Combinatorica (2023) 43:1179–1213
https://doi.org/10.1007/s00493-023-00057-0

ORIGINAL PAPER

A Generalization of the Chevalley–Warning and Ax–Katz Theorems with a View Towards Combinatorial Number Theory

David J. Grynkiewicz[1]

Received: 24 February 2023 / Revised: 15 July 2023 / Accepted: 29 July 2023 /
Published online: 29 September 2023

Abstract

Let $\mathbb{F}_q$ be a finite field of characteristic p and order q. The Chevalley–Warning Theorem asserts that the set V of common zeros of a collection of polynomials must satisfy $|V| \equiv 0 \mod p$, provided the number of variables is sufficiently large with respect to the degrees of the polynomials. The Ax–Katz Theorem generalizes this by giving tight bounds for higher order p-divisibility for $|V|$. Besides the intrinsic algebraic interest of these results, they are also important tools in the Polynomial Method, particularly in the prime field case $\mathbb{F}_p$, where they have been used to prove many results in Combinatorial Number Theory. In this paper, we begin by explaining how arguments used by Wilson to give an elementary proof of the $\mathbb{F}_p$ case for the Ax–Katz Theorem can also be used to prove the following generalization of the Ax–Katz Theorem for $\mathbb{F}_p$, and thus also the Chevalley–Warning Theorem, where we allow varying prime power moduli. Given any box $\mathcal{B} = \mathcal{I}_1 \times \ldots \times \mathcal{I}_n$, with each $\mathcal{I}_j \subseteq \mathbb{Z}$ a complete system of residues modulo p, and a collection of nonzero polynomials $f_1, \ldots, f_s \in \mathbb{Z}[X_1, \ldots, X_n]$, then the set of common zeros inside the box,

$$V = \{\mathbf{a} \in \mathcal{B} : \ f_1(\mathbf{a}) \equiv 0 \mod p^{m_1}, \ldots, f_s(\mathbf{a}) \equiv 0 \mod p^{m_s}\},$$

satisfies $|V| \equiv 0 \mod p^m$, provided $n > (m-1)\max_{i\in[1,s]}\left\{p^{m_i-1}\deg f_i\right\} + \sum_{i=1}^{s}\frac{p^{m_i}-1}{p-1}\deg f_i$. The introduction of the box $\mathcal{B}$ adds a degree of flexibility, in comparison to prior work of Sun. Indeed, incorporating the ideas of Sun, a weighted version of the above result is given. We continue by explaining how the added flexibility, combined with an appropriate use of Hensel's Lemma to choose the complete system of residues $\mathcal{I}_j$, allows many combinatorial applications of the Chevalley–Warning and Ax–Katz Theorems, previously only valid for $\mathbb{F}_p^n$, to extend with bare

✉ David J. Grynkiewicz
diambri@hotmail.com

[1] Department of Mathematical Sciences, University of Memphis, Memphis, TN 38152, USA

minimal modification to validity for an arbitrary finite abelian p-group G. We illustrate this by giving several examples, including a new proof of the exact value of the Davenport Constant $\mathsf{D}(G)$ for finite abelian p-groups, and a streamlined proof of the Kemnitz Conjecture. We also derive some new results, for a finite abelian p-group G with exponent q, regarding the constant $\mathsf{s}_{kq}(G)$, defined as the minimal integer ℓ such that any sequence of ℓ terms from G must contain a zero-sum subsequence of length kq. Among other results for this constant, we show that $\mathsf{s}_{kq}(G) \le kq + \mathsf{D}(G) - 1$ provided $k > \frac{d(d-1)}{2}$ and $p > d(d-1)$, where $d = \left\lceil \frac{\mathsf{D}(G)}{q} \right\rceil$, answering a problem of Xiaoyu He in the affirmative by removing all dependence on p from the bound for k.

Keywords Chevalley–Warning theorem · Ax–Katz theorem · Zero-sum · Erdős–Ginzburg–Ziv · Davenport constant · Polynomial method

Mathematics Subject Classification 11T06 · 11B75 · 20D60 · 11G25

1 Introduction and Notation

1.1 Basic Notation

Let $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$ and $\mathbb{N} = \{1, 2, \ldots, \}$, and let $\mathbb{F}_q$ denote a finite field of order q, whose characteristic must then be a prime $p \ge 2$ with q a power of p. For a commutative ring R, we let $R[X_1, \ldots, X_n]$ denote the polynomial ring in the variables $X_1, \ldots, X_n$ with coefficients from R, and we often use $\mathbf{x} = (X_1, \ldots, X_n)$ to denote the tuple of variable inputs. Each $f \in R[X_1, \ldots, X_n]$ is then a finite sum of *monomials* $f(\mathbf{x}) = \sum_{(k_1,\ldots,k_n)\in\mathbb{N}_0^n} c_{k_1,\ldots,k_n} X_1^{k_1} \cdots X_n^{k_n}$ with coefficients $c_{k_1,\ldots,k_n} \in R$. The monomials that occur in f are then the summands with $c_{k_1,\ldots,k_n} \neq 0$. The *degree* of f is denoted $\deg f$ and is the maximal value of $k_1 + \ldots + k_n$ as we range over all tuples $(k_1, \ldots, k_n) \in \mathbb{N}_0^n$ with $c_{k_1,\ldots,k_n} \neq 0$. The zero-polynomial $f = 0$ has $\deg f = -1$ by convention. For $j \in [1, n]$, we use $\deg_j f$ to denote the degree of f in the j-th variable X_j. Throughout the paper, the expression $0^0 := 1$, being interpreted as the constant polynomial $X^0 = 1$ evaluated at 0. A polynomial $f \in \mathbb{Q}[X_1, \ldots, X_n]$ is called an *integer–valued polynomial* if $f(\mathbf{a}) \in \mathbb{Z}$ for all $\mathbf{a} \in \mathbb{Z}^n$. We use $\mathsf{Int}(\mathbb{Z})$ to denote the set of all integer–valued polynomials $f \in \mathbb{Q}[X]$, which is the sub-ring of $\mathbb{Q}[X_1, \ldots, X_n]$ consisting of all polynomials f with $f(x) \in \mathbb{Z}$ for all $x \in \mathbb{Z}$. A map $f : \mathbb{Z} \to \mathbb{Z}$ is *periodic* with period m if $f(x + m) = f(x)$ for all $x \in \mathbb{Z}$. In this paper, all intervals are discrete, so $[a, b] = \{x \in \mathbb{Z} : a \le x \le b\}$ for $a,\ b \in \mathbb{R}$, and variables introduced with an inequality are assumed to be integers. Given an integer $m \ge 1$, a *complete system of residues modulo m* is a set $\mathcal{I} \subseteq \mathbb{Z}$ with $|\mathcal{I}| = m$ whose elements are distinct modulo m, i.e., $\mathcal{I}$ contains exactly one representative for every residue class modulo m. We use φ to denote the Euler totient function, so $\varphi(n)$ is the number of elements $x \in [1, n]$ that are relatively prime to the integer $n \ge 1$. In particular,

$$\varphi(1) = 1 \quad \text{and} \quad \varphi(q) = \frac{(p-1)q}{p}$$

for a prime power $q = p^s > 1$. Given a prime $p \geq 2$ and $x \in \mathbb{Z}$, we let $\mathsf{v}_p(x)$ denote the p-adic valuation of x, which is simply the multiplicity of the prime p in the prime factorization of x, and we extend this for $x = \frac{a}{b} \in \mathbb{Q}$ with $a,\ b \in \mathbb{Z}$ by the standard definition $\mathsf{v}_p(x) = \mathsf{v}_p(a) - \mathsf{v}_p(b)$. For an element X in a commutative ring containing $\mathbb{Q}$, the binomial coefficient is defined as

$$\binom{X}{n} = \frac{X(X-1)\cdots(X-n+1)}{n!},$$

with $\binom{X}{0} := 1$. If $x \in \mathbb{N}_0$ is an integer, then $\binom{x}{n}$ counts the number of ways to choose n elements from a set of size x, and is thus an integer. Moreover, $\binom{x}{n} = 0$ for $x \in \mathbb{N}_0$ and $n > x$.

1.2 Introduction

The study of the common roots of a collection of polynomials $f_1, \ldots, f_s \in R[X_1, \ldots, X_n]$ is a classical object of study in Number Theory and Arithmetic Geometry. When $R = \mathbb{F}_q$ is a finite field of characteristic p, one of the most well-known such results is the Chevalley–Warning Theorem [14] [49] [26, Theorem 22.4] [35, Theorem 2.6] [45, Theorem 9.24].

Theorem 1.1 (Chevalley–Warning Theorem (1936)) *Let $\mathbb{F}_q$ be a finite field of characteristic p, let $f_1, \ldots, f_s \in \mathbb{F}_q[X_1, \ldots, X_n]$ be nonzero polynomials, where $s \geq 1$, and let*

$$V = \{\boldsymbol{a} \in \mathbb{F}_q^n : \ f_1(\boldsymbol{a}) = 0, \ldots, f_s(\boldsymbol{a}) = 0\}.$$

If $n > \sum_{i=1}^{s} \deg f_i$, then $|V| \equiv 0 \mod p$.

As a particular case, if there is one common zero for the polynomials $f_1, \ldots, f_s$, then there must be at least one nontrivial zero, which was the original result of Chevalley [14]. His argument could be extended to yield the more general Theorem 1.1, as noted by Warning [49], who also gave the lower bound $|V| \geq q^{n-\sum_{i=1}^{s} \deg f_i}$ (assuming the system has a solution), now known as Warning's Second Theorem. Later, the higher order p-divisibility of $|V|$ was considered by Ax [4, p. 255] (for $s = 1$, with this case also implying weaker bounds for larger s) and then with tight bounds for general s by Katz [30, Theorem 1.0], resulting in what is known as the Ax–Katz Theorem.

Theorem 1.2 (Ax–Katz Theorem (1971)) *Let $\mathbb{F}_q$ be a finite field of characteristic p and order q, let $f_1, \ldots, f_s \in \mathbb{F}_q[X_1, \ldots, X_n]$ be nonzero polynomials, where $s \geq 1$, and let*

$$V = \{\boldsymbol{a} \in \mathbb{F}_q^n : \ f_1(\boldsymbol{a}) = 0, \ldots, f_s(\boldsymbol{a}) = 0\}.$$

If $n > (m-1)\max_{i\in[1,s]}\{\deg f_i\} + \sum_{i=1}^{s} \deg f_i$, *where* $m \geq 1$, *then* $|V| \equiv 0 \mod q^m$.

Both the Chevalley–Warning and Ax–Katz Theorems have attracted considerable attention in Number Theory, including many extensions, refinements, variants and alternative proofs. See [1, 6, 8, 10, 11, 13, 16, 17, 29, 33, 34, 47, 48, 52] for a handful of such instances among many more. However, the interest in these results extends much further, also to areas such as Discrete Mathematics, where they form a standard tool in the "Polynomial Method." Here, the interest lies not directly in the results themselves but rather in what other results can be proved by their usage in combination with appropriately chosen polynomials. For such reasons, the Chevalley–Warning Theorem is often found in many texts on Additive Combinatorics, e.g. [26, Theorem 22.4] [35, Theorem 2.6] [45, Theorem 9.24], and is an indispensable tool in many parts of Combinatorics. As this will be a prime focus in this paper, we will shortly see concrete examples of how this works. Worth noting, regarding the use of the Ax–Katz and Chevalley–Warning Theorems in Discrete Mathematics, the case $\mathbb{F}_p$ is the main focus of interest, and thus for this paper as well.

Despite the rather elementary formulation of the Ax–Katz Theorem, most proofs are rather non-elementary, to varying extents. Perhaps the most elementary proof, though only valid for the prime field $\mathbb{F}_p$, was given by Wilson [52]. His interest was primarily in using the method he developed to give striking applications in Coding Theory, and while his work received some attention in Coding Theory, its importance outside Coding Theory seems not fully realized. The first part of this paper is devoted to detailing how the method of Wilson readily adapts to prove the following generalization of the prime field case in the Ax–Katz and Chevalley–Warning Theorems, where we are allowed to consider polynomial equations modulo varying prime powers p^{m_i}.

We remark that Clark and Schauz [15] have recently combined Wilson's arguments along with the functional calculus of Aichinger and Moosbacher [1], giving a Chevalley–Warning type theorem for maps between finite abelian p-groups. Also, after having seen the initial posting of this paper, Cao and Wan [12] were able to give a complete (non-weighted) generalization of the Ax–Katz Theorem along the lines of Theorem 1.3 for *any* finite field, not just the prime field case as is done here. Their proof uses finite Witt rings, thus providing an alternative proof of Theorem 1.3 in the non-weighted case, when all weight functions $w_i(X) = 1$.

Theorem 1.3 *Let* $p \geq 2$ *be prime, let* $n \geq 1$ *and* $\mathcal{B} = \mathcal{I}_1 \times \ldots \times \mathcal{I}_n$ *with each* $\mathcal{I}_j \subseteq \mathbb{Z}$ *for* $j \in [1, n]$ *a complete system of residues modulo* p, *let* $s \geq 1$ *and* $m_1, \ldots, m_s \geq 0$ *be integers, let* $f_1, \ldots, f_s \in \mathbb{Z}[X_1, \ldots, X_n]$ *be nonzero polynomials, let* $w_1, \ldots, w_s \in \mathbb{Q}[X]$ *be integer–valued polynomials with respective degrees* $t_1, \ldots, t_s \geq 0$, *and let*

$$V = \{\boldsymbol{a} \in \mathcal{B} : \ f_i(\boldsymbol{a}) \equiv 0 \mod p^{m_i} \text{ for all } i \in [1, s]\} \quad \text{and}$$

$$N = \sum_{\boldsymbol{a}\in V} \prod_{i=1}^{s} w_i\Big(\frac{f_i(\boldsymbol{a})}{p^{m_i}}\Big).$$

If $n > (m-1)\max_{i\in[1,s]}\left\{1,\ \frac{\varphi(p^{m_i})}{p-1}\deg f_i\right\}+\sum_{i=1}^{s}\frac{(t_i+1)p^{m_i}-1}{p-1}\deg f_i$, *where* $m \geq 0$ *and* φ *denotes the Euler totient function, then*

$$N \equiv 0 \mod p^m.$$

In the special case in Theorem 1.3 when all $w_i = 1$ are constant polynomials, we find that $N = |V|$ is simply the cardinality of V, with $t_i = 0$ for all i. Additionally assuming $m_i = 1$ for all i, we then recover the Ax–Katz Theorem for $\mathbb{F}_p$. In general, the quantity N counts the elements $\mathbf{a} \in V$ each with multiplicity $w_i\left(\frac{f_i(\mathbf{a})}{p^{m_i}}\right)$, meaning N may be view as the weighted size of V using the integer–valued polynomials $w_1, \ldots, w_s \in \mathbb{Q}[X]$ as weight functions. The idea to consider such weight functions is due to Sun [43], who indeed noticed (in his unpublished preprint from 2006) that Wilson's argument could be used to prove a result of the form stated in Theorem 1.3, specifically, in the case $\mathcal{I}_j = [0,\ p-1]$ for all j. However, as already alluded to, we are primarily interested in the *application* of Theorem 1.3, particularly to Combinatorial Number Theory, and for this, the added flexibility gained by considering common zeros inside the box $\mathcal{B} = \mathcal{I}_1 \times \ldots \times \mathcal{I}_n$, with the $\mathcal{I}_j$ allowed to be *any* complete system of residues modulo p, will be quite crucial. This will become clearer once we have some examples, but the crux of the matter is that, by choosing the $\mathcal{I}_j$ carefully, we can simulate behavior modulo p^m that could normally only be expected modulo p, at least so long as we restrict to elements $x \in \mathcal{I}_j$.

