Warning's Second Theorem with restricted variables

COMBINATORICA
Bolyai Society – Springer-Verlag

Combinatorica 21pp.
DOI: 10.1007/s00493-015-3267-8

WARNING'S SECOND THEOREM WITH RESTRICTED VARIABLES

PETE L. CLARK, ADEN FORROW, JOHN R. SCHMITT

Received May 5, 2014

We present a restricted variable generalization of Warning's Second Theorem (a result giving a lower bound on the number of solutions of a low degree polynomial system over a finite field, assuming one solution exists). This is analogous to Schauz-Brink's restricted variable generalization of Chevalley's Theorem (a result giving conditions for a low degree polynomial system *not* to have exactly one solution). Just as Warning's Second Theorem implies Chevalley's Theorem, our result implies Schauz-Brink's Theorem. We include several combinatorial applications, enough to show that we have a general tool for obtaining quantitative refinements of combinatorial existence theorems.

Let $q = p^\ell$ be a power of a prime number p, and let $\mathbb{F}_q$ be "the" finite field of order q.

For $a_1, \ldots, a_n, N \in \mathbb{Z}^+$, we denote by $\mathfrak{m}(a_1, \ldots, a_n; N) \in \mathbb{Z}^+$ a certain combinatorial quantity defined and computed in Section 2.1.

1. Introduction

A **$\mathbf{C_1}$-field** is a field F such that for all positive integers $d < n$ and every homogeneous polynomial $f(t_1, \ldots, t_n) \in F[t_1, \ldots, t_n]$ of degree d, there is $x \in F^n \setminus \{(0, \ldots, 0)\}$ such that $f(x) = 0$. This notion is due to E. Artin. However, already in 1909 L. E. Dickson had conjectured that (in Artin's language) every finite field is a C_1-field [13]. Tsen showed that function fields in one variable over an algebraically closed field are C_1-fields [26], but this left the finite field case open. Artin assigned the problem of proving Dickson's conjecture to his student Ewald Warning. In 1934 C. Chevalley visited Artin,

Mathematics Subject Classification (2000): 11T99

asked about his student's work, and quickly proved a result which implies that finite fields are C_1-fields. In danger of losing his thesis problem, Warning responded by establishing a further improvement. The papers of Chevalley and Warning were published consecutively [10], [29], and the following result is now a classic of elementary number theory.

Theorem 1.1. *(Chevalley-Warning Theorem) Let $n, r, d_1, \ldots, d_r \in \mathbb{Z}^+$ with*

$$d := d_1 + \ldots + d_r < n. \tag{1}$$

For $1 \leq i \leq r$, let $P_i(t_1, \ldots, t_n) \in \mathbb{F}_q[t_1, \ldots, t_n]$ be a polynomial of degree d_i. Let

$$Z = Z(P_1, \ldots, P_r) = \{x \in \mathbb{F}_q^n \mid P_1(x) = \ldots = P_r(x) = 0\}$$

be the common zero set in $\mathbb{F}_q^n$ of the P_i's, and let $\mathbf{z} = \#Z$. Then:

a) (Chevalley's Theorem [10]) We have $\mathbf{z} = 0$ or $\mathbf{z} \geq 2$.

b) (Warning's Theorem [29]) We have $\mathbf{z} \equiv 0 \pmod{p}$.

In fact very easy modifications of Chevalley's argument prove Warning's Theorem. The more substantial contribution of [29] is the following result.

Theorem 1.2. *(Warning's Second Theorem) With hypotheses as in Theorem 1.1,*

$$\mathbf{z} = 0 \text{ or } \mathbf{z} \geq q^{n-d}. \tag{2}$$

There is a rich body of work on extensions and refinements of Theorem 1.1 – too much to recall here! – but let us mention work of Ax and Katz which computes the minimal p-adic valuation of $\mathbf{z}$ as $P_1, \ldots, P_r$ range over all polynomials of degrees $d_1, \ldots, d_r$ and work of Esnault showing that various geometric classes of varieties – including all Fano varieties – over finite fields must have rational points [4], [18], [16]. In contrast we know of only one refinement of Theorem 1.2: [17].

The above generalizations of the Chevalley-Warning Theorem point in the direction of arithmetic geometry. Here we are more interested in interfaces with combinatorics. Here is the first result in this direction.

Theorem 1.3. *(Schanuel's Theorem [24]) Let $n, r, v_1, \ldots, v_r \in \mathbb{Z}^+$. For $1 \leq j \leq r$, let $P_j(t_1, \ldots, t_n) \in \mathbb{Z}/p^{v_j}\mathbb{Z}[t_1, \ldots, t_n]$ be a polynomial without constant term. Let*

$$Z^\circ = \{x \in \mathbb{Z}^n \setminus (p\mathbb{Z})^n \mid P_j(x) \equiv 0 \pmod{p^{v_j}} \text{ for all } 1 \leq j \leq r\}.$$

a) If $\sum_{j=1}^r \deg(P_j) \left(\frac{p^{v_j}-1}{p-1}\right) < n$, then $Z^\circ \neq \emptyset$.

b) If $\sum_{j=1}^r (p^{v_j} - 1) \deg(P_j) < n$, then $Z^\circ \cap \{0,1\}^n \neq \emptyset$.

c) Let $b_1, \ldots, b_n$ be non-negative integers. If $\sum_{j=1}^r (p^{v_j} - 1) \deg(P_j) < \sum_{i=1}^n b_i$, then $Z^\circ \cap \prod_{i=1}^n [0, b_i] \neq \emptyset$.

These results have been revisited in light of the **Polynomial Method**, initiated by N. Alon [3] and continued by many others. The first application in [3] is to Chevalley's Theorem. Recently U. Schauz [25] and then D. Brink [6] used Alon's ideas to prove a **restricted variable** generalization.

Theorem 1.4. *(Restricted Variable Chevalley Theorem) Let* $P_1, \ldots, P_r \in \mathbb{F}_q[t] = \mathbb{F}_q[t_1, \ldots, t_n]$. *For* $1 \leq i \leq n$, *let* $\emptyset \neq A_i \subseteq \mathbb{F}_q$ *and put* $A = \prod_{i=1}^n A_i$. *Put*

$$Z_A = \{a = (a_1, \ldots, a_n) \in A \mid P_1(a) = \ldots = P_r(a) = 0\}, \ \mathbf{z}_A = \#Z_A.$$

If $\sum_{i=1}^r (q-1) \deg P_i < \sum_{i=1}^n (\#A_i - 1)$, *then* $\mathbf{z}_A \neq 1$.

Schauz and Brink (independently) gave a common generalization of Theorem 1.3 and of Theorem 1.4 for $q = p$.

Theorem 1.5. *(Schauz-Brink Theorem [25], [6]) Let*

$$P_1(t_1, \ldots, t_n), \ldots, P_r(t_1, \ldots, t_n) \in \mathbb{Z}[t_1, \ldots, t_n]$$

be polynomials, let p *be a prime, let* $v_1, \ldots, v_r \in \mathbb{Z}^+$, *and let* $A_1, \ldots, A_n$ *be nonempty subsets of* $\mathbb{Z}$ *such that for each* i, *the elements of* A_i *are pairwise incongruent modulo* p, *and put* $A = \prod_{i=1}^n A_i$. *Let*

$$Z_A = \{x \in A \mid P_j(x) \equiv 0 \pmod{p^{v_j}} \ \forall 1 \leq j \leq r\}, \ \mathbf{z}_A = \#Z_A.$$

a) If $\sum_{j=1}^r (p^{v_j} - 1) \deg(P_j) < \sum_{i=1}^n (\#A_i - 1)$, *then* $\mathbf{z}_A \neq 1$.

