WARNING'S SECOND THEOREM WITH RELAXED OUTPUTS

PETE L. CLARK

Abstract. We present a generalization of Warning's Second Theorem to polynomial systems over a finite local principal ring with restricted input and relaxed output variables. This generalizes a recent result with Forrow and Schmitt (and gives a new proof of that result). Applications to additive group theory, graph theory and polynomial interpolation are pursued in detail.

Contents

1. Introduction

1.1. Notation and Terminology.

We denote the non-negative integers by $\mathbb{N}$ and the positive integers by $\mathbb{Z}^+$.

Let $n, a_1, \ldots, a_n \in \mathbb{Z}^+$, and let $N \leq \sum_{i=1}^n a_i$ be an integer. As in [CFS14, §2.1], we put

$$\mathfrak{m}(a_1, \ldots, a_n; N) := \begin{cases} 1 & N < n \\ \min \prod_{i=1}^n y_i & n \leq N \leq \sum_{i=1}^n a_i \end{cases};$$

the minimum is over $(y_1,\ldots,y_n) \in \mathbb{Z}^n$ with $y_i \in [1,a_i]$ for all i and $\sum_{i=1}^n y_i = N$.

All of our rings will be commutative and with multiplicative identity. Let R be a ring, $B \subset R$ a subset, I an ideal of R, and $x \in R$. We write "$x \in B \pmod{I}$" to mean that there is $b \in B$ such that $x - b \in I$.

Let R be a ring. As in [Cl14], we say a subset $A \subset R$ satisfies **Condition (F)** (resp. **Condition (D)**) if A is nonempty, finite and for any distinct elements $x, y \in A$, $x - y$ is a unit in R (resp. is not a zero-divisor in R).

Throughout this paper $\mathbb{F}_q$ denotes an arbitrary finite field, of order q and characteristic p.

1.2. **Prior Results.**

We begin with the results of Chevalley and Warning.

Theorem 1.1. *Let $n, r, d_1, \ldots, d_r \in \mathbb{Z}^+$ with $d := d_1 + \ldots + d_r < n$. For $1 \leq i \leq r$, let $f_i(t_1,\ldots,t_n) \in \mathbb{F}_q[\mathbf{t}] = \mathbb{F}_q[t_1,\ldots,t_n]$ be a polynomial of degree d_i. Put*

$$Z := Z(f_1,\ldots,f_r) = \{x \in \mathbb{F}_q^n \mid f_1(x) = \ldots = f_r(x) = 0\}.$$

a) (Chevalley's Theorem [Ch35]*) We have $\#Z = 0$ or $\#Z \geq 2$.*
b) (Warning's Theorem [Wa35]*) We have $\#Z \equiv 0 \pmod{p}$.*
c) (Warning's Second Theorem [Wa35]*) We have $\#Z = 0$ or $\#Z \geq q^{n-d}$.*

Chevalley's proof of Theorem 1.1a) can be easily modified to yield Theorem 1.1b). Warning's real contribution was Theorem 1.1c), a result which has, perhaps, been too little appreciated. It is sharp in the following strong sense: for any $d_1,\ldots,d_r \in \mathbb{N}$ with $d := d_1 + \ldots + d_r < n$, there are $f_1,\ldots,f_r \in \mathbb{F}_q[\mathbf{t}]$ with $\deg f_i = d_i$ for all $1 \leq i \leq r$ such that $\#Z(f_1,\ldots,f_r) = q^{n-d}$. One can build such examples by combining norm forms associated to field extensions $\mathbb{F}_{q^a}/\mathbb{F}_q$ and linear polynomials. On the other hand, although in these examples the equations are generally nonlinear, the solution sets are still affine subspaces. In [HB11], Heath-Brown showed that under the hypotheses of Theorem 1.1c), when Z is nonempty and is not an affine subspace of $\mathbb{F}_q^n$ one always has $\#Z > q^{n-d}$, and in fact $\#Z \geq 2q^{n-d}$ for all $q \geq 4$.

Apart from [HB11] there had been little further exploration of Theorem 1.1c) until [CFS14], which established the following result.

Theorem 1.2. *(Restricted Variable Warning's Second Theorem* [CFS14]*) Let K be a number field with ring of integers $\mathbb{Z}_K$, let $\mathfrak{p}$ be a nonzero prime ideal of $\mathbb{Z}_K$, and let $q = \#\mathbb{Z}_K/\mathfrak{p}$, so $\mathbb{Z}_K/\mathfrak{p} \cong \mathbb{F}_q$. Let $A_1,\ldots,A_n$ be nonempty subsets of $\mathbb{Z}_K$ such that for each i, the elements of A_i are pairwise incongruent modulo $\mathfrak{p}$, and put $\mathbf{A} = \prod_{i=1}^n A_i$. Let $r, v_1,\ldots,v_r \in \mathbb{Z}^+$. Let $P_1,\ldots,P_r \in \mathbb{Z}_K[t_1,\ldots,t_n]$. Put*

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

Then $\mathbf{z}_{\mathbf{A}} = 0$ or $\mathbf{z}_{\mathbf{A}} \geq \mathfrak{m}\left(\#A_1,\ldots,\#A_n; \#A_1 + \ldots + \#A_n - \sum_{j=1}^r (q^{v_j} - 1)\deg(P_j)\right)$.

This generalizes Theorem 1.1c) in two directions: first, instead of working over finite fields, we work modulo powers of a prime ideal in the ring of integers of a number field. In the case $K = \mathbb{Q}$ we are studying systems of congruence modulo (varying) powers of a (fixed) prime p. Second, we study solutions in which each variable is independently restricted to a finite subset of $\mathbb{Z}_K$ satisfying the condition that no two distinct elements are congruent modulo $\mathfrak{p}$.