For instance, Fermat's Little Theorem tells us that

$$x^{p-1} \equiv \begin{cases} 1 \mod p \text{ if } x \not\equiv 0 \mod p \\ 0 \mod p \text{ if } x \equiv 0 \mod p. \end{cases}$$

From a combinatorial point of view, this is quite nice, as it tells us that the polynomial X^{p-1} can be used as an indicator function modulo p. Indeed, in many applications of the Chevalley–Warning or Ax–Katz Theorem in Combinatorial Number Theory, this is the key means of translating between combinatorial information and the algebraic information gleaned from the Chevalley–Warning or Ax–Katz Theorem. Fermat's Little Theorem, of course, fails modulo higher powers of p. Nonetheless, Hensel's Lemma can be used to find an appropriate $\mathcal{I}_j$ for which Fermat's Little Theorem holds modulo p^m, when restricted to $x \in \mathcal{I}_j$. We include the short derivation of Proposition 1.4 at the end of Sect. 2, though this result is a special case of more general and now standard results from Algebraic Number Theory, in this case involving the Teichmuller Character and Witt Vectors (see [12] [42, Sects. 2.4 and 2.5]).

Proposition 1.4 *Let* $p \geq 2$ *be prime and let* $m \geq 1$. *There exists a complete system of residues* $\mathcal{I} \subseteq [0,\ p^m - 1]$ *modulo* p *such that*

$$x^{p-1} \equiv \begin{cases} 1 \mod p^m \text{ if } x \not\equiv 0 \mod p \\ 0 \mod p^m \text{ if } x \equiv 0 \mod p, \end{cases} \quad \text{for every } x \in \mathcal{I}.$$

The main point is that, using Proposition 1.4 (or a more general application of Hensel's Lemma) to choose the $\mathcal{I}_j$ appropriately, it is then often possible to use Theo-

rem 1.3, in place of either the Chevalley–Warning or Ax–Katz Theorem, and *de facto* obtain a result via the Polynomial Method for a general finite abelian p-group G that could previously only be achieved by the same means for the special case $G = \mathbb{F}_p^r$. It is this point that we wish to particularly highlight, and for which we provide several examples illustrating the idea.

The first example regards the Davenport Constant $\mathsf{D}(G)$ of a finite abelian group G, defined as the minimal integer ℓ such that every sequence of ℓ terms from G must contain a nontrivial subsequence whose terms sum to zero (called a zero-sum subsequence). It is an invariant that has received considerable attention, in part due to its connection with Commutative Algebra. It is perhaps best simply to refer to the texts [25] [26], and the many references therein, for broader context. In general, if $G = (\mathbb{Z}/n_1\mathbb{Z}) \times \ldots \times (\mathbb{Z}/n_r\mathbb{Z})$ with $n_1 \mid \ldots \mid n_r$, then a rather simple argument and construction [26, Theorem 10.2] and [25, Proposition 5.1.8.2] shows that

$$|G| \geq \mathsf{D}(G) \geq \mathsf{D}^*(G) := 1 + \sum_{i=1}^{r} (n_i - 1).$$

While even the (near) exact determination of $\mathsf{D}(G)$ remains an important and challenging question for a general finite abelian group G, the following classical result of Olson [37, Eq. (1)] and also Kruyswijk [5] showed that the trivial lower bound is tight for p-groups. Both these original proofs relied upon ideals and group algebras. Our first application will be to use Theorem 1.3 to give a fairly direct proof of Theorem 1.5.

Theorem 1.5 *Let G be a finite abelian p-group. Then*

$$\mathsf{D}(G) = \mathsf{D}^*(G).$$

The next example regards the Erdős–Ginzburg–Ziv Constant $\mathsf{s}(G)$ of the finite abelian group G, defined as the minimal integer ℓ such that every sequence of ℓ terms from G must contain a zero-sum subsequence of length $\exp(G)$ (the exponent of G). The Erdős–Ginzburg–Ziv Theorem implies that $\mathsf{s}(\mathbb{Z}/n\mathbb{Z}) = 2n-1$ [19, Theorem] [25, Corollary 5.7.5] [26, Theorem 10.1] [35, Theorem 2.5]. It was a conjecture of Kemnitz [31] that $\mathsf{s}((\mathbb{Z}/n\mathbb{Z})^2) = 4n - 3$, for which a simple argument shows that it suffices to consider the case $n = p$ prime. Partial progress towards this conjecture was achieved by Alon and Dubiner [2, Theorem 1.3] and by Rónyai [39, Theorem 1.1] before finally being resolved by Reiher [38, 40]. Regarding higher rank groups $(\mathbb{Z}/n\mathbb{Z})^r$, Alon and Dubiner gave a linear bound via Algebraic Graph Theory [3, Theorem 1.1]. Reiher's proof involved combining the Chevalley–Warning Theorem with several combinatorial double counting arguments. Rónyai's proof was also algebraic, but instead made use of linear algebra surrounding multi-linear monomials. Our second application will be to use Theorem 1.3 to give a streamlined proof of Theorem 1.6. As we will see, the flexibility of being able to use more general weights allows us to directly derive some of the congruences used in Reiher's proof, reducing the number of ad-hoc combinatorial doubling counting arguments needed. This is not surprising since the elementary proof of Wan's Weighted Weisman–Fleck congruence [44, Theorem 1.0], which is one of the

key components used in the proof of Theorem 1.3, incorporates such double counting arguments into its proof, meaning they are in some sense built into Theorem 1.3 itself. While the proof of Theorem 1.6 is only a minor variation on Reiher's, it does highlight how the weight functions can be used to generate additional linearly independent congruences in a routine manner. For more complicated arguments, this can simplify the technical calculations and help focus attention on the more involved parts of the argument.

Theorem 1.6 (Kemnitz Conjecture) *Let C_p be a cyclic group of order $p \geq 2$ prime. Then*

$$\mathsf{s}(C_p^2) = 4p - 3.$$

The final examples regard a generalized Erdős-Ginzburg-Ziv constant $\mathsf{s}_{k\exp(G)}(G)$ of the finite abelian group G, defined as the minimal integer ℓ such that every sequence of ℓ terms from G must contain a zero-sum subsequence of length $k\exp(G)$. See [7, 21–23, 27, 28, 32, 50] for some relevant examples of results regarding $\mathsf{s}_{k\exp(G)}(G)$. More generally, given a subset $X \subseteq \mathbb{N}_0$, we let $\mathsf{s}_X(G)$ be the minimal integer ℓ such that every sequence of ℓ terms from G must contain a zero-sum subsequence T with length $|T| \in X$. Here, we will particularly focus on a question initially raised by Kubertin [32, Conjecture] and later extended in [50, Definition 3.1]. The problem, for a finite abelian group G, is to find an optimal bound $\ell(G)$ such that $\mathsf{s}_{k\exp(G)}(G) = k\exp(G)+\mathsf{D}(G)-1$ for all $k \geq \ell(G)$. The corresponding lower bound for $s_{k\exp(G)}(G)$ follows from a rather basic construction, so the issue is how large must k be to ensure $\mathsf{s}_{k\exp(G)}(G) \leq k\exp(G) + \mathsf{D}(G) - 1$. An older result of Gao implies this is true for $k \geq \frac{|G|}{\exp(G)}$ [22, Theorem 3.2] [50, Eq. (2)], and it was conjectured in [32, Conjecture] [23, Conjecture 4.7] that the optimal bound for k should be $k \geq d := \left\lceil \frac{\mathsf{D}(G)}{\exp(G)} \right\rceil$. For p-groups, this was proven for $d \leq 4$ when $p \geq 2d - 1$ by Dongchun Han [27]. For more general p-groups, Xiaoyu He could show $\mathsf{s}_{k\exp(G)}(G) \leq k\exp(G) + \mathsf{D}(G) - 1$ holds for $k \geq p + d$ when $p \geq \frac{7}{2}d - \frac{3}{2}$, and they posed the problem of obtaining a significant improvement of their result by removing the dependence on p from the lower bound for k [28, pp. 405].

Our concluding applications are to use Theorem 1.3 to give a much shorter proof of Dongchun Han's [27] result (Theorem 1.8), and to also answer the problem of Xiaoyu He [28] in the affirmative by showing $k > \frac{d(d-1)}{2}$, which is independent of p, suffices when $p > d(d-1)$ (Theorem 1.9). Both these results make use of Theorem 1.7, which is derived from Theorem 1.3 and generalizes [28, Theorem 3] by relaxing the hypothesis $X \subseteq [1, p]$ to that given in (1). Xiaoyu He proved [28, Theorem 3] by an extension of the method used by Kubertin [32], which was based on the methods developed by Rónyai for his result regarding the Kemnitz Conjecture [39]. In this way, Theorem 1.3 simultaneously generalizes both the Chevalley–Warning Theorem and the main applications of the algebraic method of Rónyai into a single algebraic tool.

Theorem 1.7 *Let G be a finite abelian p-group with exponent $q > 1$, let $d = \left\lceil \frac{\mathsf{D}^*(G)}{q} \right\rceil$, let $m \geq 0$, let $X \subseteq \mathbb{N}$ be a subset of positive integers with $|X| \geq d + m$, and let*

$\{x_1, \ldots, x_s\} = [1, \max X] \backslash X$ *with the* x_i *distinct. Suppose*

$$\prod_{i=1}^{s} x_i \prod_{1 \le i < j \le s} (x_j - x_i) \not\equiv 0 \mod p^{m+1}. \tag{1}$$

Then

$$\begin{aligned} \mathsf{s}_{X \cdot q}(G) &\le \big(\max X - |X| + \frac{m(p-1)}{p} + 1\big)q + \mathsf{D}^*(G) - 1 \\ &\le \big(\max X + 1 - \frac{m}{p}\big)q - r, \end{aligned}$$

where $r \in [1, q]$ *is the integer such that* $d = \frac{\mathsf{D}^*(G)+r-1}{q}$.

Theorem 1.8 *Let* G *be a finite abelian* p*-group with exponent* q*, let* $d = \left\lceil \frac{\mathsf{D}^*(G)}{q} \right\rceil$*, and suppose* $p \ge 2d - 1$ *and* $d \le 4$*. Then*

$$\mathsf{s}_{kq}(G) \le kq + \mathsf{D}^*(G) - 1 \quad \textit{for every } k \ge d.$$

Theorem 1.9 *Let* G *be a finite abelian* p*-group with exponent* q*, let* $d = \left\lceil \frac{\mathsf{D}^*(G)}{q} \right\rceil$*, and suppose* $p > d(d-1)$*. Then*

$$\mathsf{s}_{kq}(G) \le kq + \mathsf{D}^*(G) - 1 \quad \textit{for every } k > \frac{d(d-1)}{2}.$$

1.3 Additional Notation

For our applications in Combinatorial Number Theory, we will have need to deal with (combinatorial) sequences S of terms from a finite abelian group G. Here, per tradition in Combinatorial Number Theory, a *sequence* is considered to be a finite and unordered string of elements from G, which we write as

$$S = g_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_\ell$$

with the $g_i \in G$ the terms in the sequence S and each term separated by the concatenation operation $\boldsymbol{\cdot}$. From a combinatorial perspective, a sequence is simply a multi-set, where we use the natural language of sequences to describe its properties, and use the formal algebraic notation from free abelian monoids to easily describe and manipulate its terms [25, 26]. The former avoids confusion with ordinary sets, and the latter is very helpful in more complicated combinatorial arguments. Then $|S| = \ell$ denotes the length of the sequence S. Analogous to the definition of the p-adic valuation, for $g \in G$, $\mathsf{v}_g(S)$ denotes the multiplicity of the term g in S, in which case $S = \prod_{g \in G}^{\bullet} g^{[\mathsf{v}_g(S)]}$, where $g^{[n]} = \underbrace{g \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g}_{n}$ denotes the sequence consisting of the element g repeated n times. The notation $T \mid S$ indicates that T is a subsequence of S, meaning $\mathsf{v}_g(T) \le \mathsf{v}_g(S)$

for all $g \in G$, and then $T^{[-1]} \cdot S$ or $S \cdot T^{[-1]}$ denotes the sequence obtained from S by removing the terms in T, so $\mathsf{v}_g(T^{[-1]} \cdot S) = \mathsf{v}_g(S) - \mathsf{v}_g(T)$ for all $g \in G$. The sum of terms in S is denoted

$$\sigma(S) = g_1 + \ldots + g_\ell \in G,$$

and the sequence S is *zero-sum* if $\sigma(S) = 0$. Given a subset $X \subseteq \mathbb{N}_0$, we use the notation

$$\Sigma_X(S) = \{\sigma(T) : \ T \mid S, \ |T| \in X\}$$

to denote all elements $g \in G$ that can be represented of a sum of terms from a subsequence of G whose length lies in X. In the case $X = \{1, 2, \ldots, \}$, we use the abbreviation

$$\Sigma(S) = \Sigma_{\{1,2,\ldots\}}(S) = \{\sigma(T) : \ T \mid S, \ |T| \ge 1\}$$

to denote all elements that are a sum of terms from a nontrivial subsequence of S. The sequence S is called *zero-sum free* if it has no nontrivial zero-sum subsequences, i.e., if $0 \notin \Sigma(S)$. For $j \ge 0$, we let

$$N_j(S) = |\big\{I \subseteq [1, \ell] : \ |I| = j, \ \sigma\big(\prod\nolimits_{i\in I}^{\cdot} g_i\big) = 0\big\}|$$

count the number of (indexed) zero-sum subsequences of $S = g_1 \cdot \ldots \cdot g_\ell$ with length j.

Regarding finite abelian groups G, we let C_n denote a cyclic group of order $n \ge 1$. Then $G = C_{n_1} \oplus \ldots \oplus C_{n_r}$ with $1 \le n_1 \mid \ldots \mid n_r$ and $n_r = \exp(G)$ the *exponent* of G, and we set

$$\mathsf{D}^*(G) = 1 + \sum_{i=1}^{r} (n_i - 1).$$

The order of an element $g \in G$ is denoted $\mathrm{ord}(g)$. A *basis* for G is a tuple $(e_1, \ldots, e_r)$ of elements $e_1, \ldots, e_r \in G$ with $G = \langle e_1 \rangle \oplus \ldots \oplus \langle e_r \rangle$. Finally, given a subset $X = \{x_1, \ldots, x_s\} \subseteq \mathbb{Z}$ and $q \in \mathbb{Z}$, we let

$$X \cdot q = \{x_1 q, \ldots, x_s q\}.$$

2 Proof of the Weighted Ax–Katz-Wilson Theorem

In this section, we give the details of the proof of Theorem 1.3. The following congruence is the first key component in the proof. The case when $w(X) = 1$ is a constant polynomial is a result of Weisman [51, Corollary 14], generalizing an older congruence of Fleck [18, 20] who treated the case $s = 1$. The more general version involving

the polynomial weight $w(X)$ was originally proved by Daqing Wan [46, Thoerem 1.3], with an elementary proof via complex roots of unity later found by Zhi-Wei Sun and Daqing Wan [44, Theorem 1.0]. Note, in both these cases, Theorem 2.1 was only stated with $w(X)$ equal to a binomial coefficient. However, since the binomial coefficients form a basis for all integer–valued polynomials [9, pp. xiii], the formulation below is immediately implied.

Theorem 2.1 (Wan's Weighted Weisman–Fleck Congruence) *Let $n, r, s \geq 0$ be integers, let $p \geq 2$ be prime, and let $w(X) \in \mathbb{Q}[X]$ be an integer–valued polynomial of degree $t \geq 0$. Then*

$$\sum_{\substack{i \equiv r \mod p^s \\ i \geq 0}} (-1)^i \binom{n}{i} w\left(\frac{i-r}{p^s}\right) \equiv 0 \mod p^m,$$

$$\text{where } m = \max\left\{0, \left\lceil \frac{n-(t+1)p^s+1}{\varphi(p^s)} \right\rceil\right\}.$$

The set

$$\mathsf{Map}(\mathbb{Z}) = \{f : \mathbb{Z} \to \mathbb{Z}\}$$

of all maps $f : \mathbb{Z} \to \mathbb{Z}$ forms an abelian group with addition defined pointwise: $(f+g)(x) = f(x) + g(x)$ for $f, g \in \mathsf{Map}(\mathbb{Z})$ and $x \in \mathbb{Z}$. We then have an endomorphism ring for this abelian group,

$$\mathsf{End}(\mathsf{Map}(\mathbb{Z})) = \{F : \mathsf{Map}(\mathbb{Z}) \to \mathsf{Map}(\mathbb{Z}) : \ F \text{ is an abelian group homomorphism}\},$$

with addition in $\mathsf{End}(\mathsf{Map}(\mathbb{Z}))$ again defined pointwise and multiplication given by composition, so $(FG)(f) = F(G(f))$ and $(F+G)(f) = F(f) + G(f)$ for $F, G \in \mathsf{End}(\mathsf{Map}(\mathbb{Z}))$ and $f \in \mathsf{Map}(\mathbb{Z})$.