*b) (**Boolean Case**) If* $A = \{0,1\}^n$ *and* $\sum_{j=1}^r (p^{v_j} - 1) \deg(P_j) < n$, *then* $\mathbf{z}_A \neq 1$.

Following a remark of Brink, we state in Section 3.1 a generalization to number fields, Theorem 3.1, which fully recovers Theorem 1.4.

The main result of this paper simultaneously generalizes Theorems 1.2 and 3.1.

Theorem 1.6. *(Restricted Variable Warning's Second Theorem) Let* K *be a number field with ring of integers* R, *let* $\mathfrak{p}$ *be a nonzero prime ideal of* R, *and let* $q = p^\ell$ *be the prime power such that* $R/\mathfrak{p} \cong \mathbb{F}_q$. *Let* $A_1, \ldots, A_n$ *be nonempty subsets of* R *such that for each* i, *the elements of* A_i *are pairwise incongruent modulo* $\mathfrak{p}$, *and put* $A = \prod_{i=1}^n A_i$. *Let* $r, v_1, \ldots, v_r \in \mathbb{Z}^+$. *Let* $P_1, \ldots, P_r \in R[t_1, \ldots, t_n]$. *Let*

$$Z_A = \{x \in A \mid P_j(x) \equiv 0 \pmod{\mathfrak{p}^{v_j}} \ \forall 1 \leq j \leq r\}, \ \mathbf{z}_A = \#Z_A.$$

a) $\mathbf{z}_A = 0$ *or*

$$\mathbf{z}_A \geq \mathfrak{m}\left(\#A_1, \ldots, \#A_n; \#A_1 + \ldots + \#A_n - \sum_{j=1}^r (q^{v_j} - 1) \deg(P_j)\right).$$

b) We recover Theorem 1.2 and Theorem 3.1 as special cases.

*c) (**Boolean Case**) We have* $\mathbf{z}_{\{0,1\}^n} = 0$ *or* $\mathbf{z}_{\{0,1\}^n} \geq 2^{n-\sum_{j=1}^r (q^{v_j}-1)\deg(P_j)}$.

Theorem 1.6 includes all of the results stated so far except Theorem 1.1b). In this regard we should first mention that J. Ax gave a *ten line proof* of Theorem 1.1b) [4]. Chevalley's original proof is longer but seems more penetrating: it adapts easily to give a restricted variable generalization of Theorem 1.1b): see [11, Thm. 16]. Adapting Chevalley's method for finitely restricted variables over an arbitrary field leads to a **Coefficient Formula** which has appeared in the recent literature [25, Thm. 3.2], [20, Thm. 3], [19, Thm. 4], [11, §3.3] as a natural sharpening of Alon's Combinatorial Nullstellensatz II [3, Thm. 1.2].

Whereas the Combinatorial Nullstellensatz and its refinements are key to the proof of the results of Schanuel, Schauz and Brink, the key to the proof of the Restricted Variable Warning's Second Theorem is a different Polynomial Method: the **Alon-Füredi Theorem**. Section 2 of this paper recalls the statement of this theorem and gives some other needed preliminaries. The proof of Theorem 1.6 occurs in Section 3.

Chevalley's Theorem has some combinatorial applications, notably the Theorem of Erdős, Ginzburg and Ziv (henceforth EGZ). Schanuel's refinement has a very striking application in additive combinatorics: it yields a theorem of Olson computing the Davenport constant of a finite commutative p-group. Further, it is the main technical input of a result of Alon, Kleitman, Lipton, Meshulam, Rabin and Spencer (henceforth AKLMRS) on selecting from set systems to get a union of cardinality divisible by a prime power q. As Brink shows, his Theorem 1.5 can be applied in additive combinatorics to convert theorems asserting the existence of subsequences into theorems asserting the existence of "generalized subsequences" formed by taking linear combinations with coefficients in a restricted variable set. This is a natural generalization, going back at least as far as the Shannon capacity: c.f. [21]. Analogues of the EGZ Theorem in the context of generalized subsequences (or "weighted subsequences") in p-groups are pursued in the recent work [12] of Das Adhikari, Grynkiewicz and Sun (henceforth DAGS).

In Section 4 we apply Theorem 1.6 to each of the above situations, getting in each case a quantitative refinement which also includes the **inhomogeneous case**: thus whereas Brink gave an upper bound on the length of a sequence in a p-group G with no generalized 0-sum subsequence, we give a lower bound on the *number* of g-sum generalized subsequences (for any $g \in G$) which recovers Brink's result when we specialize to $g = 0$ and ask only for one nontrivial subsequence. Specializing to the case of "classical" g-sum subsequences we recover a recent result of Chang, Chen, Qu, Wang and

Zhang (henceforth CCQWZ) [8]. We give similar refinements of the results of AKLMRS and DAGS.

We hope these combinatorial results will be of interest. But more than any single application, our main goal is to demonstrate that Theorem 1.6 is a tool that can be broadly applied to refine combinatorial existence theorems into theorems which give explicit (and sometimes sharp) lower bounds on the *number* of combinatorial objects asserted to exist and to treat inhomogeneous cases with results in which the lower bounds are conditional on the existence of any objects of a given type (a plainly necessary restriction in many natural situations). We tried to find applications which are substantial enough to serve as a true "proof of concept," and we hope to convince the reader that this tool can be a useful one for researchers in branches of mathematics where polynomial methods are currently being applied.

2. Preliminaries

2.1. Balls in bins

Let $n \in \mathbb{Z}^+$, and let $a_1 \geq \ldots \geq a_n \geq 1$ be integers. Consider bins $A_1, \ldots, A_n$ such that A_i can hold at most a_i balls. For $N \in \mathbb{Z}^+$, a **distribution of N balls in the bins** $A_1, \ldots, A_n$ is an n-tuple $y = (y_1, \ldots, y_n)$ with $y_1 + \ldots + y_n = N$ and $1 \leq y_i \leq a_i$ for all i. Such distributions exist if and only if $n \leq N \leq a_1 + \ldots + a_n$.

For a distribution y of N balls into bins $A_1, \ldots, A_n$, let $P(y) = y_1 \ldots y_n$. If $n \leq N \leq a_1 + \ldots + a_n$, let $\mathfrak{m}(a_1, \ldots, a_n; N)$ be the minimum value of $P(y)$ as y ranges over all distributions of N balls into bins $A_1, \ldots, A_n$. We have $\mathfrak{m}(a_1, \ldots, a_n; n) = 1$. If $N \in \mathbb{Z}$ is such that $N < n$, put $\mathfrak{m}(a_1, \ldots, a_n; N) = 1$. Similarly, we have $\mathfrak{m}(a_1, \ldots, a_n; a_1 + \ldots + a_n) = a_1 \ldots a_n$. If $N \in \mathbb{Z}$ is such that $N > a_1 + \ldots + a_n$, put $\mathfrak{m}(a_1, \ldots, a_n; N) = a_1 \ldots a_n$. Note that if $N_1 \leq N_2$ then $\mathfrak{m}(a_1, \ldots, a_n; N_1) \leq \mathfrak{m}(a_1, \ldots, a_n; N_2)$.