Theorem 1.2 extends work of Schanuel [Sc74], Baker-Schmidt [BS80], Schauz [Sc08], Wilson [Wi06] and Brink [Br11]. These works are largely motivated by applications to combinatorics. For combinatorial applications we work over $K = \mathbb{Q}$ and get congruences modulo powers of p. The most classical applications concern the case in which each variable is restricted to take values 0 and 1. More recently there has been a surge of interest in more general subsets A_i: this yields weighted analogues of the more classical combinatorial problems.

The previous works used either *ad hoc* methods or Alon's Combinatorial Nullstellensatz and yielded *nonuniqueness theorems*: results with conclusion "there cannot be exactly one solution." To prove Theorem 1.2 we instead applied the Alon-Füredi Theorem, which yields a lower bound on the number of solutions in terms of the quantity $\mathfrak{m}(a_1, \ldots, a_n; N)$. To collapse this type of result to a nonuniqueness theorem one simply uses the following observation, a form of the Pigeonhole Principle:

$$\mathfrak{m}(a_1, \ldots, a_n; N) \geq 2 \iff N > n. \tag{1}$$

Applying (1) to Theorem 1.2, one recovers a result of Brink.

Corollary 1.3. *(Brink* [Br11]*) Let K be a number field with ring of integers $\mathbb{Z}_K$, let $\mathfrak{p}$ be a nonzero prime ideal of $\mathbb{Z}_K$, and let $q = p^\ell$ be the prime power such that $\mathbb{Z}_K/\mathfrak{p} \cong \mathbb{F}_q$. Let $P_1(t_1, \ldots, t_n), \ldots, P_r(t_1, \ldots, t_n) \in \mathbb{Z}_K[t_1, \ldots, t_n]$, let $v_1, \ldots, v_r \in \mathbb{Z}^+$, and let $A_1, \ldots, A_n$ be nonempty subsets of $\mathbb{Z}_K$ such that for each i, the elements of A_i are pairwise incongruent modulo $\mathfrak{p}$, and put $\mathbf{A} = \prod_{i=1}^n A_i$. Put*

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

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

The case of $K = \mathbb{Q}$ had earlier been established by Schauz and Wilson (independently), so we call this result the **Schauz-Wilson-Brink Theorem**. If we further specialize to $A_i = \{0, 1\}$ for all i we recover **Schanuel's Theorem**.

1.3. The Main Theorem.

For the convenience of readers who are primarily interested in combinatorial applications, we state the main result of this paper first in a special case.

Theorem 1.4. *Let p be a prime, let $n, r, v \in \mathbb{Z}^+$, and for $1 \leq i \leq r$, let $1 \leq v_j \leq v$. Let $A_1, \ldots, A_n, B_1, \ldots, B_r \subset \mathbb{Z}$ be nonempty subsets each having the property that no two distinct elements are congruent modulo p. Let $f_1, \ldots, f_r \in \mathbb{Z}[t_1, \ldots, t_n]$. Put*

$$Z_{\mathbf{A}}^{\mathbf{B}} := \{x \in \prod_{i=1}^n A_i \mid \forall 1 \leq j \leq r, \ f_j(x) \in B_j \pmod{p^{v_j}}\}.$$

Then $Z_{\mathbf{A}}^{\mathbf{B}} = \varnothing$ or

$$\# Z_{\mathbf{A}}^{\mathbf{B}} \geq \mathfrak{m}\left(\# A_1, \ldots, \# A_n; \sum_{i=1}^n \# A_i - \sum_{j=1}^r (p^{v_j} - \# B_j) \deg f_j\right).$$

Corollary 1.5. *Maintain the setup of Theorem 1.4.*
a) If $A_i = \{0,1\}$ for all $1 \leq i \leq n$, then $Z_{\mathbf{A}}^{\mathbf{B}} = \varnothing$ or

$$\# Z_{\mathbf{A}}^{\mathbf{B}} \geq 2^{n - \sum_{j=1}^{r} (p^{v_j} - \# B_j) \deg(f_j)}.$$

b) If $A_i = \{0,1\}$ for all i and $f_j(0) = 0 \in B_j$ for all j, there is $0 \neq x \in Z_{\mathbf{A}}^{\mathbf{B}}$ if

$$n > \sum_{j=1}^{r} (p^{v_j} - \# B_j) \deg(f_j).$$

Proof. Applying Theorem 1.4 in the case $A_1 = \ldots = A_n = \{0,1\}$ and using the fact that for any $0 \leq k \leq n$, we have $\mathfrak{m}(2,\ldots,2;2n-k) = 2^{n-k}$ [CFS14, Lemma 2.2c)], we get part a). Combining with (1) we get part b). □

If in Corollary 1.5b) we further require that all the polynomials are linear, we recover a result of Alon-Friedland-Kalai [AFK84, Thm. A.1]. For some (not all) combinatorial applications linear polynomials are sufficient, and $A_i = \{0,1\}$ corresponds to the "unweighted" combinatorial setup. In this setting we see that the advantage of Corollary 1.5a) over part b) is directly analogous to that of Theorem 1.2 over Brink's Theorem, namely a quantitative refinement of Alon-Füredi type. In fact this gives an accurate glimpse of our method of proof of the Main Theorem: we will establish and apply suitably generalized versions of a valuation-theoretic lemma of Alon-Friedland-Kalai and of the Alon-Füredi Theorem.