Let $I \in \mathsf{End}(\mathsf{Map}(\mathbb{Z}))$ denote the identity map and let $E \in \mathsf{End}(\mathsf{Map}(\mathbb{Z}))$ be the shift operator, defined by

$$E(f)(x) := f(x+1) \quad \text{for} f \in \mathsf{Map}(\mathbb{Z}) \text{ and} x \in \mathbb{Z}.$$

The finite difference operator is then the map

$$\Delta := E - I \in \mathsf{End}(\mathsf{Map}(\mathbb{Z})),$$

meaning

$$\Delta f(x) := \Delta(f)(x) = f(x+1) - f(x) \quad \text{for} f \in \mathsf{Map}(\mathbb{Z}) \text{ and} x \in \mathbb{Z}.$$

The next component in Wilson's argument is the classical Newton Expansion of an integer–valued function, which is easily derived from the above set-up. We include the brief proof for the reader's benefit.

Proposition 2.2 (Newton Expansion) *For any map $f : \mathbb{Z} \to \mathbb{Z}$, we have*

$$f(x) = \sum_{n=0}^{\infty} (\Delta^n f)(0) \binom{x}{n} \quad \text{for all } x \in \mathbb{N}_0. \tag{2}$$

Proof Iterating the identity $(\Delta + I) f(y) = f(y+1)$, for $y \in \mathbb{Z}$, it follows that $(\Delta + I)^x f(y) = f(y+x)$ for $y \in \mathbb{Z}$ and $x \geq 0$, whence

$$\sum_{n=0}^{\infty} (\Delta^n f)(0) \binom{x}{n} = \left(\sum_{n=0}^{x} \binom{x}{n} \Delta^n \right) f(0) = (\Delta + I)^x f(0) = f(x)$$

for all $x \in \mathbb{N}_0$. □

To deal with general weight functions $w(X)$, we recall the well-known fact that the integer–valued polynomials $\mathsf{Int}(\mathbb{Z}) \subseteq \mathbb{Q}[X]$ are a free abelian group with basis the binomial functions [9, pp. xiii]. This means there is little loss of generality to only consider $w(X) = \binom{X}{t}$, where $t \geq 0$, when using a weight function, or even simply $w(X) = X^t$ for $t \geq 0$ if linear independence is all that is required.

Proposition 2.3 $\mathsf{Int}(\mathbb{Z})$ *is a free abelian group with basis* $\{\binom{X}{t} : \ t = 0, 1, \ldots\}$.

Next, we come to the main step in Wilson's proof, which he modestly named a lemma. The case where $w(X) = 1$ is the constant polynomial equal to 1 is found in Wilson's original paper [52, Lemma 1]. Exchanging the use of the non-weighted Weisman–Fleck congruence with its weighted version (Theorem 2.1) in Wilson's argument, one obtains the following weighted version with no other major modifications needed. In order to obtain a more self-contained work, we include the details below, which may also be found in an unpublished paper of Zhi–Wei Sun [43], who was the first to realize Wilson's ideas could readily be extended to include weights.

Theorem 2.4 (Weighted Wilson's Lemma) *Let $m \geq 1$ and $s \geq 0$ be integers, let $p \geq 2$ be prime, let $w(X) \in \mathbb{Q}[X]$ be an integer–valued polynomial of degree $t \geq 0$, and let $f : \mathbb{Z} \to \mathbb{Z}$ be a map that is periodic with period p^s. Then there exists a rational polynomial $g(X) = \sum_{n=0}^{d} a_n \binom{X}{n} \in \mathbb{Q}[X]$ with $a_n \in \mathbb{Z}$ and $d < (t+1)p^s + (m-1)\varphi(p^s)$ such that*

$$g(x) \equiv w\left(\left\lfloor \frac{x}{p^s} \right\rfloor \right) f(x) \mod p^m \quad \text{for all} x \in \mathbb{Z}, \quad \text{and}$$

$$a_n \equiv 0 \mod p^{\ell} \quad \text{for all} n \in [0, d], \quad \text{where } \ell = \max\left\{ 0, \left\lceil \frac{n - (t+1)p^s + 1}{\varphi(p^s)} \right\rceil \right\}.$$

Proof Define the map $h : \mathbb{Z} \to \mathbb{Z}$ by

$$h(x) = w\left(\left\lfloor \frac{x}{p^s} \right\rfloor \right) f(x) \quad \text{for } x \in \mathbb{Z}$$

and use Proposition 2.2 to write

$$w\Big(\Big\lfloor \frac{x}{p^s} \Big\rfloor\Big) f(x) = h(x) = \sum_{n=0}^{\infty} (\Delta^n h)(0) \binom{x}{n} \quad \text{for all } x \in \mathbb{N}_0. \tag{3}$$

Let $I,\ E, \Delta = E - I \in \mathsf{End}(\mathsf{Map}(\mathbb{Z}))$ be as defined earlier. Since f is periodic with period p^s, we have $f(i) = f(r)$ whenever $i \equiv r \mod p^s$, which we use below. For any $n \geq 0$, it follows that

$$\begin{aligned}
(\Delta^n h)(0) = ((E-I)^n h)(0) &= \left(\Big(\sum_{i=0}^{n} \binom{n}{i} (-I)^{n-i} E^i \Big) h \right)(0) \\
&= \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} (E^i h)(0) \\
&= \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} h(i) = \sum_{r=0}^{p^s-1} \sum_{\substack{i \equiv r \mod p^s \\ i \geq 0}} (-1)^{n-i} \binom{n}{i} w\Big(\Big\lfloor \frac{i}{p^s} \Big\rfloor\Big) f(i) \\
&= \sum_{r=0}^{p^s-1} f(r) \left(\sum_{\substack{i \equiv r \mod p^s \\ i \geq 0}} (-1)^{n-i} \binom{n}{i} w\Big(\frac{i-r}{p^s}\Big) \right).
\end{aligned}$$

Applying Theorem 2.1, it follows that

$$a_n := (\Delta^n h)(0) \equiv 0 \mod p^{\ell}, \quad \text{where } \ell = \max\left\{0, \left\lceil \frac{n - (t+1)p^s + 1}{\varphi(p^s)} \right\rceil \right\}.$$

As a particular consequence, we have $a_n \equiv 0 \mod p^m$ for all $n \geq (t+1)p^s + (m-1)\varphi(p^s)$. Combined with (3), we obtain

$$g(x) \equiv h(x) = w\Big(\Big\lfloor \frac{x}{p^s} \Big\rfloor\Big) f(x) \mod p^m \quad \text{for all } x \in \mathbb{N}_0, \tag{4}$$

where

$$g(X) := \sum_{n=0}^{d} a_n \binom{X}{n} \in \mathbb{Q}[X] \quad \text{and} \quad d = (t+1)p^s + (m-1)\varphi(p^s) - 1.$$

To complete the proof, we need to show (4) also holds for $x < 0$.

For $n \geq 0$ and $x,\ y \in \mathbb{Z}$, we have $\binom{x+y}{n} = \binom{x}{n} + y\frac{z}{n!}$, for some $z \in \mathbb{Z}$, whence

$$\binom{x+y}{n} \equiv \binom{x}{n} \mod p^m \quad \text{for any } x,\ y \in \mathbb{Z} \text{ with } \mathsf{v}_p(y) \geq m + \mathsf{v}_p(n!). \tag{5}$$

Proposition 2.3 implies that $w(X) = \sum_{n=0}^{t} b_n \binom{X}{n}$ for some $b_n \in \mathbb{Z}$. Combined with (5), we conclude that

$$w(x+y) \equiv w(x) \mod p^m \quad \text{for any } x,\ y \in \mathbb{Z} \text{ with } \mathsf{v}_p(y) \geq m + \mathsf{v}_p(t!). \tag{6}$$

Let $x \in \mathbb{Z}$ be arbitrary and let $y \geq 0$ be an integer with $x + y \geq 0$ and

$$\mathsf{v}_p(y) \geq \max\{s + m + \mathsf{v}_p(t!),\ m + \mathsf{v}_p(d!)\}.$$

Then

$$\begin{aligned} g(x) = \sum_{n=0}^{d} a_n \binom{x}{n} \equiv \sum_{n=0}^{d} a_n \binom{x+y}{n} = g(x+y) \equiv w\Big(\Big\lfloor \frac{x+y}{p^s} \Big\rfloor\Big) f(x+y) \\ = w\Big(\Big\lfloor \frac{x}{p^s} \Big\rfloor + \frac{y}{p^s}\Big) f(x) \equiv w\Big(\Big\lfloor \frac{x}{p^s} \Big\rfloor\Big) f(x) \mod p^m, \end{aligned}$$

which establishes (4) for $x < 0$, completing the proof. □

The following simple lemma is well-known (combine Fermat's Little Theorem with [26, Lemma 22.3]).

Lemma 2.5 *Let $p \geq 2$ be prime and let $m \geq 0$ be an integer. Then*

$$\sum_{x \in \mathbb{F}_p} x^m = \begin{cases} 0 & \text{if } m = 0 \text{ or } m \not\equiv 0 \mod p-1 \\ -1 & \text{if } m > 0 \text{ and } m \equiv 0 \mod p-1. \end{cases}$$

The next lemma is a variation on Chevalley's key observation used in the proof of the Chevalley–Warning Theorem [14, 26, 35, 45, 49]. The case when all $\mathcal{I}_j = [0, p-1]$ is found in Wilson's original paper [52], but the argument is sufficiently robust to also work when replacing $[0, p-1]$ with an arbitrary complete system of residues modulo p. As the added flexibility of being able to consider arbitrary complete system of residues is rather crucial, we include the details.

Lemma 2.6 *Let $p \geq 2$ be prime, let $n \geq 1$, let $\mathcal{B} = \mathcal{I}_1 \times \ldots \times \mathcal{I}_n$ with each $\mathcal{I}_j \subseteq \mathbb{Z}$ for $j \in [1, n]$ a complete system of residues modulo p, and suppose $f \in \mathbb{Q}[X_1, \ldots, X_n]$ is an integer–valued polynomial with $\deg_j(f) \leq p-2$ for every $j \in [1, n]$, and $\mathsf{v}_p(c) \geq 0$ for every coefficient $c \in \mathbb{Q}$ of a monomial in $f(\boldsymbol{x})$. Then*

$$\sum_{\boldsymbol{a} \in \mathcal{B}} f(\boldsymbol{a}) \equiv 0 \mod p^n.$$

Proof Let $g(\mathbf{x}) = c_g X_1^{k_1} X_2^{k_2} \cdots X_n^{k_n}$ be an arbitrary monomial occurring in $f(\mathbf{x})$, so $c_g \in \mathbb{Q}\backslash\{0\}$ and $\mathsf{v}_p(c_g) \geq 0$ by hypothesis. Now

$$\sum_{\mathbf{a} \in \mathcal{B}} g(\mathbf{a}) = \sum_{(a_1, \ldots, a_n) \in \mathcal{B}} c_g a_1^{k_1} a_2^{k_2} \cdots a_n^{k_n} = \sum_{(a_1, \ldots, a_{n-1}) \in \mathcal{B}'} \left(c_g a_1^{k_1} \cdots a_{n-1}^{k_{n-1}} \sum_{a_n \in \mathcal{I}_n} a_n^{k_n} \right),$$

where $\mathcal{B}' = \mathcal{I}_1 \times \ldots \times \mathcal{I}_{n-1}$. By hypothesis, we have $k_j \leq p-2$ for every $j \in [1, n]$. Combined with the hypothesis that $\mathcal{I}_n$ is a complete system of residues modulo p, we can apply Lemma 2.5 to conclude that $\sum_{a_n \in \mathcal{I}_n} a_n^{k_n} = b'p$ for some $b' \in \mathbb{Z}$. Consequently,

$$\sum_{\mathbf{a} \in \mathcal{B}} g(\mathbf{a}) = b'p \sum_{\mathbf{a} \in \mathcal{B}'} h(\mathbf{a}),$$

where $h(\mathbf{x}) = c_g X_1^{k_1} \cdots X_{n-1}^{k_{n-1}} \in \mathbb{Q}[X_1, \ldots, X_{n-1}]$. Iterating this argument n times, it follows that

$$\sum_{\mathbf{a} \in \mathcal{B}} g(\mathbf{a}) = c_g b_g p^n \quad \text{for some } b_g \in \mathbb{Z}.$$

Thus $\sum_{\mathbf{a} \in \mathcal{B}} f(\mathbf{a}) = \sum_g \sum_{\mathbf{a} \in \mathcal{B}} g(\mathbf{a}) = \left(\sum_g c_g b_g \right) p^n$, where the sum $\sum_g$ is taken over all monomials g occurring in f. Hence, since f is integer–valued with $b_g \in \mathbb{Z}$ and $\mathsf{v}_p(c_g) \geq 0$ for all g, it follows that $\sum_{\mathbf{a} \in \mathcal{B}} f(\mathbf{a}) \equiv 0 \mod p^n$, as desired. □

The final component in Wilson's argument is the following consequence of Lemma 2.6. Again, the case when all $\mathcal{I}_j = [0, p-1]$ is found in Wilson's original paper [52], and the more general case simply requires using Lemma 2.6 in Wilson's original argument, with the details given below.

Lemma 2.7 *Let $p \geq 2$ be prime, let $n \geq 0$, let $\mathcal{B} = I_1 \times \ldots \times I_n$ with each $I_j \subseteq \mathbb{Z}$ for $j \in [1, n]$ a complete system of residues modulo p, let $f_1, \ldots, f_s \in \mathbb{Z}[X_1, \ldots, X_n]$ be nonzero polynomials, and suppose*

$$f(\boldsymbol{x}) = \binom{f_1(\boldsymbol{x})}{k_1} \binom{f_2(\boldsymbol{x})}{k_2} \cdots \binom{f_s(\boldsymbol{x})}{k_s} \in \mathbb{Q}[X_1, \ldots, X_n] \tag{7}$$

for some $k_1, \ldots, k_s \geq 0$ and $s \geq 1$. If $n \geq (m-1) + \frac{\deg f + 1}{p-1}$, where $m \geq 1$, then

$$\sum_{\boldsymbol{a} \in \mathcal{B}} f(\boldsymbol{a}) \equiv 0 \mod p^m.$$

Proof For $k \geq 0$ and $t \geq 1$, we utilize the polynomial identity

$$\binom{Y_1 + \ldots + Y_t}{k} = \sum_{\substack{k_1 + \ldots + k_t = k \\ (k_1, \ldots, k_t) \in \mathbb{N}_0^t}} \binom{Y_1}{k_1} \cdots \binom{Y_t}{k_t}, \tag{8}$$

which holds when each $Y_i > 0$ is an integer by a basic combinatorial counting argument, and extends to the case when each Y_i is a polynomial by noting that the difference of both sides is then a polynomial with all $\mathbf{a} \in \mathbb{N}^t$ as roots. We can write each $f_j(\mathbf{x}) \in \mathbb{Z}[X_1, \ldots, X_n]$, for $j \in [1, s]$, as a sum of $t_j \geq 1$ nonzero monomials with

integer coefficients, and then use the identity given in (8) to write $f(\mathbf{x})$ as a sum of expressions of the form given in (7) (with s replaced by $\sum_{j=1}^{s} t_j$ and the k_i varying), with each such expression in the sum individually satisfying the hypotheses of the lemma and having each $f_j(\mathbf{x})$ occurring in a given expression replaced by a single nonzero monomial. As it would then suffice to prove the lemma individually for each of the expressions in this sum, it follows that we can w.l.o.g. assume each $f_j(\mathbf{x})$ is itself a monomial. As a result, it follows that there is a unique monomial in $f(\mathbf{x})$ whose degree equals $\deg f$, namely, the monomial

$$h(\mathbf{x}) := \frac{1}{k_1! \cdots k_s!} f_1(\mathbf{x})^{k_1} \cdots f_s(\mathbf{x})^{k_s}.$$

Additionally, any monomial $cX_1^{b_1} \cdots X_s^{b_s}$ occurring in $f(\mathbf{x})$ must have $b_j \leq \deg_j(h)$ for all $j \in [1, s]$.