Lemma 2.1. *Let $n, a_1, \ldots, a_n \in \mathbb{Z}^+$ with $\max\{a_1, \ldots, a_n\} \geq 2$. Let $N > n$ be an integer. Then $\mathfrak{m}(a_1, \ldots, a_n; N) \geq 2$.*

Proof. This is, literally, the pigeonhole principle. ∎

The following simple result describes the minimal distribution in all cases and thus essentially computes $\mathfrak{m}(a_1, \ldots, a_n; N)$. A formula in the general case would be unwieldy, but we give exact formulas in some special cases that we will need later.

Lemma 2.2. *Let $n \in \mathbb{Z}^+$, and let $a_1 \geq \ldots \geq a_n \geq 1$ be integers. Let N be an integer with $n \leq N \leq a_1 + \ldots + a_n$.*

a) We define the ***greedy configuration*** $y_G = (y_1, \ldots, y_n)$*: after placing one ball in each bin, place the remaining balls into bins from left to right, filling each bin completely before moving on to the next bin, until we run out of balls. Then*

$$\mathfrak{m}(a_1, \ldots, a_n; N) = P(y_G) = y_1 \ldots y_n.$$

b) Suppose $a_1 = \ldots = a_n = a \geq 2$*. If* $n \leq N \leq an$*, then*

$$\mathfrak{m}(a, \ldots, a; N) = (R+1)a^{\lfloor \frac{N-n}{a-1} \rfloor},$$

where $R \equiv N - n \pmod{a-1}$ *and* $0 \leq R < a-1$*.*

c) For all non-negative integers k*, we have*

$$\mathfrak{m}(2, \ldots, 2; 2n-k) = 2^{n-k}.$$

Proof. a) Consider the following two kinds of "elementary moves" which transform one distribution y of N balls in bins of size $a_1 \geq \ldots \geq a_n \geq 1$ into another y':

(i) (Bin Swap): If for $i < j$ we have $y_i < y_j$, then let y' be obtained from y by interchanging the ith and jth coordinates. Then $P(y') = P(y)$.

(ii) (Unbalancing Move): Suppose that for $1 \leq i \neq j \leq n$ we have $1 < y_i \leq y_j < a_j$. Then we may remove a ball form the ith bin and place it in the jth bin to get a new distribution $y' = (y'_1, \ldots, y'_n)$ and

$$P(y') = \frac{y'_i y'_j}{y_i y_j} P(y) = \frac{y_i y_j + y_i - y_j - 1}{y_i y_j} P(y) < P(y).$$

Starting with any distribution y, we may perform a sequence of bin swaps to get a distribution y' with and $y'_1 \geq \ldots \geq y'_n$ and then a sequence of unbalancing moves, each of which has i maximal such that $1 < y_i$ and j minimal such that $y_j < a_j$, to arrive at the greedy configuration y_G. Thus $P(y) = P(y') \geq P(y_G)$.

b) Put $k = \lfloor \frac{N-n}{a-1} \rfloor$, so via division with remainder we have

$$N - n = k(a-1) + R.$$

The greedy configuration is then

$$y_G = (\overbrace{a, \ldots, a}^{k}, R+1, \overbrace{1, \ldots, 1}^{n-k-1}).$$

c) This is the special case $a = 2$ of part b). ∎

2.2. The Alon-Füredi Theorem

Theorem 2.3. *(Alon-Füredi Theorem) Let F be a field, let $A_1, \ldots, A_n$ be nonempty finite subsets of F. Put $A = \prod_{i=1}^n A_i$ and $a_i = \#A_i$ for all $1 \leq i \leq n$. Let $P \in F[t] = F[t_1, \ldots, t_n]$ be a polynomial. Let*

$$\mathcal{U}_A = \{x \in A \mid P(x) \neq 0\}, \ \mathfrak{u}_A = \#\mathcal{U}_A.$$

Then $\mathfrak{u}_A = 0$ or $\mathfrak{u}_A \geq \mathfrak{m}(a_1, \ldots, a_n; a_1 + \ldots + a_n - \deg P)$.

Proof. See [2, Thm. 5]. ∎

2.3. The Schanuel-Brink operator

Let p be a prime number. For $1 \leq i \leq n$, let A_i be a set of coset representatives of $p\mathbb{Z}$ in $\mathbb{Z}$; put $A = \prod_{i=1}^n A_i$. In [24], Schanuel proves the following result.

Lemma 2.4. *Let $v \in \mathbb{Z}^+$, and let $f \in \mathbb{Z}/p^v\mathbb{Z}[t] = \mathbb{Z}/p^v\mathbb{Z}[t_1, \ldots, t_n]$ be a polynomial of degree d. There are polynomials $f_1, \ldots, f_v \in \mathbb{Z}/p\mathbb{Z}[t]$ of degrees $d, pd, \ldots, p^{v-1}d$ such that for all $x \in A$, $f(x) \equiv 0 \pmod{p^v}$ iff $f_i(x) \equiv 0 \pmod{p}$ for all $1 \leq i \leq v$.*

Since the sum of the degrees of the f_i's in Lemma 2.4 is $d + pd + \ldots + p^{v-1}d = \left(\frac{p^v - 1}{p-1}\right) d$, Lemma 2.4 reduces Theorem 1.3a) to the $q = p$ case of Chevalley's Theorem.

Although the statement concerns only finite rings, all known proofs use characteristic 0 constructions. Schanuel's proof works in the ring of p-adic integers $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$: as he mentions, it is really motivated by the theory of **Witt vectors** but can be – and was – presented in a self-contained way. In [6], Brink generalized and simplified Schanuel's construction (actually some of Brink's simplifications have already been incorporated in our statement of Lemma 2.4; Schanuel spoke of solutions with coordinates in the set of Teichmüller representatives for $\mathbb{F}_p$ in $\mathbb{Z}_p$) by working in the localization of $\mathbb{Z}$ at the prime ideal (p), namely

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} \text{ such that } p \nmid b \right\}.$$

Following Schanuel, Brink introduces an operator (which depends on the choice of A, though we suppress it from the notation)

$$\Delta \colon \mathbb{Z}_{(p)}[t] \to \mathbb{Z}_{(p)}[t]$$

such that $\deg \Delta(f) \leq p \deg f$ and for all $x \in A$ we have $f(x) \equiv 0 \pmod{p^v}$ iff $(\Delta^i f)(x) \equiv 0 \pmod{p}$ for $0 \leq i \leq v-1$. This is all we need to prove Theorem 1.6 in the $q=p$ case. Since this is the only case which gets applied in Section 4, readers who are more interested in combinatorics than algebraic number theory may wish to move on to the next section. However, we wish to state Theorem 1.6 so that it includes Warning's Second Theorem over $\mathbb{F}_q$ and to deduce a suitable strengthening of Schauz-Brink's Theorem from it, and this necessitates the following setup.

Let K be a number field with ring of integers R. Let $\mathfrak{p}$ be a prime ideal of R, so $R/\mathfrak{p} \cong \mathbb{F}_q$ for a prime power $q = p^\ell$. Let $R_\mathfrak{p}$ be the localization of R at the prime ideal $\mathfrak{p}$, which is a discrete valuation ring with discrete valuation $v_\mathfrak{p}$. Let π in R be such that $v_\mathfrak{p}(\pi)=1$, so $\mathfrak{p}R_\mathfrak{p} = \pi R_\mathfrak{p}$.

