proof will be another application of the Combinatorial Nullstellensatz, in the spirit of Károlyi's approach [65].

The essential part of the proof of Theorem 3.1.2 will be carried out in Subsection 3, where (after supposing that one cannot find distinct field elements $b_1, \ldots, b_q$ such that $a_1b_1 + \cdots + a_qb_q = 0$), we will use the information gained in Subsection 2 to deduce first that most of the a_is are equal, and later that exactly $q - 2$ of them are equal.

Subsection 4 will be devoted to the q even case.

3.4.1 Easy combinatorial observations

LEMMA 3.4.1. *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 $\sum a_ib_i = 0$, 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. □

Note that if the a_is 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_is.

LEMMA 3.4.2. *Theorem 3.1.2 is true if $n = q$ odd and the a_is admit at most* 3 *different values.*

Proof. If all the a_is 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 $b_1 \neq 0$ be arbitrary, $b_2 = -b_1$, b_3 any non-zero value, which has not been used, $b_4 = -b_3$,... If m is even, then after we determined the first m b_is, the rest of the values are 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 can be applied again. □

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

LEMMA 3.4.3. *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_is 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_is 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 we have at least 4 different values, then it is easy to see that the arrangement is possible. If there are exactly 3 different values, then at least two values occur at least twice because we have at least 5 elements, and it is again easy to find the desired arrangement.

□

3.4.2 The algebraic tool

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

THEOREM 3.4.4. *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:

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

Then

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

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

Proof. First we will prove that the following polynomial vanishes for all substitutions:

$$F(X_1, \ldots, X_k) = \left((a_1X_1 + \cdots + a_kX_k)^{q-1} - 1\right) \prod_{1 \le i < j \le k} (X_i - X_j).$$

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

On the other hand, $(a_1X_1 + \cdots + a_kX_k)^{q-1} - 1 = 0$ if and only if $a_1X_1 + \cdots + a_kX_k \neq 0$. By the assumption, such X_is cannot be all distinct.

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

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

Now replace the variables of F with $Y_i := a_i X_i$ $(i = 1, \ldots, k)$. Using that $\prod_{1 \le i < j \le k}(X_i - X_j)$ 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:

$$\begin{vmatrix} 1 & (Y_1/a_1) & (Y_1/a_1)^2 & . & . & . & (Y_1/a_1)^{k-1} \\ . & . & . & . & . & & \\ . & . & . & . & . & & \\ . & . & . & . & . & & \\ 1 & (Y_k/a_k) & (Y_k/a_k)^2 & . & . & . & (Y_k/a_k)^{k-1} \end{vmatrix}$$

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 2.1.5, G has the claimed form. □

Note that the above theorem shows that in any term of G of maximal degree, at least one of the Y_is 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_is) of well-chosen terms with all degrees at most $q - 1$ to deduce conditions on the a_is.

3.4.3 The essential part of the proof

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

LEMMA 3.4.5. *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_is. Consider the polynomial G from Theorem 3.4.4 with $k = p$. The theorem states that 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 $3|p-1$ and let us determine the coefficient of the following term:

$$(Y_1Y_2Y_3)^{p-1}(Y_4Y_5Y_6)^{p-4}\cdots(Y_{p-3}Y_{p-2}Y_{p-1})^3.$$

First of all note that the degree of this term equals the degree of G, which is $\frac{(p-1)(p+2)}{2}$. According to the remark after the proof of Theorem 3.4.4, the coefficient (depending on the a_is) has to be zero. However, there is another way to express this coefficient.

PROPOSITION 3.4.6. *Apart from a nonzero scalar (depending on the* a_i*s), the coefficient of the term* $(Y_1Y_2Y_3)^{p-1}(Y_4Y_5Y_6)^{p-4}\cdots(Y_{p-3}Y_{p-2}Y_{p-1})^3$ *is*

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

Proof. To see this note that all terms of D (the determinant defined earlier, in the statement of Theorem 3.4.4) are of the form $Y_{\pi(1)}^{p-1}Y_{\pi(2)}^{p-2}\cdots Y_{\pi(p)}^{0}$, where π is a permutation of the indices $\{1,\ldots,p\}$. In order to obtain the monomial $(Y_1Y_2Y_3)^{p-1}\cdots(Y_{p-3}Y_{p-2}Y_{p-1})^3$, this must be multiplied by a factor of the form $Y_1^{n_1}\cdots Y_p^{n_p}$ (coming from $(Y_1+\cdots+Y_p)^{p-1}-1$) for which $n_p = 0$ and for all $0 \le i \le \frac{p-4}{3}$ we have $\{n_{1+3i}, n_{2+3i}, n_{3+3i}\} = \{0,1,2\}$. Under this condition, one can always find a unique complementary factor from D, notably:

$$\prod_{i=0}^{r-1} Y_{1+3i}^{3(r-i)-n_{1+3i}} Y_{2+3i}^{3(r-i)-n_{2+3i}} Y_{3+3i}^{3(r-i)-n_{3+3i}}$$

where $r = \frac{p-1}{3}$. One can then deduce that the terms from D that contribute are those from the determinant given below.

$$\begin{vmatrix}
 & & & & & & a_1^2Y_1^{p-3} & a_1Y_1^{p-2} & Y_1^{p-1} \\
 & & & & & & a_2^2Y_2^{p-3} & a_2Y_2^{p-2} & Y_2^{p-1} \\
 & & & & & & a_3^2Y_3^{p-3} & a_3Y_3^{p-2} & Y_3^{p-1} \\
 & & & a_4^5Y_4^{p-6} & a_4^4Y_4^{p-5} & a_4^3Y_4^{p-4} & & & \\
 & & & a_5^5Y_5^{p-6} & a_5^4Y_5^{p-5} & a_5^3Y_5^{p-4} & & & \\
 & & & a_6^5Y_6^{p-6} & a_6^4Y_6^{p-5} & a_6^3Y_6^{p-4} & & & \\
 & a_7^8Y_7^{p-9} & a_7^7Y_7^{p-8} & a_7^6Y_7^{p-7} & & & & & \\
 & a_8^8Y_8^{p-9} & a_8^7Y_8^{p-8} & a_8^6Y_8^{p-7} & & & & & \\
 & a_9^8Y_9^{p-9} & a_9^7Y_9^{p-8} & a_9^6Y_9^{p-7} & & & & & \\
 \vdots & & & & & & & & \\
a_p^{p-1} & & & & & & & &
\end{vmatrix}$$

It is easy to see that the coefficient of $(Y_1Y_2Y_3)^{p-1}\cdots(Y_{p-3}Y_{p-2}Y_{p-1})^3$ equals, up to a non-zero scalar, the determinant of this matrix after substituting 1 for all Y_is. The determinant of this matrix is the product of the determinants of the blocks of rank 3, thus we finished the proof of the claim. □

Before we write up G, we can permute the a_is, hence we get that for any permutation π of the indices,

$$(a_{\pi(1)}-a_{\pi(2)})(a_{\pi(2)}-a_{\pi(3)})(a_{\pi(3)}-a_{\pi(1)})\cdot(a_{\pi(4)}-a_{\pi(5)})(a_{\pi(5)}-a_{\pi(6)})(a_{\pi(6)}-a_{\pi(4)})\cdots$$

$$\cdots(a_{\pi(p-3)}-a_{\pi(p-2)})(a_{\pi(p-2)}-a_{\pi(p-1)})(a_{\pi(p-1)}-a_{\pi(p-3)})=0. \tag{1}$$

Now suppose the maximal multiplicity in the multiset $\{a_1,\ldots,a_p\}$ is $l\leq\frac{p-1}{3}$. By Lemma 3.4.3 (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,..., 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:

$$(Y_1Y_2Y_3)^{p-1}(Y_4Y_5Y_6)^{p-4}\cdots(Y_{p-4}Y_{p-3}Y_{p-2})^4Y_{p-1}Y_p.$$

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

$$(a_1 - a_2)(a_2 - a_3)(a_3 - a_1) \cdot (a_4 - a_5)(a_5 - a_6)(a_6 - a_4) \cdots$$

$$\cdots (a_{p-4} - a_{p-3})(a_{p-3} - a_{p-2})(a_{p-2} - a_{p-4}) \cdot (a_{p-1} - a_p).$$

The rest is similar to the proof of the previous case. Here we need to use Lemma 3.4.3 (ii) at the end. □

LEMMA 3.4.7. *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 $\sum_i a_i b_i = 0$. Then at least $\frac{q+3}{2}$ of the a_is are the same.*

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.

After transformation suppose 0 is not among the a_is. Consider the polynomial G from Theorem 3.4.4 with $k = q$. By 3.4.4, 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_is this time is the following:

$$(\prod_{i=1}^{q} Y_i^{i-1}) \cdot (Y_1 Y_3 Y_5 \cdots Y_{2p-3})(Y_{2p-1} Y_{2p} \cdots Y_{3p-3})^p (Y_{p^2+1} Y_{p^2+2} \cdots Y_{p^2+p-1})^{p^2} \cdots$$

$$\cdots (Y_{p^{h-1}+1} Y_{p^{h-1}+2} \cdots Y_{p^{h-1}+p-1})^{p^{h-1}}$$

The degree of this term is $1+2+\cdots+(q-1)+(p-1)(1+p+p^2+\cdots+p^{h-1}) = \binom{q}{2}+q-1$, this is the degree of G. A little calculation shows that all Y_is 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 $\prod_{i=1}^{q} Y_i^{i-1}$ 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 and Y_2 (both of degree 1), Y_3 and Y_4 (both of degree 3),..., Y_{2p-3} and Y_{2p-2} (both of degree $2p-3$);
Y_{2p-1} and Y_{3p-1} (both of degree $3p-2$), Y_{2p} and Y_{3p} (both of degree $3p-1$),...,Y_{3p-3}

and Y_{4p-3} (both of degree $4p-4$);
Y_{p^2+1} and Y_{2p^2+1} (both of degree $2p^2$), Y_{p^2+2} and Y_{2p^2+2} (both of degree $2p^2+1$),...,Y_{p^2+p-1} and Y_{2p^2+p-1} (both of degree $2p^2+p-2$);
...;
$Y_{p^{h-1}+1}$ and $Y_{2p^{h-1}+1}$ (both of degree $2p^{h-1}$), $Y_{p^{h-1}+2}$ and $Y_{2p^{h-1}+2}$ (both of degree $2p^{h-1}+1$),...,$Y_{p^{h-1}+p-1}$ and $Y_{2p^{h-1}+p-1}$ (both of degree $2p^{h-1}+p-2$).

Let us look for the term in question. From the Vandermonde part, all terms are of the form $Y_{\pi(1)}^0 \cdots Y_{\pi(q)}^{q-1}$ for a permutation π of the indices. In the term in question, we have only two Y_is of degree less than 2: Y_1 and 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 first part of the term coming from $(Y_1+\cdots+Y_q)^{q-1}$ is $Y_{\pi(1)}Y_{\pi(3)}\cdots Y_{\pi(2p-3)}$. The coefficient of such a term in $(Y_1+\cdots+Y_q)^{q-1}$ is $(q-1)(q-2)\cdots(q-p+1)$ times something depending on the degrees of the rest of the Y_is. If the degree of any of the rest of the Y_is is not divisible by p, then (by Lucas' theorem) the coefficient is zero, since it is divisible by $(q-1)(q-2)\cdots(q-p+1)\binom{q-p}{k}$ 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 $Y_{\pi(1)}Y_{\pi(3)}\cdots Y_{\pi(2p-3)}$ and continues with all the Y_is having degree divisible by p.

So far we have identified all Y_is come 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 $\{\pi(2p-1),\pi(3p-1)\} = \{2p-1,3p-1\}$, $\{\pi(2p),\pi(3p)\} = \{2p,3p\}$,...,$\{\pi(3p-3),\pi(4p-3)\} = \{3p-3,4p-3\}$.

After this there are terms with unique degrees, hence the Vandermonde part has to have this part: $Y_{4p-2}^{4p-3}Y_{4p-1}^{4p-2}\cdots Y_{p^2}^{p^2-1}$.

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_is have to have degree divisible by p^2, since otherwise we would get a coefficient starting with

$$(q-1)(q-2)\cdots(q-p+1)\binom{q-p}{p}\binom{q-2p}{p}\cdots\binom{q-(p-1)p}{p}\binom{q-p^2}{k},$$

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) π is a permutation of the indices such that $\pi(i) = i$, except for a couple of values: $\{\pi(1), \pi(2)\} = \{1, 2\}$, $\{\pi(3), \pi(4)\} = \{3, 4\}$,..., $\{\pi(2p-3), \pi(2p-2)\} = \{2p-3, 2p-2\}$;

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

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

...

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

This means that apart form 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 2×2 determinants of the form

$$\begin{vmatrix} a_i^{q-1-k} Y_i^k & a_i^{q-1-k-p^m} Y_i^{k+p^m} \\ a_j^{q-1-k} Y_j^k & a_j^{q-1-k-p^m} Y_j^{k+p^m} \end{vmatrix}.$$

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

$$(a_1 - a_2)(a_3 - a_4)\cdots(a_{2p-3} - a_{2p-2})\cdot$$

$$(a_{2p-1} - a_{3p-1})(a_{2p} - a_{3p})\cdots(a_{3p-3} - a_{4p-3})\cdot$$

$$(a_{p^2+1} - a_{2p^2+1})(a_{p^2+2} - a_{2p^2+2}) \cdots (a_{p^2+p-1} - a_{2p^2+p-1}) \cdot$$

$$\ldots$$

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

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 3.4.3 (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 $\{a_1, ..., a_q\}$. 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_is.

LEMMA 3.4.8. *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 3.4.4. By 3.4.4, 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_is.

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 $Y_i Y_j^{\frac{q-1}{2}} Y_k^{\frac{q-3}{2}}$, where $i = 3$ or 4 and $\{j, k\} = \{1, 2\}$. Each of them comes with coefficient $(q-1)\binom{q-2}{(q-1)/2} \neq 0$. 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 3.4.3, this implies that there is a value among the a_is with

multiplicity at least $k-1$ contradicting the assumption that the a_is 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):

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

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 3.4.3) that there is a value among the a_is 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):

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

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 3.1.2*) By Lemma 3.4.2 that there are at least 4 different values among the a_is. Suppose there is no ordering $b_1, \dots, b_q$ of the elements of GF(q) giving $\sum_i a_i b_i = 0$. We have to find a contradiction. After transformation (by Lemma 3.4.1 and the sentence after its proof) suppose 0 is not among the a_is. Apply Lemma 3.4.5 or 3.4.7 to get that a significant part of the elements must be identical. Apply a transformation to make this value zero and apply Lemma 3.4.8 for the rest of the a_is. We cannot have different b_is 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_is 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. □

3.4.4 Proof for even q

The proof is similar for q even. We can use Lemma 3.4.1 (the proof presented works for q even). Lemma 3.4.2 should be replaced by the following.

LEMMA 3.4.9. *If our multiset has only* 1 *or* 2 *different values and $n = q$ is even, then Theorem 3.1.2 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 larger than $q/2$ and 1 is the other value with multiplicity smaller than $q/2$. 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 $b_1, \cdots, b_{m-1}$ be arbitrary distinct elements of G. If $b_1 + \cdots + b_{m-1}$ is distinct from all the b_is, 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_is, b_{m-1} say, then we have $b_1 + \cdots + b_{m-2} = 0$. Let $a \in \mathrm{GF}(q) \setminus G$. 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_is are distinct and their sum is zero. □

Lemma 3.4.3 and Theorem 3.4.4 are true for q even (the proofs presented did not assume q is odd). Lemma 3.4.7 should be replaced by the following.

LEMMA 3.4.10. *Suppose $q = 2^h > 8$, and that there is no ordering $b_1, \ldots, b_q$ of the elements of* GF(q) *such that $\sum_i a_i b_i = 0$. Then at least $\frac{q+3}{2}$ of the a_is are the same.*

Proof. After transformation suppose 0 is not among the a_is. Consider the polynomial G from Theorem 3.4.4 with $k = q$. By 3.4.4, terms of maximal degree of G have at least one Y_i with degree at least q.

Consider the following term:

$$Y_1 \prod_{i=1}^{h-1} Y_{i+2}^{2^{h-i}} \prod_{i=1}^{h} Y_i^{i-1}$$

Similarly to the proof of Lemma 3.4.7, one can use Lucas' theorem to find the coefficient of this term. This is the sum of some subterms from $G(Y_1, \ldots, Y_q)$. If a subterm from $G(Y_1, \ldots, Y_q)$ is non-zero, 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 must imply 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 one of the a_is has multiplicity $q - h + 1$ because of Lemma 3.4.3 (iii).

□

Instead of Lemma 3.4.8, one can immediately prove the following.

LEMMA 3.4.11. *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_is are the same.*

Proof. Consider the polynomial G from Theorem 3.4.4. By 3.4.4, terms of maximal degree of G have at least one Y_i with degree at least q.

Considering 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_is are the same. □

After these lemmas, the proof is easy.

3.5 Final remarks

At the end of this chapter, we discuss some possible generalizations of the presented results. Theorem 3.2.1, concerning range of polynomials over finite fields, raises natural questions. We deduced that if $M = \{a_1, a_2, \ldots, a_q\}$ is a multiset over $\mathrm{GF}(q)$ with $a_1 + \cdots + a_q \neq 0$, then every reduced degree polynomial whose range is M has degree $q - 1$.

NOTATION 3.5.1. *Let $\Delta_q(M)$ denote the least integer d such that there exists a polynomial of degree d over $\mathrm{GF}(q)$ whose range is M.*

Is there a natural property that describes whether $\Delta_q(M)$ is small or large? First, we have to assume that the elements of the multiset add up to zero, otherwise $\Delta_q(M)$ is clearly $q - 1$.
On the one hand, it is easy to see that the greatest multiplicity $m(M)$ in M - if it is less than q - gives a lower bound on $\Delta_q(M)$. Indeed, if an element a has multiplicity $m(a)$, then clearly $f - a$ has $m(a)$ roots in $\mathrm{GF}(q)$ for any polynomial f whose range is M, which shows that $\deg(f) \geq m(a)$.
On the other hand, Theorem 3.2.1 implies that, given $a_1 + \cdots + a_q = 0$, $\Delta_q(M)$ is $q - 2$ only if there is an element with multiplicity $q - 2$. (In this case, the multiset must have the structure $\{a, \ldots a, a+b, a-b\}$.) Furthermore, $\Delta_q(M) = 1$ if and only if every element in M has multiplicity 1, i.e, M is the set of all elements of the field.

These observations would suggest that if $a_1 + \cdots + a_q = 0$, then $\Delta_q(M)$ only depends on $m(M)$, the largest multiplicity in M and probably $\Delta_q(M) = m(M)$. However, this is not the case.