By hypothesis, $\deg f \leq (n-m+1)(p-1)-1$, which combined with the Pigeonhole Principle means there are at most $n-m$ variables X_j having $\deg_j(h(\mathbf{x})) \geq p-1$. By re-indexing, we can w.l.o.g. assume that $\deg_j(h(\mathbf{x})) \leq p-2$ for every $j \in [1, m]$. Since every monomial in $f(\mathbf{x})$ has its degree in the variable X_j bounded by $\deg_j(h(\mathbf{x}))$, we conclude that

$$\deg_j(f(\mathbf{x})) \leq p-2 \quad \text{for all } j \in [1, m]. \tag{9}$$

This has the useful consequence that any variable X_j with $j \in [1, m]$ cannot occur with positive degree in any monomial $f_i(\mathbf{x})$ having $k_i \geq p-1$.

We can write

$$\sum_{\mathbf{a} \in \mathcal{B}} f(\mathbf{a}) = \sum_{\mathbf{b} \in \mathcal{I}_{m+1} \times \ldots \times \mathcal{I}_n} \sum_{\mathbf{c} \in \mathcal{I}_1 \times \ldots \times \mathcal{I}_m} f_{\mathbf{b}}(\mathbf{c}), \tag{10}$$

where $f_{\mathbf{b}}(\mathbf{x}) = f(X_1, \ldots, X_m, b_{m+1}, \ldots, b_n) \in \mathbb{Q}[X_1, \ldots, X_m]$ for $\mathbf{b} = (b_{m+1}, \ldots, b_n)$. Then

$$f_{\mathbf{b}}(\mathbf{x}) = \binom{f_1(X_1, \ldots, X_m, b_{m+1}, \ldots, b_n)}{k_1} \cdots \binom{f_s(X_1, \ldots, X_m, b_{m+1}, \ldots, b_n)}{k_s} \tag{11}$$

is a polynomial in the variables $X_1, \ldots, X_m$. Moreover, in view of (9), we have

$$\deg_j f_{\mathbf{b}} \leq p-2 \quad \text{for all } j \in [1, m].$$

From (11) and the fact that $f_i \in \mathbb{Z}[X_1, \ldots, X_n]$ for all $i \in [1, s]$, we see that $f_{\mathbf{b}} \in \mathbb{Q}[X_1, \ldots, X_m]$ is an integer–valued polynomial.

Let $\mathbf{b} = (b_{m+1}, \ldots, b_n) \in \mathcal{I}_{m+1} \times \ldots \times \mathcal{I}_n$ be arbitrary. In view of (11), $f_{\mathbf{b}}(\mathbf{x})$ is a product of s factors of the form $\binom{f_i(X_1, \ldots, X_m, b_{m+1}, \ldots, b_n)}{k_i}$, for $i \in [1, s]$. If $k_i \geq p$, then none of the variables $X_1, \ldots, X_m$ occur with positive degree in $f_i(\mathbf{x})$, as already noted, meaning the factor $\binom{f_i(X_1, \ldots, X_m, b_{m+1}, \ldots, b_n)}{k_i}$ is a constant, which must then be an integer

since $\binom{f_i(\mathbf{x})}{k_i}$ is an integer–valued polynomial (in view of $f_i \in \mathbb{Z}[X_1, \ldots, X_n]$). From this, and the fact that all $f_i \in \mathbb{Z}[X_1, \ldots, X_n]$, we conclude that the every coefficient c of a monomial in $f_{\mathbf{b}}(\mathbf{x})$ must have the denominator of its coefficient c dividing $\prod_{i\in J} k_i!$, where $J \subseteq [1, s]$ is the subset of all indices $i \in [1, s]$ with $k_i \leq p-1$, which ensures that $\mathsf{v}_p(c) \geq 0$ (as p is prime). Combined with the conclusions of the previous paragraph, we can now apply Lemma 2.6 to $f_{\mathbf{b}}$ to conclude that

$$\sum_{\mathbf{c}\in\mathcal{I}_1\times\ldots\times\mathcal{I}_m} f_{\mathbf{b}}(\mathbf{c}) \equiv 0 \mod p^m \quad \text{for all } \mathbf{b} \in \mathcal{I}_{m+1} \times \ldots \times \mathcal{I}_n,$$

which combined with (10) yields the desired congruence. □

We can now complete the proof of Theorem 1.3.

Proof of Theorem 1.3 The hypotheses give

$$n > (m-1) \max_{i\in[1,s]} \left\{1, \frac{\varphi(p^{m_i})}{p-1} \deg f_i\right\} + \sum_{i=1}^{s} \frac{(t_i+1)p^{m_i}-1}{p-1} \deg f_i. \tag{12}$$

For each $j \in [1, s]$, apply Theorem 2.4 to the integer–valued function with period p^{m_j} which sends 0 to 1 and all elements of $[1, p^{m_j}-1]$ to 0, using $w_j(X)$ as weight function, to find a rational polynomial

$$g_j(X) = \sum_{i=0}^{d_j} b_i^{(j)} \binom{X}{i} \in \mathbb{Q}[X],$$

with all $b_i^{(j)} \in \mathbb{Z}$ and $d_j \leq (t_j+1)p^{m_j} + (m-1)\varphi(p^{m_j}) - 1$, such that

$$g_j(x) \equiv \begin{cases} w_j\left(\frac{x}{p^{m_j}}\right) \mod p^m & \text{if } x \equiv 0 \mod p^{m_j} \\ 0 \mod p^m & \text{if } x \not\equiv 0 \mod p^{m_j}, \end{cases} \quad \text{and} \tag{13}$$

$$b_i^{(j)} \equiv 0 \mod p^{\ell}, \quad \text{where } \ell = \max\left\{0, \left\lceil \frac{i-(t_j+1)p^{m_j}+1}{\varphi(p^{m_j})} \right\rceil\right\}. \tag{14}$$

In view of all definitions involved,

$$\begin{aligned} N &\equiv \sum_{\mathbf{a}\in\mathcal{B}} g_1\big(f_1(\mathbf{a})\big) g_2\big(f_2(\mathbf{a})\big) \cdots g_s\big(f_s(\mathbf{a})\big) \mod p^m \\ &= \sum_{\mathbf{a}\in\mathcal{B}} \left(\sum_{i=0}^{d_1} b_i^{(1)} \binom{f_1(\mathbf{a})}{i}\right)\left(\sum_{i=0}^{d_2} b_i^{(2)} \binom{f_2(\mathbf{a})}{i}\right) \cdots \left(\sum_{i=0}^{d_s} b_i^{(s)} \binom{f_s(\mathbf{a})}{i}\right) \\ &= \sum_{(k_1,\ldots,k_s)\in\prod_{i=1}^{s}[0,d_i]} b_{k_1}^{(1)} b_{k_2}^{(2)} \cdots b_{k_s}^{(s)} \sum_{\mathbf{a}\in\mathcal{B}} \binom{f_1(\mathbf{a})}{k_1}\binom{f_2(\mathbf{a})}{k_2} \cdots \binom{f_s(\mathbf{a})}{k_s}. \end{aligned} \tag{15}$$

It suffices to show each summand in (15) is divisible by p^m. With this goal in mind, let $(k_1, \ldots, k_s) \in \prod_{i=1}^{s}[0, d_i]$ be arbitrary. For $j \in [1, s]$, define $\ell_j := \max\{0, \left\lceil \frac{k_j-(t_j+1)p^{m_j}+1}{\varphi(p^{m_j})} \right\rceil\} \geq \frac{k_j-(t_j+1)p^{m_j}+1}{\varphi(p^{m_j})}$, in which case

$$k_j \leq \ell_j \varphi(p^{m_j}) + (t_j + 1)p^{m_j} - 1. \tag{16}$$

All summands in (15) with $\ell_1 + \ldots + \ell_s \geq m$ are congruent to 0 modulo p^m by (13), since this ensures that $b_{k_1}^{(1)} \cdots b_{k_s}^{(s)} \equiv 0 \mod p^m$. We need only consider those with

$$\ell_1 + \ldots + \ell_s = m - t \quad \text{for some } t \geq 1. \tag{17}$$

In this case, (13) instead ensures that the coefficient $b_{k_1}^{(1)} b_{k_2}^{(2)} \cdots b_{k_s}^{(s)}$ is divisible by p^{m-t}, so we just need to show that the summation $\sum_{\mathbf{a}\in\mathcal{B}} \binom{f_1(\mathbf{a})}{k_1}\binom{f_2(\mathbf{a})}{k_2} \cdots \binom{f_s(\mathbf{a})}{k_s}$ is divisible by p^t.

In view of (16), (17), (12) and $t \geq 1$, we have

$$\begin{aligned}
&\deg\left(\binom{f_1(\mathbf{x})}{k_1}\binom{f_2(\mathbf{x})}{k_2}\cdots\binom{f_s(\mathbf{x})}{k_s}\right) = k_1 \deg f_1 + \ldots + k_s \deg f_s \\
&\leq \sum_{j=1}^{s}\Big(\ell_j\varphi(p^{m_j}) + (t_j+1)p^{m_j} - 1\Big)\deg f_j \\
&= (p-1)\Big(\sum_{i=1}^{s}\ell_i \frac{\varphi(p^{m_i})}{p-1}\deg f_i + \sum_{i=1}^{s}\frac{(t_i+1)p^{m_i}-1}{p-1}\deg f_i\Big) \\
&\leq (p-1)\Big((\ell_1+\ldots+\ell_s)\max_{i\in[1,s]}\Big\{1, \frac{\varphi(p^{m_i})}{p-1}\deg f_i\Big\} + \sum_{i=1}^{s}\frac{(t_i+1)p^{m_i}-1}{p-1}\deg f_i\Big) \\
&= (p-1)\Big((m-1-(t-1))\max_{i\in[1,s]}\Big\{1, \frac{\varphi(p^{m_i})}{p-1}\deg f_i\Big\} + \sum_{i=1}^{s}\frac{(t_i+1)p^{m_i}-1}{p-1}\deg f_i\Big) \\
&< (p-1)\Big(n-(t-1)\max_{i\in[1,s]}\Big\{1, \frac{\varphi(p^{m_i})}{p-1}\deg f_i\Big\}\Big) \leq (p-1)(n+1-t),
\end{aligned}$$

implying that

$$n \geq (t-1) + \frac{\deg\left(\binom{f_1(\mathbf{x})}{k_1}\binom{f_2(\mathbf{x})}{k_2}\cdots\binom{f_s(\mathbf{x})}{k_s}\right)+1}{p-1}.$$

But now Lemma 2.7 implies that $\sum_{\mathbf{a}\in\mathcal{B}} \binom{f_1(\mathbf{x})}{k_1}\binom{f_2(\mathbf{x})}{k_2} \cdots \binom{f_s(\mathbf{x})}{k_s}$ is divisible by p^t, completing the proof as already noted. □

To effectively use Theorem 1.3 requires a "good" choice for the complete system of residues modulo p. This can generally be achieved by use of Hensel's Lemma [36, Theorem 2.23]. We state one commonly used version below.

Theorem 2.8 (Hensel's Lemma) *Let $p \geq 2$ be prime, let $m \geq 1$ be an integer, and let $f(X) \in \mathbb{Z}[X]$ be a polynomial. If $f(x) \equiv 0 \mod p^m$ and $f'(x) \not\equiv 0 \mod p$, where $x \in \mathbb{Z}$, then there is some $y \in \mathbb{Z}$ with*

$$y \equiv x \mod p^m \quad \text{and} \quad f(y) \equiv 0 \mod p^{m+1}.$$

Moreover, the value of y is uniquely determined modulo p^{m+1}.

We conclude the section by giving the short derivation of Proposition 1.4 using Hensel's Lemma, which provides the appropriate choice for the complete system of residues for many combinatorial applications of Theorem 1.3.

Proof of Proposition 1.4 Let $z \in [1, p-1]$ be a primitive residue class modulo the prime p, meaning $\{0\} \cup \{z^i : i \in [1, p-1]\}$ is a complete system of residues modulo p (since $\mathbb{Z}/p\mathbb{Z}$ is a finite field with cyclic multiplicative group, such z exists) and

$$z^{p-1} \equiv 1 \mod p.$$

Let

$$f(X) = X^{p-1} - 1 \in \mathbb{Z}[X]$$

and note that $f'(x) = (p-1)x \equiv -x \not\equiv 0 \mod p$ for any $x \in \mathbb{Z}$ with $x \not\equiv 0 \mod p$. For each $i \in [1, p-1]$, we have $f(z^i) = (z^{p-1})^i - 1 \equiv 1^i - 1 = 0 \mod p$. Thus we can repeatedly apply Hensel's Lemma (Theorem 2.8) to find some $y_i \in [0, p^m - 1]$ with

$$y_i \equiv z^i \not\equiv 0 \mod p \quad \text{and} \quad y_i^{p-1} - 1 = f(y_i) \equiv 0 \mod p^m, \tag{18}$$

for all $i \in [1, p-1]$. Let $\mathcal{I} = \{0\} \cup \{y_i : i \in [1, p-1]\}$. Since $\{0\} \cup \{z^i : i \in [1, p-1]\}$ was a complete system of residues modulo p with $y_i \equiv z^i \mod p$ for all i, it follows that $\mathcal{I}$ remains a complete system of residues modulo p, and one with the needed properties in view of (18). □

3 Applications in Combinatorial Number Theory

In this section, we give the proofs of the applications of Theorem 1.3.

Proposition 3.1 *Let G be a finite abelian p-group with exponent $q > 1$, and let S be a sequence of terms from G with $|S| \geq m\frac{(p-1)q}{p} + \mathsf{D}^*(G)$, where $m \geq 0$. Then*

$$\sum_{j=0}^{\infty} (p-1)^j N_j(S) \equiv 0 \mod p^{m+1}.$$

Proof Write $G = C_{q_1} \oplus \ldots \oplus C_{q_r}$ with each q_i a power of p and

$$1 < q_1 \le \ldots \le q_r = q.$$

Then $\mathsf{D}^*(G) = \sum_{i=1}^{r}(q_i - 1) + 1$. Let $(e_1, \ldots, e_r)$ be a basis for G with $\mathrm{ord}(e_i) = q_i$ for $i \in [1, r]$. Let $S = g_1 \cdot \ldots \cdot g_\ell$, so $\ell = |S| \ge m\frac{(p-1)q}{p} + \mathsf{D}^*(G)$. For each $i \in [1, \ell]$, write

$$g_i = \sum_{j=1}^{r} a_i^{(j)} e_j \quad \text{with } a_i^{(j)} \in [0, q_j - 1].$$

Let

$$f_j(\mathbf{x}) = \sum_{i=1}^{\ell} a_i^{(j)} X_i^{p-1} \in \mathbb{Z}[X_1, \ldots, X_\ell], \quad \text{for } j \in [1, r].$$

In view of Proposition 1.4, let $\mathcal{I} \subseteq [0, q-1]$ be a complete system of residues modulo p such that

$$x^{p-1} \equiv \begin{cases} 1 \mod q \text{ if } x \not\equiv 0 \mod p \\ 0 \mod q \text{ if } x \equiv 0 \mod p, \end{cases} \quad \text{for every } x \in \mathcal{I}. \tag{19}$$

Observe that $\max_{j\in[1,r]}\left\{1, \frac{\varphi(q_j)}{p-1}\deg f_j\right\} = \max_{j\in[1,r]}\left\{\varphi(q_j)\right\} = \varphi(q) = \frac{(p-1)q}{p}$ and

$$\ell = |S| \ge m \max_{j\in[1,r]}\left\{1, \frac{\varphi(q_j)}{p-1}\deg f_j\right\} + \sum_{j=1}^{r}\frac{q_j - 1}{p-1}\deg f_j + 1.$$

Thus we can apply Theorem 1.3, with m taken to be $m + 1$, taking $\mathcal{I}_j = \mathcal{I}$ for all j, and using the polynomials $f_1, \ldots, f_r$, prime powers $q_1, \ldots, q_r = q$, and weight functions $w_j(X) = 1$ for all $j \in [1, r]$. As a result, letting

$$V = \{\mathbf{a} \in \mathcal{I}^\ell : \ f_j(\mathbf{a}) \equiv 0 \mod q_j \ \text{ for all } j \in [1, r]\},$$

it follows that

$$|V| \equiv 0 \mod p^{m+1}. \tag{20}$$

Let us next describe what $|V|$ equals in terms of the zero-sum subsequences of S.