For $1 \leq i \leq n$, let $\emptyset \neq A_i \subset R$ be such that distinct elements of A_i are incongruent modulo $\mathfrak{p}$. (So $\#A_i \leq q$ for all i.) Put $A = \prod_{i=1}^n A_i$. For $1 \leq i \leq n$, there is $\tau_i(x) \in K[x]$ of degree less than q such that $\tau_i(a_i) = \frac{a_i - a_i^q}{\pi}$ for all $a_i \in A_i$:

$$\tau_i(x) = \sum_{a_i \in A_i} \frac{a_i - a_i^q}{\pi} \prod_{b_i \in A_i \setminus \{a_i\}} \frac{x - b_i}{a_i - b_i}.$$

This formula makes clear that $\tau_i(x) \in R_\mathfrak{p}[x]$. For $1 \leq i \leq n$, put

$$\sigma_i(x) = x^q + \pi \tau_i(x).$$

It follows that:

- $\sigma_i(x) \in R_\mathfrak{p}[x]$;
- $\deg \sigma_i = q$;
- for all $a_i \in A_i$, $\sigma_i(a_i) = a_i$; and
- $\sigma_i(x) \equiv x^q \pmod{\mathfrak{p}R_\mathfrak{p}[x]}$.

We define the **Schanuel-Brink operator** $\Delta\colon K[t_1, \ldots, t_n] \to K[t_1, \ldots, t_n]$ by

$$\Delta\colon f(t_1, \ldots, t_n) \mapsto \frac{f(t_1, \ldots, t_n)^q - f(\sigma_1(t_1), \ldots, \sigma_n(t_n))}{\pi}.$$

Lemma 2.5. *(Properties of the Schanuel-Brink Operator)*

a) For all $f \in K[t]$, $\deg \Delta(f) \leq q \deg f$.

b) If $c \in K$, then $\Delta(c) = \frac{c^q - c}{\pi}$.

c) For all $f \in R_\mathfrak{p}[t]$, we have $\Delta(f) \in R_\mathfrak{p}[t]$.

d) For all $f \in R_\mathfrak{p}[t]$, $a = (a_1, \ldots, a_n) \in A$, $i \in \mathbb{Z}^+$, we have $(\Delta^i f)(a) = \Delta^i(f(a))$.

e) For all $c \in R_\mathfrak{p}$ and $v \in \mathbb{Z}^+$, the following are equivalent:

(i) $c \equiv 0 \pmod{\mathfrak{p}^v}$.

(ii) We have $c, \Delta c, \ldots, \Delta^{v-1}(c) \equiv 0 \pmod{\mathfrak{p}}$.

Proof. Parts a) and b) are immediate.

c) It is enough to show that the image in $\mathbb{F}_q[t]$ of

$$f(t)^q - f(\sigma_1(t_1), \ldots, \sigma_n(t_n))$$

is zero. In characteristic p we have $(x+y)^p = x^p + y^p$, and applying this ℓ times gives $(x+y)^q = x^q + y^q$. Since also $a^q = a$ for all $a \in \mathbb{F}_q$ it follows that for any

$$f(t) = \sum_I c_I t_1^{a_1} \ldots t_n^{a_n}$$

we have that as elements of $\mathbb{F}_q[t]$,

$$f(t)^q = \sum_I c_I t_1^{qa_1} \ldots t_n^{qa_n} = f(\sigma_1(t_1), \ldots, \sigma_n(t_n)).$$

d) Since $\sigma_i(a_i) = a_i$ for all $a_i \in A_i$,

$$(\Delta f)(a) = \frac{f(a_1, \ldots, a_n)^q - f(a_1, \ldots, a_n)}{\pi} = \Delta(f(a)),$$

establishing the $i = 1$ case. The general case follows by induction.

e) If $c = 0$ then (i) and (ii) hold. Each of (i) and (ii) implies $c \equiv 0 \pmod{\mathfrak{p}}$, so we may assume $c \neq 0$ and $c \equiv 0 \pmod{\mathfrak{p}}$. Since $c \equiv 0 \pmod{\mathfrak{p}}$, $v_{\mathfrak{p}}(c) \geq 1$ and thus

$$v_{\mathfrak{p}}(c^q) = q v_{\mathfrak{p}}(c) > v_{\mathfrak{p}}(c).$$

It follows that $v_{\mathfrak{p}}(c^q - c) = v_{\mathfrak{p}}(c)$ (if $\mathfrak{p}^{v_{\mathfrak{p}}(c)+1}$ divided $c^q - c$, then it would divide c^q and hence it would divide c, contradiction) and thus

$$v_{\mathfrak{p}}(\Delta(c)) = v_{\mathfrak{p}}\left(\frac{c^q - c}{\pi}\right) = v_{\mathfrak{p}}(c^q - c) - 1 = v_{\mathfrak{p}}(c) - 1.$$

The equivalence (i) $\iff$ (ii) follows. ∎

The following immediate consequence is the main result of this section.

Corollary 2.6. *For all $f \in R_{\mathfrak{p}}[t]$, $a \in A$ and $v \in \mathbb{Z}^+$, we have $f(a) \equiv 0 \pmod{\mathfrak{p}^v}$ iff $(\Delta^i f)(a) \equiv 0 \pmod{\mathfrak{p}}$ for all $0 \leq i \leq v-1$.*

3. The restricted variable Warning's Second Theorem

3.1. The Schauz-Brink Theorem in a number field

Theorem 3.1. *Let K be a number field with ring of integers R, let $\mathfrak{p}$ be a nonzero prime ideal of R, and let $q = p^\ell$ be the prime power such that $R/\mathfrak{p} \cong \mathbb{F}_q$. Let $P_1(t_1,\ldots,t_n),\ldots,P_r(t_1,\ldots,t_n) \in R[t_1,\ldots,t_n]$, let $v_1,\ldots,v_r \in \mathbb{Z}^+$, and let $A_1,\ldots,A_n$ be nonempty subsets of R such that for each i, the elements of A_i are pairwise incongruent modulo $\mathfrak{p}$, and put $A = \prod_{i=1}^n A_i$. Let*

$$Z_A = \{x \in A \mid P_j(x) \equiv 0 \pmod{\mathfrak{p}^{v_j}}\ \forall 1 \le j \le r\},\ \mathbf{z}_A = \#Z_A.$$

a) If $\sum_{j=1}^r (q^{v_j}-1)\deg(P_j) < \sum_{i=1}^n (\#A_i - 1)$, then $\mathbf{z}_A \neq 1$.
*b) (**Boolean Case**) If $A = \{0,1\}^n$ and*

$$\sum_{j=1}^r (q^{v_j}-1)\deg(P_j) < n,$$

then $\mathbf{z}_A \neq 1$.

Brink states (but does not prove) Theorem 3.1 [6, p. 130]. Having carried over the Schanuel-Brink operator to number fields, we could apply Brink's proof verbatim. Rather than replicate this argument, we will deduce Theorem 3.1 as a consequence of Theorem 1.6.