Let us suppose that $q = p$ is prime and define the multiset as 1 taken with multiplicity m, $p - m$ taken with multiplicity 1, and 0 taken with multiplicity $p - m - 1$. By a result of Biró [18], 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 in the $q = p$ prime case if the greatest multiplicity of M is smaller than $c \cdot p$ with $c < 3/4$, then it might happen that $\Delta_q(M)$ is bigger than the greatest multiplicity. Moreover, the difference between $\Delta_q(M)$ and the greatest multiplicity $m(M)$ of M can be linear in p.

The papers of Muratović-Ribić and Wang [78, 79] reveals that for every large enough q, the relation $\Delta_q(M) > m(M)$ may hold for many possible values of $m(M)$:

THEOREM 3.5.2. *[78, 79] For every m with $\frac{q}{2} \leq m < q-3$ there exists a multiset M with highest multiplicity $m(M) = m$ whose elements add up to zero, such that every polynomial over* GF(q) *with the prescribed range M has degree greater than m, that is, $\Delta_q(M) \geq m(M) + 1$.*

COROLLARY 3.5.3. *Among all multisets M with $\Delta_q(M) = q-3$, there must be some in which the greatest multiplicity is less than $q-3$.*

The proof is based on a delicate enumeration argument. However, it is still open to determine $\Delta_q(M)$ in general or even provide good bounds on it.

Another way to generalize the main result is presented in the Chapter 4.

Chapter 4

Extension to cyclic groups

4.1 Introduction and background

In the previous chapter we considered multisets over finite fields. We exploited the field structure when we applied the Combinatorial Nullstellensatz. However, the formulation of the problem itself, at least in the prime field case, only requires the abelian group structure. This motivates the forthcoming investigation.

The aim is to find a different kind of generalization of the prime case of Theorem 3.1.1, more combinatorial in nature, which refers only to the group structure. First we extend the result to cyclic groups of odd order.

THEOREM 4.1.1. *Let $\{a_1, a_2, \ldots, a_m\}$ be a multiset in the Abelian group $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$, where m is odd. Then after a suitable permutation of the indices, either $\sum_i i a_i = 0$, or $a_1 = a_2 = \cdots = a_{m-2} = a$, $a_{m-1} = a + b$, $a_m = a - b$ for some elements a and b, $(b, m) = 1$.*

The situation is somewhat different if the order of the group is even. In this case we have to deal with two types of exceptional structures. The following statements are easy to check.

PROPOSITION 4.1.2. *Let m be an even number represented as $m = 2^k n$, where n is odd.*

(i) If a multiset $M = \{a_1, a_2, \ldots, a_m\}$ of $\mathbb{Z}_m$ consists of elements having the same odd residue c mod 2^k, then M has no permutation for which $\sum_i ia_i = 0$ holds.

(ii) If $M = \{a, a, \ldots, a+b, a-b\}$ mod m, where a is even and $(b, m) = 1$ holds, then M has no permutation for which $\sum_i ia_i = 0$ holds.

These two different kinds of structures we call homogeneous and inhomogeneous exceptional multisets, respectively.

THEOREM 4.1.3. *Let $M = \{a_1, a_2, \ldots, a_m\}$ be a multiset in the Abelian group $\mathbb{Z}_m$, m even. If M is not an exceptional multiset as defined in Proposition 4.1.2, then after a suitable permutation of the indices $\sum_i ia_i = 0$ holds.*

The presented results might be extended in different directions. One may ask whether there exists a permutation of the elements of a given multiset M of $\mathbb{Z}_m$ (consisting of m elements), for which the sum $\sum_i ia_i$ is equal to a prescribed element of $\mathbb{Z}_m$. This question is related to a conjecture of Britnell and Wildon, see [22, p. 20], which can be reformulated as follows. Given a multiset $M = \{a_1, a_2, \ldots, a_m\}$ of $\mathbb{Z}_m$, all elements of $\mathbb{Z}_m$ are admitted as the value of the sum $\sum_{i=1}^{m} ia_{\pi(i)}$ for an appropriate permutation π from the symmetric group Sym_m, unless one of the following holds:

- $M = \{a, \ldots, a, a+b, a-b\}$,
- there exists a prime divisor p of m such that all elements of M are the same mod p.

Our result may in fact be considered as a major step towards the proof of their conjecture, which would provide a classification of values of determinants associated to special types of matrices. When m is a prime, the conjecture is an immediate consequence of Theorem 3.1.1 and Lemma 4.2.2 (ii). Indeed, if only one value was admitted, then the multiset would consist of a single element m times. On the other hand, if there was an admitted element $w \neq 0$, all nonzero elements would be admitted via Lemma 4.2.2 (ii). Thus the value 0 is the crucial one, and it was investigated in Theorem 3.1.1.

The chapter is organized the following way. In Section 4.1, we collect several simple observations that are used frequently throughout the paper and sketch our proof strategy. Section 4.2 is devoted to the proof of Theorem 4.1.1. In Section 4.3 we will verify Theorem 4.1.3 for some particular cases, whose proofs do not exactly fit into the general framework (and may be skipped at a first reading). The complete proof, which is more or less parallel to that of Theorem 4.1.1, is carried out in Section 4.4. Finally, we discuss related problems and conjectures in Section 4.5.

4.2 Preliminaries

DEFINITION 4.2.1. *Let $M = \{a_1, \dots, a_m\}$ be a multiset in $\mathbb{Z}_m$. A permutational sum of the elements of M is any sum of the form $\sum_{i=1}^{m} i a_{\pi(i)}$, $\pi \in Sym_m$. If, after some rearrangement, we fix the order of the elements of M, then the permutational sum of M considered as a sequence $(a_1, \dots, a_m)$ is simply $\sum_{i=1}^{m} i a_i$.*

Accordingly, the aim is to determine which multisets admit a zero permutational sum. This property is invariant under certain transformations.

LEMMA 4.2.2. *Let m be odd, and M be a multiset in $\mathbb{Z}_m$ of cardinality m.*

(i) If no permutational sum of M admits the value 0, then the same holds for any translate $M + c$ of M, and also for any dilate cM in case $(c, m) = 1$.

(ii) If the permutational sums of M admit a value w, then they also admit the value kw for every integer k with $(m, k) = 1$. As a consequence, if $(m, w) = 1$, then the permutational sums take at least $\varphi(m)$ different values.

(iii) Assume that M has the exceptional structure, i.e. $M = \{a, \dots, a, a + b, a - b\}$ where $(b, m) = 1$. Then the permutational sums of M admit each element of $\mathbb{Z}_m$ except zero.

Proof. Parts (i) and (iii) are straightforward, for $1 + 2 + \ldots + m \equiv 0 \pmod{m}$. Part (ii) follows from the fact that $\pi \in Sym_m$ holds for the function π defined by $\pi(i) = ki$. □

REMARK 4.2.3. *Part (ii) holds also if m is even, but this is not true in general for Parts (i) and (iii). The reason is that* $1 + 2 + \ldots + m \not\equiv 0 \pmod{m}$ *if m is even, but* $1 + 2 + \ldots + m \equiv m/2 \pmod{m}$.

The sumset or Minkowski sum $C + D$ of two subsets C and D of an Abelian group G written additively is $C + D = \{c + d \mid c \in C, d \in D\}$. $|C|$ denotes the cardinality of the set C. The following statement is folklore.

LEMMA 4.2.4. *For $C, D \subseteq \mathbb{Z}_m$, $|C| + |D| > m$ implies $C + D = \mathbb{Z}_m$.*

Proof. Fix an arbitrary element $g \in \mathbb{Z}_m$. If $|C| + |D| > m$, then the set $-C + g$ (containing elements of form $-c + g : c \in C$) and D can not be disjoint, confirming the statement. □

In the remaining part of this section, we sketch the proof of Theorem 4.1.1, thus from now on, m is assumed to be odd in this section. Meanwhile, we will also use the definitions and notions introduced below in the even case.

Recall that the arithmetic function $\Omega(n)$ represents the total number of prime factors of n. Similarly to the classical result in zero-sum combinatorics due to Erdős, Ginzburg and Ziv [32], we proceed by induction on $\Omega(m)$. The initial case is covered by Theorem 3.1.1, so in the sequel we assume that m is a composite number and fix a prime divisor p of m and write $m = p^k n$, where $(p, n) = 1$.

The proof is carried out in several steps (of which the first two will be quite similar to the beginning of the proof of Theorem 4.1.3).

4.2.1. First step: choosing an initial order and partitioning into blocks

We introduce the notion of *initial order* as follows.

DEFINITION 4.2.5. *Let $s = (b_1, b_2, \ldots, b_m)$ be any sequence in $\mathbb{Z}_m$.*

(i) A cyclic translate of s is any sequence of the form $(b_i, b_{i+1}, \ldots, b_m, b_1, \ldots, b_{i-1})$.

(ii) The sequence s is separable (relative to the prime divisor p of m) if equivalent elements mod p^l are consecutive for every $1 \leq l \leq k$.

(iii) A sequence $(a_{\pi(1)}, \ldots, a_{\pi(m)})$*, where* $\pi \in Sym_m$*, is an initial order for the multiset* $M = \{a_1, \ldots, a_m\}$ *of* $\mathbb{Z}_m$*, if some cyclic translate of* $(a_{\pi(1)}, \ldots, a_{\pi(m)})$ *is separable.*

Thus separability means that for $1 \leq i < j \leq m$ and every $l \leq k$, $a_i \equiv a_j \pmod{p^l}$ implies $a_i \equiv a_h \pmod{p^l}$ for every $i < h < j$. Note that one can always order the elements of M into a separable sequence.

A useful property of such an ordering is summarized in the following lemma whose proof is straightforward.

LEMMA 4.2.6. *Consider a sequence of* m *elements in* $\mathbb{Z}_m$*, which admits a separable cyclic translate. Partition the elements into* $d \geq 3$ *consecutive blocks* $T_1, \ldots, T_d$*. If for an integer* l*, a certain residue* r *mod* p^l *occurs in every block, then at most two of the blocks may contain an element having a residue different from* r*. The same conclusion holds if the elements are rearranged inside the individual blocks.*

Let $(a_1, \ldots a_m)$ be an initial order. Form p consecutive blocks of equal size, denoted by $T_1, T_2, \ldots, T_p$, each containing $m^* := m/p$ consecutive elements. More precisely,

$$T_i = \{a_{(i-1)m^*+1}, a_{(i-1)m^*+2}, \ldots, a_{im^*}\}.$$

S_i denotes the sum of the elements in T_i, while R_i denotes the permutational sum of the block T_i (as an ordered multiset), that is, $R_i = \sum_{j=1}^{m^*} j a_{j+(i-1)m^*}$.
Writing $R = \sum_{i=1}^{p} R_i$, the permutational sum of M takes the form

$$\Phi = \sum_{j=1}^{m} j a_j = \sum_{i=1}^{p} (R_i + m^*(i-1)S_i) = R + m^* \sum_{i=0}^{p-1} i S_{i+1}.$$

4.2.2. Second step: divisibility by $m^* := m/p$

Our aim here is to ensure that $m^* \mid \Phi$ holds after a well structured rearrangement of the elements. That is, we want to achieve that $m^* \mid R$ holds. To this end we allow reordering of the elements inside the individual blocks. Such a permutation will be referred to as a *block preserving permutation*. We distinguish three different cases.

First, if there is no exceptionally structured block mod m^*, then by the inductional hypothesis the elements in each block T_i can be rearranged so that m^* divides R_i. Thus, after a block preserving permutation, $m^* \mid R$.

Next, if there is an exceptionally structured block T_i, then the permutational sums over T_i take $m^* - 1$ different values mod m^*, see Lemma 4.2.2 (iii). If there are at least two exceptionally structured blocks, then it follows from Lemma 4.2.4 that there is a block preserving permutation that ensures $m^* \mid R$.

Finally, if there is exactly one exceptionally structured block $\{a, \dots, a, a+b, a-b\}$ (mod m^*), then a permutational sum of this block can take any value except 0 mod m^*. So after a block preserving permutation we are done, unless zero is the only value that the other blocks admit, that is, all elements must be the same in each block mod m^*.
This latter case can be avoided by a suitable choice of the initial order in the first step. Indeed, translating the initial order cyclically so that it starts with an appropriate element from the exceptional block will break down this structure.

4.2.3. Third step

To complete the proof, based on the relation $m^* \mid \Phi$ we further reorganize the elements to achieve a zero permutational sum, or else to conclude that we are in (one of) the exceptional case(s). Here we only give an outline of the strategy of the proof, as the following section is devoted to the detailed discussion.

Set $R' := \frac{R}{m^*}$. As a first approximation, we try to change the order of the blocks to obtain

$$\sum_{i=0}^{p-1} iS_{i+1} \equiv -R' \pmod{p},$$

which would imply $m \mid \Phi$. One is tempted to argue that the case $R' \equiv 0 \pmod{p}$ would be easy to resolve applying Theorem 3.1.1 for the multiset $\{S_1, \dots, S_p\}$. As it turns out, the main difficulty is to handle exactly this case, since the multiset $\{S_1, \dots, S_p\}$ may have the exceptional structure. A remedy for this is what we call the 'braid trick'. The main idea of this tool will be to consider the transposition of a pair of elements whose indices differ by a fixed number x (typically a multiple of m^*). By this kind of transposition of a pair (a_i, a_{i+x}), the permutational sum

increases by $x(a_i - a_{i+x})$, providing a handy modification.

4.3 The case of odd order

In this section we complete the proof of Theorem 4.1.1, $m = p^k n$ where $(p, n) = 1$ will denote an odd integer throughout the section. We continue with the details of the third step outlined in the previous section. We distinguish two cases according to whether R' is divisible by p or not.

4.3.1. R' is not divisible by p.

Note that $\sum_{i=0}^{p-1} iS_{i+1}$ can be viewed as a permutational sum of the multiset $\mathcal{S} = \{S_1, S_2, \ldots, S_p\}$. If there are two elements $S_i \not\equiv S_j \pmod{p}$, then their transposition changes the value of the permutational sum of $\mathcal{S}$ mod p. In particular, the permutational sums of $\mathcal{S}$ admit a nonzero value mod p. From Lemma 4.2.2 (ii) it follows that they admit each nonzero element of $\mathbb{Z}_p$ and in particular $-R'$ too.

Otherwise, we have $S_1 \equiv S_2 \equiv \ldots \equiv S_p \pmod{p}$. We use the `braid trick`: we look at the pairs (a_i, a_{i+m^*}) for every i. The elements a_i and a_{i+m^*} occupy the same position in two consecutive blocks T_j, T_{j+1}, hence their transposition leaves R intact, and thus R' does not change either. On the other hand, if they have different residues mod p, S_j and S_{j+1} change whereas each other S_i remains the same, therefore the previous argument can be applied.

Finally, we have to deal with the case when $a_i \equiv a_{i+lm^*} \pmod{p}$ holds for every possible i and l. This is the point where we exploit the separability property. The initial order has changed only inside the blocks during the second step. Since the number of blocks is at least three, it follows from Lemma 4.2.6 that $a_i \equiv a_j \pmod{p}$ for all $1 \leq i < j \leq m$ in M. In this case we prove directly that M has a zero permutational sum. In view of Lemma 4.2.2 (i), we may suppose that every a_i is divisible by p. Consider $M^* := \{\frac{a_1}{p}, \frac{a_2}{p}, \ldots, \frac{a_m}{p}\}$. Apply the first two steps for this multiset M^*. It follows that M^* has a zero permutational sum mod m^*, which implies that

M has a zero permutational sum mod m.

4.3.2. R' is divisible by p

Here our aim is to prove that $p \mid \sum_{i=0}^{p-1} iS_{i+1}$ holds for a well chosen permutation of the multiset $\mathcal{S} := \{S_1, \ldots, S_p\}$. This is exactly the problem that we solved in Theorem 3.1.1, which implies that we can reorder the blocks (and hence the multiset M itself) as required, except when the multiset $\mathcal{S}$ has the form $\{A, A, \ldots, A, A+B, A-B\}$, with the condition $(B, p) = 1$.

Once again, we apply the braid trick. If a_i and a_{i+lm^*} have different residues mod p, then we try to transpose them in order to destroy this exceptional structure $\{A, A, \ldots, A, A+B, A-B\}$. As in Subsection 4.3.1, R does not change. We call a pair of elements *exchangeable* if their indices differ by a multiple of m^*.

Thus, a zero permutational sum of M is obtained unless no transposition of two exchangeable elements destroys the exceptional structure of $\mathcal{S}$. The following lemma gives a more detailed description of this situation.

LEMMA 4.3.1. *Suppose that no transposition of two exchangeable elements destroys the exceptional structure of $\mathcal{S}$. Then either this exceptional structure can be destroyed by two suitable transpositions, or M contains only three distinct elements mod p: $t, t+B, t-B$ for some t with the following properties:*

- *$t+B$ occurs only in one block, and only once;*
- *$t-B$ occurs only in one block, and only once;*
- *$t+B$ and $t-B$ occupy the same position in their respective blocks.*

Proof. Denote by T^+ and T^- the blocks for which the sum of the elements is $A+B$ and $A-B$, respectively. Apart from elements from T^+ and T^-, two exchangeable elements must have the same residue mod p. Furthermore, if a transposition between $a_j \in T^-$ and $a_{j+lm^*} \notin T^+$ does not change the structure of $\mathcal{S}$, that means $a_j \equiv a_{j+lm^*} \pmod{p}$ or $a_j \equiv a_{j+lm^*} - B \pmod{p}$. Similar proposition holds for T^+.

Consider now a set of pairwise exchangeable elements. One of the following describes their structure: either they all have the same residue mod p, or they have the same

residue t mod p except the elements from T^+ and T^-, for which the residues are $t+B$ and $t-B$, respectively.

Observe that both cases must really occur since the sums S_i of the blocks are not uniformly the same. In particular, there is a full set of p pairwise exchangeable elements having the same residue mod p.

Since the number of blocks is at least 3, we can apply Lemma 4.2.6. We only used block-preserving permutations so far, hence it follows that all elements have the same residue mod p — let us denote it by t — except some $(t+B)$'s in T^+, and the same number of $(t-B)$'s in T^-, in the very same position relative to their blocks.

We claim that this number of different elements in T^+ and T^- must be one, otherwise we can destroy the exceptional structure with two transpositions. Indeed, by contradiction, suppose that there exist two distinct set of exchangeable elements where the term corresponding to T^+ and T^- is $t+B$ and $t-B$, respectively. Pick a block different from T^+ and T^- and denote it by T. Then transpose $t+B \in T^+$ and $t \in T$ in the first set, and $t-B \in T^-$ and $t \in T$ in the second set. The new structure of $\mathcal{S}'$ obtained this way is not exceptional any more. □

LEMMA 4.3.2. *Suppose that M contains only three distinct elements mod p: $t, t+B, t-B$ for some t with the following properties:*

- *$t+B$ occurs only in one block, and only once;*
- *$t-B$ occurs only in one block, and only once;*
- *$t+B$ and $t-B$ occupy the same position in their respective blocks.*

Then either a suitable zero permutational sum exists or the conditions on M hold mod p^l for every $l \leq k$, with a suitable $B = B_l$ not divisible by p.