To state the full version of the Main Theorem we need some algebraic preliminaries. A **principal ring** is a commutative ring in which every ideal is principal. A ring is **local** if it has exactly one maximal ideal. (When we write "$(\mathfrak{r},\mathfrak{p})$ is a local ring," we mean that $\mathfrak{p}$ is the unique maximal ideal of $\mathfrak{r}$.) Let $(\mathfrak{r},\mathfrak{p})$ be a local principal ring such that $\mathfrak{p} = (\pi)$ is principal. By Nakayama's Lemma, we have $\bigcap_{i \geq 0} \mathfrak{p}^i = (0)$, so for every nonzero $x \in \mathfrak{r}$, there is a unique $i \in \mathbb{N}$ such that $x \in \mathfrak{p}^i \setminus \mathfrak{p}^{i+1}$, so $x = \pi^i y$ and y is a unit in $\mathfrak{r}$, so $(x) = (\pi^i) = \mathfrak{p}^i$. Thus every nonzero ideal of $\mathfrak{r}$ is of the form $\mathfrak{p}^i$ for some $i \in \mathbb{N}$. There are two possibilities:

(i) For all $a \in \mathbb{Z}^+$, $\mathfrak{p}^a \neq 0$. Then $\mathfrak{r}$ is a discrete valuation ring (DVR).
(ii) There is a positive integer v, the **length** of $\mathfrak{r}$, such that $\mathfrak{p}^{v-1} \neq (0)$ and $\mathfrak{p}^v = (0)$.

If $\mathfrak{r}$ is moreover finite then (ii) must hold. Thus in any (nonzero) finite principal local ring $(\mathfrak{r},\mathfrak{p})$ there is a positive integer v such that the ideals of $\mathfrak{r}$ are

$$\mathfrak{r} = \mathfrak{p}^0 \supsetneq \mathfrak{p} \supsetneq \mathfrak{p}^1 \supsetneq \ldots \supsetneq \mathfrak{p}^v = (0).$$

Theorem 1.6. *Let $(\mathfrak{r},\mathfrak{p})$ be a finite local principal ring of length v and with residue field $\mathbb{F}_q$. Let $n, r \in \mathbb{Z}^+$, and for $1 \leq j \leq r$, let $1 \leq v_j \leq v$. Let $\mathfrak{a}_1,\ldots,\mathfrak{a}_n,\mathfrak{b}_1,\ldots,\mathfrak{b}_r \subset \mathfrak{r}$ be nonempty subsets each having the property that no two distinct elements are congruent modulo $\mathfrak{p}$. Let $f_1,\ldots,f_r \in \mathfrak{r}[\mathbf{t}] = \mathfrak{r}[t_1,\ldots,t_n]$. Put*

$$\mathfrak{z}_{\mathfrak{a},\mathfrak{b}} := \{x \in \prod_{i=1}^{n} \mathfrak{a}_i \mid \forall 1 \leq j \leq r,\ f_j(x) \in \mathfrak{b}_j \pmod{\mathfrak{p}^{v_j}}\}.$$

Then $\mathfrak{z}_{\mathfrak{a},\mathfrak{b}} = \varnothing$ or

$$\# \mathfrak{z}_{\mathfrak{a},\mathfrak{b}} \geq \mathfrak{m}\left(\#\mathfrak{a}_1,\ldots,\#\mathfrak{a}_n; \sum_{i=1}^{n} \#\mathfrak{a}_i - \sum_{j=1}^{r} (q^{v_j} - \#\mathfrak{b}_j) \deg f_j \right).$$

Consider the following variant of Theorem 1.6.

Theorem 1.7. *Let R be a domain, and let $\mathfrak{p}$ be a maximal ideal of R with finite residue field $R/\mathfrak{p} \cong \mathbb{F}_q$ and such that the localization $R_{\mathfrak{p}}$ is a DVR.*[1] *Let $n, r, v_1, \ldots, v_r \in \mathbb{Z}^+$. Let $A_1, \ldots, A_n, B_1, \ldots, B_r \subset R$ be nonempty subsets each having the property that no two distinct elements are congruent modulo $\mathfrak{p}$. Let $r, v_1, \ldots, v_r \in \mathbb{Z}^+$. Let $f_1, \ldots, f_r \in R[\mathbf{t}] = R[t_1, \ldots, t_n]$. Put*

$$Z_{\mathbf{A}}^{\mathbf{B}} := \left\{ x \in \prod_{i=1}^n A_i \mid \forall 1 \leq j \leq r, f_j(x) \in B_j \pmod{\mathfrak{p}^{v_j}} \right\}.$$

Then $\# Z_{\mathbf{A}}^{\mathbf{B}} = 0$ or

$$\# Z_{\mathbf{A}}^{\mathbf{B}} \geq \mathfrak{m}\left(\# A_1, \ldots, \# A_n; \sum_{i=1}^n \# A_i - \sum_{j=1}^r (q^{v_j} - \# B_j) \deg(f_j) \right).$$

Proposition 1.8. *Theorems 1.6 and 1.7 are equivalent.*

Proof. Theorem 1.6 $\Longrightarrow$ Theorem 1.7: let $\mathfrak{r} = R/\mathfrak{p}^v$ and let $q : R \to \mathfrak{r}$ be the quotient map. For $1 \leq i \leq n$, let $\mathfrak{a}_i = q(A_i)$; for $1 \leq j \leq r$, let $\overline{f_j} = q(f_j)$ and $\mathfrak{b}_j = q(B_j)$. Then $\deg \overline{f_j} \leq \deg f_j$. The hypothesis that no two distinct elements of any one of these sets are congruent modulo $\mathfrak{p}$ ensures $\# \mathfrak{a}_i = \# A_i$ and $\# \mathfrak{b}_j = \# B_j$. Applying Theorem 1.6 to $\mathfrak{r}$,$\mathfrak{a}_1, \ldots, \mathfrak{a}_n, \mathfrak{b}_1, \ldots, \mathfrak{b}_r$,$v_1, \ldots, v_r$,$\overline{f_1}, \ldots, \overline{f_r}$ gives

$$\# Z_{\mathbf{A}}^{\mathbf{B}} = \# \mathfrak{z}_{\mathfrak{a},\mathfrak{b}} \geq \mathfrak{m}\left(\# \mathfrak{a}_1, \ldots, \# \mathfrak{a}_n; \sum_{i=1}^n \# \mathfrak{a}_i - \sum_{j=1}^r (q^{v_j} - \# \mathfrak{b}_j) \deg(\overline{f_j}) \right)$$
$$\geq \mathfrak{m}\left(\# A_1, \ldots, \# A_n; \sum_{i=1}^n \# A_i - \sum_{j=1}^r (q^{v_j} - \# B_j) \deg(f_j) \right).$$