3.2. Proof of the restricted variable Warning's Second Theorem

Proof. a) Step 1: Suppose each $v_i = 1$. Put $d = \sum_{i=1}^r \deg(P_i)$ and

$$P(t) = \prod_{i=1}^r (1 - P_i(t)^{q-1}).$$

Then $\deg P = (q-1)d$, and

$$\mathcal{U}_A = \{x \in A \mid P(x) \neq 0\} = Z_A,$$

so

$$z_A = \#Z_A = \#\mathcal{U}_A = \mathfrak{u}_A.$$

Applying the Alon-Füredi Theorem we get $\mathbf{z}_A = 0$ or

$$\mathbf{z}_A \ge \mathfrak{m}(\#A_1 + \ldots + \#A_n; \#A_1 + \ldots + \#A_n - (q-1)d).$$

Step 2: Let $a \in A$ and $f \in R_{\mathfrak{p}}[t_1, \ldots, t_n]$. By Corollary 2.6,

$$f(a) \equiv 0 \pmod{\mathfrak{p}^{v_i}} \iff (\Delta^i f)(a) \equiv 0 \pmod{\mathfrak{p}} \forall\ i \leq v_i - 1.$$

Moreover, by Lemma 2.5a), $\deg \Delta^i f \leq q^i \deg f$. Thus for each $1 \leq j \leq r$, we have exchanged the congruence $P_j \equiv 0 \pmod{\mathfrak{p}^{v_j}}$ for the system of congruences

$$P_j \equiv 0 \pmod{\mathfrak{p}},\ \Delta P_j \equiv 0 \pmod{\mathfrak{p}}, \ldots, \Delta^{v_j - 1} P_j \equiv 0 \pmod{\mathfrak{p}}$$

of degrees at most $\deg P_j,\ q \deg P_j, \ldots, q^{v_j - 1} \deg P_j$. Hence the sum of the degrees of all the polynomial congruences is at most

$$\sum_{j=1}^{r} (1 + q + \ldots + q^{v_j - 1}) \deg P_j = \sum_{j=1}^{r} \frac{q^{v_j} - 1}{q - 1} \deg(P_j).$$

Apply Step 1.

b) To recover Theorem 1.2: for all i, take A_i to be a set of coset representatives for $\mathfrak{p}R$ in R, so $\#A_i = q$ for all i. Let $k = n - (d_1 + \ldots + d_r) = n - d$, so

$$\#A_1 + \ldots + \#A_n - \deg P = nq - (q-1)d = kq + n - k.$$

Lemma 2.2b) gives

$$\begin{aligned} &\mathfrak{m}(\#A_1, \ldots, \#A_n; \#A_1 + \ldots + \#A_n - \deg P) \\ &\quad = \mathfrak{m}(q, \ldots, q; kq + n - k) = q^k = q^{n-d}. \end{aligned}$$

To recover Theorem 3.1: apply Lemma 2.1 and part a).

c) For all i take $A_i = \{0, 1\}$. Lemma 2.2c) gives

$$\begin{aligned} &\mathfrak{m}(\#A_1, \ldots, \#A_n; \#A_1 + \ldots + \#A_n - \deg P) \\ &= \mathfrak{m}(2, \ldots, 2; 2n - \sum_{j=1}^{r} (q^{v_j} - 1) \deg(P_j)) = 2^{n - \sum_{j=1}^{r} (q^{v_j} - 1) \deg(P_j)}. \end{aligned}$$ ∎

3.3. Deductions from the unrestricted cases

Schanuel proved part b) of Theorem 1.3 by applying part a) to the polynomials $P_j(t_1^{p-1}, \ldots, t_n^{p-1})$: this works since for all $x \in \mathbb{F}_p$, $x^{p-1} \in \{0, 1\}$. He proved part c) by applying part a) to the polynomials $P_j(t_{1,1}^{p-1} + \ldots + t_{1,b_1}^{p-1}, \ldots, t_{n,1}^{p-1} + \ldots + t_{n,b_n}^{p-1})$ in the $b_1 + \ldots + b_n$ variables $t_{1,1}, \ldots, t_{1,b_1}, \ldots, t_{n,1}, \ldots, t_{n,b_n}$. In particular, the case of Theorem 1.3b) in which all congruences are modulo p

is reduced to Chevalley's Theorem. This substitution underlies many of the combinatorial applications of the Chevalley-Warning Theorem, e.g. [5]: see Section 4.4.

Question 1. *For which $A = \prod_{i=1}^n A_i \subset \mathbb{F}_q^n$ can one deduce the Restricted Variable Chevalley Theorem (Theorem 1.4) from its unrestricted version (Theorem 1.1a))?*

We turn to Warning's Second Theorem. Since the bound obtained in Theorem 1.6 is in terms of the combinatorially defined quantity $\mathfrak{m}(a_1, \ldots, a_n; N)$, it is natural to wonder to what extent Theorem 1.6 could be deduced from Theorem 1.2 by purely combinatorial arguments. Consider again $A = \{0,1\}^n$. It turns out that some work has been done on this problem: in Theorem 1.6c), take $r = v_1 = 1$ and $q = p$, write P for P_1, and put $d = \deg P$, so

$$\mathbf{z}_{\{0,1\}^n} = 0 \text{ or } \mathbf{z}_{\{0,1\}^n} \geq 2^{n-(p-1)d}. \tag{3}$$

Using Warning's Second Theorem and purely combinatorial arguments, Chattopadhyay, Goyal, Pudlák and Thérien showed [9, Thm. 11] that

$$\mathbf{z}_{\{0,1\}^n} = 0 \text{ or } \mathbf{z}_{\{0,1\}^n} \geq 2^{n-(\log_2 p)(p-1)d}. \tag{4}$$

For $p = 2$, (3) and (4) coincide with (2). For $p > 2$, (3) is an improvement of (4).

4. Combinatorial applications

4.1. The Davenport constant and g-sum subsequences

Let $(G, +)$ be a nontrivial finite commutative group. For $n \in \mathbb{Z}^+$, let $x = (x_1, \ldots, x_n) \in G^n$. We view x as a length n sequence $x_1, \ldots, x_n$ of elements in G and a subset $J \subset \{1, \ldots, n\}$ as giving a subsequence x_J of x. For $g \in G$, we say x_J is a **g-sum subsequence** if $\sum_{i \in J} x_i = g$. When $g = 0$ we speak of **zero-sum subsequences**.

The **Davenport constant** $D(G)$ is the least $d \in \mathbb{Z}^+$ such that every $x \in G^d$ has a nonempty zero-sum subsequence. The pigeonhole principle gives

$$D(G) \leq \#G. \tag{5}$$

The Davenport constant arises naturally in the theory of factorization in integral domains. We mention one result to show the flavor.

Theorem 4.1. *Let K be a number field, let R be its ring of integers, and let $\mathrm{Cl}\,R$ be the ideal class group of R. For $x \in R$ nonzero and not a unit, let $L(x)$ (resp. $l(x)$) be the maximum (resp. the minimum) of all lengths of factorizations of x into* irreducible elements, *let*

$$\rho(x) = \frac{L(x)}{l(x)},$$

and let $\rho(R)$ be the supremum of $\rho(x)$ as x ranges over nonzero nonunits.

a) (Carlitz [7]) We have $\rho(R)=1 \iff \#\mathrm{Cl}\,R \le 2$.

b) (Valenza [28]) We have $\rho(R)=\max\left(\frac{D(\mathrm{Cl}\,R)}{2},1\right)$.

For any finite commutative group G, there are unique positive integers $r, n_1, \ldots, n_r$ with $1 < n_r \,|\, n_{r-1} \,|\, \ldots \,|\, n_1$ such that $G \cong \bigoplus_{i=1}^r \mathbb{Z}/n_i\mathbb{Z}$. Put

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

Let $e_i \in \bigoplus_{i=1}^r \mathbb{Z}/n_i\mathbb{Z}$ be the element with ith coordinate 1 and all other coordinates zero. Then the sequence

$$\overbrace{e_1, \ldots, e_1}^{n_1-1}, \overbrace{e_2, \ldots, e_2}^{n_2-1}, \ldots, \overbrace{e_r, \ldots, e_r}^{n_r-1}$$

shows that

$$d(G) \le D(G). \tag{6}$$

Comparing (5) and (6) shows $D(G)=\#G=d(G)$ when G is cyclic. In 1969, J. E. Olson conjectured that $D(G) = d(G)$ for all G and proved it in the following cases.