Proof. We proceed by induction on l. Evidently, it holds for $l = 1$.
According to Lemma 4.2.2 (i) we may assume that $t \equiv 0 \pmod{p}$. Let a^+ and a^- denote the elements of T^+ and T^- for which $a^+ \equiv B \pmod{p}$ and $a^- \equiv -B \pmod{p}$. Note that their position is the same in their blocks.

Suppose that $l \geq 2$ and the conditions hold mod p^{l-1}. Consider the residues of the elements mod p^l now. We use again the braid trick. Suppose that there exist

$a_i, a_j \notin \{a^-, a^+\}$ such that $i-j$ is divisible by p^{k-l} but not by p^{k-l+1}, and $a_i \not\equiv a_j \pmod{p^l}$. After we transpose them, (the residue of) R does not change mod p^{k-1}, but it changes by $(i-j)(a_j-a_i) \neq 0 \pmod{p^k}$. For the new permutational sum thus obtained, $R' \not\equiv 0 \pmod{p}$ holds, while the multiset $\mathcal{S}$ may change, but certainly it does not become homogeneous mod p. Thus M has a zero permutational sum, as in Subsection 3.1.

Otherwise, in view of Lemma 4.2.6 it is clear that all the residues must be the same mod p^l, and we may suppose they are zero, except the residues of a^+ and a^-. In addition, $a^+ + a^- \equiv 0 \pmod{p^l}$ must hold too, since $R' \equiv 0 \pmod{p}$. This completes the inductive step. □

Lemma 4.3.2 applied for $l = k$ completes the proof of Theorem 4.1.1 when $m = p^k$ is a prime power. In the sequel we assume that $n \neq 1$. Let $m = p_1^{k_1} p_2^{k_2} \dots p_n^{k_r}$ be the canonical form of m. Note that the whole argument we had so far is valid for any prime divisor p of m. Therefore, to complete the proof , we may assume that M has the exceptional structure mod $p_i^{k_i}$ as described in Lemma 4.3.2 for every $p = p_i$.

LEMMA 4.3.3. *The conclusion of Theorem 4.1.1 holds if M has exceptional structure modulo each $p_i^{k_i}$.*

Proof. We look at the permutational sums of M leaving the elements of M in a fixed order $a_1, a_2, \dots, a_m$ while permuting the coefficients $1, 2, \dots, m$. According to Lemma 4.2.2 (i) we may assume that all elements, except two, are divisible by $p_1^{k_1}$; all elements, except two, are divisible by $p_2^{k_2}$, and so on. It follows that at least $m-2r$ elements are zero mod m, so their coefficients are irrelevant. So we only have to assign different coefficients to the nonzero elements x_i of M. For any $0 \neq x \in M$, we choose its coefficient c_x to be either $\frac{m}{(m,x)}$ or $-\frac{m}{(m,x)}$, ensuring that $c_x x = 0$ in $\mathbb{Z}_m$. If such an assignment is possible, the permutational sum will be zero .

First, observe that $\frac{m}{(m,x)}$ and $-\frac{m}{(m,x)}$ are the same if and only if $(m,x) = 1$. Note that for each i, p_i divides (m, x_i) for all x_i, except two. Hence there is no triple x_1, x_2, x_3 of the elements for which (m, x_i) would be the same. Thus we can assign a different coefficient to each $x_i \neq 0$, except when there exist two of them, for which $(m, x_i) = 1$. But this is exactly the exceptional case $M = \{0, 0, \dots, 0, c, -c\}$, where $(c, m) = 1$. □

4.4 Special cases of Theorem 4.1.3

In this section we prove that Theorem 4.1.3 holds for some specially structured multisets.

LEMMA 4.4.1. *Let $m = 2n$, $n > 1$ odd, and let M be a multiset in $\mathbb{Z}_m$ consisting of two blocks of size n in the form $T_1 = \{a, \ldots, a, a+b, a-b\}$ and $T_2 = \{c, \ldots, c\}$ (mod n), where $(b, n) = 1$. If one of the blocks contains elements from only one parity class then Theorem 4.1.3 holds.*

Proof. First we obtain a permutation for which n divides the permutational sum of M. We choose an element c^* from T_2. Assume that $c^* \neq a - b \pmod{n}$ and exchange c^* with $a - b \in T_1$. (If the assumption does not hold then we pick $a + b$ instead of $a - b$ and continue the proof similarly.) This way we get two blocks T_1' and T_2', which do not have the exceptional structure mod n. Thus there exists a block preserving permutation ensuring that n divides the obtained permutational sums of T_1' and T_2', thus n also divides the permutational sum of M.

We assume that both odd and even elements occur in M, otherwise either 2 is trivially a divisor of Φ or M has exceptional homogeneous structure. If the relation $m \mid \Phi$ does not hold, then we apply the braid trick by looking at the pairs (x_i, x_{i+n}). If a pair consists of an odd and an even element, then we may transpose them and the proof is done.

Otherwise the exchangement of c^* and $a - b$ must have destroyed the property of having a uniform block mod 2 among T_1 and T_2, that is, c^* and $a - b$ have different parity. Since the choice of $c^* \in T_2$ was arbitrary, we may assume that $T_2 = \{c, \ldots, c\} \pmod{2n}$. Moreover, since the braid trick did not help us, every element in T_1 congruent to a mod n must have the same parity as the elements c, and the parity of element $a + b$ must coincide with that of $a - b$.

In this remaining case consider the blocks $\{a, \ldots, a, c, c\}$ and $\{c, \ldots, c, a+b, a-b\}$. First, if $c \not\equiv a \pmod{n}$, then neither block is exceptional as a multiset in $\mathbb{Z}_n$, hence an appropriate block preserving permutation ensures that n divides the permutational sum. If the permutational sum happens to be odd, then a suitable transposition via the braid trick will increase its value by n, for the first block contains

elements from the same parity class in contrast to the second. Finally, if $c \equiv a \pmod{n}$, then either $c = a$ is even, providing that M has inhomogeneous exceptional structure, or $c = a$ is odd, in which case the permutational sum will be zero if we set $a_n = a + b$ and $a_{2n} = a - b \pmod{n}$.

□

LEMMA 4.4.2. *Let $m = 2^k n > 4$, n odd and $k > 1$. Let M be a multiset of $\mathbb{Z}_m$, consisting of two even elements and $m-2$ odd elements having residue c mod 2^{k-1}. Then the permutational sum of M admits the value zero.*

Proof. Denote the even elements by q_1 and q_2. We distinguish the elements having residue c mod 2^{k-1} according to their residues mod 2^k, which are c and $c^* \equiv c + 2^{k-1} \pmod{2^k}$. We may suppose that the number of elements c is greater than or equal to the number of elements c^*.

First we solve the case $n = 1$ meaning $m = 2^k$, $k > 2$. Taking $a_{m/2} = q_1$, $a_m = q_2$, the permutational sum will be divisible by $m/2$. If there is no element c^*, then the permutational sum is in fact divisible by m. If there exist some elements c^* among the odd elements and the permutational sum is not yet divisible by m, then a transposition between two elements c and c^* whose indices differ by an odd number will result in a zero permutational sum mod m.

Turning to the general case $n > 1$, we initially order the elements as follows. Even elements precede the others, elements c mod 2^k precede the elements c^* mod 2^k, and equivalent elements mod m are consecutive. Form 2^k blocks of equal size n.

With an argument similar to the one in Section 4.2.2 we arrive at two cases. Either we obtain a permutational sum congruent to zero mod n after a block preserving permutation, or the structures of the blocks are as follows: there is exactly one exceptional block (as a multiset in $\mathbb{Z}_n$) and the other blocks only admit a zero permutational sum mod n meaning that each of them consists of equivalent elements mod n.

Case 1) Consider the block preserving permutation, which results in a permutational sum Φ_0 divisible by n. We modify this permutation, if necessary, to get one

corresponding to a zero permutational sum mod 2^k, while the divisibility by n is preserved.

We denote by f and g the indices of q_1 and q_2 in the considered permutation. Thus

$$\Phi_0 \equiv c\frac{2^k(2^k-1)}{2} + f(q_1 - c) + g(q_2 - c) \pmod{2^{k-1}}. \qquad (*)$$

Note that $\{ln : l = 0, 1, \ldots, 2^k - 1\}$ is a complete system of residues mod 2^k. Let l be the solution of the congruence

$$(q_1 - c)ln \equiv -\Phi_0 \pmod{2^k}.$$

Thus transposing $q_1 = a_f$ with a_{f+ln} implies that

$$\Phi_1 \equiv \begin{cases} 0 \pmod{2^k} & \text{if } a_{f+ln} \equiv c \pmod{2^k} \\ 2^{k-1} \pmod{2^k} & \text{if } a_{f+ln} \equiv c^* \pmod{2^k}. \end{cases}$$

The relation $n \mid \Phi_1$ still holds. So in the case when $a_{f+ln} \equiv c \pmod{2^k}$ we are done, and if $a_{f+ln} \equiv c^* \pmod{2^k}$ we have to increase the value of the permutational sum by $2^{k-1}n$ mod m. Recall that each element in the second block is c mod 2^k. Therefore transposing $a_f \equiv c^* \pmod{2^k}$ with $a_{f+n} \equiv c \pmod{2^k}$ in this latter case does the job.

Case 2) One of the blocks (not necessarily the first one) has the exceptional structure, while every other is homogeneous mod n. We can still argue as in the previous case if, performing the following operation, we can destroy the exceptional structure without changing the position of the even elements q_1, q_2 and the entire second block. Namely, we try to transpose two nonequivalent elements mod n, one from the exceptional block and one from another block. If this is not possible with the above mentioned constraints, then the exceptional block must be among the first two. Furthermore, every element congruent to c mod 2^k in the first two blocks must be equivalent mod n. Thus we only have to deal with the following structure: the first block is the exceptional one, q_1 and q_2 correspond to $a + b$ and $a - b$ in the exceptional structure, all the other elements contained in the first two blocks are equivalent mod m (and congruent to c mod 2^k), and the remaining blocks are all homogeneous mod n.

Exchanging q_2 with any element from the second block destroys the exceptional structure of the first block, which means that after a suitable block preserving permutation the permutational sum of each block becomes 0 mod n, ensuring $n \mid \Phi$ for the multiset. At this point the indices of the even elements are n and $2n$.

Next, keeping the order inside the blocks we rearrange them so that the first and second blocks become the 2^{k-1}th and 2^kth, that is, $a_{m/2} = q_1$ and $a_m = q_2$. Hence, maintaining $n \mid \Phi$ we also achieve $2^{k-1} \mid \Phi$ via equality $(*)$.

Either we are done or $\Phi \equiv 2^{k-1}n \pmod{m}$. The latter can only happen if there exists an element of type c^*. If a block contains both elements of type c and c^*, then a transposition of a consecutive pair of them within that block increases Φ by $2^{k-1}n$. Otherwise there must exist a block containing only elements of type c^*. This implies the existence of a pair of c and c^* whose position differs by n. Their transposition increases Φ by $2^{k-1}n^2 \equiv 2^{k-1}n \pmod{m}$, solving the case. □

4.5 The case of even order

One main difference between the odd and the even order case is due to the fact that Lemma 4.2.2 (i) does not hold if m is even, for $1 + 2 + \ldots + m$ is not divisible by m. That explains the emergence of the exceptional structure, see Proposition 4.1.2.

REMARK 4.5.1. *It is easy to check that after a suitable permutation of the indices,* $\sum_i ia_i \equiv m/2 \pmod{m}$ *holds for the exceptionally structured multisets.*

In order to prove Theorem 4.1.3, we fix the notation $m = 2^k n$, where n is odd and $k > 0$. Since the cases $m = 2$ and $m = 4$ can be checked easily, we assume that $m > 4$ and prove the theorem by induction on k.

Initial step

We have $m = 2n$, where $n > 1$ according to our assumption. Take the multiset $M = \{a_1, \ldots, a_m\}$ of $\mathbb{Z}_m$. Arrange the elements in such a way that both the odd

and the even elements are consecutive. Form two consecutive blocks of equal size, denoted by T_1 and T_2, each containing n elements. Using the notation of Section 2, the permutational sum of M is

$$\Phi = \sum_{j=1}^{m} j a_j = \left(R_1 + R_2 + \frac{m}{2} S_2 \right) = R + nS_2.$$

Our first aim is to ensure that $n \mid \Phi$ holds after a well structured rearrangement of the elements.

To this end, we may take an appropriate block preserving permutation providing that $n \mid R_i$ holds for $i = 1, 2$. Such a permutation exists, except when at least one of the blocks are exceptional mod n. However it is enough to obtain a block preserving permutation for which $n \mid R$, and such a permutation exists via Lemma 4.2.2 (iii), unless one of the blocks has exceptional structure (mod n) and the other consists of equivalent elements (mod n). This latter case was fully treated in Lemma 4.4.1.

The next step is to modify the block preserving permutation such that $2 \mid \Phi$ also holds.
If it does not hold, then we try to transpose a pair (a_i, a_{i+n}) for which a_i and a_{i+n} have different parity, according to the braid trick. The permutational sum would change by n (mod m) and we are done. If all pairs have the same parity, then all elements have the same parity. Therefore either Φ is automatically even or M has homogeneous exceptional structure. This completes the initial step.

Inductive step

Assume that $k > 1$ and Theorem 4.1.3 holds for every even proper divisor of m. Recalling Definition 2.4, we choose a separable sequence relative to the prime divisor 2 of m as an initial order. Partition the multiset into two blocks of equal size, T_1 and T_2. Introduce $m^* := m/2 = 2^{k-1}n$, and assume first that $m^* \mid R_1 + R_2$ can be achieved by a suitable block preserving permutation. By induction, we can do it if both blocks as multisets have a structure different from the ones mentioned in Proposition 4.1.2. If both blocks as multisets have exceptional structure mod m^*, then in view of Remark 4.5.1 there exists a block preserving permutation for each

block such that $\sum_i ia_i \equiv m/4 \pmod{m^*}$, thus $m^* \mid R_1 + R_2$ holds. Finally, we can also achieve this relation if exactly one of the blocks has exceptional structure, and the permutational sum of the other block admits the value $m/4 \bmod m^*$.

Suppose that $m \mid R_1 + R_2$ does not hold, otherwise we are done. Apply the braid trick and consider the pairs $(a_i, a_{i+2^{k-1}n})$. They must have the same parity, otherwise transposing them would make Φ divisible by m, which would complete the proof. Due to the separability of the initial order, all elements must have the same parity.

Consider now the pairs $(a_i, a_{i+2^{k-2}n})$. Either we can transpose the elements of such a pair to achieve a zero permutational sum, or the elements must have the same residue mod 2^2. Apply this argument consecutively with exponent $s = 1, 2, \ldots k$, for pairs $(a_i, a_{i+2^{k-s}n})$ and modulo 2^{k-s}, respectively. Either $m \mid \Phi$ is obtained during this process by a suitable transposition of a pair $(a_i, a_{i+2^{k-s}n})$ or all elements must have the same residue r mod 2^k.

If r is odd, then M has homogeneous exceptional structure described in Proposition 4.1.2. If r is even, then 2^k would divide Φ, for $\Phi \equiv r\frac{2^k(2^k-1)}{2} \pmod{2^k}$. Thus the conclusion of the theorem holds in this case.

The remaining part of the proof is the case when only one of the blocks is exceptional mod m^*, and the permutational sum of the other block does not admit the value $m/4 \pmod{m^*}$. We refer to this latter condition by (**), and we may suppose that the second block is the exceptional one (otherwise we reverse the sequence). According to Proposition 4.1.2, there are two cases to consider.

4.5.1. The inhomogeneous case

$T_2 = \{a, a, \ldots, a, q_1 = a + b, q_2 = a - b\} \bmod m^*$, where a is even and $(b, m) = 1$. Note that T_2 contains both even and odd elements. Due to the separability of the initial order, all elements in T_1 have the same parity.

If T_1 consists of odd elements, then we exchange a pair of different odd elements mod m^*, one from each block. This way T_2 becomes non-exceptional. Moreover, an appropriate choice from $\{q_1, q_2\}$ ensures that T_1 does not become exceptional either.

Thus m^* will be a divisor of the permutational sum after a suitable block preserving permutation. If $m \mid \Phi$ does not hold, we apply the braid trick for a pair (a_i, a_{i+m^*}) for which their parity differs and we are done.

If all elements of T_1 are even, then we try to transpose a pair of different even elements mod m^*, one from each block. Note that if it is possible, T_1 will not become exceptional. Hence after a block preserving permutation m^* will be a divisor of the permutational sum. If $m \mid \Phi$ did not hold, we apply the braid trick for a pair (a_i, a_{i+m^*}) for which their parity differs and we are done.

Assume that no appropriate transposition exists, that is, T_1 must consist of even elements having the same residue a mod m^*. It may occur that M has the inhomogeneous exceptional structure. Otherwise either $q_1 + q_2 = 2a + m^*$, or there exists a pair $a^{(1)} \not\equiv a^{(2)} \pmod{m}$ in M such that $a^{(1)} \equiv a^{(2)} \equiv a \pmod{m^*}$.

We set the permutation now for these cases. Let q_1 and q_2 be in the positions 1 and $1 + m^*$. Fix arbitrary positions for the rest of elements supposing that if a pair of type $\{a^{(1)}, a^{(2)}\}$ exists, then the elements of such a pair are consecutive. Hence either we are done, or $\Phi \equiv m^* \pmod{m}$. In the latter case, note that there must exist a pair of type $\{a^{(1)}, a^{(2)}\}$ that is arranged consecutively. Their transposition provides a zero permutational sum which completes the proof.

4.5.2. The homogeneous case

$T_2 = \{c, c, \ldots, c\}$ mod 2^{k-1} where c is odd and (**) holds for T_1.

Subcase 1) Every odd element $c' \in T_1$ is congruent to c mod 2^{k-1}. Since T_1 is not exceptional mod m^*, it must contain some even elements. Thus T_1 consists of even elements and possibly also some odd elements having residue c mod 2^{k-1}. Choose an even element q_1 from T_1 and transpose it with c in T_2. Since (**) holds for T_1, neither T_1 nor T_2 become exceptional by this transposition.

Take a permutation of each block for which the permutational sum is zero mod m^*. Either we are done or $\Phi \equiv m^* \pmod{m}$ holds. Look at the pairs $(a_i, a_i + m^*)$ according to the braid trick. If a pair takes different residues mod 2, then their

transposition makes the permutational sum divisible by m and we are done. Otherwise we must have two even elements, and the others have residue c mod 2^{k-1}. Hence Lemma 4.4.2 completes the proof.

Subcase 2) There exists an odd $c' \in T_1$ for which $c' \not\equiv c \pmod{2^{k-1}}$. We transpose c and c' to obtain $T_2' = \{c', c, \ldots, c\} \pmod{2^{k-1}}$. We claim that $m^* \mid \Phi$ holds for the new blocks T_1' and T_2' after a suitable block preserving permutation.