Associate to each $\mathbf{a} \in \mathcal{I}^\ell$ the subsequence $S_\mathbf{a} = \prod_{j\in I_\mathbf{a}}^{\bullet} g_j$, where $I_\mathbf{a} \subseteq [1, \ell]$ consists of all $j \in [1, \ell]$ for which the j-th coordinate of $\mathbf{a}$ is nonzero modulo p. Thus the nonzero (modulo p) terms in $\mathcal{I}$ "select" the terms included in the sequence $S_\mathbf{a}$. In view of (19), the conditions $f_j(\mathbf{a}) \equiv 0 \mod q_j$ in the definition of V, for $j \in [1, r]$, restrict to tuples $\mathbf{a} \in \mathcal{I}^\ell$ for which the associated sequence $S_\mathbf{a}$ is zero-sum.

This means that the tuples $\mathbf{a} \in V$ are precisely those whose associated sequence $S_{\mathbf{a}}$ is a zero-sum subsequence, in which case $|S_{\mathbf{a}}| = j$ for some $j \geq 0$. Moreover, each zero-sum subsequence of length j is associated to exactly $(p-1)^j$ tuples $\mathbf{a} \in \mathcal{I}^\ell$, for there are $(p-1)$ elements of $\mathcal{I}$ that are nonzero modulo p, each of which selects one term in $S_{\mathbf{a}}$, while the unique element of $\mathcal{I}$ congruent to zero is the only way to *not* select a term in $S_{\mathbf{a}}$. As a result, $|V| = \sum_{j=0} \infty (p-1)^j N_j(S)$, which combined with (20) yields the desired conclusion. □

We now can complete the proof regarding the Davenport Constant. We remark that Proposition 3.1 is only formulated as a congruence involving the number of zero-sum subsequences of S, but the method also produces a similar congruence involving the number of subsequences of S with sum g, for any fixed $g \in G$. The collection of all such congruences (with $m = 0$), when rephrased in terms of group algebras, is then equivalent to [37, Theorem 1], which was the original main step for proving Theorem 1.5, just as Proposition 3.1 is the main step here. For this simple application, only the existence of a nontrivial solution to the linear equation featuring in Proposition 3.1 is needed, meaning a generalization of Chevalley's Theorem (rather than the Chevalley–Warning Theorem) would suffice. In this sense, the proof below may be viewed as a variation on one given by Schanuel [41].

Proof of Theorem 1.5 Let $G = C_{q_1} \oplus \ldots \oplus C_{q_s}$ and let $(e_1, \ldots, e_s)$ be a basis for G with $\mathrm{ord}(e_i) = q_i$ for all $i \in [1, s]$. We can assume G is nontrivial else $\mathsf{D}(G) = \mathsf{D}^*(G) = 1$. Now $\mathsf{D}^*(G) = 1 + \sum_{i=1}^{s} (q_i - 1)$ and the sequence $\prod_{i\in[1,s]}^{\bullet} e_i^{[q_i-1]}$ is zero-sum free, showing $\mathsf{D}(G) \geq \mathsf{D}^*(G)$. To show the upper bound, let S be a sequence of terms from G with length $\mathsf{D}^*(G)$. Assuming by contradiction that S is zero-sum free, we obtain $N_i(S) = 0$ for all $i > 0$, in which case Proposition 3.1 applied with $m = 0$ yields the contradiction $1 = N_0 \equiv 0 \mod p$. □

As a minor variation on Proposition 3.1, we have the following result giving a system of t linear equations (modulo p^{m+1}) in the variables $N_\alpha(S), N_{q+\alpha}(S), N_{2q+\alpha}(S), \ldots$.

Proposition 3.2 *Let G be a finite abelian p-group with exponent $q > 1$, let $\alpha \in [0, q-1]$, let $t \geq 1$, and let S be a sequence of terms from G with $|S| \geq m\frac{(p-1)q}{p} + tq - 1 + \mathsf{D}^*(G)$, where $m \geq 0$. Then*

$$\sum_{j=0}^{\infty} (p-1)^{jq+\alpha} \Big(j^i N_{jq+\alpha}(S) \Big) \equiv 0 \mod p^{m+1}, \quad \text{for every } i \in [0, t-1].$$

Proof Write $G = (\mathbb{Z}/q_1\mathbb{Z}) \oplus \ldots \oplus (\mathbb{Z}/q_r\mathbb{Z})$ with each q_i a power of p and

$$1 < q_1 \leq \ldots \leq q_r = q_{r+1} := q.$$

Then $\mathsf{D}^*(G) = \sum_{i=1}^{r} (q_i - 1) + 1$. Let $(e_1, \ldots, e_r)$ be a basis for G with $\mathrm{ord}(e_i) = q_i$ for $i \in [1, r]$. Let $S = g_1 \cdot \ldots \cdot g_\ell$, so $\ell = |S| \geq m\frac{(p-1)q}{p} + tq - 1 + \mathsf{D}^*(G)$. For

each $i \in [1, \ell]$, write

$$g_i = \sum_{j=1}^{r} a_i^{(j)} e_j \quad \text{with } a_i^{(j)} \in [0, q_j - 1].$$

Let

$$f_j(\mathbf{x}) = \sum_{i=1}^{\ell} a_i^{(j)} X_i^{p-1} \in \mathbb{Z}[X_1, \ldots, X_\ell], \quad \text{for } j \in [1, r].$$

Let

$$f_{r+1}(\mathbf{x}) = \sum_{i=1}^{\ell} X_i^{p-1} - \alpha \in \mathbb{Z}[X_1, \ldots, X_\ell].$$

For each $i \in [0, t-1]$, let

$$w_i(X) = X^i \in \mathbb{Z}[X].$$

In view of Proposition 1.4, let $\mathcal{I} \subseteq [0, qp^{m+1} - 1]$ be a complete system of residues modulo p such that

$$x^{p-1} \equiv \begin{cases} 1 \mod qp^{m+1} & \text{if } x \not\equiv 0 \mod p \\ 0 \mod qp^{m+1} & \text{if } x \equiv 0 \mod p, \end{cases} \quad \text{for every } x \in \mathcal{I}. \tag{21}$$

Observe that $\max_{j\in[1,r+1]} \left\{1, \frac{\varphi(q_j)}{p-1} \deg f_j\right\} = \max_{j\in[1,r+1]} \left\{\varphi(q_j)\right\} = \varphi(q) = \frac{(p-1)q}{p}$ and

$$\ell = |S| \geq m \max_{j\in[1,r+1]} \left\{1, \frac{\varphi(q_j)}{p-1} \deg f_j\right\} + \frac{tq-1}{p-1} \deg f_{r+1} + \sum_{j=1}^{r} \frac{q_j - 1}{p-1} \deg f_j + 1.$$

Thus, for any fixed $i \in [0, t-1]$, we can apply Theorem 1.3, with m taken to be $m+1$, taking $\mathcal{I}_j = \mathcal{I}$ for all j, and using the polynomials $f_1, \ldots, f_r, f_{r+1}$, weights $\underbrace{w_0, \ldots, w_0}_{r}, w_i$, and prime powers $q_1, \ldots, q_r, q_{r+1} = q$. As a result, letting

$$V = \{\mathbf{a} \in \mathcal{I}^\ell : \ f_j(\mathbf{a}) \equiv 0 \mod q_j \ \text{ for all } j \in [1, r+1]\},$$

it follows that the weighted size of V is congruent to 0 modulo p^{m+1}. Let us next describe what this size equals.

Associate to each $\mathbf{a} \in \mathcal{I}^\ell$ the subsequence $S_{\mathbf{a}} = \prod_{j\in I_{\mathbf{a}}}^{\bullet} g_j$, where $I_{\mathbf{a}} \subseteq [1, \ell]$ consists of all $j \in [1, \ell]$ for which the j-th coordinate of $\mathbf{a}$ is nonzero modulo p. In view of (21), the conditions $f_j(\mathbf{a}) \equiv 0 \mod q_j$ in the definition of V, for $j \in [1, r]$,

restrict to tuples $\mathbf{a} \in \mathcal{I}^\ell$ for which the associated sequence $S_\mathbf{a}$ is zero-sum. Likewise, the additional condition $f_{r+1}(\mathbf{a}) \equiv 0 \mod q$ further restricts to tuples $\mathbf{a} \in \mathcal{I}^\ell$ whose associated sequence $S_\mathbf{a}$ has length $|S_\mathbf{a}| = |I_\mathbf{a}| \equiv \alpha \mod q$. This means that the tuples $\mathbf{a} \in V$ are precisely those whose associated sequence $S_\mathbf{a}$ is a zero-sum subsequence of length $|S_\mathbf{a}| \equiv \alpha \mod q$, meaning $|S_\mathbf{a}| = jq + \alpha$ for some $j \geq 0$. Moreover, each zero-sum subsequence of length $jq + \alpha$ is associated to exactly $(p-1)^{jq+\alpha}$ tuples $\mathbf{a} \in \mathcal{I}^\ell$, and the weighted size of each such tuple is $w_i(j) \equiv j^i \mod p^{m+1}$ (in view of (21)). As a result, given any $i \in [0, t-1]$, the weighted size of V equals $\sum_{j=0}^{\infty}(p-1)^{jq+\alpha}\Big(j^i N_{jq+\alpha}(S)\Big)$ modulo p^{m+1}, meaning the conclusion of Theorem 1.3 is precisely the desired conclusion of the proposition. □

We now give the proof of the Kemnitz Conjecture, which contains Alon and Dubiner's argument that $N_{3p}(S) \neq 0$ implies $N_p(S) \neq 0$ [2, Lemma 3.2]. We remark that it would also be possible to derive the congruences below using the higher order p divisibility of $|V|$ in Theorem 1.3 (combined with combinatorial double counting arguments of the type used by Reiher [38]) rather than the weight functions. However, using the weight functions directly is simpler.

Proof of Theorem 1.6 Let $G = C_p^2$ with (e_1, e_2) a basis for G. Note that $0^{[p-1]} \cdot e_1^{[p-1]} \cdot e_2^{[p-1]} \cdot (e_1+e_2)^{[p-1]}$ is a sequence of $4p-4$ terms from G containing no p-term zero-sum subsequence, showing $\mathsf{s}_p(C_p^2) \geq 4p-3$. To show the upper bound, assume by contradiction that S is a sequence of terms from G with $|S| = 4p-3$ and $0 \notin \Sigma_p(S)$. If $p = 2$, then $|S| = 4p-3 = 5$ ensures via the Pigeonhole Principle that S contains a term g with multiplicity at least two, in which case $g^{[2]}$ will be a p-term zero-sum subsequence, contrary to assumption. Therefore we can assume $p \geq 3$.

If $T \mid S$ is any subsequence with $|T| \geq 3p-2$, then Proposition 3.2 (applied with $\alpha = 0$, $m = 0$ and $t = 1$) implies that $N_0(T) - N_p(T) + N_{2p}(T) - N_{3p}(T) \equiv 0 \mod p$. In particular, since $N_p(S) = 0$ by assumption, it follows that any zero-sum subsequence $T \mid S$ with $|T| = 3p$ has $N_{2p}(T \cdot g^{[-1]}) \equiv -N_0(T \cdot g^{[-1]}) = -1 \mod p$, for any $g \in \mathrm{Supp}(T)$, ensuring that $T \cdot g^{[-1]}$ has a zero-sum subsequence R of length $2p$. However, the complement of R in T would then be a zero-sum subsequence of length $|T| - |R| = p$, contradicting that $N_p(S) = 0$. Therefore we instead conclude that

$$N_p(S) = N_{3p}(S) = 0, \tag{22}$$

and now Proposition 3.2 implies that

$$N_{2p}(T) \equiv -1 \mod p \quad \text{for all } T \mid S \text{ with } |T| \geq 3p-2. \tag{23}$$

For $j \geq 0$, let

$$N_j = N_j(S).$$

Since $|S| \geq 3p-2$, Proposition 3.2 (applied with $\alpha = p-1$, $m=0$ and $t=1$) implies that

$$N_{p-1} - N_{2p-1} + N_{3p-1} \equiv 0 \mod p \tag{24}$$

Let $T \mid S$ be an arbitrary zero-sum sequence with $|T| = 3p-1$. Then $N_{p-1}(T) = N_{2p}(T) \equiv -1 \mod p$ by (23), with the first equality holding since the complement in T of a zero-sum subsequence of T is also zero-sum. Thus $\sum_T N_{p-1}(T) \equiv -N_{3p-1} \mod p$, where the sum is taken over all zero-sum subsequences $T \mid S$ with $|T| = 3p-1$. On the other hand, every zero-sum subsequence $R \mid S$ with $|R| = p-1$ is contained in exactly $N_{2p}(S \cdot R^{[-1]})$ zero-sum subsequences $T \mid S$ with $|T| = 3p-1$. Since $|S \cdot R^{[-1]}| = 3p-2$, (23) ensures that $N_{2p}(S \cdot R^{[-1]}) \equiv -1 \mod p$ for any such R, in which case $-N_{3p-1} \equiv \sum_T N_{p-1}(T) = \sum_R N_{2p}(S \cdot R^{[-1]}) \equiv -N_{p-1} \mod p$, where the second sum is taken over all zero-sum subsequences $R \mid S$ with $|R| = p-1$. Hence

$$N_{p-1} \equiv N_{3p-1} \mod p. \tag{25}$$

Observe that $N_j(S \cdot 0) = N_j + N_{j-1}$ for every $j > 0$. Thus, since $|S \cdot 0| = |S| + 1 = 4p-2$, applying Proposition 3.2 (with $\alpha = 0$, $m=0$ and $t=2$) to $S \cdot 0$ implies

$$N_p + N_{p-1} - 2N_{2p} - 2N_{2p-1} + 3N_{3p-1} + 3N_{3p} \equiv 0 \mod p.$$

We have $N_{2p} \equiv -1 \mod p$ by (23), and $N_p = N_{3p} = 0$ by (22). Thus

$$N_{p-1} - 2N_{2p-1} + 3N_{3p-1} \equiv -2 \mod p. \tag{26}$$

The equations (24), (25) and (26) form a system of 3 linear equations in the variables N_{p-1}, N_{2p-1} and N_{3p-1} over the field $\mathbb{Z}/p\mathbb{Z}$. However, for $p \geq 3$, this system is inconsistent, yielding a proof concluding contradiction. □

The remainder of the section is devoted to the constant $\mathsf{s}_{k\exp(G)}(G)$. We begin with the refinement to the result obtained via Rónyai's method.

Proof of Theorem 1.7 Letting $X' \subseteq X$ be the subset consisting of the smallest $d+m$ elements in X, we have $\max X' \leq \max X - (|X| - d - m)$. Since $\max X' < \min(X \setminus X')$, it follows that (1) also holds for X'. If the result holds whenever $|X| = d+m$, then applying this case to X' yields

$$\begin{aligned}
\mathsf{s}_{X\cdot q}(G) \leq s_{X'\cdot q}(G) &\leq \big(\max X' - d - \frac{m}{p} + 1\big)q + \mathsf{D}^*(G) - 1 \\
&\leq \big(\max X - |X| + \frac{m(p-1)}{p} + 1\big)q + \mathsf{D}^*(G) - 1 \\
&\leq \big(\max X + 1 - \frac{m}{p}\big)q - r,
\end{aligned}$$

with the third inequality in view of the hypothesis $|X| \geq d+m$, as desired. Therefore it suffices to handle the case when $|X| = d+m$, which we now assume. We need to show

$$\mathsf{s}_{X\cdot q}(G) \leq \big(k-d-\frac{m}{p}+1\big)q + \mathsf{D}^*(G) - 1,$$

where $k = \max X$. Let $\{x_1, \ldots, x_s\} = [1,k]\backslash X$, where $s = k-d-m$ and $1 \leq x_1 < \ldots < x_s < k$.