Theorem 4.2. *(Olson) For a finite commutative group G, $d(G) = D(G)$ holds if:*

(i) G is a direct product of two *cyclic groups; or*

(ii) G is a p-group (i.e., $\#G=p^a$ for some $a \in \mathbb{Z}^+$).

Proof. Part (i) is [23, Cor. 1.1]. Part (ii) is [22, (1)]. ∎

However, at almost the same time Olson's conjecture was disproved.

Theorem 4.3. *(van Emde Boas-Kruyswijk [14]) For $G = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, we have $d(G) < D(G)$.*

In the intervening years there has been an explosion of work on the Davenport constant and related quantities. Nevertheless, for most finite commutative groups G, the exact value of $D(G)$ remains unknown.

Let us turn to g-sum subsequences with $g \neq 0$. There is no analogue of the Davenport constant here, because for all $n \in \mathbb{Z}^+$, $(0,\ldots,0) \in G^n$ has length n and no g-sum subsequence. On the other hand, for $g \in G$ and $x \in G^n$, let

$$N_g(x) = \#\left\{ J \subset \{1,\ldots,n\} \;\middle|\; \sum_{i \in J} x_i = g \right\}.$$

Theorem 4.4. *Let $(G,+)$ be a finite commutative group, let $n \in \mathbb{Z}^+$, and let $g \in G$.*

a) ([23, Thm. 2]) We have $\min_{x \in G^n} N_0(x) = \max\{1, 2^{n+1-D(G)}\}$.

b) ([8, Thm. 2]) For all $x \in G^n$, if $N_g(x) > 0$ then $N_g(x) \geq 2^{n+1-D(G)}$.

Now let $G = \bigoplus_{i=1}^r \mathbb{Z}/p^{v_i}\mathbb{Z}$ be a p-group.

As Schanuel observed, in this case Theorem 4.2 is a quick consequence of Theorem 1.3. Indeed, suppose $n > d(G) = \sum_{i=1}^r (p^{v_i} - 1)$, and represent elements of G by r-tuples of integers $(a_1,\ldots,a_r)$. For $1 \leq i \leq n$ and $1 \leq j \leq r$, let

$$g_j = (a_1^{(j)}, \ldots, a_r^{(j)})$$

and

$$P_i(t_1,\ldots,t_n) = \sum_{j=1}^n a_i^{(j)} t_j.$$

Theorem 1.3b) applies to give $x \in \{0,1\}^n \setminus \{(0,\ldots,0)\}$ such that

$$\sum_{j=1}^n a_i^{(j)} x_j \equiv 0 \pmod{p^{v_i}} \; \forall 1 \leq i \leq r.$$

Then we get a zero-sum subsequence from $J = \{j \,|\, x_j = 1\}$.

Moreover, in this case the Restricted Variable Warning's Second Theorem implies a combination of Theorem 4.2 and Theorem 4.4: namely Theorem 4.4 with $D(G)$ replaced by the explicit value $d(G) = \sum_{i=1}^r (p^{v_i} - 1)$. By part a), Theorem 1.6 and Lemma 2.2, we get $N_g(x) = 0$ or

$$N_g(x) \geq \mathfrak{m}\left(2,\ldots,2; n + (n - \sum_{i=1}^r (p^{v_i} - 1)\right) = 2^{n - \sum_{i=1}^r (p^{v_i} - 1)}.$$

4.2. Generalized subsequences

The following results are the analogues of those of the previous section for generalized g-sum subsequences. The proofs are the same.

Theorem 4.5. *(Troi-Zannier [27], Brink [6]) Let $G \cong \bigoplus_{j=1}^{r} \mathbb{Z}/p^{v_i}\mathbb{Z}$ be a finite commutative p-group. Let $A_1, \ldots, A_n \subset \mathbb{Z}$ be nonempty subsets such that each A_i has pairwise incongruent elements modulo p. Put $A = \prod_{i=1}^{n} A_i$. Suppose that*

$$\sum_{i=1}^{n} (\#A_i - 1) > \sum_{j=1}^{r} (p^{v_j} - 1).$$

Let $x = (x_1, \ldots, x_n) \in G^n$ be a sequence of elements in G.

a) Then $\#\{(a_1, \ldots, a_n) \in A \mid a_1x_1 + \ldots + a_nx_n = 0\} \neq 1$.

b) If $0 \in A$, then there is $0 \neq a = (a_1, \ldots, a_n) \in A$ such that $a_1x_1 + \ldots + a_nx_n = 0$.

Remark 4.6. Theorem 4.5 was first proven by Troi and Zannier [27, Thm. 1]. The original argument of Troi and Zannier uses group ring methods. They remark on their inability to carry out a Chevalley-Warning style proof. It seems to us that Brink's proof using the Schauz-Brink Theorem is precisely the type of the argument that Troi and Zannier were looking for.

Theorem 4.7. *Let p be a prime, let $r, v_1, \ldots, v_r \in \mathbb{Z}^+$; put $G = \bigoplus_{i=1}^{r} \mathbb{Z}/p^{v_i}\mathbb{Z}$. For $n \in \mathbb{Z}^+$, let $x = (x_1, \ldots, x_n) \in G^n$ be a sequence of elements in G. Let $A_1, \ldots, A_n$ be nonempty subsets of $\mathbb{Z}$ such that for each i the elements of A_i are pairwise incongruent modulo p, and put $A = \prod_{i=1}^{n} A_i$. For $g = (g_1, \ldots, g_r) \in G$, let*

$$N_{g,A}(x) = \#\{a = (a_1, \ldots, a_n) \in A \mid a_1x_1 + \ldots + a_nx_n = g\}.$$

Then $N_{g,A}(x) = 0$ or

$$N_{g,A}(x) \geq \mathfrak{m}\left(\#A_1, \ldots, \#A_n; \#A_1 + \ldots + \#A_n - \sum_{i=1}^{r} (p^{v_i} - 1)\right).$$

4.3. Counting sub-(set systems) with union cardinality 0 modulo q

In [1], AKLMRS applied Schanuel's Theorem to deduce a result on set systems. This is an interesting case for these methods because (i) unlike the applications of the previous section the polynomials are not linear (or even

obtained from linear polynomials by applying the Schanuel-Brink operator); (ii) there is no known purely combinatorial proof; and (iii) the bound obtained is sharp in all cases. By applying Theorem 1.6 instead of Schanuel's Theorem, we immediately derive a quantitative refinement of this result and also treat the "inhomogeneous case."