The permutational sum of T_2' admits the value $m/4$ mod m^*. Indeed, it has a non-exceptional structure, hence it admits the value zero mod m^*, and then one transposition between c' and another element is sufficient. Thus, neither (**) holds for T_2' nor has it exceptional structure. Hence we may suppose that $m^* \mid \Phi$ holds for the new blocks T_1' and T_2'. Either we are done or $\Phi \equiv m^* \pmod{m}$. In the latter case we need a transposition in T_2' between c' and another element congruent to c mod 2^{k-1}, for which the permutation sum changes by m^* mod m. Such a transposition clearly exists.

4.6 Abelian groups and sumsets - related topics

In combinatorial number theory, one of the classical subfields is the so called zero-sum theory. Let G be a finite abelian group written additively. A typical zero-sum problem studies conditions which guarantee that a given multiset M of group elements have a non-empty sub-multiset (for which some extra conditions may hold) such that the sum of the elements of the sub-multiset is zero.

Probably the most natural question in this area is related to the Davenport constant. For a finite abelian group G, $D(G)$ denotes the least integer l for which any multiset $\{g_1, \ldots, g_l\}$ of G contains a sub-multiset where the sum of the elements equals zero. In spite of its relevance in algebraic number theory [42], the exact behavior of $D(G)$ is still not known in general. Another variant of this problem allows to consider only sets instead of multisets, and hence studies the least integer l for which any set $\{g_1, \ldots, g_l\}$ of G contains a subset where the sum of the elements equals zero. This number is the so-called Olson constant.

For more details we refer to [4, 16, 24, 31, 41].

A classical result in this area is the Erdős-Ginzburg-Ziv theorem [32], mentioned already in the first introductory chapter, in which the zero-sum sub-multisets has prescribed size $|G|$.

THEOREM 4.6.1 (Erdős-Ginzburg-Ziv). *Let G be an arbitrary finite abelian group of order n. Then every multiset M of size $2n-1$ contains a sub-multiset of size n such that the sum of the elements equals zero. The condition on the size of M is tight.*

We note that this theorem was originally proved for cyclic groups only, but it is not difficult to deduce the generalization. The inverse problem is to characterize all multisets of size $2n-2$ without a zero-sum sub-multiset of size n.

Grynkiewicz in [48] went much further: he proved that in an s element multiset in $\mathbb{Z}_n$, $2n-2 \leq s \leq 6\frac{1}{3}n$ there exist at least

$$\binom{\lfloor \frac{s}{2} \rfloor}{n} + \binom{\lceil \frac{s}{2} \rceil}{n}$$

sub-multisets zero-sum sub-multisets of size n. This was conjectured by Bialostocki [17] for any s, proved by Kisin for prime powers [69], and known asymptotically for fixed n and $s \to \infty$ due to Füredi and Kleitman [38]. Notice that this would be sharp in general, since the multiset containing 0s and 1s, $\lfloor s/2 \rfloor$ and $\lceil s/2 \rceil$ times, respectively, attains the bound.

This inverse approach inspires the following generalization.

PROBLEM 4.6.2. *Let R be a commutative ring and $P(x_1, \ldots, x_n)$ be an n-variate (homogeneous) polynomial over R. Determine the minimal cardinality $m(R, P)$ for which the following holds: for every multiset M of R, $|M| = m$, probably under some extra conditions, there exists a sub-multiset $\{a_1, \ldots, a_n\}$ for which $P(a_1, \ldots, a_n) = 0$.*

For $R = \mathbb{Z}_n$, $P = x_1 + \ldots + x_n$, the Erdős-Ginzburg-Ziv theorem claims that the corresponding minimal cardinality is $m = 2n - 1$.

Another conjecture of Bialostocki [17] is strongly related to Theorem 4.1.3 and the Erdős-Ginzburg-Ziv theorem as well.

CONJECTURE 4.6.3. *Suppose that $a_1, \ldots, a_n$, and $b_1, \ldots, b_n$ are sequences of elements from $\mathbb{Z}_n$, satisfying $\sum_{i=1}^n a_i = \sum_{i=1}^n b_i = 0$. If n is even, then there exists a permutation α such that $\sum_{i=1}^n a_i b_{\alpha(i)} = 0$.*

Clearly, the condition on the parity of n is necessary: Theorem 4.1.1 shows that if n is odd and the sequence (b_i) consists of distinct elements then $\sum_{i=1}^n b_i = 0$ holds, whereas there is no such permutation for the exceptional multisets introduced in Section 4.1. On the other hand, the sequence consisting of distinct elements does not fulfill the condition if n is even.

If true, this conjecture would imply a recent theorem of Grynkiewicz [46] (at least in the case when n is even), which can be considered as a remarkable generalization of the Erdős-Ginzburg-Ziv theorem and a special case of Problem 4.6.2. This was conjectured before by Caro [23].

THEOREM 4.6.4. *[Grynkiewicz, weighted Erdős-Ginzburg-Ziv] Let $b_1, \ldots, b_n$ be elements of $\mathbb{Z}_n$ such that $\sum_{i=1}^n b_i = 0$ holds. If M is a multiset of $\mathbb{Z}_n$ of size $2n-1$, then there exists a sub-multiset $M' = \{a_1, \ldots, a_n\} \subset M$ and a permutation α of the elements of M' such that $\sum_{i=1}^n a_i b_{\alpha(i)} = 0$.*

Note that in the formulation of Problem 4.6.2, this theorem gives an upper bound on the minimal cardinality for all linear n-variate polynomials $P(\mathbf{x})$ over $\mathbb{Z}_n$ for which $P(\mathbf{1}) = 0$.

This conjecture of Caro turned considerable attention to various weighted subsequence sum questions, which provides a natural formulation for our main result, too. Let $M = \{a_1, a_2, \ldots, a_n\}$ be a multiset of $\mathbb{Z}_n$ and consider the elements $w_i : i \in [1, n]$ as integer (not necessarily distinct) weights. The sum

$$\sum_{a_i \in M} a_i w_{\pi(i)}$$

is called a weighted sum of M via the permutation $\pi \in Sym(n)$. Since a weighted sum depends only on the weights' congruence classes $\pmod n$, we may suppose that actually $w_i \in [0, n-1]$ for all i. Hence the most obvious weight set to consider (besides the constant weight set, which is essentially equivalent to the Erdős-Ginzburg-Ziv Theorem) is the set of elements of $\mathbb{Z}_n$. The result of this chapter

describes those multisets, where zero cannot be achieved as a value of the weighted sum.
Very recently, Grynkiewicz, Philipp and Ponomarenko [49] proved a theorem, which can be viewed as an extension of Theorem 4.1.1. They considered arbitrary finite abelian groups G, and asked for necessary and sufficient conditions on multisets for which any $g \in G$ is attained as a value of a weighted sum of $W = \{0, 1, \ldots |G| - 1\}$.

THEOREM 4.6.5 (Grynkiewicz, Philipp, Ponomarenko). *If some $g \in G$ is not attained as a value of a weighted sum of $W = \{0, 1, \ldots |G| - 1\}$, then either*

- *every element of M comes from a coset of a proper subgroup of G, or*
- *G is the Klein group and M consists of all elements of the group, or*
- *G is cyclic and M is of the form $\{a, a, \ldots, a, a+b, a-b\}$ where b is a generator of G.*

Our Theorem 4.1.3 refines and completes the above characterization when G is a cyclic group of even order. On the other hand, in the odd order case, Theorem 4.1.1 easily implies the following corollary concerning Problem 4.6.2.

COROLLARY 4.6.6. *Let $R = \mathbb{Z}_n$, $P(\boldsymbol{x}) = x_1 + 2x_2 + \ldots + nx_n$. For every multiset M of R, $|M| = m(\mathbb{Z}_n, P) = n + 1$, there exists a sub-multiset $\{a_1, \ldots, a_n\}$ for which $P(a_1, \ldots, a_n) = 0$. (That is, the minimal cardinality is $n + 1$.)*

We supplement this chapter with a list of some open problems, more precisely, with a generalization of Bialostocki's Conjecture 4.6.3, which was closely related to the chapter's main result.

Consider a complete bipartite graph $K_{n,n}$. We associate an element of $\mathbb{Z}_n$ to each vertex. The weight of an edge is simply the product of the two values associated to the endvertices, and a weight of a matching is the sum of the weights of the edges in the matching. We call $x \in \mathbb{Z}_n$ *permitted* if there exists a perfect matching (PM) of weight x.

General Problem: describe the structure of the set H consisting of the elements of $\mathbb{Z}_n$ that are permitted in the above sense.

More specific problems are the following ones. Give conditions which imply that

a) H is the whole set $\mathbb{Z}_n$

b) H contains 0.

c) $K_{n,n}$ can be partitioned into n PMs which have distinct weights.

Note that if one vertex color class of $K_{n,n}$ is the set $\mathbb{Z}_n$, we get back to Theorem 4.6.5 and Theorems 4.1.1, 4.1.3, in case a) and case b), respectively.

On the other hand, Conjecture 4.6.3 asserts that if n is even and $\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} b_i = 0 \pmod{n}$ holds for the elements associated to the color classes, then b) holds.

Case c) appears to be widely open. It is easy to give necessary conditions such as $\sum a_i \sum b_i = \sum_{g \in \mathbb{Z}_n} g$ must hold. That is, if n is odd, $\sum a_i \sum b_i = 0 \pmod{n}$, if n is even, $\sum a_i \sum b_i = n/2 \pmod{n}$. If n is a prime, it seems reasonable to think that polynomial techniques may help to deduce a necessary and sufficient condition on the multisets at least in the case when one color class of $K_{n,n}$ is associated to the set of elements of $\mathbb{Z}_n$.

Chapter 5

Quantitative Nullstellensatz and applications concerning Dyson-type polynomials and their q-analogues

5.1 Introduction

In this chapter, we summarize an approach which turned out to be effective in solving conjectures concerning constant term identities, and seems to be useful in several other fields as well.

Our main tool will be a variant of the Combinatorial Nullstellensatz, which enables us to determine the coefficients of maximal monomials of a multivariate polynomial exactly by a simple sum formula, if the polynomial is evaluated on a Cartesian product of large enough sets. This formula appeared recently in the papers of Lasoń [73] and of Karasev and Petrov [64], later generalized in [68]. The statement, already formulated and proved in the second chapter (Theorem 2.1.8) is the following.

THEOREM 5.1.1. *Let $\mathbb{F}$ be a field, and let $P \in \mathbb{F}[x_1, x_2, \ldots, x_m]$ be a multivariate polynomial for which $\deg(P) \leq d_1 + d_2 + \ldots + d_m$. Take an arbitrary set system $A_1, A_2, \ldots, A_m$ such that $A_i \subseteq \mathbb{F}$ and $|A_i| = d_i + 1$. Then the coefficient of $\prod x_i^{d_i}$ is*

$$\sum_{z_1 \in A_1} \sum_{z_2 \in A_2} \sum_{z_m \in A_m} \frac{P(z_1, z_2, \ldots z_m)}{\phi_1'(z_1)\phi_2'(z_2)\cdots\phi_m'(z_m)},$$

where $\phi_i(x) = \prod_{a \in A_i}(x - a)$.

Although we will use this form, we mention that a similar theorem still holds if we want to express the coefficient of any maximal monomial $\prod x_i^{d_i}$ of a polynomial P. That is, for monomials where there is no monomial $\prod_{i=1}^{k} x_i^{\delta_i}$ of P such that $\delta_i \geq d_i$ for all i aside from $\prod x_i^{d_i}$ itself, just as in Remark 2.1.3.

The key to apply Theorem 5.1.1 effectively is to reduce the seemingly difficult evaluation of the sum which is equal to the coefficient. To this end, some combinatorial observations enable us to choose the arbitrary set system $A_1, A_2, \ldots, A_m$ in such a way that the vast majority of the summands vanish. In fact, optimal choice of the sets provides that all but one of the summands vanish in several cases when some symmetries in the polynomial P can be exploited combinatorially.

To present the phenomenon, we introduce the theory of q-analogue identities and provide a very short proof for an ex-conjecture of Andrews [8], first proven by Bressoud and Zeilberger [98] in an essentially combinatorial however slightly complicated way. Then we demonstrate the strength of the method by reproving many known constant term identities, a long-standing conjecture and their common generalization.

5.2 The Dyson-identity and the q-analogue

Let $x_1, \ldots, x_n$ denote independent variables, each x_i associated with a nonnegative integer a_i. In 1962, motivated by a problem in statistical physics Dyson [29] formulated the hypothesis that the constant term of the Laurent polynomial

$$\prod_{1 \leq i \neq j \leq n} \left(1 - \frac{x_i}{x_j}\right)^{a_i}$$

is equal to a certain multinomial coefficient.

THEOREM 5.2.1 (Dyson-identity). *The constant term of*

$$P_{\mathcal{D}}(\boldsymbol{x}, \boldsymbol{a}) := \prod_{1 \leq i \neq j \leq n} \left(1 - \frac{x_i}{x_j}\right)^{a_i}$$

is equal to

$$\frac{(a_1 + a_2 + \cdots + a_n)!}{a_1! \cdot a_2! \cdots a_n!}.$$

Independently Gunson [unpublished] and Wilson [95] confirmed the statement in the same year, then Good gave an elegant proof [45] using Lagrange interpolation. (Wilson later received the Nobel Prize for his outstanding contributions to mathematical physics.)

Let q denote yet another independent variable. In 1975 Andrews [8] suggested the following q-analogue of Dyson's conjecture:

THEOREM 5.2.2 (q-Dyson-identity). *The constant term of the Laurent polynomial*

$$Q_{\mathcal{D}}(\boldsymbol{x}, \boldsymbol{a}) := \prod_{1 \le i < j \le n} \left(\frac{x_i}{x_j}\right)_{a_i} \left(\frac{q x_j}{x_i}\right)_{a_j} \in \mathbb{Q}(q)[\boldsymbol{x}, \boldsymbol{x}^{-1}]$$

must be

$$\frac{(q)_{a_1+a_2+\cdots+a_n}}{(q)_{a_1} (q)_{a_2} \dots (q)_{a_n}}.$$

Here $(t)_k$ denotes the q-shifted factorial, also known as the q-Pochhammer-symbol, that is, $(t)_k = (1-t)(1-tq)\dots(1-tq^{k-1})$ with $(t)_0$ defined to be 1. Recall that the Pochhammer symbol of parameter k is simply the falling factorial $x(x-1)\cdots(x-k+1)$ in strong connection with the binomial coefficient $\binom{x}{k}$ and with hypergeometric series.

Specializing at $q = 1$, Andrews' conjecture gives back that of Dyson.

Despite several attempts [57, 87, 88] the problem remained unsolved until 1985, when Zeilberger and Bressoud [98] found a combinatorial proof. Shorter proofs for the equal parameter case $a_1 = a_2 = \ldots = a_n$ are due to Habsieger [51], Kadell [58] and Stembridge [89]. A shorter proof of the Zeilberger–Bressoud theorem, manipulating formal Laurent series, was given by Gessel and Xin [43].

Following up a recent idea of Karasev and Petrov [64] we present a very short combinatorial proof.

First note that if $a_i = 0$ for some i, then we may omit all factors that include the variable x_i without affecting the constant term of $Q_{\mathcal{D}}$. Accordingly, we may

assume that each a_i is a positive integer. Let σ denotes the sum of all a_is, that is, $\sigma = \sum_{i=1}^{n} a_i$. Consider the homogeneous polynomial

$$F(x_1, x_2, \ldots, x_n) = \prod_{1 \le i < j \le n} \left(\prod_{t=0}^{a_i - 1} (x_j - x_i q^t) \cdot \prod_{t=1}^{a_j} (x_i - x_j q^t) \right) \in \mathbb{Q}(q)[\mathbf{x}].$$

Clearly, the constant term of $Q_{\mathcal{D}}(\mathbf{x})$ is equal to the coefficient of $\prod_i x_i^{\sigma - a_i}$ in the polynomial $F(\mathbf{x})$. Since F is homogeneous, this term will be of maximal degree.

Now we are to apply Theorem 5.1.1. The idea is to take $\mathbb{F} = \mathbb{Q}(q)$ with a suitable choice of the sets A_i such that F vanishes for all but one element in $A_1 \times \cdots \times A_n$. To this end, we want to choose A_i so that the cardinality is $|A_i| = \sigma - a_i + 1$, and would like to guarantee that the product $\prod_{1 \le i < j \le n} \left(\prod_{t=0}^{a_i - 1} (x_j - x_i q^t) \cdot \prod_{t=1}^{a_j} (x_i - x_j q^t) \right)$ vanishes for the largest possible amount of n-tuples $(x_1, x_2, \ldots x_n) = (c_1, c_2, \ldots, c_n) \in A_1 \times \cdots \times A_n$.

This aim motivates the choice $A_i = \{1, q, \ldots, q^{\sigma - a_i}\}$ for all $i \in [1, n]$. Here and thereafter $[u, v]$ stands for the set of integers ℓ satisfying $u \le \ell \le v$, and ${}_qM$ stands for the set of q-powers of a set $M = \{m_1, m_2, \ldots\}$, that is, ${}_qM = \{q^{m_1}, q^{m_2}, \ldots\}$. Using these notations, $A_i = {}_q[0, \sigma - a_i]$.

Let us introduce the notation $\sigma_i := \sum_{j=1}^{i-1} a_j$. Thus, $\sigma_1 = 0$ and $\sigma_{n+1} = \sigma$. The following proposition provides a combinatorial argument to reveal why this choice is the right one to exploit the symmetries of the polynomial.

PROPOSITION 5.2.3. *For $\mathbf{c} \in A_1 \times \cdots \times A_n$ we have $F(\mathbf{c}) = 0$, unless $c_i = q^{\sigma_i}$ for all i.*

Proof. Suppose that $F(\mathbf{c}) \neq 0$ for the numbers $c_i = q^{\alpha_i} \in A_i$. Here α_i is an integer satisfying $0 \le \alpha_i \le \sigma - a_i$. Then for each pair $j > i$, either $\alpha_j - \alpha_i \ge a_i$, or $\alpha_i - \alpha_j \ge a_j + 1$. In other words, $\alpha_j - \alpha_i \ge a_i$ holds for every pair $j \neq i$, with strict inequality if $j < i$. In particular, all of the α_i are distinct.