Write $G = C_{q_1} \oplus \ldots \oplus C_{q_r}$ with each q_i a power of p and

$$1 < q_1 \leq \ldots \leq q_r = q_{r+1} := q.$$

Then $\mathsf{D}^*(G) = \sum_{i=1}^{r}(q_i - 1) + 1$. Let $(e_1, \ldots, e_r)$ be a basis for G with $\mathrm{ord}(e_i) = q_i$ for $i \in [1,r]$. Let $S = g_1 \cdot \ldots \cdot g_\ell$ be a sequence of terms from G with $|S| = \ell = (k-d-\frac{m}{p}+1)q + \mathsf{D}^*(G) - 1$. We have

$$\left\lfloor \frac{|S|}{q} \right\rfloor \leq k-d+\left\lfloor 1+\frac{\mathsf{D}^*(G)-1}{q} \right\rfloor = k. \tag{27}$$

For each $i \in [1,\ell]$, write

$$g_i = \sum_{j=1}^{r} a_i^{(j)} e_j \quad \text{with } a_i^{(j)} \in [0, q_j - 1].$$

Let

$$f_j(\mathbf{x}) = \sum_{i=1}^{\ell} a_i^{(j)} X_i^{p-1} \in \mathbb{Z}[X_1, \ldots, X_\ell], \quad \text{for } j \in [1,r].$$

Let

$$f_{r+1}(\mathbf{x}) = \sum_{i=1}^{\ell} X_i^{p-1} \in \mathbb{Z}[X_1, \ldots, X_\ell].$$

For $i \in [0, k-d-m]$, let

$$w_i(X) = X^i \in \mathbb{Z}[X].$$

In view of Proposition 1.4, let $\mathcal{I} \subseteq [0, qp^{m+1}-1]$ be a complete system of residues modulo p such that

$$x^{p-1} \equiv \begin{cases} 1 \mod qp^{m+1} & \text{if } x \not\equiv 0 \mod p \\ 0 \mod qp^{m+1} & \text{if } x \equiv 0 \mod p, \end{cases} \quad \text{for every } x \in \mathcal{I}. \tag{28}$$

Observe that $\max_{j\in[1,r+1]}\left\{1,\ \frac{\varphi(q_j)}{p-1}\deg f_j\right\} = \max_{j\in[1,r+1]}\left\{\varphi(q_j)\right\} = \varphi(q) = (p-1)\frac{q}{p}$ and

$$\begin{aligned}\ell = |S| &= m(p-1)\frac{q}{p} + \sum_{j=1}^{r}(q_j-1) + (k-d-m+1)q\\ &= m\max_{j\in[1,r+1]}\left\{1,\ \frac{\varphi(q_j)}{p-1}\deg f_j\right\} + \sum_{j=1}^{r}\frac{q_j-1}{p-1}\deg f_j\\ &\quad + \frac{(k-d-m+1)q-1}{p-1}\deg f_{r+1} + 1.\end{aligned}$$

Thus, for each $i \in [0, k-d-m]$, we can apply Theorem 1.3, with m taken to be $m+1$, taking $\mathcal{I}_j = \mathcal{I}$ for all j, and using the polynomials $f_1, \ldots, f_r, f_{r+1}$, weights $\underbrace{w_0, \ldots, w_0}_{r}, w_i$, and prime powers $q_1, \ldots, q_r, q$. As a result, letting

$$V = \{\mathbf{a} \in \mathcal{I}^\ell :\ f_j(\mathbf{a}) \equiv 0 \mod q_j \text{ for all } j \in [1, r+1]\},$$

it follows that the weighted size of V is congruent to 0 modulo p^{m+1}, for each $i \in [0, k-d-m]$. Let us next describe what this size equals.

Let

$$N_j := N_{jq}(S) \quad \text{for } j \in [0,k].$$

Let $i \in [0, k-d-m]$ be arbitrary. Associate to each $\mathbf{a} \in \mathcal{I}^\ell$ the subsequence $S_\mathbf{a} = \prod^\bullet_{j\in I_\mathbf{a}} g_j$, where $I_\mathbf{a} \subseteq [1,\ell]$ consists of all $j \in [1,\ell]$ for which the j-th coordinate of $\mathbf{a}$ is nonzero modulo p. In view of (28), the conditions $f_j(\mathbf{a}) \equiv 0 \mod q_j$, for $j \in [1,r]$, restrict to tuples $\mathbf{a} \in \mathcal{I}^\ell$ for which the associated sequence $S_\mathbf{a}$ is zero-sum. Likewise, the additional condition $f_{r+1}(\mathbf{a}) \equiv 0 \mod q$ further restricts to tuples $\mathbf{a} \in \mathcal{I}^\ell$ whose associated sequence $S_\mathbf{a}$ has length $|S_\mathbf{a}| = |I_\mathbf{a}| \equiv 0 \mod q$. This means that the tuples $\mathbf{a} \in V$ are precisely those whose associated sequence $S_\mathbf{a}$ is a zero-sum subsequence of length $|S_\mathbf{a}| \equiv 0 \mod q$, meaning $|S_\mathbf{a}| = jq$ for some $j \in [0,k]$ (in view of (27)). Moreover, each zero-sum subsequence of length jq is associated to exactly $(p-1)^{jq}$ tuples $\mathbf{a} \in \mathcal{I}^\ell$, and the weighted size of each such tuple is $w_i(j) \equiv j^i \mod p^{m+1}$ (in view of (28)). As a result, for $i \in [0, k-d-m]$, the weighted size of V equals $\sum_{j=0}^{k} j^i (p-1)^{jq} N_j \mod p^{m+1}$, meaning the conclusion of Theorem 1.3 is that

$$\begin{aligned}&(p-1)^q N_1 + (p-1)^{2q} N_2 + \ldots + (p-1)^{jq} N_j + \ldots + (p-1)^{kq} N_k\\ &\equiv -N_0 = -1 \mod p^{m+1}\end{aligned}$$

and

$$(p-1)^q N_1 + 2^i (p-1)^{2q} N_2 + \ldots + j^i (p-1)^{jq} N_j + \ldots + k^i (p-1)^{kq} N_k \equiv 0 \mod p^{m+1},$$

for every $i \in [1, k-d-m]$.

Assuming by contradiction that S has no zero-sum subsequence of length kq with $k \in X$, it follows that $N_j = 0$ for all $j \in X$. This leaves us with a system of $k-d-m+1$ linear equations, one for each $i \in [0, k-d-m]$, in the $k-d-m$ variables N_j, where $j \in [1,k]\backslash X$, over the ring $R = \mathbb{Z}/p^{m+1}\mathbb{Z}$. We proceed to show this system is inconsistent, which will complete the proof.

Let A' be $(k-d-m+1) \times (k-d-m)$ matrix, with rows indexed by $i \in [0, k-d-m]$, columns indexed by $j \in [1,k] \setminus X$, and (i,j)-th entry equal to $j^i (p-1)^{jq}$, and let $\mathbf{y}$ be the column vector $[N_j]_{j \in [1,k]\setminus X}$. Then the above system of linear equations can be written as $A'\mathbf{y} \equiv [-1, 0, \ldots, 0] \mod p^{m+1}$. To show this system is inconsistent, it suffices to show a nonzero (modulo p^{m+1}) multiple of the first row of A' can be written as a linear combination of the remaining rows. To this end, let $A = [j^i (p-1)^{jq}]_{i \in [1,k-d-m],\, j \in [1,k]\setminus X}$ be the $(k-d-m) \times (k-d-m)$ matrix obtained from A' by removing the first row. We continue by calculating $\det A$. Note that A can be obtained from the matrix $B = [j^i]_{i \in [0,k-d-m-1],\, j \in [1,k]\setminus X}$ by multiplying each j-th column of B by $j(p-1)^{jq}$. Thus

$$\det A = \Big(\prod_{j \in [1,k]\setminus X} j(p-1)^{jq} \Big) \det B = \Big(\prod_{j=1}^{s} x_j (p-1)^{x_j q} \Big) \det B,$$

where we recall that $[1,k] \setminus X = \{x_1, \ldots, x_s\}$ with $x_1 < \ldots < x_s$ (by hypothesis). However, note that B is simply a Vandermonde matrix, whose well-known determinant (see [24, Theorem 17.1.1]) equals $\det B = \prod_{1 \le i < j \le s} (x_j - x_i)$. It follows that

$$\det A = \Big(\prod_{j=1}^{s} x_j (p-1)^{x_j q} \Big) \Big(\prod_{1 \le i < j \le s} (x_j - x_i) \Big) \not\equiv 0 \mod p^{m+1},$$

with this determinant being nonzero by hypothesis. In consequence, the rows of A are linearly independent over $\mathbb{Q}$, meaning there is some $\mathbb{Q}$-linear combination of the rows of A equal to the first row in A'. Moreover, since the entries of A' are integers, Cramer's Rule (see [24, pp. 348]) ensures that each coefficient in this linear combination has its denominator dividing $\det A$. By clearing denominators, it then follows that there is a $\mathbb{Z}$-linear combination of the rows of A equal to the first row of A' multiplied by the integer $\det A \not\equiv 0 \mod p^{m+1}$. Reducing modulo p^{m+1}, we obtain a linear combination of the rows of A equal to a nonzero (modulo p^{m+1}) multiple of the first row of A', which shows that the system of linear equations is inconsistent, completing the proof as noted earlier. □

The following is the main step in the proof of Theorem 1.9.

Proposition 3.3 *Let G be a finite abelian p-group with exponent q, let $d = \left\lceil \frac{\mathsf{D}^*(G)}{q} \right\rceil$, and let k be an integer such that $\frac{d(d-1)}{2} + 1 \le k \le p$. Then*

$$\mathsf{s}_{kq}(G) \le kq + \mathsf{D}^*(G) - 1.$$

Proof If $q = 1$, then G is trivial with $\mathsf{s}_{kq}(G) = kq = kq + \mathsf{D}^*(G) - 1$, as desired. Therefore we can assume $q > 1$. Let $r \in [1, q]$ be the integer such that $d = \frac{\mathsf{D}^*(G)+r-1}{q}$. Note that $d \ge 1$. Assume by contradiction that S is a sequence of terms from G with

$$0 \notin \Sigma_{kq}(S) \quad \text{and} \quad |S| = kq + \mathsf{D}^*(G) - 1 = (k+d)q - r.$$

Claim A: There are disjoint subsequences $T_1 \cdot \ldots \cdot T_{d-1} \mid S$ such that each T_i is zero-sum with $|T_i| = iq$, for every $i \in [1, d-1]$.

Proof Let $Y \subseteq [1, d-1]$ be a maximal subset (possibly empty) such that there are disjoint subsequences $\prod_{i\in Y}^{\bullet} T_i \mid S$ with each T_i is zero-sum and $|T_i| = iq$, for every $i \in Y$. To establish the claim, we need to show $Y = [1, d-1]$. If $d = 1$, then the claim is trivial taking $Y = \emptyset$, so we can assume $d \ge 2$.

We begin by showing $|Y| \ge 1$. To this end, let $X = [1, d-1] \cup \{k\}$. In view of $k \ge \frac{d(d-1)}{2} + 1 \ge d \ge 1$, we have $X \subseteq \mathbb{N}$ and $|X| = d$. In view of $k \le p$, we have $[1, \max X] \setminus X = [d, k-1] \subseteq [d, p-1]$. Thus, since $|S| = (k+d)q - r \ge (k+1)q - r$ (as $d \ge 1$), we can apply Theorem 1.7 with $X = [1, d-1] \cup \{k\}$ and $m = 0$ to conclude that there is some zero-sum subsequence $T \mid S$ with $|T| \in ([1, d-1] \cup \{k\}) \cdot q$. Since $0 \notin \Sigma_{kq}(S)$, it thus follows that $|T| = iq$ for some $i \in [1, d-1]$, and taking $T_i = T$ and $Y = \{i\}$ now shows that $|Y| \ge 1$. The claim is now complete unless $d \ge 3$.

We continue by showing that $|Y| \ge 2$. If this fails, then we have $Y = \{y_1\}$ for some $y_1 \in [1, d-1]$, and there is a zero-sum subsequence $T_1 \mid S$ with $|T_1| = y_1 q$. Since $0 \notin \Sigma_{kq}(S)$, we have

$$0 \notin \Sigma_{\{(k-y_1),k\}\cdot q}(T_1^{[-1]} \cdot S). \tag{29}$$

Let $X = \big([1, d-1] \setminus \{y_1\}\big) \cup \{k - y_1\} \cup \{k\}$. Since $k \ge \frac{d(d-1)}{2} + 1 \ge 2(d-1)$ and $y_1 \in [1, d-1]$, we have $X \subseteq \mathbb{N}$ with $|X| = d$. Since $k \le p$, we have $[1, \max X] \setminus X \subseteq [1, k-1] \subseteq [1, p-1]$. Since $y_1 \le d-1$, we have $|T_1^{[-1]} \cdot S| = (k - y_1 + d)q - r \ge (k+1)q - r$. As a result, we can apply Theorem 1.7 to $T_1^{[-1]} \cdot S$ with $X = \big([1, d-1] \setminus \{y_1\}\big) \cup \{k - y_1\} \cup \{k\}$ and $m = 0$ to find a zero-sum subsequence $T_2 \mid T_1^{[-1]} \cdot S$ with $|T_2| = y_2 q$ for some $y_2 \in [1, d-1] \setminus \{y_1\}$ (in view of (29)). But now the set $\{y_1, y_2\}$ can be taken for Y, showing that $|Y| \ge 2$. The claim is now complete unless $d \ge 4$.