A **set system** is a finite sequence $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_n)$ of finite subsets of some fixed set X. We say that n is the **length** of $\mathcal{F}$. The **maximal degree** of $\mathcal{F}$ is $\max_{x \in X} \#\{1 \leq i \leq n \,|\, x \in \mathcal{F}_i\}$. For m a positive integer and $g \in \mathbb{Z}/m\mathbb{Z}$, let

$$N_{\mathcal{F}}(m, g) = \#\{J \subset \{1, \ldots, n\} \mid \#(\bigcup_{i \in J} \mathcal{F}_i) \equiv g \pmod{m}\},$$

and for $n, d \in \mathbb{Z}^+$, let

$$\mathcal{N}_{n,d}(m) = \min N_{\mathcal{F}}(m, 0),$$

the minimum ranging over set systems of length n and maximal degree at most d. Let $f_d(m)$ be the least $n \in \mathbb{Z}^+$ such that for any degree d set system $\mathcal{F}$ of length n, there is a nonempty subset $J \subset \{1, \ldots, n\}$ such that $m \,|\, \#(\bigcup_{i \in J} \mathcal{F}_i)$. Thus

$$f_d(m) = \min\{n \in \mathbb{Z}^+ \mid \mathcal{N}_{n,d}(m) \geq 2\}. \tag{7}$$

Lemma 4.8. *([1]) We have $f_d(m) \geq d(m-1)+1$.*

Proof. Let A_{ij} be a family of pairwise disjoint sets each of cardinality m, as $1 \leq i \leq m-1,\ 1 \leq j \leq d$. Let $\{v_1, \ldots, v_{m-1}\}$ be a set of cardinality $m-1$, disjoint from all the A_{ij}'s. Then $\mathcal{F} = \{A_{ij} \cup \{v_i\} \mid 1 \leq i \leq m-1,\ 1 \leq j \leq d\}$ has length $d(m-1)$ and for no nonempty subset $J \subset \{1, \ldots, d(m-1)\}$ do we have $m \,|\, \#(\bigcup_{i \in J} \mathcal{F}_i)$. ∎

Theorem 4.9. *Let $q = p^v$ be a prime power, $g \in \mathbb{Z}/p^v\mathbb{Z}$, $d, n \in \mathbb{Z}^+$, and $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_n)$ a set system of maximal degree d. Then:*

a) $\mathcal{N}_{\mathcal{F}}(p^v, g)$ is either 0 or at least $2^{n-d(p^v-1)}$. We deduce:

b) $\mathcal{N}_{n,d}(p^v) \geq 2^{n-d(p^v-1)}$; and thus

c) ([1]) $f_d(q) = d(p^v-1)+1$.

Proof. a) For $\mathcal{F}$ a set system of length n and maximal degree at most d, put

$$h(t_1, \ldots, t_n) = \sum_{\emptyset \neq J \subset \{1, \ldots, n\}} (-1)^{\#J+1} \#(\bigcap_{j \in J} \mathcal{F}_i) \prod_{j \in J} t_j.$$

Then $\deg h \le d$ and $h(0) = 0$. For any $x \in \{0,1\}^n$, let $J_x = \{1 \le j \le n \,|\, x_j = 1\}$. The Inclusion-Exclusion Principle implies

$$h(x) = \# \bigcup_{j \in J_x} \mathcal{F}_j,$$

so $\mathcal{N}_{\mathcal{F}}(p^v, g)$ counts the number of solutions $x \in \{0,1\}^n$ to the congruence $h(t) - g \equiv 0 \pmod{p^v}$. Applying Theorem 1.6 establishes part a).

b) Taking $J = \emptyset$ shows $\mathcal{N}_{\mathcal{F}}(p^v, 0) \ge 1$. Apply part a).

c) By part a) and (7), we see that $f_d(q) \le d(q-1)+1$. Apply Lemma 4.8. ∎

4.4. An EGZ-type theorem

As we saw in Section 4.1, computing the Davenport constant of a finite cyclic group is an easy exercise. A more interesting variant is to ask how large n needs to be in order to ensure that any sequence of length n in the group $\mathbb{Z}/m\mathbb{Z}$ has a zero-sum subsequence of length m. The sequence

$$(\overbrace{0, \ldots, 0}^{m-1}, \overbrace{1, \ldots, 1}^{m-1})$$

shows that we need to take $n \ge 2m-1$. The following converse is one of the founding results in this branch of additive combinatorics.

Theorem 4.10. *(Erdős-Ginzburg-Ziv [15]) Every sequence of length $2m-1$ in $\mathbb{Z}/m\mathbb{Z}$ has a zero-sum subsequence of length m.*

It is not hard to see that if Theorem 4.10 holds for positive integers m_1 and m_2, then it holds for their product, and thus one reduces to the case in which m is prime. The original work [15] showed this via a combinatorial argument. Later it was realized that one can get a quick proof using Chevalley's Theorem [5].

A recent paper of DAGS [12] treats the analogous problem in any finite commutative p-group, with zero-sum subsequences replaced by generalized zero-sum subsequences in the sense of Section 4.2. As before, using Theorem 1.6 we get a quantitative refinement which also includes the inhomogeneous case.

For a finite commutative group G, let $\exp G$ denote the exponent of G, i.e., the least common multiple of all orders of elements in G.

Lemma 4.11. *Let $\{0\} \subset A \subset \mathbb{Z}$ be a finite subset, no two of whose elements are congruent modulo p. There is $C_A \in \mathbb{Z}_{(p)}[t]$ of degree $\#A-1$ such that for $a \in A$,*

$$C_A(a) = \begin{cases} 0 & a = 0 \\ 1 & a \neq 0 \end{cases}.$$

Proof. We may take $C_A(t) = 1 - \prod_{a \in A \setminus \{0\}} \frac{a-t}{a}$. ∎

Theorem 4.12. *Let k, r, $v_1 \leq \ldots \leq v_r$ be positive integers, and let $G = \bigoplus_{i=1}^r \mathbb{Z}/p^{v_i}\mathbb{Z}$. Let $A_1, \ldots, A_n$ be nonempty subsets of $\mathbb{Z}$, each containing 0, such that for each i the elements of A_i are pairwise incongruent modulo p. Put*

$$A = \prod_{i=1}^n A_i, \ a_M = \max \#A_i.$$

For $x \in G$, let $\mathrm{EGZ}_{A,k}(x)$ be the number of $(a_1, \ldots, a_n) \in A$ such that $a_1 x_1 + \ldots + a_n x_n = x$ and $p^k \,|\, \#\{1 \leq i \leq n \,|\, a_i \neq 0\}$. Then either $\mathrm{EGZ}_{A,k}(x) = 0$ or

$$\begin{aligned} &\mathrm{EGZ}_{A,k}(x) \\ &\geq \mathfrak{m}\left(\#A_1, \ldots, \#A_n; \#A_1 + \ldots + \#A_n - \sum_{i=1}^r (p^{v_i} - 1) - (a_M - 1)(p^k - 1)\right). \end{aligned} \tag{8}$$

Proof. We apply Theorem 1.6 as in the proof of Theorem 4.7. The extra condition that the number of nonzero terms in the zero-sum generalized subsequence is a multiple of p^k is enforced via the polynomial congruence

$$C_{A_1}(t_1) + \ldots + C_{A_n}(t_n) \equiv 0 \pmod{p^k},$$

which has degree $a_M - 1$. ∎

Corollary 4.13. *In Theorem 4.12, let $0 \in A_1 = \ldots = A_n$, $k = v_r$. Put $a = \#A_1$.*

a) Suppose

$$n \geq \exp G - 1 + \frac{D(G)}{a-1}.$$

Let R be such that $R \equiv -\sum_{i=1}^r (p^{v_i} - 1) \pmod{a-1}$ and $0 \leq R < a-1$. Then

$$\mathrm{EGZ}_{A,v_r}(0) \geq (R+1) a^{n+1-\exp G + \lfloor \frac{1-D(G)}{a-1} \rfloor}. \tag{9}$$

b) ([12, Thm. 1.1]) Every sequence of length n in G has a nonempty zero-sum generalized subsequence of length divisible by $\exp G$ when

$$n \geq \exp G - 1 + \frac{D(G)}{a-1}. \tag{10}$$

Proof. a) The empty subsequence ensures $\mathrm{EGZ}_{A,v_r}(0) \geq 1$, so Theorem 4.12 gives

$$\mathrm{EGZ}_{A,v_r}(0) \geq \mathfrak{m}\left(a, \ldots, a; na - \sum_{i=1}^{r} (p^{v_i} - 1) - (a-1)(p^{v_r} - 1)\right).$$