Consider the unique permutation π satisfying $\alpha_{\pi(1)} < \alpha_{\pi(2)} < \cdots < \alpha_{\pi(n)}$. Adding up the inequalities $\alpha_{\pi(i+1)} - \alpha_{\pi(i)} \ge a_{\pi(i)}$ for $i = 1, 2 \ldots, n-1$ we obtain

$$\alpha_{\pi(n)} - \alpha_{\pi(1)} \ge \sum_{i=1}^{n-1} a_{\pi(i)} = \sigma - a_{\pi(n)}.$$

Given that $\alpha_{\pi(1)} \geq 0$ and $\alpha_{\pi(n)} \leq \sigma - a_{\pi(n)}$, strict inequality is excluded in all of these inequalities. It follows that π must be the identity permutation and $\alpha_i = \alpha_{\pi(i)} = \sum_{j=1}^{i-1} a_{\pi(j)} = \sigma_i$ must hold for every $i = 1, 2, \ldots, n$. This proves the statement. $\square$

This way finding the constant term of $Q_{\mathcal{D}}$ is reduced to the evaluation of

$$\frac{F(q^{\sigma_1}, q^{\sigma_2}, \ldots, q^{\sigma_n})}{\phi_1'(q^{\sigma_1})\phi_2'(q^{\sigma_2}) \ldots \phi_n'(q^{\sigma_n})},$$

where $\phi_i(z) = (z-1)(z-q)\ldots(z-q^{\sigma-a_i})$.

Thus one rather simple calculation will imply the result of Theorem 5.2.2.

$$\begin{aligned} F(q^{\sigma_1}, q^{\sigma_2}, \ldots, q^{\sigma_n}) &= \prod_{1 \leq i < j \leq n} \left(\prod_{t=0}^{a_i - 1} q^{\sigma_i + t}(q^{\sigma_j - \sigma_i - t} - 1) \cdot \prod_{t=1}^{a_j} q^{\sigma_i}(1 - q^{\sigma_j - \sigma_i + t}) \right) \\ &= (-1)^u q^v \prod_{1 \leq i < j \leq n} \left(\frac{(q)_{\sigma_j - \sigma_i}}{(q)_{\sigma_j - \sigma_{i+1}}} \cdot \frac{(q)_{\sigma_{j+1} - \sigma_i}}{(q)_{\sigma_j - \sigma_i}} \right) \\ &= (-1)^u q^v \prod_{i=1}^{n} \frac{(q)_{\sigma_i} (q)_{\sigma - \sigma_i}}{(q)_{\sigma_{i+1} - \sigma_i}}, \end{aligned}$$

with $u = \sum_{i=1}^{n} (n-i)a_i$ and $v = \sum_{i=1}^{n} \left((n-i)a_i\sigma_i + (n-i)\binom{a_i}{2} + \sigma_i(\sigma - \sigma_{i+1}) \right)$, while

$$\begin{aligned} \phi_i'(q^{\sigma_i}) &= \prod_{t=0}^{\sigma_i - 1} (q^{\sigma_i} - q^t) \cdot \prod_{t=\sigma_i + 1}^{\sigma - a_i} (q^{\sigma_i} - q^t) \\ &= \prod_{t=0}^{\sigma_i - 1} q^t(q^{\sigma_i - t} - 1) \cdot \prod_{t=1}^{\sigma - \sigma_{i+1}} q^{\sigma_i}(1 - q^t) \\ &= (-1)^{\sigma_i} q^{\tau_i} (q)_{\sigma_i} (q)_{\sigma - \sigma_{i+1}} \end{aligned}$$

with $\tau_i = \binom{\sigma_i}{2} + \sigma_i(\sigma - \sigma_{i+1})$.

In order to get the desired identity, we prove first that the powers of (-1) and q cancel out. Indeed, $u = \sum_{i=1}^{n} (n-i)a_i = \sum_{i=1}^{n} \sigma_i$ is straightforward since $\sum_{i=1}^{n} \sigma_i = \sum_{i=1}^{n} \sum_{j=1}^{i-1} a_j$.

The powers of q similarly cancel out due to the following observation, which implies $v = \sum_{i=1}^{n} \tau_i$.

PROPOSITION 5.2.4.

$$\sum_{i=1}^{n}(n-i)\left(a_i\sigma_i+\binom{a_i}{2}\right)=\sum_{i=1}^{n}\binom{\sigma_i}{2}.$$

Proof. We proceed by a routine induction on n. When $n=0$, both expressions are 0, and one readily checks the relation

$$\sum_{i=1}^{n}\left(a_i\sigma_i+\binom{a_i}{2}\right)=\binom{\sigma_{n+1}}{2},$$

which completes the induction. □

Putting everything together we obtain that the constant term of $Q_{\mathcal{D}}$ is indeed

$$\begin{aligned}\frac{F(q^{\sigma_1},q^{\sigma_2},\dots,q^{\sigma_n})}{\phi_1'(q^{\sigma_1})\phi_2'(q^{\sigma_2})\dots\phi_n'(q^{\sigma_n})}&=\prod_{i=1}^{n}\frac{(q)_{\sigma_i}(q)_{\sigma-\sigma_i}}{(q)_{\sigma_i}(q)_{\sigma-\sigma_{i+1}}(q)_{\sigma_{i+1}-\sigma_i}}\\&=\frac{(q)_{\sigma}}{\prod_{i=1}^{n}(q)_{\sigma_{i+1}-\sigma_i}}\\&=\frac{(q)_{a_1+a_2+\cdots+a_n}}{(q)_{a_1}(q)_{a_2}\dots(q)_{a_n}}.\end{aligned}$$

Finally, we mention that Dyson's identity implies also the identity of Dixon [94].

THEOREM 5.2.5.

$$\sum_{l=-a_1}^{a_1}(-1)^l\binom{a_1+a_2}{l+a_2}\binom{a_2+a_3}{l+a_3}\binom{a_3+a_1}{l+a_1}=\frac{(a_1+a_2+a_3)!}{a_1!\cdot a_2!\cdot a_3!}$$

holds for any non-negative integers a_1,a_2,a_3.

Proof. Consider the Dyson identity for $n=3$. We will show that

$$\sum_{l=-a_1}^{a_1}(-1)^l\binom{a_1+a_2}{a_1+l}\binom{a_2+a_3}{a_2+l}\binom{a_3+a_1}{a_3+l}$$

expresses the constant term in

$$\prod_{1\le i\ne j\le 3}\left(1-\frac{x_i}{x_j}\right)^{a_i}.$$

Introducing new variables z_{12}, z_{23}, z_{31} as $z_{ij} := \frac{x_i}{x_j}$, the Dyson product transforms to

$$\prod_{1\le i\neq j\le 3}\left(1-\frac{x_i}{x_j}\right)^{a_i} =$$

$$= \left(1-\frac{x_1}{x_2}\right)^{a_1}\left(1-\frac{x_2}{x_1}\right)^{a_2}\left(1-\frac{x_1}{x_3}\right)^{a_1}\left(1-\frac{x_3}{x_1}\right)^{a_3}\left(1-\frac{x_2}{x_3}\right)^{a_2}\left(1-\frac{x_3}{x_2}\right)^{a_3} =$$

$$= (-1)^{a_1+a_2+a_3}\times\frac{(1-z_{12})^{a_1+a_2}}{z_{12}^{a_2}}\times\frac{(1-z_{23})^{a_2+a_3}}{z_{23}^{a_3}}\times\frac{(1-z_{31})^{a_3+a_1}}{z_{31}^{a_1}}.$$

Taking into consideration that $z_{12}\cdot z_{23}\cdot z_{31}=1$, a term in the latter form contributes to the constant term if and only if we gain a product of form

$$\frac{z_{12}^{l+a_2}}{z_{12}^{a_2}}\frac{z_{23}^{l+a_3}}{z_{23}^{a_3}}\frac{z_{31}^{l+a_1}}{z_{31}^{a_1}},$$

for some integer l, $|l|\le\min\{a_1,a_2,a_3\}$. Applying the binomial theorem, we get exactly the desired result. □

5.3 Generalizations and q-analogues

The aforementioned Dyson-identity can be considered as a special case of a large family of constant term identities corresponding to multivariate Laurent polynomials. Let $x_0, x_1, \ldots, x_n$ be independent variables. We consider Laurent polynomials of form

$$P(x_0,x_1,\ldots,x_n) := \prod_{0\le i\neq j\le n}\left(1-\frac{x_i}{x_j}\right)^{\beta_{ij}}.$$

Our main aim is to determine the constant term of these kinds of polynomials by a closed formula. This goal does not seem feasible in general, however there are certain subfamilies of polynomials, where our approach turns out to be fruitful.

To make the notations more transparent we introduce the $(n+1)\times(n+1)$ square matrix $\mathbf{B}$ with rows and columns numbered from 0 to n, corresponding to the exponents of the variables (in natural order) in P, as follows.

NOTATION 5.3.1. *Using* $\boldsymbol{x} := (x_1, \ldots, x_n)$, $\mathbf{B} = ((\beta_{ij}))$,

$$P(x_0,\ \boldsymbol{x}, \mathbf{B}) := \prod_{0 \le i \ne j \le n} \big(1 - \frac{x_i}{x_j}\big)^{\beta_{ij}}.$$

It is assumed that the entries of $\mathbf{B}$ are nonnegative integers, and all the diagonal entries are zero. The formula puts an emphasis on the variable x_0, since the row and column corresponding to x_0 often looks different from the ones corresponding to the other variables. In fact, P is considered to be independent of x_0 in some cases - when we take the corresponding row and column to be allzero, or simply omit it -, while the dependence from x_0 has special nature as we will see later on. Using this notation, the matrix associated to the Dyson product is

$$\boldsymbol{B}_{\mathcal{D}} = \left(\begin{array}{c|ccccc} 0 & 0 & 0 & 0 & \ldots & 0 \\ \hline 0 & 0 & a_1 & a_1 & \ldots & a_1 \\ 0 & a_2 & 0 & a_2 & \ldots & a_2 \\ 0 & a_3 & a_3 & 0 & \ldots & a_3 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & a_n & a_n & a_n & \ldots & 0 \end{array}\right).$$

Constant term identities and their generalizations are intimately related to Selberg's integral formula [86]. Colloquially referred to as the Selberg integral, it asserts

$$\begin{aligned} S_n(\alpha, \beta, \gamma) &:= \int_0^1 \ldots \int_0^1 \prod_{i=1}^n t_i^{\alpha-1}(1-t_i)^{\beta-1} \prod_{1 \le i < j \le n} |t_i - t_j|^{2\gamma} dt_1 \ldots dt_n \\ &= \prod_{j=0}^{n-1} \frac{\Gamma(\alpha + j\gamma)\Gamma(\beta + j\gamma)\Gamma(1 + (j+1)\gamma)}{\Gamma(\alpha + \beta + (n+j-1)\gamma)\Gamma(1+\gamma)}, \end{aligned}$$

where the complex parameters α, β, γ satisfy

$$\Re(\alpha) > 0,\ \Re(\beta) > 0,\ \Re(\gamma) > -\min\{1/n, \Re(\alpha)/(n-1), \Re(\beta)/(n-1)\}.$$

The continued interest in the Selberg integral, demonstrated for example by the most recent article [81], is due to its role in random matrix theory, statistical mechanics, special function theory among other fields; see the comprehensive exposition [35].

Properly speaking, the motivation of Dyson came from statistical physics, as he proposed to replace Wigner's classical Gaussian-based random matrix models by

what now is known as the circular ensembles. The study of their joint eigenvalue probability density functions led him to the Dyson-identity.

One of the most important classical mechanical systems (of finite dimensional phase space) is the so called Calogero-Moser-Sutherland model, describing a quantum many-body system. It influenced the study of further Dyson type identities.

We first recall the constant term identity of Morris [77] which has turned out to be equivalent to the Selberg integral. It can be interpreted as a generalization of a special case of the Dyson-identity, where an additional variable x_0 is also considered in the Laurent polynomial, while the exponents $a_i = k$ for each $i \in [1, n]$. It asserts that if we consider the Laurent polynomial

$$\begin{aligned} P_{\mathcal{M}}(x_0, \boldsymbol{x}; a, b, k) :&= \prod_{j=1}^{n} \big(1 - \frac{x_j}{x_0}\big)^a \big(1 - \frac{x_0}{x_j}\big)^b \cdot P_{\mathcal{D}}(\boldsymbol{x}; k \cdot \mathbf{1}) \\ &= \prod_{j=1}^{n} \big(1 - \frac{x_j}{x_0}\big)^a \big(1 - \frac{x_0}{x_j}\big)^b \prod_{1 \le i \ne j \le n} \left(1 - \frac{x_i}{x_j}\right)^k \end{aligned}$$

of nonnegative integer parameters a, b, k, the constant term can be determined as

$$\mathrm{CT}\left[P_{\mathcal{M}}(x_0, \boldsymbol{x}; a, b, k)\right] = \prod_{j=0}^{n-1} \frac{(a+b+kj)!(kj+k)!}{(a+kj)!(b+kj)!k!}.$$

Using

$$M(n; a, b, k) := \prod_{j=0}^{n-1} \frac{(a+b+kj)!(kj+k)!}{(a+kj)!(b+kj)!k!},$$

and the matrix $\boldsymbol{B}_{\mathcal{M}}$

$$\boldsymbol{B}_{\mathcal{M}} = \left(\begin{array}{c|cccccc} 0 & b & b & b & \dots & b \\ \hline a & 0 & k & k & \dots & k \\ a & k & 0 & k & \dots & k \\ a & k & k & 0 & \dots & k \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a & k & k & k & \dots & 0 \end{array}\right)$$

associated to the Laurent polynomial $P_{\mathcal{M}}$, we get

THEOREM 5.3.2 (Morris-identity, [77]). $\mathrm{CT}\left[P(x_0,\boldsymbol{x};\boldsymbol{B}_{\mathcal{M}})\right]=M(n;a,b,k)$.

Since then, several generalizations and extensions were revealed.

In 1987, introducing an extra $t_1\cdots t_m$ factor into the integrand Aomoto [10] proved an extension of the Selberg integral. Based on the fundamental theorem of calculus, it yields besides Anderson's [7] one of the simplest known proofs of the Selberg integral itself. Turned into a constant term identity, Aomoto's integral reads as

$$\mathrm{CT}\left[\prod_{j=1}^{n}\left(1-\frac{x_j}{x_0}\right)^{a+\chi(j\le m)}\left(1-\frac{x_0}{x_j}\right)^{b}\cdot P_{\mathcal{D}}(\mathbf{x};k\cdot\mathbf{1})\right]=$$
$$\prod_{j=0}^{n-1}\frac{(a+b+kj+\chi(j\ge n-m))!(kj+k)!}{(a+kj+\chi(j\ge n-m))!(b+kj)!k!},$$

where $\chi(S)$ is equal to 1 if the statement S is true and 0 otherwise.

Introducing the corresponding matrix

$$\boldsymbol{B}_{\mathcal{A}}=\left(\begin{array}{c|ccc|ccc}
0 & b & \dots & b & b & \dots & b\\
\hline
a & 0 & \dots & k & k & \dots & k\\
\vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots\\
a & k & \dots & 0 & k & \dots & k\\
\hline
a+1 & k & \dots & k & 0 & \dots & k\\
\vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots\\
a+1 & k & \dots & k & k & \dots & 0
\end{array}\right),$$

where the last m rows/columns are separated, we may formulate

THEOREM 5.3.3 (Aomoto-identity, [10]).

$$\mathrm{CT}\left[P(x_0,\boldsymbol{x};\boldsymbol{B}_{\mathcal{A}})\right]=\prod_{j=0}^{n-1}\frac{(a+b+kj+\chi(j\ge n-m))!(kj+k)!}{(a+kj+\chi(j\ge n-m))!(b+kj)!k!}.$$

The q-analogue of the above identity which also implies a q-version of Selberg's integral formula conjectured by Askey [12] was first established by Kadell [58].

Forrester, examining the wavefunction of a generalized Calogero-Moser-Sutherland model, initiated the study of a different extension of the Morris-identity 5.3.2. Consider the Laurent polynomial

$$P_{\mathcal{F}}(x_0,\boldsymbol{x};n_0;a,b,k)=P_{\mathcal{M}}(x_0,\boldsymbol{x};a,b,k)\cdot\prod_{n_0<i\ne j\le n}\left(1-\frac{x_i}{x_j}\right),$$

corresponding to the matrix

$$\boldsymbol{B}_{\mathcal{F}} = \left(\begin{array}{c|ccc|ccc} 0 & b & \dots & b & b & \dots & b \\ \hline a & 0 & \dots & k & k & \dots & k \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a & k & \dots & 0 & k & \dots & k \\ \hline a & k & \dots & k & 0 & \dots & k+1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a & k & \dots & k & k+1 & \dots & 0 \end{array}\right),$$

where the last $n - n_0$ rows/columns are separated.

Conjecture 5.3.4 (Forrester conjecture, [34]).

$$\mathrm{CT}\left[P_{\mathcal{F}}(x_0, \boldsymbol{x}; n_0; a, b, k)\right] =$$
$$= M(n_0; a, b, k) \times \prod_{j=0}^{n-n_0-1} \frac{(j+1)(a+b+kn_0+(k+1)j)!(kn_0+(k+1)j+k)!}{(a+kn_0+(k+1)j)!(b+kn_0+(k+1)j)!k!}.$$

While Kadell established the q-analogue of the Aomoto-identity [58], and recently Xin and Zhou also claimed an elementary proof [101] for it, the conjecture of Forrester and its q-analogue have been resolved only in some particular cases, despite several further attempts [13, 15, 44, 52, 60, 61, 62, 63].

In the forthcoming section, using our Nullstellensatz-like approach, we prove the q-analogue of the Aomoto-identity and the conjectured identity of Forrester, which implicitly imply the original versions as well. Moreover, we present our main result

concerning the overlay of matrices $\boldsymbol{B}_{\mathcal{A}}$ and $\boldsymbol{B}_{\mathcal{F}}$ when $m \geq n-n_0$, that is, the matrix

$$\boldsymbol{B}_{\mathcal{AF}} = \left(\begin{array}{c|ccc|ccc|ccc} 0 & b & \dots & b & b & \dots & b & b & \dots & b \\ \hline a & 0 & \dots & k & k & \dots & k & k & \dots & k \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a & k & \dots & 0 & k & \dots & k & k & \dots & k \\ \hline a+1 & k & \dots & k & 0 & \dots & k & k & \dots & k \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a+1 & k & \dots & k & k & \dots & 0 & k & \dots & k \\ \hline a+1 & k & \dots & k & k & \dots & k & 0 & \dots & k+1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a+1 & k & \dots & k & k & \dots & k & k+1 & \dots & 0 \end{array}\right) \begin{array}{c} 0 \\ \hline 1 \\ \vdots \\ n-m \\ \hline n-m+1 \\ \vdots \\ n_0 \\ \hline n_0+1 \\ \vdots \\ n \end{array}$$

and derive the q-analogue of a constant term identity corresponding to $P(x_0, \boldsymbol{x}; \boldsymbol{B}_{\mathcal{AF}})$ which includes both the Aomoto- and the Forrester-identity.

5.4 The proof of the general identity

Recall that $(t)_k = (1-t)(1-tq)\dots(1-tq^{k-1})$ denotes the q-Pochhammer symbol.