In view of the our prior work, let $s := |Y| \ge 2$, let $Y = \{y_1, \ldots, y_s\}$, and let $T_1 \cdot \ldots \cdot T_s \mid S$ with each T_i a zero-sum subsequence of length $|T_i| = y_i q$ with $y_i \in [1, d-1]$, for every $i \in [1, s]$. Assume by contradiction that $2 \le s \le d-2$. Let $y = y_1 + \ldots + y_s$ and let

$$\max([1, d-1] \setminus Y) = d - s_0, \quad \text{where } s_0 \in [1, s+1].$$

Observe that

$$y \le \sum_{i=1}^{s+1}(d-i) - (d-s_0) = \frac{s(2d-s-3)}{2} + s_0 - 1 \le \frac{d(d-1)}{2} - 1 \le k-2, \tag{30}$$

with the final inequality holding by hypothesis. Let $T^* = y_1 \cdot \ldots \cdot y_s$, which is a sequence of terms from $\mathbb{Z}$. Since $0 \notin \Sigma_{kq}(S)$, we have

$$0 \notin \Sigma_{(k-t)q}\big((T_1 \cdot \ldots \cdot T_s)^{[-1]} \cdot S\big), \quad \text{for every } t \in \Sigma(T^*) \cap [1, k-1]. \tag{31}$$

Since $s \ge 2$, we have

$$y \in \Sigma(T^*) \quad \text{and} \quad y - y_i = y_1 + \ldots + y_{i-1} + y_{i+1} + \ldots + y_s \in \Sigma(T^*), \quad \text{for every } i \in [1, s].$$

Hence, in view of (30) and $y_1, \ldots, y_s \ge 1$, it follows that $y, y-y_1, \ldots, y-y_s \in \Sigma(T^*) \cap [1, k-1]$ are distinct elements. Thus (31) implies that

$$0 \notin \Sigma_{\{(k-y),(k-y+y_1),\ldots,(k-y+y_s)\}\cdot q}\big((T_1 \cdot \ldots \cdot T_s)^{[-1]} \cdot S\big). \tag{32}$$

Now let $X = \big([1, d-1]\backslash\{y_1, \ldots, y_s\}\big) \cup \{k-y,\ k-y+y_1,\ \ldots,\ k-y+y_s\}$. By definition of s_0, we have $\max\big([1, d-1] \setminus \{y_1, \ldots, y_s\}\big) = d - s_0$. If $k - y \le d - s_0$, then (30) and $s \le d-2$ yield

$$k \le d - s_0 + y \le d + \frac{s(2d-s-3)}{2} - 1 \le \frac{d(d-1)}{2},$$

contrary to hypothesis. Therefore, we must instead have $k - y > d - s_0$, which ensures that

$$\max\big([1, d-1] \setminus \{y_1, \ldots, y_s\}\big) < \min\Big(\{k-y,\ k-y+y_1,\ \ldots,\ k-y+y_s\}\Big) \quad \text{and} \quad |X| = d.$$

In view of $k \le p$, we have $[1, \max X]\backslash X \subseteq [1, k-2] \subseteq [1, p-2]$. We also have $|(T_1 \cdot \ldots \cdot T_s)^{[-1]} \cdot S| = |S| - yq = (k-y+d)q - r$. As a result, in view of $y_1, \ldots, y_s \in [1, d-1]$, it follows that we can apply Theorem 1.7 using $m = 0$ and

$$X = \big([1, d-1] \setminus \{y_1, \ldots, y_s\}\big) \cup \{k-y,\ k-y+y_1,\ \ldots,\ k-y+y_s\}$$

to conclude in view of (32) that there is a zero-sum subsequence $T_{s+1} \mid (T_1 \cdot \ldots \cdot T_s)^{[-1]} \cdot S$ with $|T_{s+1}| = y_{s+1}q$ for some $y_{s+1} \in [1, d-1]\backslash Y = [1, d-1]\backslash\{y_1, \ldots, y_s\}$. But now $\{y_1, \ldots, y_s, y_{s+1}\}$ contradicts the maximality of Y, completing the proof of the claim. □

Let $y = \frac{d(d-1)}{2} = \sum_{i\in[1,d-1]} i$, and let $X = [k-y, k-y+d-1]$. Since $k \geq \frac{d(d-1)}{2} + 1$ by hypothesis, we have $X \subseteq \mathbb{N}$ and $|X| = d$. Since $k \leq p$, we have $[1, \max X] \setminus X = [1, k-y-1] \subseteq [1, p-1]$. In view of Claim A, we have $|(T_1 \cdot \ldots \cdot T_{d-1})^{[-1]} \cdot S| = |S| - yq = (k-y+d)q - r$. As a result, we can apply Theorem 1.7 to $(T_1 \cdot \ldots \cdot T_{d-1})^{[-1]} \cdot S$ with $X = [k-y, k-y+d-1]$ and $m = 0$ to conclude that

$$0 \in \Sigma_{[(k-y),k-y+d-1]\cdot q}\big((T_1 \cdot \ldots \cdot T_{d-1})^{[-1]} \cdot S\big). \tag{33}$$

In view of Claim A, we have $0 \in \Sigma_{tq}(T_1 \cdot \ldots \cdot T_{d-1})$ for every $t \in [0, y]$, which combined with (33) implies that $0 \in \Sigma_{kq}(S)$, contrary to assumption, completing the proof. □

Next, we handle the main step in the proof of Theorem 1.8.

Proposition 3.4 *Let G be a finite abelian p-group with exponent q, let $d = \left\lceil \frac{\mathsf{D}^*(G)}{q} \right\rceil$. Suppose $d \leq 4$ and k is an integer with $d \leq k \leq p$. Then*

$$\mathsf{s}_{kq}(G) \leq kq + \mathsf{D}^*(G) - 1.$$

Proof If $q = 1$, then G is trivial with $\mathsf{s}_{kq}(G) = kq = kq + \mathsf{D}^*(G) - 1$, as desired. Therefore we can assume $q > 1$. Note that $d \geq 1$. Assume by contradiction that S is a sequence of terms from G with

$$0 \notin \Sigma_{kq}(S) \quad \text{and} \quad |S| = kq + \mathsf{D}^*(G) - 1 = (k+d)q - r,$$

where $r \in [1, q]$ is the integer such that $d = \frac{\mathsf{D}^*(G)+r-1}{q}$.

Case 1: $d = 1$

Let $X = \{k\}$. Since $1 = d \leq k \leq p$, we have $X \subseteq \mathbb{N}$ and $[1, \max X]\setminus X = [1, k-1] \subseteq [1, p-1]$, allowing us to apply Theorem 1.7 using $X = \{k\}$ and $m = 0$ to conclude that $\mathsf{s}_{kq}(G) \leq kq + \mathsf{D}^*(G) - 1$, as desired.

Case 2: $d = 2$

Note that $k \geq d = 2$. Suppose there is a zero-sum subsequence $T \mid S$ with $|T| = q$. Then $0 \notin \Sigma_{kq}(S)$ ensures that $0 \notin \Sigma_{\{(k-1),k\}\cdot q}(T^{[-1]} \cdot S)$. Let $X = \{k-1, k\}$. In view of $k \geq 2$, we have $X \subseteq \mathbb{N}$ and $|X| = 2$. In view $k \leq p$, we have $[1, \max X]\setminus X = [1, k-2] \subseteq [1, p-2]$ and $|T^{[-1]} \cdot S| = (k+1)q - r$, allowing us to apply Theorem 1.7 to $T^{[-1]} \cdot S$ using $X = \{k, k-1\}$ and $m = 0$ to conclude that $0 \in \Sigma_{\{(k-2),k\}\cdot q}(T^{[-1]} \cdot S)$, contradicting that the opposite was just shown. So we instead conclude that

$$0 \notin \Sigma_{\{1,k\}\cdot q}(S). \tag{34}$$

Now let $X = \{1, k\}$. In view of $k \geq 2$, we have $X \subseteq \mathbb{N}$ and $|X| = 2$. In view of $k \leq p$, we have $[1, \max X]\setminus X = [2, k-1] \subseteq [1, p-1]$ and $|S| \geq (k+1)q - r$, allowing us to apply Theorem 1.7 to S using $X = \{1, k\}$ and $m = 0$ to conclude that $0 \in \Sigma_{\{1,k\}\cdot q}(S)$, contrary to (34).

Case 3: $d = 3$

Note that $k \ge d = 3$. Suppose there is a zero-sum subsequence $T_1 \mid S$ with $|T_1| = q$. Then $0 \notin \Sigma_{kq}(S)$ ensures that $0 \notin \Sigma_{\{(k-1),k\}\cdot q}(T_1^{[-1]} \cdot S)$. Let $X = \{1, k-1, k\}$. In view of $k \ge d = 3$, we have $X \subseteq \mathbb{N}$ with $|X| = 3$. In view of $k \le p$, we have $[1, \max X]\backslash X = [2, k-2] \subseteq [2, p-2]$ and $|T_1^{[-1]} \cdot S| = (k+2)q - r$, allowing us to apply Theorem 1.7 using $X = \{1, k-1, k\}$ and $m = 0$ to conclude that $0 \in \Sigma_{\{1,(k-1),k\}\cdot q}(T_1^{[-1]} \cdot S)$, which in view of $0 \notin \Sigma_{\{(k-1),k\}\cdot q}(T_1^{[-1]} \cdot S)$ means there is some zero-sum subsequence $T_2 \mid T_1^{[-1]} \cdot S$ with $|T_2| = q$. But now $0 \notin \Sigma_{kq}(S)$ ensures that

$$0 \notin \Sigma_{\{(k-2),(k-1),k\}\cdot q}(T_1^{[-1]} \cdot T_2^{[-1]} \cdot S).$$

Now let $X = \{k-2, k-1, k\}$. Note $X \subseteq \mathbb{N}$ with $|X| = 3 = d$ in view of $k \ge d = 3$. In view of $k \le p$, we have $[1, \max X]\backslash X = [1, k-3] \subseteq [1, p-3]$ and $|T_1^{[-1]} \cdot T_2^{[-1]} \cdot S| = (k+1)q - r$, allowing us to apply Theorem 1.7 using $X = \{k-2, k-1, k\}$ and $m = 0$ to conclude that $0 \in \Sigma_{\{(k-2),(k-1),k\}\cdot q}(T_1^{[-1]} \cdot T_2^{[-1]} \cdot S)$, contrary to what was just noted. So we instead conclude that

$$0 \notin \Sigma_{\{1,k\}\cdot q}(S). \tag{35}$$

Suppose there is a zero-sum subsequence $T \mid S$ with $|T| = (k+2)q$. Let $X = \{1, k, k+1\}$. Then $X \subseteq \mathbb{N}$ with $|X| = 3$ in view of $k \ge 2$. Since the complement of a zero-sum subsequence in T is also zero-sum, we conclude from (35) that $0 \notin \Sigma_{\{1,k,(k+1)\}\cdot q}(T)$. In view of $k \le p$, we have $[1, \max X]\backslash X = [2, k-1] \subseteq [2, p-1]$ and $|T| = (k+2)q \ge (k+2)q - r$, allowing us to apply Theorem 1.7 using $X = \{1, k, k+1\}$ and $m = 0$ to conclude that $0 \in \Sigma_{\{1,k,(k+1)\}\cdot q}(T)$, contrary to what was just noted. So we instead conclude that

$$0 \notin \Sigma_{\{1,k,(k+2)\}\cdot q}(S). \tag{36}$$

Now let $X = \{1, k, k+2\}$. Then $|S| = (k+3)q - r$ and $[1, \max X]\backslash X = [2, k-1] \cup \{k+1\}$. We also have $k \le p$. As a result, unless $p = k+1$, we can apply Theorem 1.7 using $X = \{1, k, k+2\}$ and $m = 0$ to conclude that $0 \in \Sigma_{\{1,k,(k+2)\}\cdot q}(S)$, contrary to (36). Therefore we must have $p = k+1 \ge d+1 = 4$, whence $k+1 = p \ge 5$ as p is prime. In particular, $k \ge 4$.

Now let $X = \{1, 2, k\}$. Note that $|X| = 3$ in view of $k \ge 3$. In view of $k \le p$, we have $[1, \max X]\backslash X = [3, k-1] \subseteq [3, p-1]$ and $|S| = (k+3)q - r$, allowing us to apply Theorem 1.7 using $X = \{1, 2, k\}$ and $m = 0$ to conclude that $0 \in \Sigma_{\{1,2,k\}\cdot q}(S)$, which in view of (36) implies that there is a zero-sum subsequence $T \mid S$ with $|T| = 2q$. But now $0 \notin \Sigma_{kq}(S)$ ensures that $0 \notin \Sigma_{(k-2)q}(T^{[-1]} \cdot S)$. Thus (36) yields

$$0 \notin \Sigma_{\{1,(k-2),k\}\cdot q}(T^{[-1]} \cdot S). \tag{37}$$

Now let $X = \{1, k-2, k\}$. In view of $k \ge 4$, we have $X \subseteq \mathbb{N}$ and $|X| = 3$. In view of $k \le p$, we have $[1, \max X]\backslash X \subseteq [2, k-1] \subseteq [2, p-1]$ and $|T^{[-1]} \cdot S| = (k+1)q - r$,

allowing us to apply Theorem 1.7 using $X = \{1, k-2, k\}$ and $m = 0$ to conclude that $0 \in \Sigma_{\{1,(k-2),k\}\cdot q}(T^{[-1]} \cdot S)$, contrary to (37).

Case 4: $d = 4$.

Note that $k \geq d = 4$. We divide the proof into five subcases. Note, since p is prime, that $k = 5$ and $p = k + 1$ cannot both hold, ensuring all possibilities are covered.

CASE 4.1: $0 \notin \Sigma_{\{1,2\}\cdot q}(S)$.

Suppose there is a zero-sum subsequence $T \mid S$ with $|T| = (k+1)q$. Then, since the complement of zero-sum subsequence of T is also zero-sum, it follows from the subcase hypothesis $0 \notin \Sigma_{\{1,2\}\cdot q}(S)$ that $0 \notin \Sigma_{\{1,2,(k-1),k\}\cdot q}(T)$. Let $X = \{1, 2, k-1, k\}$. Since $k \geq 4$, we have $X \subseteq \mathbb{N}$ and $|X| = 4$. In view of $k \leq p$, we have $[1, \max X] \setminus X = [3, k-2] \subseteq [3, p-2]$ and $|T| = (k+1)q \geq (k+1)q - r$, allowing us to apply Theorem 1.7 to T with $X = \{1, 2, k-1, k\}$ and $m = 0$ to conclude that $0 \in \Sigma_{\{1,2,(k-1),k\}\cdot q}(T)$, contrary to what was just noted. So we instead conclude that

$$0 \notin \Sigma_{\{1,2,k,(k+1)\}\cdot q}(S). \tag{38}$$

Now let $X = \{1, 2, k, k+1\}$. Since $k \geq 3$, we have $X \subseteq \mathbb{N}$ and $|X| = 4$. In view of $k \leq p$, we have $[1, \max X]\setminus X = [3, k-1] \subseteq [3, p-1]$ and $|S| = (k+4)q - r$. But now Theorem 1.7 applied to S with $X = \{1, 2, k, k+1\}$ and $m = 0$ yields $0 \in \Sigma_{\{1,2,k,(k+1)\}\cdot q}(S)$, contrary to (38).

CASE 4.2: There exists disjoint subsequences $T_1 \cdot T_2 \mid S$ with $|T_1| = q$, $|T_2| = 2q$, and T_1 and T_2 each zero-sum.

In this case, there are zero-sum subsequences of $T_1 \cdot T_2$ having lengths q, $2q$ and also $3q$. As a result, since $0 \notin \Sigma_{kq}(S)$, we have

$$0 \notin \Sigma_{\{(k-3),(k-2),(k-1),k\}\cdot q}(T_1^{[-1]} \cdot T_2^{[-1]} \cdot S).$$

Let $X = [k-3, k]$. Since $k \geq d = 4$, we have $X \subseteq \mathbb{N}$ and $|X| = 4$. Since $k \leq p$, we have $[1, \max X]\setminus X = [1, k-4] \subseteq [1, p-4]$. Hence, since $|T_1^{[-1]} \cdot T_2^{[-1]} \cdot S| = (k+1)q - r$, we can apply Theorem 1.7 to $T_1^{[-1]} \cdot T_2^{[-1]} \cdot S$ with $X = [k-3, k]$ and $m = 0$ to conclude that $0 \in \Sigma_{\{(k-3),(k-2),(k-1),k\}\cdot q}(T_1^{[-1]} \cdot T_2^{[-1]} \cdot S)$, contrary to what was just noted.

CASE 4.3: $0 \in \Sigma_q(S)$.

Let $T_1 \mid S$ be a zero-sum subsequence with $|T_1| = q$, which exists by subcase hypothesis. In view of CASE 4.2 and $0 \notin \Sigma_{kq}(S)$, we can assume

$$0 \notin \Sigma_{\{2,(k-1),k\}\cdot q}(T_1^{[-1]} \cdot S). \tag{39}$$

Suppose there is a zero-sum subsequence $T \mid T_1^{[-1]} \cdot S$ with $|T| = (k+1)q$. Then, since the complement of a zero-sum subsequence of T is also zero-sum, it follows from (39) that $0 \notin \Sigma_{\{1,2,(k-1),k\}}(T)$. Let $X = \{1, 2, k-1, k\}$. Since $k \geq d = 4$, we have $X \subseteq \mathbb{N}$ and $|X| = 4$. Since $p \geq k$, we have $[1, \max X]\setminus X = [3, k-2] \subseteq [3, p-2]$. Hence, since $|T| = (k+1)q \geq (k+1)q - r$, we can apply Theorem 1.7 to T with $X = \{1, 2, k-1, k\}$ and $m = 0$ to conclude that $0 \in \Sigma_{\{1,2,(k-1),k\}\cdot q}(T)$, contrary to

what was just noted. So we instead conclude that $0 \notin \Sigma_{(k+1)q}(T_1^{[-1]} \cdot S)$, which along with (39) ensures that

$$0 \notin \Sigma_{\{2,(k-1),k,(k+1)\}\cdot q}(T_1^{[-1]} \cdot S). \tag{40}$$

Now let $X = \{2, k-1, k, k+1\}$. Since $k \geq d = 4$, we have $X \subseteq \mathbb{N}$ and $|X| = 4$. Since $p \geq k$, we have $[1, \max X]\backslash X = \{1\} \cup [3, k-2] \subseteq [1, p-2]$. Hence, since $|T_1^{[-1]} \cdot S| = (k+3)q - r$, we can apply Theorem 1.7 to $T_1^{[-1]} \cdot S$ with $X = \{2, k-1, k, k+1\}$ and $m = 0$ to conclude that $0 \in \Sigma_{\{2,(k-1),k,(k+1)\}\cdot q}(T)$, contrary to (40).