Theorem 1.7 $\Longrightarrow$ Theorem 1.6: by [Hu68, Cor. 11], there is a principal ideal domain R and a maximal ideal $\mathfrak{p}$ in R such that $R/\mathfrak{p}^v \cong \mathfrak{r}$. Thus the pair $(R, \mathfrak{p})$ satisifes the hypotheses of Theorem 1.7. We may lift $A_1, \ldots, A_n$, $B_1, \ldots, B_r$, $f_1, \ldots, f_r$ from $\mathfrak{r}$ to R so as to preserve the sizes of the sets and the degrees of the polynomials. Apply Theorem 1.7. □

Example 1.9. *Let $\mathfrak{r}$ be a finite ring, and let $A \subset \mathfrak{r}$ satisfy Condition (D). For $1 \leq j \leq r$, let $f_j \in \mathfrak{r}[t_1]$ be a univariate polynomial of degree $d_j \geq 0$, and let $B_1, \ldots, B_r \subset \mathfrak{r}$ be finite and nonempty. Put*

$$\mathfrak{z}_A^{\mathbf{B}} := \{x \in A \mid f_1(x) \in B_1, \ldots, f_r(x) \in B_r\}.$$

Suppose first that $d_j \geq 1$ for all j. Then for each $y \in \mathfrak{r}$, the polynomial $f_j - y$ also has degree d_j, and because A satisfies Condition (D), there are at most $\deg(f_j)$ *elements of A such that $f_j(x) = y$. So there are at most* $(\# \mathfrak{r} - \# B_j)(\deg f_j)$ *elements $x \in A$ such that $f_j(x) \notin B_j$ and thus*

$$\# \mathfrak{z}_A^{\mathbf{B}} \geq \# A - \sum_{j=1}^r (\# \mathfrak{r} - \# B_j)(\deg f_j).$$

[1] The latter condition holds for all maximal ideals when R is a Dedekind domain and for all maximal divisorial ideals when R is a Krull domain [GHK, Thm. 2.3.11].

Now suppose that some f_j is constant. Then: if the constant value lies in B_j then $f_j(A) \subset B_j$, whereas if the constant value does not lie in B_j then $\mathfrak{z}_A^{\mathbf{B}} = \varnothing$.

This establishes a stronger result than Theorem 1.6 when $n = 1$. In particular: the finite ring $\mathfrak{r}$ need not be local and principal, the target sets $B_1, \ldots, B_r$ may be arbitrary nonempty subsets, and we do not need to separately allow $\mathfrak{z}_{\mathbf{A}}^B = \varnothing$ if each polynomial has positive degree.

1.4. **Comparison With Theorem 1.2.**

Theorem 1.2 is the special case of Theorem 1.7 obtained by taking $R = \mathbb{Z}_K$ and $B_j = \{0\}$ for all j. So on the face of it Theorem 1.7 is a twofold generalization of Theorem 1.2: in place of $(\mathbb{Z}_K, \mathfrak{p})$ we may take any pair $(R, \mathfrak{p})$ with R a domain and $\mathfrak{p}$ a maximal ideal of R such that $R/\mathfrak{p}$ is finite; and in place of polynomial congruences we are studying polynomial systems with **relaxed output sets** B_j.

However, the first generalization turns out not to be an essential one. Indeed, Theorem 1.6 shows that the result can be phrased in terms of finite, local principal rings. But every finite local principal ring is isomorphic to $\mathbb{Z}_K/\mathfrak{p}^v$ for some prime ideal $\mathfrak{p}$ in the ring of integers $\mathbb{Z}_K$ of a number field K [Ne71], [BC15, Thm. 1.12].

Example 1.10. *Consider $\mathfrak{r} = \mathbb{F}_p[t]/(t^2)$: it is a finite, local principal ring with residue cardinality p and length 2. Further, it is a commutative $\mathbb{F}_p$-algebra of dimension 2 that is not reduced (i.e., it has nonzero nilpotent elements), and these properties characterize $\mathfrak{r}$ up to isomorphism. So let $K = \mathbb{Q}(\sqrt{p})$ and let $\mathfrak{p}$ be the unique prime ideal of $\mathbb{Z}_K$ dividing p. The ring $\mathbb{Z}_K/p\mathbb{Z}_K = \mathbb{Z}_K/\mathfrak{p}^2$ is also a nonreduced $\mathbb{F}_p$-algebra of dimension 2, so $\mathfrak{r} = \mathbb{F}_p[t]/(t^2) \cong \mathbb{Z}_K/\mathfrak{p}^2$.*

Nevertheless it is natural to think in terms of domains, and the reduction to the ring of integers of a number field seems artificial. The proof of Theorem 1.2 used the fact that $\mathbb{Z}_K$ has characteristic zero in an essential way: a key technical tool was the use of **Schanuel-Brink operators** to replace a congruence modulo $\mathfrak{p}^v$ in $\mathbb{Z}_K$ with a system of congruences modulo $\mathfrak{p}$. As Schanuel pointed out, this construction is morally about **Witt vectors** and thus particular to unequal characteristic. Our proof of Theorem 1.7 does not reduce to the number field case but works directly in any Dedekind domain. Applied to $R = \mathbb{Z}_K$ with $B_j = \{0\}$ for all j, it gives a *new proof* of Theorem 1.2. This new approach feels more transparent and more fundamental, and we hope that it will be more amenable to further generalization.