NOTATION 5.4.1. *Using* $\boldsymbol{x} := (x_1, \dots, x_n)$, $\mathbf{B} = ((\beta_{ij}))$,
$Q(x_0, \ \boldsymbol{x}, \mathbf{B})$ *denotes the Laurent polynomial corresponding to the q-analogue of the Laurent polynomial*

$$P(x_0, \ \boldsymbol{x}, \mathbf{B}) = \prod_{0 \leq i \neq j \leq n} \left(1 - \frac{x_i}{x_j}\right)^{\beta_{ij}},$$

that is,

$$Q(x_0, \ \boldsymbol{x}, \mathbf{B}) := \prod_{0 \leq i < j \leq n} \left(\frac{x_i}{x_j}\right)_{\beta_{ij}} \left(\frac{qx_j}{x_i}\right)_{\beta_{ji}}.$$

The main result is the following

THEOREM 5.4.2. *Let n be a positive integer. For arbitrary nonnegative integers a, b, k and $m, n_0 \leq n \leq m + n_0$,*

$$\mathrm{CT}[Q(x_0, \boldsymbol{x}; \boldsymbol{B}_{\mathcal{AF}})] =$$

$$= \prod_{j=0}^{n-1} \frac{(q)_{a+b+kj+\chi(j>n_0)(j-n_0)+\chi(j\geq n-m)}(q)_{kj+\chi(j>n_0)(j-n_0)+k}}{(q)_{a+kj+\chi(j>n_0)(j-n_0)+\chi(j\geq n-m)}(q)_{b+kj+\chi(j>n_0)(j-n_0)}(q)_k} \times \prod_{j=1}^{n-n_0} \frac{1-q^{(k+1)j}}{1-q^{k+1}}.$$

When $m = 0$, this proves Baker and Forrester's conjecture [13, Conjecture 2.1], and further specializing at $q = 1$, Forrester's original conjecture as well. The $n_0 = n$ case gives the following q-analogue of Aomoto's identity.

COROLLARY 5.4.3. *[q-Aomoto identity] Let n be a positive integer. For arbitrary nonnegative integers a, b, k and $m \leq n$,*

$$\mathrm{CT}[Q(x_0, \boldsymbol{x}; \boldsymbol{B}_{\mathcal{A}})] = \prod_{j=0}^{n-1} \frac{(q)_{a+b+kj+\chi(j\geq n-m)}(q)_{kj+k}}{(q)_{a+kj+\chi(j\geq n-m)}(q)_{b+kj}(q)_k}.$$

We will follow the guidance of the proof of the q-Dyson identity, Section 5.1. Let us introduce the homogeneous polynomial

$$F_q(x_0, \boldsymbol{x}; \boldsymbol{B}) := \prod_{0\leq i<j\leq n} \Bigg(\prod_{t=0}^{\beta_{ij}-1} (x_j - q^t x_i) \times \prod_{t=1}^{\beta_{ji}} (x_i - q^t x_j) \Bigg),$$

with $\boldsymbol{B} = \boldsymbol{B}_{\mathcal{AF}}$. Clearly $\mathrm{CT}[Q(x_0, \boldsymbol{x}; \boldsymbol{B}_{\mathcal{AF}})]$ equals the coefficient of $\prod_j x_j^{B_j}$, where $B_j = \sum_i \beta_{ij}$ in the polynomial $F_q(x_0, \boldsymbol{x}; \boldsymbol{B}_{\mathcal{AF}})$. Note that

$$\prod_j x_j^{B_j} = x_0^{an+m} \prod_{j=1}^{n} x_j^{b+(n-1)k+(n-n_0-1)\chi(j>n_0)}$$

is a monomial of maximum degree in the polynomial $F_q(x_0, \boldsymbol{x}; \boldsymbol{B}_{\mathcal{AF}})$, hence we can apply Theorem 5.1.1 with a suitably chosen system of sets $\{A_j, j = 0 \dots n\}$ for which $|A_j| = B_j + 1$ for every j.

For some technical reasons, we assume first that $k > a$.

5.4.1 The choice for the multisets A_i

NOTATION 5.4.4. *Let γ_i be defined as $\gamma_i = \beta_{in}$ for $0 \leq i < n$ and let $\Delta_t = \sum_{i=0}^{t} \gamma_i$. We introduce the intervals I_t denoting $I_t = [\Delta_t - \gamma_t + 1, \Delta_t] = [\Delta_{t-1} + 1, \Delta_t]$.*

Observe that

$$\gamma_0 = b,\ \gamma_1 = \cdots = \gamma_{n_0} = k,\ \gamma_{n_0+1} = \cdots = \gamma_{n-1} = k+1$$

and $\beta_{ij} = \gamma_{\min\{i,j\}}$ for $1 \le i \ne j \le n$.

Note also, that the intervals $I_0, I_1, \ldots, I_{n-1}$ are mutually disjoint. The sets A_i are defined in the form

$$A_j = \{q^0\} \cup \bigcup_{t=0}^{n-1} {}_q[\Delta_t - \gamma_{\min\{t,j\}} + 1, \Delta_t] \subseteq \{q^0\} \cup \bigcup_{t=0}^{n-1} {}_qI_t = {}_q[0, \Delta_{n-1}]$$

for $1 \le j \le n$ and

$$A_0 = \{q^0\} \cup \bigcup_{t=0}^{n-1} {}_q[\Delta_t - b + 1, \Delta_t - b + \beta_{t+1,0}].$$

Since we assume that $k > a$, A_0 is an ordinary set (as well as the other A_is).

Then $|A_i| = B_i + 1$ holds for every $0 \le i \le n$.

5.4.2 The combinatorics

We start with an easy observation on the structure of polynomial

$$F_q(x_0, \boldsymbol{x}; \boldsymbol{B}) := \prod_{0 \le i < j \le n} \left(\prod_{t=0}^{\beta_{ij}-1} (x_j - q^t x_i) \times \prod_{t=1}^{\beta_{ji}} (x_i - q^t x_j) \right).$$

Claim 5.4.5. *Suppose that $c_i = q^{\alpha_i}$ for some integers α_i such that $F_q(c_0, \boldsymbol{c}; \boldsymbol{B}) \ne 0$. Let $j > i$. Then $\alpha_j \ge \alpha_i$ implies $\alpha_j \ge \alpha_i + \beta_{ij}$, and $\alpha_i > \alpha_j$ implies $\alpha_i \ge \alpha_j + \beta_{ji} + 1$. Both statements are valid even if the corresponding entry in $\boldsymbol{B}$ is zero.* □

We are to show that

$$F(c_0, \ldots, c_n) = 0$$

holds for $F = F_q(.; \boldsymbol{B}_{\mathcal{AF}})$ for all but one selection of elements $c_i \in A_i$, namely when $c_0 = 1$, $c_i = q^{\Delta_{i-1}}$ for $1 \le i \le n$.

This statement is verified by the juxtaposition of the following two lemmas.

LEMMA 5.4.6. *Let* $\alpha_0 = 0$. *If* $F(c_0, c_1, \ldots, c_n) \neq 0$, *then* $\alpha_i = \Delta_{i-1}$ *for every* $1 \leq i \leq n$.

LEMMA 5.4.7. *If* $\alpha_0 \neq 0$, *then* $F(c_0, \ldots, c_n) = 0$.

One key to each is the following consequence of Claim 5.4.5.

LEMMA 5.4.8. *Suppose that* $F(c_0, \ldots, c_n) \neq 0$. *Then for every* $1 \leq t \leq n-1$ *there is at most one index* $1 \leq i \leq n$ *such that* $\alpha_i \in I_t$.

Proof. Assume that, on the contrary, there is a pair $1 \leq i \neq j \leq n$ such that $\alpha_i, \alpha_j \in I_t$. Let $\alpha_j \geq \alpha_i$, then it follows from Claim 5.4.5 that $\alpha_j - \alpha_i \geq k$. The length of I_t is $\gamma_t \in \{k, k+1\}$. Thus, it must be $\gamma_t = k+1$, $\alpha_i = \Delta_t - k$ and $\alpha_j = \Delta_t$. Consequently, $t > n_0$, $i < j$ and $i \leq n_0$. Therefore $\Delta_t - \gamma_{\min\{t,i\}} + 1 = \Delta_t - k + 1$ and $\alpha_i \notin A_i$, a contradiction. □

Proof of Lemma 5.4.6. For every $1 \leq i \leq n$ we have $\alpha_i \geq \alpha_0$, therefore $\alpha_i \geq \beta_{0i} = b$ by Claim 5.4.5. Moreover, $k > a \geq 0$ implies that $\alpha_1, \ldots, \alpha_n$ are all distinct, thus it follows from Lemma 5.4.8 that each of the intervals $I_0, I_1, \ldots, I_{n-1}$ contains precisely one of them. Let $\pi \in Sym_n$ denote the unique permutation for which $\alpha_{\pi(1)} < \cdots < \alpha_{\pi(n)}$, then $\alpha_{\pi(i)} \in I_{i-1}$. By Claim 5.4.5 we have

$$\alpha_{\pi(i+1)} \geq \alpha_{\pi(i)} + \beta_{\pi(i),\pi(i+1)} + \chi(\pi(i) > \pi(i+1)).$$

Consequently,

$$\alpha_{\pi(n_0+1)} \geq b + kn_0 + \sum_{i=1}^{n_0} \chi(\pi(i) > \pi(i+1)) \geq \Delta_{n_0} + \sum_{i=1}^{n_0} \chi(\pi(i) > \pi(i+1)).$$

Since $\alpha_{\pi(n_0+1)} \leq \Delta_{n_0}$, it follows that $\alpha_{\pi(1)} = b$, $\pi(1) < \cdots < \pi(n_0+1)$, and $\beta_{\pi(i),\pi(i+1)} = k$ for $1 \leq i \leq n_0$. This in turn implies that $\pi(n_0) \leq n_0$, thus $\pi(i) = i$ and $\alpha_i = \Delta_{i-1}$ for $1 \leq i \leq n_0$.

Now for $n_0 < i < n$ we have $\pi(i), \pi(i+1) > n_0$ and thus $\beta_{\pi(i),\pi(i+1)} = k+1$. Restricting π to the set $[n_0+1, n]$ and starting with $\alpha_{\pi(n_0+1)} = \Delta_{n_0}$, a similar argument completes the proof. □

Proof of Lemma 5.4.7. Assume that, contrary to the statement, $F(c_0, \ldots, c_n) \neq 0$.

Since $\alpha_0 \neq 0$, $\alpha_0 \in \bigcup_{t=0}^{n-1} {}_q[\Delta_t - b + 1, \Delta_t - b + \beta_{t+1,0}]$, that is,

$$\Delta_u - b + 1 \leq \alpha_0 \leq \Delta_u - b + \beta_{u+1,0}.$$

It is implied by Lemma 5.4.8 that at most $n-1-u$ of the distinct numbers $\alpha_1, \ldots, \alpha_n$ can lie in the interval $[\Delta_{u+m_0}+1, \Delta_{n-1}]$. Thus, at least $u+1$ of the numbers $\alpha_1, \ldots, \alpha_n$ satisfy $\alpha_j \leq \Delta_u$.

Furthermore, if α_j lies in the interval

$$T_{uj} = [\Delta_u - b + \beta_{u+1,0} - \beta_{j0}, \Delta_u]$$

for some $1 \leq j \leq n$, then $\alpha_0 - \beta_{j0} \leq \alpha_j \leq \alpha_0 + \beta_{0j} - 1$ and there is a term of the form $x_j - q^t x_0$ or $x_0 - q^t x_j$ in F which attains 0 when evaluated at the point $(c_0, \boldsymbol{c})$.

It follows that at least $u+1$ of the numbers α_j satisfy $\alpha_j \leq \Delta_u - b + \beta_{u+1,0} - \beta_{j0} - 1$. This is clearly impossible if $u+1 \leq n-m$, for then $\Delta_u - b + \beta_{u+1,0} - \beta_{j0} - 1 \leq uk - 1$ in view of $n - m \leq n_0$, and on the other hand the difference between any two such α_j is at least k in view of Claim 5.4.5. Thus, $u \geq n-m$ and $\beta_{u+1,0} = a+1$. Consider

$$\alpha_{\nu(1)} < \cdots < \alpha_{\nu(u+1)} \leq \Delta_u - b + \beta_{u+1,0} - \beta_{\nu(u+1),0} - 1 \leq \Delta_u - b.$$

If $u \leq n_0$, then it must be $\alpha_{\nu(i)} = (i-1)k$ and $\nu(1) < \cdots < \nu(u+1)$, but then $\nu(u+1) \geq u+1 > n-m$, $\beta_{\nu(u+1),0} = a+1$, implying $\alpha_{\nu(u+1)} \in T_{u,\nu(u+1)}$, which is absurd. This means that $u \geq n_0 + 1$. It is easy to see that $\alpha_{\nu(i+1)} - \alpha_{\nu(i)} \geq \gamma_{\nu(i)}$ for $i \leq u$, thus $\alpha_{\nu(u+1)} \geq \sum_{i=1}^{u} \gamma_{\nu(i)} \geq \Delta_u - b$. Therefore $\sum_{i=1}^{u} \gamma_{\nu(i)} = \Delta_u - b$, which implies that $\{\nu(1), \ldots, \nu(u)\} \supseteq \{1, \ldots, n_0\}$. Consequently, $\nu(u+1) \geq n_0+1 > n-m$, which leads to a contradiction as before. □

5.4.3 The computation

It only remains to evaluate

$$\frac{F_q(q^0, q^{\Delta_0}, \ldots, q^{\Delta_{n-1}}; \boldsymbol{B})}{\psi_0 \psi_1 \ldots \psi_n}, \tag{4.1}$$

where

$$\psi_j = \prod\nolimits_{\alpha \in A_j \setminus \{\Delta_{j-1}\}} (q^{\Delta_{j-1}} - q^{\alpha})$$

for $j = 1, \dots n$, and with the shorthand notation $\Delta_u^v = \gamma_u + \cdots + \gamma_v = \Delta_v - \Delta_{u-1}$,

$$\psi_0 = \prod_{t=0}^{n-1} \prod_{\alpha=\Delta_1^t+1}^{\Delta_1^t+\beta_{t+1,0}} (1-q^\alpha) = \prod_{j=1}^{n} \left[\Delta_1^{j-1}+1, \Delta_1^{j-1}+\beta_{j0}\right]_q . \tag{4.2}$$

From now on, $[u,v]_q := (1-q^u)\dots(1-q^v) = (q)_v/(q)_{u-1}$, with $[u,u]_q$ abbreviated as $[u]_q$. Both the numerator and the denominator in (4.1) is the product of factors in the form $\pm q^u(1-q^v)$ with some non-negative integers u, v. More precisely, collecting factors of a similar nature together we find that the numerator is the product of the factors

$$(-1)^{\gamma_0} \times q^{1+\cdots+(\gamma_0-1)} \times \left[\Delta_1^{j-1}+1, \Delta_0^{j-1}+\beta_{j0}\right]_q \quad \text{for} \quad 1 \le j \le n, \tag{4.3}$$

$$(-1)^{\gamma_i} \times q^{\Delta_{i-1}+\cdots+(\Delta_{i-1}+\gamma_i-1)} \times \left[\Delta_i^{j-1}-\gamma_i+1, \Delta_i^{j-1}\right]_q \quad \text{for} \quad 1 \le i < j \le n, \tag{4.4}$$

and

$$q^{\gamma_i\Delta_{i-1}} \times \left[\Delta_i^{j-1}+1, \Delta_i^{j-1}+\gamma_i\right]_q \quad \text{for} \quad 1 \le i < j \le n. \tag{4.5}$$

In the denominator, besides (4.2) we have the factors

$$(-1) \times [\Delta_{j-1}]_q \times \psi_{j_<} \times \psi_{j_=} \times \psi_{j_>} \quad \text{for} \quad 1 \le j \le n, \tag{4.6}$$

where

$$\psi_{j_<} = \prod_{t=0}^{j-2} (-1)^{\gamma_t} \times q^{(\Delta_t-\gamma_t+1)+\cdots+\Delta_t} \times \left[\Delta_{t+1}^{j-1}, \Delta_{t+1}^{j-1}+\gamma_t-1\right]_q , \tag{4.7}$$

$$\psi_{j_=} = (-1)^{\gamma_{j-1}-1} \times q^{(\Delta_{j-1}-\gamma_{j-1}+1)+\cdots+(\Delta_{j-1}-1)} \times [1, \gamma_{j-1}-1]_q , \tag{4.8}$$

and

$$\psi_{j_>} = \prod_{t=j}^{n-1} q^{\gamma_j\Delta_{j-1}} \times \left[\Delta_j^t-\gamma_j+1, \Delta_j^t\right]_q . \tag{4.9}$$

Now the powers of -1 and q cancel out due to the simple identity

$$n\gamma_0 + \sum_{1\le i<j\le n} \gamma_i = n + \sum_{0\le t<j-1\le n-1} \gamma_t + \sum_{1\le j\le n} (\gamma_{j-1}-1)$$

and the somewhat more subtle

$$n\binom{\gamma_0}{2} + \sum_{1\le i<j\le n} \left(2\gamma_i\Delta_{i-1} + \binom{\gamma_i}{2}\right)$$
$$= \sum_{0\le t<j-1\le n-1} \left(\gamma_t\Delta_t - \binom{\gamma_t}{2}\right) + \sum_{j=1}^{n} \left((\gamma_{j-1}-1)\Delta_{j-1} - \binom{\gamma_{j-1}-1}{2}\right) + \sum_{0\le j-1<t\le n-1} \gamma_j\Delta_{j-1}.$$

It remains to deal with the factors of the form $[u,v]_q$. Those from (4.4) and (4.9) cancel out. Those from (4.3) and (4.2) yield

$$\prod_{j=1}^{n}\frac{(q)_{\Delta_0^{j-1}+\beta_{j0}}}{(q)_{\Delta_1^{j-1}+\beta_{j0}}}=\prod_{j=0}^{n-1}\frac{(q)_{a+b+kj+\chi(j>n_0)(j-n_0)+\chi(j\geq n-m)}}{(q)_{a+kj+\chi(j>n_0)(j-n_0)+\chi(j\geq n-m)}}. \tag{4.10}$$

As for the rest, the contribution from (4.5) and (4.7) with the substitution $t+1=i$ gives

$$\begin{aligned}\prod_{1\leq i<j\leq n}\frac{\left[\Delta_i^{j-1}+1,\Delta_i^{j-1}+\gamma_i\right]_q}{\left[\Delta_i^{j-1},\Delta_i^{j-1}+\gamma_{i-1}-1\right]_q}&=\prod_{1\leq i<j\leq n}\frac{\left[\Delta_i^{j-1},\Delta_i^{j-1}+\gamma_i\right]_q\cdot\left[\Delta_i^{j-1}+\gamma_{i-1}\right]_q}{\left[\Delta_i^{j-1},\Delta_i^{j-1}+\gamma_{i-1}\right]_q\cdot\left[\Delta_i^{j-1}\right]_q}\\&=\prod_{j=2}^{n}\frac{\left[\Delta_1^{j-1},\Delta_1^{j-1}+\gamma_1\right]_q}{\left[\Delta_1^{j-1},\Delta_1^{j-1}+\gamma_0\right]_q}\times\Psi\times\prod_{1\leq i<j\leq n}\frac{\left[\Delta_{i-1}^{j-1}\right]_q}{\left[\Delta_i^{j-1}\right]_q}\\&=\prod_{j=2}^{n}\frac{(q)_{\Delta_1^{j-1}+\gamma_1}}{(q)_{\Delta_1^{j-1}+\gamma_0}}\times\Psi\times\prod_{j=2}^{n}\frac{[\Delta_{j-1}]_q}{1-q^{\gamma_{j-1}}}\end{aligned} \tag{4.11}$$

in the first place, where the factor

$$\Psi=\prod_{j=n_0+2}^{n}\left[\Delta_{n_0+1}^{j-1}+\gamma_{n_0+1}\right]_q=\prod_{j=2}^{n-n_0}(1-q^{(k+1)j})$$

only occurs when $n_0>0$. Combining (4.11) with the contribution of the factors $[\Delta_{j-1}]_q=1-q^{\Delta_{j-1}}$ from (4.6) and the factors $[1,\gamma_{j-1}-1]_q=(q)_{\gamma_{j-1}-1}$ from (4.8), shifting indices we obtain

$$\prod_{j=1}^{n-1}\frac{(q)_{\Delta_1^{j}+\gamma_1}}{(q)_{\Delta_1^{j}+\gamma_0}}\times\prod_{j=0}^{n-1}\frac{1}{(q)_{\gamma_j}}\times\left(\prod_{j=2}^{n-n_0}(1-q^{(k+1)j})\right)^{\chi(n_0>0)},$$

in agreement with

$$\frac{(q)_{kj+\chi(j>n_0)(j-n_0)+k}}{(q)_{b+kj+\chi(j>n_0)(j-n_0)}(q)_k}\times\prod_{j=1}^{n-n_0}\frac{1-q^{(k+1)j}}{1-q^{k+1}}. \tag{4.12}$$

Putting together (4.10) and (4.12) completes the proof of Theorem 5.4.2 in the case $k>a$. Avoiding this restriction, we extend it in the next subsection.