We have

$$n \geq \exp G - 1 + \frac{D(G)}{a-1} > \exp G - 1 + \frac{D(G)-1}{a-1},$$

hence

$$na - (D(G)-1) - (a-1)(\exp G - 1) = na - \sum_{i=1}^{r} (p^{v_i} - 1) - (a-1)(p^{v_r} - 1) > n.$$

By Lemma 2.2b), we have

$$\mathfrak{m}\left(a, \ldots, a; na - \sum_{i=1}^{r} (p^{v_i} - 1) - (a-1)(p^{v_r} - 1)\right) = (R+1)a^{n+1-\exp G + \lfloor \frac{1-D(G)}{a-1} \rfloor}.$$

b) Since $n \geq \exp G - 1 + \frac{D(G)}{a-1} > \exp G - 1 + \frac{D(G)-1}{a-1}$, we have

$$na - \sum_{i=1}^{r} (p^{v_i} - 1) - (a-1)(p^{v_r} - 1) > n.$$

It follows from part a) and Lemma 2.1 that $\mathrm{EGZ}_{A,v_r}(0) \geq 2$. ∎

In the proof of Corollary 4.13b), rather than using part a) we could have applied Theorem 1.5. It is interesting to compare this approach with the proof of Corollary 4.13b) given in [12]. Their argument proves the needed case of Theorem 1.5 by exploiting properties of binomial coefficients $\binom{t}{d}$ viewed as integer-valued polynomials and reduced modulo powers of p. In 2006 IPM lecture notes [30], R. Wilson proves Theorem 1.3 in this manner. His method works to prove Theorem 1.5.

References

[1] N. Alon, D. Kleitman, R. Lipton, R. Meshulam, M. Rabin and J. Spencer: Set systems with no union of cardinality 0 modulo m, *Graphs Combin.* **7** (1991), 97–99.

[2] N. Alon and Z. Füredi: Covering the cube by affine hyperplanes, *Eur. J. Comb.* **14** (1993), 79–83.

[3] N. Alon: Combinatorial Nullstellensatz, Recent trends in combinatorics (Mátraháza, 1995). *Combin. Probab. Comput.* **8** (1999), 7–29.
[4] J. Ax: Zeroes of polynomials over finite fields, *Amer. J. Math.* **86** (1964), 255–261.
[5] C. Bailey and R. B. Richter: Sum zero (mod n), size n subsets of integers, *Amer. Math. Monthly* **96** (1989), 240–242.
[6] D. Brink: Chevalley's theorem with restricted variables, *Combinatorica* **31** (2011), 127–130.
[7] L. Carlitz: A Characterization of Algebraic Number Fields with Class Number Two, *Proc. AMS* **11** (1960), 391–392.
[8] G. J. Chang, S.-H. Chen., Y. Qu, G. Wang and H. Zhang: *On the number of subsequences with a given sum in a finite abelian group*, *Electron. J. Combin.* **18** (2011), Paper 133.
[9] A. Chattopadhyay, N. Goyal, P. Pudlák and D. Thérien: Lower bounds for circuits with MOD_m gates, *Proc. 47th Annual Symp. on Foundations of Computer Science*, IEEE 2006, 709–718.
[10] C. Chevalley: Démonstration d'une hypothèse de M. Artin, *Abh. Math. Sem. Univ. Hamburg* **11** (1935), 73–75.
[11] P. L. Clark: The Combinatorial Nullstellensätze Revisited, *Electronic Journal of Combinatorics* **21** (2014), Paper #P4.15.
[12] S. Das Adhikari, D. J. Grynkiewicz and Z.-W. Sun: On weighted zero-sum sequences, *Adv. in Appl. Math.* **48** (2012), 506–527.
[13] L. E. Dickson: On the representation of numbers by modular forms, *Bull. Amer. Math. Soc.* **15** (1909), 338–347.
[14] P. van Emde Boas and D. Kruyswijk: *A combinatorial problem on finite abelian groups, III*, Report ZW-1969-008, Math. Centre, Amsterdam, 1969.
[15] P. Erdős, A. Ginzburg and A. Ziv: Theorem in the additive number theory, *Bull. Research Council Israel* **10F** (1961), 41–43.
[16] H. Esnault: Varieties over a finite field with trivial Chow group of 0-cycles have a rational point, *Invent. Math.* **151** (2003), 187–191.
[17] D. R. Heath-Brown: On Chevalley-Warning theorems, *Uspekhi Mat. Nauk* **66** (2011), 223–232; translation in: *Russian Math. Surveys* **66** (2011), 427–436.
[18] N. M. Katz: On a theorem of Ax, *Amer. J. Math.* **93** (1971), 485–499.
[19] R. N. Karasev and F. V. Petrov: Partitions of nonzero elements of a finite field into pairs, *Israel J. Math.* **192** (2012), 143–156.
[20] M. Lasoń: A generalization of combinatorial Nullstellensatz, *Electron. J. Combin.* **17** (2010), Note 32.
[21] D. G. Mead and W. Narkiewicz: The capacity of C_5 and free sets in C_m^2, *Proc. Amer. Math. Soc.* **84** (1982), 308–310.
[22] J. E. Olson: A combinatorial problem on finite Abelian groups, *I. J. Number Theory* **1** (1969), 8–10.
[23] J. E. Olson: A combinatorial problem on finite Abelian groups, II, *J. Number Theory* **1** (1969), 195–199.
[24] S. H. Schanuel: An extension of Chevalley's theorem to congruences modulo prime powers, *J. Number Theory* **6** (1974), 284–290.
[25] U. Schauz: Algebraically solvable problems: describing polynomials as equivalent to explicit solutions, *Electron. J. Combin.* **15** (2008), Research Paper 10.
[26] C. C. Tsen: Divisionsalgebren über Funktionenkörpern, *Nachr. Ges. Wiss. Göttingen* (1933), 335–339.

[27] G. Troi and U. Zannier: On a theorem of J. E. Olson and an application (vanishing sums in finite abelian p-groups), *Finite Fields Appl.* **3** (1997), 378–384.
[28] R. J. Valenza: Elasticity of factorizations in number fields, *J. Number Theory* **36** (1990), 212–218.
[29] E. Warning: Bemerkung zur vorstehenden Arbeit von Herrn Chevalley, *Abh. Math. Sem. Hamburg* **11** (1935), 76–83.
[30] R. M. Wilson: Some applications of polynomials in combinatorics, *EPM lectures*, May, 2006.

Pete L. Clark

Department of Mathematics
University of Georgia
Athens, GA, USA
plclark@gmail.com

Aden Forrow

Department of Mathematics
Massachusetts Institute of Technology
Cambridge, MA, USA
aforrow@mit.edu

John R. Schmitt

Department of Mathematics
Middleburg College
Middleburg, UT, USA
jschmitt@middleburg.edu