1.5. **Applications of the Main Theorem.**

The generalization from polynomial congruences to polynomial congruences with relaxed outputs enables a wide range of applications. As in [CFS14], whenever one has a combinatorial existence theorem proved via the Schauz-Wilson-Brink Theorem (or an argument that can be viewed as a special case thereof) one can instead apply Theorem 1.2 to get a lower bound on the number of solutions. Moreover, most applications of Schauz-Wilson-Brink include a homogeneity condition ensuring the existence of a trivial solution. Theorem 1.2 applies also in the inhomogeneous case.

All of these applications can be generalized by allowing relaxed outputs. In [CFS14] we gave three combinatorial applications of Theorem 1.2: to hypergraphs, to generalizations of the Erdős-Ginzburg-Ziv Theorem, and to weighted Davenport constants. In the former two cases, we can (and shall) immediately apply the Main Theorem to get stronger results. We include the proof of the hypergraph theorem to showcase the use of nonlinear polynomials. We omit the proof of the EGZ-type theorem: the proof given in [CFS14] of the special case adapts immediately.

Our Main Theorem leads to a generalization of the weighted Davenport constant that we call the **relaxed weighted Davenport constant**. This constant may be of interest in its own right; moreover, it can be used to extend results of Alon-Friedland-Kalai on *divisible subgraphs*. This is a privileged application as the relaxed output aspect of the Main Theorem was inspired by [AFK84].

One reason that the combinatorial applications are interesting is that the upper bounds they give are – in the unweighted, zero-output case – accompanied by lower bounds coming from elementary combinatorial constructions, which has the effect of showing sharpness in Schanuel's Theorem in certain cases. It is an interesting challenge, not met here, to find other types of restricted input sets A_i and relaxed output sets B_j illustrating sharpness in our generalized theorems.

Finally, we give an application of the Main Theorem to "relaxed polynomial interpolation". As a special case we will deduce a generalization of a Theorem of Troi-Zannier [TZ97] which was proved by them via more combinatorial means.

1.6. **Acknowledgments.**

Thanks to Dino Lorenzini, Paul Pollack, Bob Rumely and Lori D. Watson for helpful discussions. Thanks to J.R. Schmitt for introducing me to this rich circle of ideas, for many helpful remarks, and for Example 3.2. I am grateful to the referee for an extraordinarily careful, detailed and informative report.

2. Proof of the Main Theorem

2.1. **A Generalized Alon-Friedman-Kalai Lemma.**

The following result is a generalization of [AFK84, Lemma A.3].

Lemma 2.1. *Let R be a DVR, with maximal ideal $\mathfrak{p} = (\pi)$ and finite residue field $\mathbb{F}_q$. Let $v \in \mathbb{Z}^+$, and let $\mathcal{S}(v)$ be a set of coset representatives for $\mathfrak{p}^v$ in R. Let $T \subset R$ satisfy Condition (F): no two distinct elements of T are congruent modulo $\mathfrak{p}$, and let $\overline{T}$ be the image of T in $R/\mathfrak{p}^v$. Let $x \in R$. Put*

$$\mathbf{P}(x, v, T) := \prod_{y \in \mathcal{S}(v) \setminus \overline{T}} (x - y)$$

and

$$c(v) := \sum_{i=1}^{v-1} \left(q^i - 1\right).$$

Then we have:

$$\operatorname{ord}_{\mathfrak{p}} \mathbf{P}(x, v, T) \geq c(v), \tag{2}$$

$$\operatorname{ord}_{\mathfrak{p}} \mathbf{P}(x, v, T) = c(v) \iff \text{there is } y \in \overline{T} \text{ such that } \operatorname{ord}_{\mathfrak{p}}(x - y) \geq v. \tag{3}$$

Proof. Put $\mathbf{P}_0 = \prod_{y \in \mathcal{S}(v) \setminus \{\mathfrak{p}^v\}} y$.
Step 1: Suppose $\overline{T} = \{y_0\}$ and $\operatorname{ord}_{\mathfrak{p}}(x - y_0) \geq v$. If y runs through $\mathcal{S}(v) \setminus \overline{T}$, then $x - y$ runs through a set of representatives of the nonzero cosets of $\mathfrak{p}^v$ in R, and since if $x \equiv y \not\equiv 0 \pmod{\mathfrak{p}^v}$ then $\operatorname{ord}_{\mathfrak{p}} x = \operatorname{ord}_{\mathfrak{p}} y$, we have

$$\operatorname{ord}_{\mathfrak{p}} \mathbf{P}(x, v, T) = \operatorname{ord}_{\mathfrak{p}} \mathbf{P}_0$$

$$= \sum_{i=0}^{v-1} i \cdot (\#\{x \in (\mathfrak{p}^i \cap \mathcal{S}(v)) \setminus (\mathfrak{p}^{i+1} \cap \mathcal{S}(v))\}) = \sum_{i=0}^{v-1} i \cdot (q^{v-i} - q^{v-i-1})$$

$$= (q^{v-1} - q^{v-2}) + 2(q^{v-2} - q^{v-3}) + 3(q^{v-3} - q^{v-4}) + \ldots + (v-1)(q-1)$$

$$= (q^{v-1} + q^{v-2} + \ldots + 1) - (v-1) = \sum_{i=1}^{v-1} (q^i - 1) = c(v).$$

Step 2: Suppose $\overline{T} = \{y_0\}$ and $\operatorname{ord}_{\mathfrak{p}}(x - y_0) < v$. Then there is a unique $y_1 \in \mathcal{S}(v)$ with $x \equiv y_1 \pmod{\mathfrak{p}^v}$, and $y_1 \neq y_0$. Then we have $\mathbf{P}(x, v, T) = \mathbf{P}_0 \left(\frac{x - y_1}{x - y_0} \right)$, so

$$\operatorname{ord}_{\mathfrak{p}} \mathbf{P}(x, v, T) = c(v) + \operatorname{ord}_{\mathfrak{p}}(x - y_1) - \operatorname{ord}_{\mathfrak{p}}(x - y_0) > c(v).$$