5.4.4 The rationality result

The extension of the result that includes all non-negative integers for the parameter k depends on the following rationality lemma, inspired by [44, Proposition 2.4].

Recall that $Q_{\mathcal{D}}(\boldsymbol{x}; k \cdot \mathbf{1})$ denotes the q-analogue of the Laurent polynomial $P_{\mathcal{D}}(\boldsymbol{x}; k \cdot \mathbf{a})$ corresponding to the special case when $a_i = k$ for all i,in the Dyson identity (and also the special case $a = b = 1$ of the Morris identity).

LEMMA 5.4.9. *Fix nonnegative integers r_i, s_i for $1 \leq i \leq n$, satisfying $\sum r_i = \sum s_i$. There exists a rational function $R = R(z) \in \mathbb{Q}(q)(z)$ that depends only on n and the numbers r_i, s_i such that*

$$\mathrm{CT}\left[\frac{x_1^{r_1} \dots x_n^{r_n}}{x_1^{s_1} \dots x_n^{s_n}} Q_{\mathcal{D}}(\boldsymbol{x}; k \cdot \mathbf{1})\right] = R(q^k) \frac{(q)_{nk}}{(q)_k^n}.$$

Proof. The constant term of $Q_{\mathcal{D}}(\boldsymbol{x}; k \cdot \mathbf{1})$ equals the coefficient of $\prod x_i^{(n-1)k}$ in the polynomial

$$F_q(\boldsymbol{x}) = \prod_{1 \leq i < j \leq n} \left(\prod_{t=0}^{k-1} (x_j - q^t x_i) \times \prod_{t=1}^{k} (x_i - q^t x_j) \right).$$

Set $A_i = {}_q[0, (n-1)k]$. Then $F_q(\boldsymbol{c}) = 0$ for every $\boldsymbol{c} \in A_1 \times \cdots \times A_n$ except when $c_i = q^{(i-1)k}$ for every i. According to Lemma 2.1.8,

$$\mathrm{CT}[Q_{\mathcal{D}}(\boldsymbol{x}; k \cdot \mathbf{1})] = \frac{F_q(q^0, q^k, \dots, q^{(n-1)k})}{\psi_1 \psi_2 \dots \psi_n} = \frac{(q)_{nk}}{(q)_k^n},$$

$$\text{where} \quad \psi_i = \prod\nolimits_{0 \leq j \leq (n-1)k, j \neq (i-1)k} (q^{(i-1)k} - q^j).$$

We compare this product to the constant term in the lemma, which equals the coefficient of $\prod x_i^{(n-1)k+s_i}$ in the polynomial $F_q^*(\boldsymbol{x}) = x_1^{r_1} \dots x_n^{r_n} F_q(\boldsymbol{x})$. Accordingly we set

$$A_i^* = {}_q[0, (n-1)k + s_i]$$

and note that for $\boldsymbol{c} \in A_1^* \times \cdots \times A_n^*$ we have $F_q^*(\boldsymbol{c}) \neq 0$ if and only if the exponents α_i are all distinct and

$$\alpha_{\pi(i+1)} \geq \alpha_{\pi(i)} + k + \chi(\ \pi(i) > \pi(i+1)\ )$$

holds for $1 \leq i \leq n-1$ with the unique permutation $\pi = \pi_{\boldsymbol{c}} \in Sym_n$ satisfying

$$\alpha_{\pi(1)} < \cdots < \alpha_{\pi(n)}.$$

Consequently, $\alpha_i = (\pi^{-1}(i) - 1)k + \epsilon_i$ for some $\epsilon_i = \epsilon_i(\boldsymbol{c}) \in [0, s_{\pi(n)}]$.

Set $\mathcal{C} = \{\boldsymbol{c} \in A_1^* \times \cdots \times A_n^* \mid F_q^*(\boldsymbol{c}) \neq 0\}$, and write $s = \max s_i$. It follows that

$$|\mathcal{C}| \leq n! \binom{s+n}{n}.$$

Moreover, the set $\mathcal{S} = \{(\pi_{\boldsymbol{c}}, \epsilon_1(\boldsymbol{c}), \ldots \epsilon_n(\boldsymbol{c})) \mid \boldsymbol{c} \in \mathcal{C}\}$ is independent of k; it depends only on n and the numbers s_i. It follows from Lemma 2.1.8 that, using the notation $\tau = \pi^{-1}$,

$$\mathrm{CT}\left[\frac{x_1^{r_1} \ldots x_n^{r_n}}{x_1^{s_1} \ldots x_n^{s_n}} \mathcal{D}_q(\boldsymbol{x}; k)\right] = \sum_{\boldsymbol{c} \in \mathcal{C}} \prod_{i=1}^{n} q^{((\tau(i)-1)k+\epsilon_i)r_i} \frac{F(\ldots, q^{(\tau(i)-1)k+\epsilon_i}, \ldots)}{\psi_1^* \psi_2^* \ldots \psi_n^*}$$

where

$$\psi_{\pi(i)}^* = \prod\nolimits_{0 \leq j \leq (n-1)k+s_{\pi(i)}, j \neq (i-1)k+\epsilon_{\pi(i)}} (q^{(i-1)k+\epsilon_{\pi(i)}} - q^j).$$

One readily checks that for each $\Sigma = (\pi, \epsilon_1, \ldots, \epsilon_n) \in \mathcal{S}$ there exist rational functions $R_i \in \mathbb{Q}(q)(z)$ that depend only on n, the numbers r_j, s_j and the sequence Σ such that

$$\prod_{i=1}^{n} q^{((\tau(i)-1)k+\epsilon_i)r_i} = R_0(q^k), \quad \frac{\psi_i}{\psi_{\pi(i)}^*} = R_i(q^k) \quad \text{and} \quad \frac{F(\ldots, q^{(\tau(i)-1)k+\epsilon_i}, \ldots)}{F(q^0, q^k, \ldots, q^{(n-1)k})} = R_{n+1}(q^k).$$

The result follows. □

Proof of Theorem 5.4.2, generalizing from $a < k$ to arbitrary k.

Notice that the q-Laurent polynomial in view,

$$Q(x_0, \boldsymbol{x}; \boldsymbol{B}_{\mathcal{AF}}) = \prod_{j=1}^{n} (qx_j)_{a+\chi(j \leq m)} (1/x_j)_b \prod_{n_0 < i < j \leq n} (1 - q^k x_i/x_j)(1 - q^{k+1} x_j/x_i) \cdot Q_{\mathcal{D}}(\boldsymbol{x}; k \cdot \mathbf{1}).$$

Expanding the degree zero part of product

$$\prod_{j=1}^{n} (qx_j)_{a+\chi(j \leq m)} (1/x_j)_b \prod_{n_0 < i < j \leq n} (1 - q^k x_i/x_j)(1 - q^{k+1} x_j/x_i)$$

into a sum of monomial terms and applying the above lemma to each such term individually, we find that there is a rational function $R \in \mathbb{Q}(q)(z)$ depending only on the parameters n, m, n_0, a, b such that

$$\mathrm{CT}[Q(x_0, \boldsymbol{x}; \boldsymbol{B}_{\mathcal{AF}})] = R(q^k) \frac{(q)_{nk}}{(q)_k^n}.$$

On the other hand,

$$\prod_{j=0}^{n-1} \frac{(q)_{a+b+kj+\chi(j>n_0)(j-n_0)+\chi(j\geq n-m)}(q)_{kj+\chi(j>n_0)(j-n_0)+k}}{(q)_{a+kj+\chi(j>n_0)(j-n_0)+\chi(j\geq n-m)}(q)_{b+kj+\chi(j>n_0)(j-n_0)}(q)_k} \times \prod_{j=1}^{n-n_0} \frac{1-q^{(k+1)j}}{1-q^{k+1}}$$

can be written in the form

$$R'(q^k)\frac{(q)_{nk}}{(q)_k^n}$$

with a rational function $R' \in \mathbb{Q}(q)(z)$ which also depends only on n, m, n_0, a, b, for $k \geq a+1$. Since $R'(q^k) = R(q^k)$ for every $k \geq a+1$, it follows that $R \equiv R'$, completing the proof. □

5.5 Remarks and variations

We take an overview on related problems and results.

First, let us look back on the framework we used to confirm the identities through q-analogues. If we consider a Laurent polynomial

$$P(x_0, x_1, \ldots, x_n, \boldsymbol{B}) := \prod_{0\leq i\neq j\leq n} \left(1-\frac{x_i}{x_j}\right)^{\beta_{ij}},$$

then obviously the order of the variables does not affect the constant term. However, this is not the case with the q-analogue version, where an asymmetry appears along the order of x_is. Indeed, taking $\left(\frac{x_i}{x_j}\right)_{\beta_{ij}}\left(\frac{x_j}{x_i}\right)_{\beta_{ji}}$ instead of $\left(\frac{x_i}{x_j}\right)_{\beta_{ij}}\left(\frac{x_j}{x_i}q\right)_{\beta_{ji}}$ would result in two essentially identical terms, $(1-\frac{x_i}{x_j})$ and $(1-\frac{x_j}{x_i})$: they both vanish if and only if $x_i = x_j$, providing the same combinatorial information. This explains the convenience of $\left(\frac{x_i}{x_j}\right)_{\beta_{ij}}\left(\frac{x_j}{x_i}q\right)_{\beta_{ji}}$, where no such overlapping occurs.

Several natural questions and problems may arise. First, all the mentioned results correspond to constant terms of Laurent polynomials of form $P(\mathbf{x}, \boldsymbol{B})$. Essentially this is due to symmetry, since this term clearly has a special role compared to other coefficients. It provides a wider range for applications and typically easier ways for the proofs at the same time. However, several papers studied the evaluation of different coefficients of Laurent-polynomials, mostly concerning the Laurent polynomial of Dyson [75, 76, 84]. We should point out here that following the approach of the rationality result (Subsection 5.3.4) is useful in general. Indeed, Lemma 5.4.9

presents a way to express other coefficients using again the Quantitative Nullstellensatz. Generally, one cannot rely on getting only one non-vanishing term as we do get in the proofs, but the number of terms is bounded in terms of the considered degree sequence corresponding to the variables. Note that this idea was independently developed by Doron Zeilberger in [30].

Another problem to consider is to describe the Laurent polynomials, or rather the corresponding matrices $\boldsymbol{B}$, where the approach is applicable. So far we do not know the limits of our method; we do not have a general argument, which, given $\boldsymbol{B}$ as an input, would tell whether the corresponding constant term can be easily evaluated this way. However, we were able to handle basically all matrices, where the combinatorial approach of Zeilberger and Bressoud [98] – built on an improvement of Good's difference-equation proof idea for the Dyson-identity [45] – or the method of Gessel, Lv, Xin and Zhou [43, 44, 96] – based on the idea of proving polynomial identities by pointing out enough values where the two polynomials are equal – were applied. Generally, our approach provides short proofs, which are easy to follow. In addition to the solution to Forrester's problem, it can be also applied to prove various conjectures of Kadell, c.f. [58, 59, 68, 66, 100].

In the proof of Theorem 5.4.2, and in the method of Gessel, Lv, Xin and Zhou as well, one might have to come up with a rationality result, see Lemma 5.4.9 or Proposition 2.4 in [44], to complete the proof. This follows from the fact that we do not allow A_i to be general multisets, only sets in the Quantitative Nullstellensatz. Indeed, A_0 would contain duplicated elements if $k \leq a$ holds. However, the Quantitative Nullstellensatz can be extended to be applicable under these circumstances as well due to Lemma 2.1.12 introduced in the second chapter. For more details we refer to [68].

Finally we present further applications of the Quantitative Nullstellensatz, related to additive combinatorics. Dias da Silva and Hamidoune [27] confirmed the long-standing conjecture of Erdős and Heilbronn [33]. Later, Alon, Nathanson and Ruzsa obtained a proof via the polynomial method, see [1, 6]. For a collection of sets $A_1, \ldots, A_n \subseteq \mathbb{Z}_p$, consider the following restricted sumset:

$$\bigwedge\nolimits_{\mathcal{S}} A_i = \{a_1 + \cdots + a_n \mid a_i \in A_i,\ a_j - a_i \notin S_{ij} \text{ for } i < j\}\,.$$

The theorem can be formulated as follows.

THEOREM 5.5.1. *[27]*

$$\left|\bigwedge\nolimits_{\mathcal{S}} A_i\right| \geq \min\left\{p, n|A| - n^2 + 1\right\},$$

□

A far-reaching generalization was obtained by Hou and Sun [55].

THEOREM 5.5.2. *Let $A_1, \ldots, A_n$ be subsets of a field $\mathbb{F}$ such that $|A_i| = k$ for $1 \leq i \leq n$ and assume that $S_{ij} \subseteq \mathbb{F}$ satisfy $|S_{ij}| \leq s$ for $1 \leq i < j \leq n$. If either* $\mathrm{char}(\mathbb{F}) = 0$ *or*

$$\mathrm{char}(\mathbb{F}) > \max\left\{n\lceil s/2\rceil, n(k-1) - n(n-1)\lceil s/2\rceil\right\},$$

then

$$\left|\bigwedge\nolimits_{\mathcal{S}} A_i\right| \geq n(k-1) - n(n-1)\lceil s/2\rceil + 1.$$

□

Clearly, $s = 0$ and $s = 1$ gives back the conditions of the Cauchy-Davenport and the Erdős- Heilbronn theorem, respectively. This extended result can also be proved by the Quantitative Nullstellensatz [68]. In fact, Lilu Zhao pointed out [99] that this can even be strengthened in the following way.

THEOREM 5.5.3. *Let $A_1, \ldots, A_n$ be subsets of a field $\mathbb{F}$ such that $|A_i| \in \{k, k+1\}$ for $1 \leq i \leq n$ and assume that $S_{ij} \subseteq \mathbb{F}$ satisfy $|S_{ij}| \leq s$ for $1 \leq i < j \leq n$. If either* $\mathrm{char}(\mathbb{F}) = 0$ *or*

$$\mathrm{char}(\mathcal{F}) > \max\left\{n\lceil s/2\rceil, \sum_{i=1}^{n}(|A_i| - 1) - n(n-1)\lceil s/2\rceil\right\},$$

then

$$\left|\bigwedge\nolimits_{\mathcal{S}} A_i\right| \geq \sum_{i=1}^{n}(|A_i| - 1) - n(n-1)\lceil s/2\rceil + 1.$$

□

His proof is based on the Combinatorial Nullstellensatz and the Aomoto identity, see Theorem 5.4.2.

Chapter 6

Summary

Our work is based on applications of the original strong, and the quantitative versions of Noga Alon's Combinatorial Nullstellensatz. The Combinatorial Nullstellensatz as a delicate, widely applicable polynomial method asserts that the zero locus of a (multivariate) polynomial cannot vanish on a large enough well structured point set. Alon pointed out that this approach is very fruitful and provides elegant proofs in many fields of combinatorics, including additive combinatorics, combinatorial or finite geometry, graph theory and extremal set theory, by finding a connection between the structure of the object in view and the zero locus of corresponding polynomials.

In Section 3, we present a result based on a joint work with András Gács, Tamás Héger and Dömötör Pálvölgyi [39]. The main theorem asserts a connection between the degree and the range of polynomials over a finite field. More precisely, all multisets $M \in GF(q)$ of size q are described which cannot be a range of a polynomial of degree at most $q-1$ or $q-2$. This statement can be formulated also in the language of finite geometries and additive number theory.

As for the additive number theory version, one may investigate extensions by studying the problem for multisets over abelian groups or cyclic groups $\mathbb{Z}_n$ rather than the problem for multisets over cyclic groups $\mathbb{Z}_p$ of prime order p. The result resembles to the one for the former problem: only some well characterized multisets provide exceptions in the corresponding structure theorem. Their description can be find in Section 4, on the basis of [80].

The next problem is connected to the theory of q-analogues. Generally speaking, q-analogue versions are extensions of statements by the introduction of a new parameter q, where the limit transition $q \to 1$ gives back the original assertion.

q-analogue identities date back to Euler and turned out to be very efficient in various combinatorial problems and in applications in statistical physics as well. For example, the Dyson identity has an important role in a quantum many body system model, and its q-analogue is proven by Zeilberger and Bressoud in [98]. The identity of Dyson asserts the following [29]: The constant term of

$$\prod_{1 \le i \ne j \le n} \left(1 - \frac{x_i}{x_j}\right)^{a_i} \quad \text{is} \quad \frac{(a_1 + a_2 + \cdots + a_n)!}{a_1! a_2! \cdots a_n!}.$$

Section 5 is based on a joint work with Gyula Károlyi. We studied the q-analogue of the Dyson-identity, and several similar constant term identities [67, 68]. The main benefit of the proofs is the application of a quantitative version of the Nullstellensatz by determining the constant term of a given multivariate polynomial as an exponentially large sum of substitution values of a function; a sum whose summands can be chosen to vanish for all but one (or a few) substitution values.

The method successfully solved some well-studied conjectures such as the Forrester conjecture [34].