CASE 4.4: $p \neq k+1$.

We have $0 \notin \Sigma_{kq}(S)$ and can assume $0 \notin \Sigma_q(S)$ in view of CASE 4.3.

Suppose there is a zero-sum subsequence $T \mid S$ with $|T| = tq$ for some $t \in [k+2, k+3]$. Then, since $0 \notin \Sigma_{\{1,k\}\cdot q}(S)$ with the complement of a zero-sum subsequence in T also zero-sum, it follows that

$$0 \notin \Sigma_{\{1,(t-k),k,(t-1)\}\cdot q}(T).$$

Let $X = \{1, t-k, k, t-1\}$. Since $k \geq d = 4$ and $k+2 \leq t \leq k+3 < 2k$, we have $X \subseteq \mathbb{N}$ and $|X| = 4$. If $t = k+2$, then $[1, \max X] \setminus X = [3, k-1]$. If $t = k+3$, then $[1, \max X]\backslash X = \{2\} \cup [4, k-1] \cup \{k+1\}$. In either case, since $p \geq k$ with $p \neq k+1$ (by subcase hypothesis), it follows in view of $|T| = tq \geq tq - r$ that we can apply Theorem 1.7 to T with $X = \{1, t-k, k, t-1\}$ and $m = 0$ to conclude that $0 \in \Sigma_{\{1,(t-k),k,(t-1)\}\cdot q}(T)$, contrary to what was noted above. So we instead conclude that $0 \notin \Sigma_{\{(k+2),(k+3)\}\cdot q}(S)$, which along with the already noted fact that $0 \notin \Sigma_{\{1,k\}\cdot q}(S)$ means

$$0 \notin \Sigma_{\{1,k,(k+2),(k+3)\}\cdot q}(S). \tag{41}$$

Now let $X = \{1, k, k+2, k+3\}$. Since $k \geq d = 4$, we have $X \subseteq \mathbb{N}$ and $|X| = 4$. Since $p \geq k$, we have $[1, \max X]\backslash X = [2, k-1] \cup \{k+1\}$. We also have $p \geq k$ with $p \neq k+1$ by subcase hypothesis. Hence, since $|S| = (k+4)q - r$, we can apply Theorem 1.7 to S with $X = \{1, k, k+2, k+3\}$ and $m = 0$ to conclude that $0 \in \Sigma_{\{1,k,(k+2),(k+3)\}\cdot q}(S)$, contrary to (41).

CASE 4.5: $k \neq 5$.

In view of CASES 4.1 and 4.3, we can assume there is a zero-sum subsequence $T_2 \mid S$ with $|T_2| = 2q$. Then, since $0 \notin \Sigma_{kq}(S)$, it follows in view of CASE 4.3 that

$$0 \notin \Sigma_{\{1,(k-2),k\}\cdot q}(T_2^{[-1]} \cdot S). \tag{42}$$

Suppose there is a zero-sum subsequence $T \mid T_2^{[-1]} \cdot S$ with $|T| = (k+1)q$. Then, since the complement of a zero-sum subsequence in T is also zero-sum, it follows from (42) that

$$0 \notin \Sigma_{\{1,3,(k-2),k\}\cdot q}(T).$$

Let $X = \{1, 3, k-2, k\}$. Since $k \ge d = 4$ and $k \ne 5$ (in view of the subcase hypothesis), we have $X \subseteq \mathbb{N}$ and $|X| = 4$. Since $p \ge k$, we have $[1, \max X] \setminus X \subseteq [2, k-1] \subseteq [2, p-1]$. Hence, since $|T| = (k+1)q \ge (k+1)q - r$, we can apply Theorem 1.7 to T with $X = \{1, 3, k-2, k\}$ and $m = 0$ to conclude that $0 \in \Sigma_{\{1,3,(k-2),k\}\cdot q}(T)$, contrary to what was noted above. So we can now assume $0 \notin \Sigma_{(k+1)q}(T_2^{[-1]} \cdot S)$, which together with (42) means

$$0 \notin \Sigma_{\{1,(k-2),k,(k+1)\}\cdot q}(T_2^{[-1]} \cdot S). \tag{43}$$

Now let $X = \{1, k-2, k, k+1\}$. In view of $k \ge d = 4$, we have $X \subseteq \mathbb{N}$ and $|X| = 4$. In view of $p \ge k$, we have $[1, \max X] \setminus X = [2, k-3] \cup \{k-1\} \subseteq [2, p-1]$. Hence, since $|T_2^{[-1]} \cdot S| = (k+2)q - r$, we can apply Theorem 1.7 to $T_2^{[-1]} \cdot S$ with $X = \{1, k-2, k, k+1\}$ and $m = 0$ to conclude that $0 \in \Sigma_{\{1,(k-2),k,(k+1)\}\cdot q}(T)$, contrary to (43), which completes the proof. □

The means of transferring Propositions 3.4 and 3.3 into Theorems 1.8 and 1.9 is the following simple lemma.

Lemma 3.5 *Let G be a finite abelian p-group with exponent q, let $d = \left\lceil \frac{\mathsf{D}^*(G)}{q} \right\rceil$, and let $k_0 \ge 1$. Suppose $\mathsf{s}_{kq}(G) \le kq + \mathsf{D}^*(G) - 1$ for all $k \in [k_0, 2k_0 - 1]$. Then*

$$\mathsf{s}_{kq}(G) \le kq + \mathsf{D}^*(G) - 1 \quad \text{for all } k \ge k_0.$$

Proof Let $k \ge k_0$ be arbitrary. Write $k = mk_0 + r$ with $m \ge 0$ and $r \in [k_0, 2k_0 - 1]$. Let S be a sequence of terms from G with $|S| = kq + \mathsf{D}^*(G) - 1 \ge mk_0q + \mathsf{D}^*(G) - 1$. We need to show $0 \in \Sigma_{kq}(S)$. By repeated application of the definition of $\mathsf{s}_{k_0q}(G) \le k_0q + \mathsf{D}^*(G) - 1$, we can find subsequences $T_1 \cdot \ldots \cdot T_m \mid S$ such that each T_i is zero-sum with $|T_i| = k_0q$, for $i \in [1, m]$. But now

$$|(T_1 \cdot \ldots \cdot T_m)^{[-1]} \cdot S| = |S| - mk_0q = rq + \mathsf{D}^*(G) - 1,$$

so applying the definition of $\mathsf{s}_{rq}(G) \le rq + \mathsf{D}^*(G) - 1$ to $(T_1 \cdot \ldots \cdot T_m)^{[-1]} \cdot S$, we find another zero-sum subsequence $T_0 \mid (T_1 \cdot \ldots \cdot T_m)^{[-1]} \cdot S$ with $|T_0| = rq$ and $r \in [k_0, 2k_0 - 1]$, and now $T = T_0 \cdot T_1 \cdot \ldots \cdot T_m$ is a zero-sum subsequence of S with $|T| = (mk_0 + r)q = kq$, as desired. □

We conclude with the proofs for both results regarding $\mathsf{s}_{k\exp(G)}(G)$.

Proof of Theorem 1.8 Let $k_0 = d$. Since $p \ge 2d - 1$, we have $p \ge k$ for every $k \in [k_0, 2k_0 - 1] = [d, 2d - 1]$. Thus Proposition 3.4 implies that $\mathsf{s}_{kq}(G) \le kq + \mathsf{D}^*(G) - 1$ for every $k \in [k_0, 2k_0 - 1]$, and the result now follows by applying Lemma 3.5. □

Proof of Theorem 1.9 Let $k_0 = \frac{d(d-1)}{2} + 1$. Since $p \ge d^2 - d + 1$, we have $p \ge k$ for every $k \in [k_0, 2k_0 - 1] = [\frac{d(d-1)}{2} + 1, d^2 - d + 1]$. Thus Proposition 3.3 implies that $\mathsf{s}_{kq}(G) \le kq + \mathsf{D}^*(G) - 1$ for every $k \in [k_0, 2k_0 - 1]$, and the result now follows by applying Lemma 3.5. □

Acknowledgements I thank the referees for their many helpful suggestions for improving the exposition of the paper.

Data Availability Not applicable.

References

1. Aichinger, E., Moosbauer, J.: Chevalley-Warning type results on abelian groups. J. Algebra **569**, 30–66 (2021)
2. Alon, N., Dubiner, M.: Zero-sum sets of prescribed size, in Combinatorics, Paul Erdős is Eighty, János Bolyai Math. Soc., Budapest. pp. 33–50 (1993)
3. Alon, N., Dubiner, M.: A lattice point problem and additive number theory. Combinatorica **15**, 301–309 (1995)
4. Ax, J.: Zeroes of polynomials over finite fields. Am. J. Math. **86**, 255–261 (1964)
5. Baayen, P.C.: Een combinatorisch probleem voor eindige abelse groepen, in Colloquium Discrete Wiskunde, MC Syllabus 5, pp. 76–108. Mathematisch Centrum, Amsterdam (1968)
6. Baoulina, I., Bishnoi, A., Clark, P.: A generalization of the theorems of Chevalley-Warning and Ax-Katz via polynomial substitutions. Proc. Am. Math. Soc. **147**(10), 4107–4122 (2019)
7. Bitz, J., Griffith, S., He, Xiaoyu: Exponential lower bounds on the generalized Erdös-Ginzburg-Ziv constant. Discret. Math. **343**(12), 112083 (2020). (**4**)
8. Brink, D.: Chevalley's theorem with restricted variables. Combinatorica **31**(1), 127–130 (2011)
9. Cahen, P.-J., Chabert, J.-L.: Integer valued polynomials, mathematical surveys and monographs 48, American Mathematical Society (1997)
10. Cao, W.: A partial improvement of the Ax-Katz theorem. J. Number Theory **132**, 485–494 (2012)
11. Cao, W., Sun, Q.: Improvements upon the Chevalley-warning-Ax-Katz-type estimates. J. Number Theory **122**(1), 135–141 (2007)
12. Cao, W., Wan, D.: Divisibility on point counting over finite Witt rings. Finite Fields Appl. **91**, 102254 (2023). (**25**)
13. Castro, F.N., Moreno an I Rubio, O.: An improvement of a theorem of Carlitz. J. Pure Appl. Algebra **224**(5), 106246 (2020). (**7**)
14. Chevalley, C.: Démonstration d'une hypothèse de M. Artin. Abh. Math. Sem. Hamburg **11**, 73–75 (1936)
15. Clark, P., Schauz, W.: Functional Degrees and Arithmetics Applications I: The Set of Fucntional Degrees, preprint
16. Clark, P., Forrow, A., Schmitt, J.R.: Warning's second theorem with restricted variables. Combinatorica **37**(3), 397–417 (2017)
17. Clark, P., Genao, T., Saia, F.: Chevalley-warning at the boundary. Expo. Math. **39**(4), 604–623 (2021)
18. Dickson, L. E.: History of the Theory of Numbers, Vol. I, AMS Chelsea Publ., (1999)
19. Erdős, P., Ginzburg, A., Ziv, A.: Theorem in additive number theory. Bull. Res. Council Israel **10F**, 41–43 (1961)
20. Fleck, A.: Sitzungs. Berlin Math. Gesell. **13**, 2–6 (1913)
21. Gao, W., Hong, S., Peng, J.: On zero-sum subsequences of length k exp(G) II, J. Combin. Theory Ser. A 187 (2022), Paper No. 105563, 34 pp
22. Gao, W.: On zero-sum subsequences of restricted size II. Discret. Math. **271**(1–3), 51–59 (2003)
23. Gao, W., Han, D., Peng, J., Sun, F.: On zero-sum subsequences of length k exp(G). J. Combin. Theory Ser. A **125**, 240–253 (2014)
24. Garrett, P.: Abstract Algebra, Chapman & Hall/CRC (2008)
25. Geroldinger, A., Halter-Koch, F.: Non-Unique Factorizations: Algebraic, Combinatorial and Analytic Theory, Pure and Applied Mathematics 278, Chapman & Hall/CRC (2006)
26. Grynkiewicz, D.J.: Structural Additive Theory, Developments in Mathematics 30. Springer, Cham (2013)
27. Han, D., Zhang, H.: On zero-sum subsequences of prescribed length. Int. J. Number Theory **14**(1), 167–191 (2018)
28. He, X.: Zero-sum subsequences of length kq over finite abelian p-groups. Discret. Math. **339**(1), 399–407 (2016)
29. Hou, X.-D.: A note on the proof of a theorem of Katz. Finite Fields Appl. **11**, 316–319 (2005)

30. Katz, N.: On a theorem of Ax. Am. J. Math. **93**, 485–499 (1971)
31. Kemnitz, A.: On a lattice point problem. ARS Combinatoria **16b**, 151–160 (1983)
32. Kubertin, S.: Zero-sums of length kq in $\mathbb{Z}_q^d$. Acta Arith. **116**(2), 145–152 (2005)
33. Moreno, O., Moreno, C.J.: Improvements of the Chevalley-warning and the Ax-Katz theorem. Am. J. Math. **117**, 241–244 (1995)
34. Moreno, O., Shum, K., Castro, F.N., Kumar, V.P.: Tight bounds for Chevalley-warning-Ax-Katz type estimates, with improved applications. Proc. London Math. Soc. (3) **88**(3), 545–564 (2004)
35. Nathanson, M.: Additive Number Theory: Inverse Problems and the Geometry of Sumsets, Graduate Textbooks in Mathematics 165. Springer, Berlin (1991)
36. Niven, I., Zuckerman, H., Montgomery, H.: An Introduction to the Theory of Numbers, 5th edn. Wiley, London (1991)
37. Olson, J.E.: A combinatorial problem on finite abelian groups I. J. Number Theory **1**, 8–10 (1969)
38. Reiher, C.: On Kemnitz' conjecture concerning lattice-points in the plane. Ramanujan J. **13**(1–3), 333–337 (2007)
39. Rónyai, L.: On a conjecture of Kemnitz. Combinatorica **20**(4), 569–573 (2000)
40. Savchev, S., Chen, F.: Note Kemnitz' conjecture revisited. Discrete Math. **297**, 196–201 (2005)
41. Schanuel, S.H.: An extension of Chevalley's theorem to congruences modulo prime powers. J. Number Theory **6**, 284–290 (1974)
42. Serre, J.-P., Fields, L.: Graduate Texts in Mathematics 67. Springer, Berlin (1979)
43. Sun, Z.-W.: Extensions of Wilson's lemma and the Ax-Katz Theorem, unpublished (2006), arXiv:math.NT/0608560
44. Sun, Z.-W., Wan, D.: Lucas type congruences for cyclotomic Ψ-coefficients. Int. J. Number Theory **4**(2), 155–170 (2008)
45. Tao T., Vu, V.: Additive Combinatorics, Cambridge Studies in Advanced Mathematics 105, Cambridge University Press (2010)
46. Wan, D.: Combinatorial congruences and Ψ-operators, Finite Fields Appl. (2006), no. 4, 693–703
47. Wan, D.: An elementary proof of a theorem of Katz. Am. J. Math. **111**, 1–8 (1989)
48. Wan, D.: A Chevalley-Warning approach to p-adic estimates of character sums. Proc. Am. Math. Soc. **123**, 45–54 (1995)
49. Warning, E.: Bemerkung zur vorstehenden Arbeit von Herrn Chevalley. Abh. Math. Sem. Hamburg **11**, 76–83 (1936)
50. Weidong, G., Thangadurai, R.: On zero-sum sequences of prescribed length. Aequationes Math. **72**(3), 201–212 (2006)
51. Weisman, C.S.: Some congruences for binomial coefficients. Michigan Math. J. **24**, 141–151 (1977)
52. Wilson, R.: A lemma on polynomials modulo p^m and applications to coding theory. Discrete Math. **306**(23), 3154–3165 (2006)