Step 3: Suppose $\#\overline{T} > 1$. Then $\mathbf{P}(x, v, T)$ is obtained from omitting factors from a product considered in Step 1 or Step 2. Because no two elements of T are congruent modulo $\mathfrak{p}$, the number of $y \in \overline{T}$ such that $\operatorname{ord}_{\mathfrak{p}}(x - y) \geq 1$ is either 0 or 1, and thus $\mathbf{P}(x, v, T)$ can be obtained from the product in Step 1 or Step 2 by omitting only factors of zero $\mathfrak{p}$-adic valuation. So $\operatorname{ord}_{\mathfrak{p}} \mathbf{P}(x, v, T) \geq c(v)$, and strict inequality holds precisely when there is some $y \in \mathcal{S}(v) \setminus \overline{T}$ with $\operatorname{ord}_{\mathfrak{p}}(x - y) \geq v$. □

2.2. **Alon-Füredi Over a Ring.**

The aim of this section is to prove the following result.

Theorem 2.2. *(Alon-Füredi Over a Ring) Let R be a ring, and let $A_1, \ldots, A_n \subset R$ satisfying Condition (D). Put $\mathbf{A} = \prod_{i=1}^n A_i$ and $a_i = \#A_i$ for all $1 \leq i \leq n$. Let $f \in R[\mathbf{t}] = R[t_1, \ldots, t_n]$. Put*

$$\mathcal{U}_{\mathbf{A}} := \{x \in A \mid f(x) \neq 0\} \text{ and } \mathfrak{u}_A := \#\mathcal{U}_{\mathbf{A}}.$$

Then either $\mathfrak{u}_{\mathbf{A}} = 0$ or $\mathfrak{u}_{\mathbf{A}} \geq \mathfrak{m}(a_1, \ldots, a_n; a_1 + \ldots + a_n - \deg f)$.

When R is a field, this is the Alon-Füredi Theorem [AF93, Thm. 4]. The key observation that the Combinatorial Nullstellensatz works over an arbitrary ring provided we impose Condition (D) is due to Schauz [Sc08]. It was further developed in [Cl14, §3]. The relevance of Condition (D) is shown in the following result.

Theorem 2.3. *(**CATS Lemma** [Cl14, Thm. 12]) Let R be a ring. For $1 \leq i \leq n$, let $A_i \subset R$ be nonempty and finite. Put $\mathbf{A} = \prod_{i=1}^r A_i$. For $1 \leq i \leq n$, let $\varphi_i = \prod_{a_i \in A_i} (t_i - a_i)$.*
a) (Schauz [Sc08]) The following are equivalent:
(i) For all $1 \leq i \leq n$, the set A_i satisfies condition (D).
(ii) For all $f \in R[\mathbf{t}] = R[t_1, \ldots, t_n]$, if $\deg_{t_i} f < \#A_i$ for all $1 \leq i \leq n$ and $f(a) = 0$ for all $a \in \prod_{i=1}^n A_i$, then $f = 0$.
(iii) If $f|_{\mathbf{A}} \equiv 0$, there are $g_1, \ldots, g_n \in R[t_1, \ldots, t_n]$ such that $f = \sum_{i=1}^n g_i \varphi_i$.
b) (Chevalley-Alon-Tarsi) The above conditions hold when R is a domain.

With Theorem 2.3 in hand, Theorem 2.2 can be established following the original argument of [AF93]. However, I find this argument a bit mysterious. Theorem 2.2 is the backbone of this work and a key barrier to further generalizations of Theorem 1.7. Because of this I feel the need to give the most conceptually transparent argument possible. For this we adapt a proof of Alon-Füredi due to Ball and Serra.

Proof. Step 1: We establish a variant of the Punctured Combinatorial Nullstellensatz of Ball-Serra [BS09, Thm. 4.1].[2] Let R be a ring, let $A_1, \ldots, A_n \subset R$ satisfying Condition (D), and for $1 \leq i \leq n$ let $\varnothing \neq Y_i \subset A_i$. Put

$$\mathbf{A} \coloneqq \prod_{i=1}^{n} A_i \text{ and } \mathbf{Y} \coloneqq \prod_{i=1}^{n} Y_i.$$

For $1 \leq i \leq n$, put

$$\varphi_i(t) = \prod_{a_i \in A_i} (t_i - a_i), \ \psi_i(t) = \prod_{y_i \in Y_i} (t_i - y_i).$$

Let $f \in R[\mathbf{t}] = R[t_1, \ldots, t_n]$. Suppose that for all $x \in \mathbf{A} \setminus \mathbf{Y}$, $f(x) = 0$. Then WE CLAIM there are $g_1, \ldots, g_n, u \in R[\mathbf{t}]$ such that

$$f = \sum_{i=1}^{n} g_i \varphi_i + u \prod_{i=1}^{n} \frac{\varphi_i}{\psi_i}, \ \deg u \leq \deg f - \sum_{i=1}^{n} (\# A_i - \# Y_i).$$

PROOF OF CLAIM: We perform polynomial division on f by the monic polynomial φ_1, then divide the remainder by the monic polynomial φ_2, and so forth, finally dividing by φ_n to get $f = \sum_{i=1}^{n} g_i \varphi_i + r$. By [Cl14, §3.1], we have $\deg r \leq \deg f$ and $\deg_{t_i} r < \deg \varphi_i$ for all i. Dividing $r\psi_1$ by φ_1 we get

$$r\psi_1 = r_1 \varphi_1 + s_1.$$

Then

$$\deg_{t_1} s_1 < \deg \varphi_1$$

whereas for all $i \neq 1$,

$$\deg_{t_i} s_1 \leq \deg_{t_i} r\psi_1 = \deg_{t_i} r < \deg \varphi_i.$$

Since s_1 vanishes identically on $\mathbf{A}$ and $\mathbf{A}$ satisfies Condition (D), Theorem 2.3 applies to show $s_1 = 0$: that is, we may write $r = \frac{\varphi_1}{\psi_1} r_1$. Continuing this process with respect to $t_2, \ldots, t_n$, we get $r = \prod_{i=1}^{n} \frac{\varphi_i}{\psi_i} u$ with

$$\deg u \leq \deg r - \sum_{i=1}^{n} (\deg(\varphi_i) - \deg(\psi_i)) \leq \deg f - \sum_{i=1}^{n} (\# A_i - \# Y_i).$$