Chapter 7

Összefoglaló - in Hungarian

Munkánkban középpontjában a Noga Alon Kombinatorikus Nullhelytételének [1], illetve ezen eredmény erősebb változatainak alkalmazása áll. A Kombinatorikus Nullhelytétel, mint egy speciális, ugyanakkor általánosan alkalmazható módszer arra épül, hogy számos kombinatorikus struktúra szerkezetét többváltozós polinomok eltűnési helyeivel lehet leírni. Alon rámutatott, hogy a számelmélet, additív kombinatorika, gráfelmélet, halmazrendszerek, véges geometria és más területek számos központi kérdése kezelhető elegáns egyszerű módszerének segítségével.

Az első általunk vizsgált problémát a [39] cikk írja le, ami Gács Andrással, Héger Tamással és Pálvölgyi Dömötörrel közös - ez képezi a 3. fejezet alapját. A főtétel az additív számelmélet, illetve a polinomok elméletének nyelvén is megfogalmazható, és a véges test feletti polinomok foka és értékkészlete közötti összefüggésre mutat rá, nevezetesen leírja azon $GF(q)$ feletti q elemű M multihalmazokat, amelyekhez nem létezik legfeljebb $q-1$ illetve legfeljebb $q-2$ fokú polinom, melyek esetén M az értékkészlet multihalmaza.

A kérdés egy másik irányú általánosítását kapjuk, ha a probléma additív számelméleti megfogalmazásában $\mathbb{Z}_n$ ($n > 1$ egész) feletti multihalmazokat vizsgálunk a prímrendű $GF(p)$ testbeliek helyett. A problémára adható válasz az előzőhöz hasonló: néhány könnyen karakterizálható multihalmaz jelent kivételes struktúrát a struktúratételben, ennek leírását a [80] cikk alapján a 4. fejezetben találhatjuk.

A másik probléma a q-analógiák elméletekhez kapcsolódik. Általánosan tekintve ez

állítások kiterjesztésére vonatkozik, ahol egy új q paraméter bevezetésével $q \to 1$ határátmenetben kapjuk az eredeti tételt.

A q-analóg azonosságok a kombinatorikában is rendkívül hasznosak lehetnek, és Eulerre vezethetőek vissza, azonban számos alkalmazásuk van a statisztikus fizikában is. A [98] cikkben például a Dyson által vizsgált statisztikai fizikus modellben kulcsszerepet játszó azonosság q- változatát bizonyítja igen komplex módon Zeilberger és Bressoud. A Dyson-azonosság a következőt állítja [29]:

$$\prod_{1\le i\neq j\le n}\left(1-\frac{x_i}{x_j}\right)^{a_i} \quad \text{konstans tagja} \quad \frac{(a_1+a_2+\cdots+a_n)!}{a_1!a_2!\cdots a_n!}.$$

Károlyi Gyulával közös cikkeinken alapuló 5. fejezetben ezen állítás q-analógját, valamint hasonló konstans együtthatós azonosságokat vizsgáltunk [67, 68]. A bizonyítások legfőbb erénye, hogy Alon Kombinatorikus Nullhelytételének egy effektív változatával bizonyos többváltozós polinomok konstans együtthatójának meghatározását olyan - exponenciális sok - függvény-helyetteítési értékek összegére vezetjük vissza, amelyekről egy transzformáció után elérhető, hogy egy vagy kevés kivételtől eltekintve, az összes helyettesítési érték nulla legyen. A módszer eredményesnek bizonyult sokat vizsgált sejtések megoldásánál is, mint amilyen a Forrester sejtés [34] volt.

Chapter 8

Bibliography

[1] N. Alon, Combinatorial Nullstellensatz, *Combin. Prob. Comp.* **8** (1999) 7-29.

[2] N. Alon, Additive Latin transversals. *Israel J. Math.* **117** (2000) 125-130.

[3] N. Alon, L. Babai, and H. Suzuki, Multilinear polynomials and Frankl-Ray-Chaudhuri-Wilson type intersection theorems, *Journal of Combinatorial Theory, Series A* **58** (1991) 165-180.

[4] N. Alon, M. Dubiner, Zero-sum sets of prescribed size, *Combinatorics, Paul Erdős is Eighty, Bolyai Soc. Math. Studies*, **1**, (1993) 33-50.

[5] N. Alon, S. Friedland, G. Kalai, Regular subgraphs of almost regular graphs, *J. Combin. Th. Ser. B* **37** (1984) 79-91.

[6] N. Alon, M.B. Nathanson, I.Z. Ruzsa, The polynomial method and restricted sums of congruence classes, *J. Number Th.* **56** (1996) 404-417.

[7] G.W. Anderson, A short proof of Selberg's generalized beta formula, *Forum Math.* **3** (1991) 415-417.

[8] G. E. Andrews, Problems and prospects for basic hypergeometric functions, *Theory and Application of Special Functions*, R. A. Askey, ed., *Academic Press, New York* (1975) 191-224.

[9] G. E. Andrews, q-Series: Their development and application in analysis, number theory, combinatorics, physics, and computer algebra, No. 66. *American Mathematical Soc.*, 1986.

[10] K. Aomoto, Jacobi polynomials associated with Selberg integrals, *SIAM J. Math. Anal.*, **18** (1987) 545-549.

[11] B. Arsovski, The proof of Snevily's conjecture, *Israel J. Math.* **182** (2011) 505-508.

[12] R. Askey, Some basic hypergeometric extensions of integrals of Selberg and Andrews, *SIAM J. Math. Anal.* **11** (1980) 938-951.

[13] T. H. Baker and P. J. Forrester, Generalizations of the q-Morris constant term identity, *J. Combin. Th. A* **81** (1998) 69-87.

[14] S. Ball, O. Serra, Punctured combinatorial Nullstellensätze, Combinatorica, **29** (2009) 511-522.

[15] W. Baratta, Some properties of Macdonald polynomials with prescribed symmetry, *Kyushu J. Math.* **64** (2010) 323-343.

[16] G. Bhowmik , J.C. Schlage-Puchta, An improvement on Olson's constant for $\mathbb{Z}_p \oplus \mathbb{Z}_p$, *Acta Arith.* **141** (2010) 311-319.

[17] A. Bialostocki, Some problems in view of recent developments of the Erdős Ginzburg Ziv theorem, *INTEGERS: Elect. J. Comb. Num. Th.*, **7** (2007) A07.

[18] A. Biró, On polynomials over prime fields taking only two values on the multiplicative group, *Finite Fields Appl.* **6** (2000) 302-308.

[19] A. Blokhuis, On the size of a blocking set in PG(2,p), *Combinatorica* **14** (1994) 273-276.

[20] A. Blokhuis, A new upper bound for the cardinality of 2-distance sets in Euclidean space. *North-Holland Mathematics Studies*, **87** (1984) 65-66.

[21] D. Bressoud, D. Zeilberger , A proof of Andrews's q-Dyson conjecture, *Discrete Math.* **54** (1985) 201-224.

[22] J.R. Britnell, M. Wildon, On types and classes of commuting matrices over finite fields, *J. London Math. Soc.*, **83** (2011) 470-492.

[23] Y. Caro, Zero-sum problems - a survey, *Discrete Math.*, **152** (1996) 93-113.

[24] S. Chapman, On the Davenport's constant, the cross number and their application in factorization theory, *Lecture Notes in Pure and Appl. Math.*, **171** (1995) 167-190.

[25] D. A. Cox, J. B. Little, D. O'Shea Ideals, Varieties, and Algorithms, *Springer* (2007).

[26] S. Dasgupta, Gy. Károlyi, O. Serra, B. Szegedy, Transversals of additive Latin squares, *Israel J. Math.* **126** (2001) 17-28.

[27] J.A. Dias da Silva, Y.O. Hamidoune, Cyclic spaces for Grassmann derivatives and additive theory, *Bull. London Math. Soc.* **26** (1994) 140-146.

[28] Z. Dvir, On the size of Kakeya sets in finite fields, *J. the Amer. Math. Soc.* **22** (2009) 1093-1097.

[29] F. J. Dyson, Statistical theory of energy levels of complex systems, *J. Math. Phys.* **3** (1962) 140-156.

[30] S.B. Ekhad, D. Zeilberger, How to extend Károlyi and Nagy's BRILLIANT proof of the Zeilberger–Bressoud q-Dyson theorem in order to evaluate ANY coefficient of the q-Dyson product, arXiv:1308.2983.

[31] P. van Emde Boas, D. Kruyswijk, A combinatorial problem on finite abelian groups II-III. *Report Math. Centre,* ZW-1969-008 (1969)

[32] P. Erdős, A. Ginzburg, A. Ziv, Theorem in additive number theory, *Bull. Research Council, Israel*, **10F** (1961) 41-43.

[33] P. Erdős, H. Heilbronn, On the addition of residue classes modulo p, *Acta Arith.* **9** (1964), 149-159.

[34] P. J. Forrester, Normalization of the wavefunction for the Calogero–Sutherland model with internal degrees of freedom, *Int. J. Mod. Phys. B* **9** (1995) 1243-1261.

[35] P. J. Forrester, S. O. Warnaar, The importance of the Selberg integral, *Bull. Amer. Math. Soc.*, **45** (2008) 489-534.

[36] P. Frankl, R. M. Wilson, Intersection theorems with geometric consequences. *Combinatorica* **1** (1981) 357-368.

[37] L. Fuchs, Abelian groups, *Budapest, Publishing house of the Hungarian Academy of Sciences,* 1958.

[38] Z. Füredi, D. J. Kleitman, The minimal number of zero sums, *Combinatorics, Paul Erdős is eighty* Vol 1 (1993) 159-172.

[39] A. Gács, T. Héger, Z. L. Nagy and D. Pálvölgyi, Permutations, hyperplanes and polynomials over finite fields, *Finite Fields Appl.*, **16** (2010) 301-314.

[40] W. Gao, A. Geroldinger, Zero-sum problems in finite abelian groups: A survey, *Expo. Math.* **24** (2006) 337-369.

[41] A. Geroldinger, R. Schneider, On Davenport's constant, *J. Combin. Th. A*, **61** (1992) 147-152.

[42] A. Geroldinger, F. Halter-Koch, Non-unique factorizations: Algebraic, combinatorial and analytic theory. *CRC Press*, 2010.

[43] I. M. Gessel and G. Xin, A short proof of the Zeilberger–Bressoud q-Dyson theorem, *Proc. Amer. Math. Soc.* **134** (2006) 2179-2187.

[44] I. Gessel, L. Lv, G. Xin, Y. Zhou, A unified elementary approach to the Dyson, Morris, Aomoto and Forrester constant term identities, *J. Combin Th. A* **115** (2008) 1417-1435.

[45] I. J. Good, Short proof of a conjecture by Dyson, *J. Math. Phys.* **11** (1970) 1884-1884.

[46] D. J. Grynkiewicz, A weighted Erdős Ginzburg Ziv theorem, *Combinatorica,* **26** (2006) 445-453.

[47] D.J. Grynkiewicz, Sumsets, zero-sums and extremal combinatorics, PhD thesis, 2006.

[48] D. J. Grynkiewicz, On the number of m-term zero-sum subsequences,*Acta Arith.* **121** (2006), 275-298.

[49] D. J. Grynkiewicz, A. Philipp, V. Ponomarenko, Aritmethic-progression-weighted subsequence sums, *Israel Journal of Mathematics* **193** (2013) 359-398.

[50] J. Gunson, Proof of a conjecture by Dyson in statistical theory of energy levels, *J. Math. Phys.* **3** (1962) 752-753.

[51] L. Habsieger, Une q-intégrale de Selberg–Askey, *SIAM J. Math. Anal.* **19** (1988) 1475-1489.

[52] S. Hamada, Proof of Baker–Forrester's constant term conjecture for the cases $N_1 = 2, 3$, *Kyushu J. Math.* **56** (2002) 243-266.

[53] D. Hefetz, A. Saluz, H.T.T. Tran, An application of the Combinatorial Nullstellensatz to a graph labelling problem, *J. Graph Theory* **65** (2010) 70-82.

[54] D. Hilbert, Über die vollen Invariantensysteme, *Math. Ann.* **42** (1893) 313-373.

[55] Q.-H. Hou, Z.-W. Sun, Restricted sums in a field, *Acta Arith.* **102** (2002) 239-249.

[56] R. Jamison, Covering Finite Fields with cosets of subspaces, *J. Combin. Th. A*, **22** (1977) 253-266.

[57] K. W. J. Kadell, A proof of Andrews's q-Dyson conjecture for $n = 4$, *Trans. Amer. Math. Soc.* **290** (1985) 127-144.

[58] K. W. J. Kadell, A proof of Askey's conjectured q-analogue of Selberg's integral and a conjecture of Morris, *SIAM J. Math. Anal.* **19** (1988) 969-986.

[59] K.W.J. Kadell, Aomoto's machine and the Dyson constant term identity, *Methods Appl. Anal.* **5** (1998) 335-350.

[60] J. Kaneko, On Forrester's generalization of Morris constant term identity, in: q-series From a Contemporary Perspective (South Hadley, MA, 1998), Contemporary Mathematics, **254** Amer. Math. Soc., Providence, (2000) 271-282.

[61] J. Kaneko, Forrester's constant term conjecture and its q-analogue, in: Physics and Combinatorics (2000) 49-62.

[62] J. Kaneko, Forrester's conjectured constant term identity. II, Ann. Comb. **6** (2002) 383-397.

[63] J. Kaneko, On Baker–Forrester's constant term conjecture, J. Ramanujan Math. Soc. **18** (2003) 349-367.

[64] R. N. Karasev and F. V. Petrov, Partitions of nonzero elements of a finite field into pairs, *Israel J. Math.*, **192** (2012) 143-156.

[65] Gy. Károlyi, An inverse theorem for the restricted est addition in abelian groups, *J. Algebra* **290** (2005) 557-593.

[66] Gy. Károlyi, A. Lascoux, S.O. Warnaar, Constant term identities and Poincaré polynomials, *Trans. Amer. Math. Soc.*, to appear.

[67] Gy. Károlyi, Z. L. Nagy, A simple proof of the Zeilberger - Bressoud q-Dyson theorem, *Proc. Amer. Math. Soc.* **142** (2014), 3007-3011.

[68] Gy. Károlyi, Z. L. Nagy, F. Petrov, V. Volkov, A new approach to constant term identities and Selberg-type integrals, Adv. Math., submitted.

[69] M. Kisin, The number of zero sums modulo m in a sequence of length n, *Mathematika* **41** (1994) 149-163.

[70] G. Kós, T. Mészáros, L. Rónyai, Some extensions of Alon's Nullstellensatz, Publ. Math. Debrecen **79** (2011) 507-519.

[71] G. Kós, L. Rónyai, Alon's Nullstellensatz for multisets, *Combinatorica* **32** (2012) 589-605.

[72] M. Kotowski, M.I. Kotowski, The polynomial method and the Kakeya conjecture, 2012.

[73] M. Lasoń, A generalization of Combinatorial Nullstellensatz, *Elect. J. Combin.* **17** (2010) #N32.

[74] R. Lidl, H. Niederreiter, Finite fields, *Cambridge University Press* (1997).

[75] L. Lv, G. Xin, Y. Zhou, A family of q-Dyson style constant term identities, *J. Combin. Th. A* **116** (2009) 12-29.

[76] L. Lv, G. Xin, Y. Zhou, Two coefficients of the Dyson product. *Elect. J. Combin* **15** (2008).

[77] W. G. Morris, Constant Term Identities for Finite and Affine Root Systems, Ph.D. Thesis, University of Wisconsin, Madison, 1982.

[78] A. Muratović-Ribić, Q. Wang, On a conjecture of polynomial with prescribed range, *Finite Fields Appl.* **18(4)** (2012) 728-737.

[79] A. Muratović-Ribić, Q. Wang, Partitions and Compositions over Finite Fields, *The Elect. J. Comb.*, **20** P34 (2013)

[80] Z. L. Nagy, Permutations over cyclic groups, *Europ. J. Comb.* **41C** (2014) 68-78.

[81] D. Ostrovsky, Selberg integral as a meromorphic function, *Int. Math. Res. Not. IMRN* (2013) 3988-4028.

[82] L. Rédei, Lacunary polynomials over finite fields, *North-Holland Publishing Company*, 1973.

[83] K. Saniee, A Simple Expression for Multivariate Lagrange Interpolation, *SIAM, SIURO*, **1** (2008).

[84] A.V. Sills, Disturbing the Dyson conjecture, in a *generally* GOOD way, *J. Combin. Th. A* **113** (2006) 1368 - 1380.

[85] H. S. Snevily, The Cayley addition table of Z_n, *Amer. Math. Monthly* **106** (1999) 584 - 585.

[86] A. Selberg, Bemerkninger om et multipelt integral, *Norsk Mat. Tidsskr.* **26** (1944) 71-78.

[87] R. P. Stanley, The q-Dyson conjecture, generalized exponents, and the internal product of Schur functions, Combinatorics and Algebra (Boulder, 1983), Contemp. Math. **34**, *Amer. Math. Soc., Providence*, (1984) 81 - 94.

[88] R. P. Stanley, The stable behavior of some characters of $\mathrm{SL}(n,\mathbb{C})$, *Lin. Multilin. Alg.* **16** (1984) 3 - 27.

[89] J. R. Stembridge, A short proof of Macdonald's conjecture for the root systems of type A, *Proc. Amer. Math. Soc.* **102** (1988) 777-786.

[90] P. Sziklai, Applications of polynomials over finite fields, Thesis for the Doctor of the Academy degree (2013).

[91] T. Szőnyi, Blocking sets in Desarguesian affine and projective planes, *Finite Fields Appl.* **3** (1997) 187-202.

[92] T. Tao, V. H. Vu, Additive Combinatorics, *Cambridge University Press*, 2006

[93] S. Vinatier, Permuting the partitions of a prime, *J. Th. Nombres Bordeaux*, **21** (2009) 455-465.

[94] H. Wilf, Generatingfunctionology, *Academic Press, Boston,* (1994).

[95] K. G. Wilson, Proof of a conjecture by Dyson, *J. Math. Phys.* **3** (1962) 1040-1043.

[96] G. Xin, Y. Zhou, A Laurent series proof of the Habsieger–Kadell q-Morris identity, arXiv:1302.6642.

[97] D. Zeilberger, A Stembridge–Stanton style elementary proof of the Habsieger–Kadell q-Morris identity, *Discrete Math.* **79** (1989) 313-322.

[98] D. Zeilberger, D.M. Bressoud, A proof of Andrews' q-Dyson conjecture, *Discrete Math.* **54** (1985) 201-224.

[99] L. Zhao, On restricted sumsets over a field, *Finite Fields Appl.* **28** (2014) 140-147.

[100] Y. Zhou, On Kadell's two conjectures for the q-Dyson product, *Electron. J. Combin.* **18** (2011) #P2.

[101] Y. Zhou, New extensions to the sumsets with polynomial restrictions, arXiv:1202.3190