Step 2: Put $A = \prod_{i=1}^{n} A_i$, and let $f \in R[t_1, \ldots, t_n]$. We may assume that f does not vanish identically on $\mathbf{A}$. We go by induction on n. The base case $n = 1$ follows from Theorem 2.3. Suppose $n \geq 2$ and the result holds for $n - 1$. Define

$$Y_i \coloneqq \begin{cases} A_i, & 1 \leq i \leq n-1 \\ \{y \in A_n \mid f(t_1, \ldots, t_{n-1}, y) \neq 0\} & i = n \end{cases}.$$

[2] The result established here is obtained from the Punctured Combinatorial Nullstellensatz by (i) working over an arbitrary ring under Condition (D) and (ii) neglecting multiplicities.

By our hypothesis on f, $Y_n \neq \varnothing$. Let $y \in Y_n$. We apply Step 1 to f, getting

$$f = \sum_{i=1}^{n} g_i \varphi_i + u \frac{\varphi_n}{\psi_n}$$

and put $w(t_1, \ldots, t_{n-1}) = u(t_1, \ldots, t_{n-1}, y)$. Then

$$\deg w \leq \deg u \leq \deg f - \#A_n + \#Y_n,$$

and for all $x' = (x_1, \ldots, x_{n-1}) \in \prod_{i=1}^{n-1} A_i$, we have $f(x', y) = 0 \iff w(x') = 0$. By induction there are $a_1, \ldots, a_{n-1} \in \mathbb{Z}^+$ with $1 \leq a_i \leq \#A_i$ for all i and

$$\sum_{i=1}^{n-1} a_i = \left(\sum_{i=1}^{n-1} \#A_i \right) - \deg w \geq \left(\sum_{i=1}^{n-1} \#A_i \right) - \deg u$$

such that w is nonvanishing at at least $\prod_{i=1}^{n-1} a_i$ points of $\prod_{i=1}^{n-1} A_i$. The $a_1, \ldots, a_{n-1}$ depend on y, but if we choose $a_1, \ldots, a_{n-1}$ so as to minimize $\prod_{i=1}^{n-1} a_i$, then we find $(\prod_{i=1}^{n-1} a_i)(\#Y_n)$ points of X at which f is nonvanishing, hence

$$\mathcal{U}_{\mathbf{A}} \geq \mathfrak{m}(\#A_1, \ldots, \#A_n; \sum_{i=1}^{n-1} a_i + \#Y_n).$$

Since

$$\sum_{i=1}^{n-1} a_i + \#Y_n \geq (\sum_{i=1}^{n-1} \#A_i) - \deg u + (\deg u + \#A_n - \deg f) = \sum_{i=1}^{n} \#A_i - \deg f,$$

we have $\mathcal{U}_{\mathbf{A}} \geq \mathfrak{m}(\#A_1, \ldots, \#A_n; \sum_{i=1}^{n} \#A_i - \deg f)$. □

Remark 2.4. *Theorem 2.2 is* sharp *in the following sense: let R be a ring, $A_1, \ldots, A_n \subset R$ satisfying Condition (D), and put $\mathbf{A} = \prod_{i=1}^{n} A_i$. Let $d \in \mathbb{Z}^+$. There is a degree d polynomial $f \in R[t_1, \ldots, t_n]$ which is nonzero at precisely $\mathfrak{m}(\#A_1, \ldots, \#A_n; \sum_{i=1}^{n} \#A_i - d)$ points of $\mathbf{A}$. In fact something stronger holds: let $y = (y_1, \ldots, y_n) \in \mathbb{Z}^n$ with $1 \leq y_i < \#A_i$ for all i. For $1 \leq i \leq n$, choose $Y_i \subset A_i$ with $\#Y_i = y_i$, and put $f = \prod_{i=1}^{n} \prod_{x \in Y_i} (t_i - x)$. Then $\deg f = \sum_{i=1}^{n} y_i$ and f is nonvanishing precisely on $\prod_{i=1}^{n} (A_i \setminus Y_i)$, a subset of size $\prod_{i=1}^{n} (\#A_i - y_i)$.*

Remark 2.5. *Both of the main results of* [BS09] *– namely Theorems 3.1 and 4.1 – can be generalized by replacing the arbitrary field $\mathbb{F}$ by an arbitrary ring R under the assumption that the sets satisfy Condition (D). In the former case the argument adapts immediately; in the latter case it requires some mild modifications.*

2.3. **Proof of the Main Theorem.**

Proof. We will prove Theorem 1.7. We may assume R is a DVR, and thus our assumption on $A_1, \ldots, A_n, B_1, \ldots, B_r$ becomes Condition (F). Let $\mathbf{A} = \prod_{i=1}^{n} A_i$. For $1 \leq j \leq r$, let $\overline{B_j}$ be the image of B_j in $R/\mathfrak{p}^{v_j}$. For $a \in \mathbb{Z}^+$, let $\mathcal{S}(a)$ be a set of coset representatives for $\mathfrak{p}^a$ in R. Put

$$Q(\mathbf{t}) := \prod_{j=1}^{r} \prod_{y \in \mathcal{S}(v_j) \setminus \overline{B_j}} (f_j(t) - y) \in R[\mathbf{t}].$$

For $1 \leq j \leq s$ put

$$c_j := \sum_{i=1}^{v_j - 1} (q^i - 1),$$

and put

$$c := \sum_{j=1}^{r} c_j.$$

Let $\overline{R} = R/\mathfrak{p}^{c+1}$. Let $\overline{Q}$ be the image of Q in $\overline{R}$ and $\overline{\mathbf{A}}$ the image of $\mathbf{A}$ in $\overline{R}^n$. Then

$$\deg \overline{Q} \leq \deg Q = \sum_{j=1}^{r} (q^{v_j} - \#B_j) \deg f_j.$$

Because of Condition (F), the natural map $\mathbf{A} \mapsto \overline{\mathbf{A}}$ is a bijection. Let

$$\mathcal{U} = \{\overline{x} \in \overline{\mathbf{A}} \mid \overline{Q}(\overline{x}) \neq 0\}.$$

Let $\overline{x} \in \overline{\mathbf{A}}$. Using Lemma (2.1), we get

$$\overline{x} \in \mathcal{U} \iff \overline{Q}(\overline{x}) \neq 0$$

$$\iff \operatorname{ord}_{\mathfrak{p}}(Q(x)) \leq c \overset{(2)}{\iff} \forall 1 \leq j \leq r,\ \operatorname{ord}_{\mathfrak{p}} \prod_{y \in \mathcal{S}(v) \setminus \overline{B_j}} (f_j(x) - y) \leq c_j$$

$$\overset{(3)}{\iff} \forall 1 \leq j \leq r, \exists b_j \in \overline{B_j} \text{ such that } \operatorname{ord}_{\mathfrak{p}}(f_j(x) - b_j) \geq v_j$$

$$\iff x \in Z_{\mathbf{A}}^{\mathbf{B}}.$$

Thus $\#\mathcal{U} = \mathbf{z}_{\mathbf{A}}^{\mathbf{B}}$. Applying Theorem 2.2 to $\overline{R}$, $\overline{Q}$ and $\overline{A}$, we get: $\#Z_{\mathbf{A}}^{\mathbf{B}} = 0$ or

$$\#Z_{\mathbf{A}}^{\mathbf{B}} \geq \mathfrak{m}(\#A_1, \ldots, \#A_n; \sum_{i=1}^{n} \#A_i - \deg \overline{Q})$$

$$\geq \mathfrak{m}(\#A_1, \ldots, \#A_n; \sum_{i=1}^{n} \#A_i - \sum_{j=1}^{r} (q^{v_j} - \#B_j) \deg(f_j)). \qquad \square$$

3. Applications

3.1. Hypergraphs.

A **hypergraph** 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 $\max_{x \in X} \#\{1 \leq i \leq n \mid x \in \mathcal{F}_i\}$. For $m \in \mathbb{Z}^+$ and $\varnothing \neq B \subset \mathbb{Z}$, put

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

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

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

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

$$f_d(m) = \min\{n \in \mathbb{Z}^+ \mid \mathcal{N}_{n,d}(m) \geq 2\}. \tag{4}$$

Theorem 3.1. *Let p be a prime number, and let $\varnothing \subset B \subset \mathbb{Z}$ be a subset, no two distinct elements of which are congruent modulo p. Let $d, n \in \mathbb{Z}^+$, and let $\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_n)$ be a hypergraph of maximal degree at most d. Then:*
a) $\mathcal{N}_{\mathcal{F}}(p^v, B)$ is either 0 or at least $2^{n-d(p^v - \#B)}$.
b) If $0 \in B$ and $n > d(p^v - \#B)$, then there is $\varnothing \neq J \subset \{1, \ldots, n\}$ such that $p^v \mid \# \bigcup_{i \in J} \mathcal{F}_i$.

Proof. Put

$$h(\mathbf{t}) \coloneqq \sum_{\varnothing \neq J \subset \{1,\ldots,n\}} (-1)^{\#J+1} (\# \bigcap_{j \in J} \mathcal{F}_i) \prod_{j \in J} t_j.$$

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

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

so $\mathcal{N}_{\mathcal{F}}(p^v, B) = \{x \in \{0,1\}^n \mid h(x) \in B \pmod{p^v}\}$. Applying Theorem 1.5a) establishes part a), and applying Theorem 1.5b) establishes part b). □

When $B = \{0\}$, Theorem 3.1a) is [CFS14, Thm. 4.8]a) and Theorem 3.1b) gives the upper bound in a result of Alon-Kleitman-Lipton-Meshulam-Rabin-Spencer [AKLMRS, Thm. 1]. They also showed that $f_d(m) \geq d(m-1) + 1$, so Theorem 3.1b) is sharp when $\#B = 1$. The following example extends this construction and implies that Theorem 3.1b) is sharp for all $d, \#B \in \mathbb{Z}^+$.

Example 3.2. *(J.R. Schmitt) Let $b, d \in \mathbb{Z}^+$. Choose $m, a \in \mathbb{Z}^+$ with $m > b$ and $\gcd(a, m) = 1$. Let $\{A_{i,j}\}_{1 \leq i \leq m-b,\ 1 \leq j \leq d}$ be pairwise disjoint sets, each of cardinality m. Let $\{V_i\}_{1 \leq i \leq m-b}$ be disjoint sets, each of cardinality a and disjoint from all the A_{ij}. Put*

$$B = \{m, m-a, m-2a, \ldots, m-(b-1)a\} \subset \mathbb{Z}/m\mathbb{Z},$$

and consider the hypergraph

$$\mathcal{F} = \{A_{ij} \cup V_i\}_{1 \leq i \leq m-b, 1 \leq j \leq d}.$$

Then $\mathcal{F}$ has length $d(m-b)$ but $\# \bigcup_{F \in \mathcal{F}_0} \notin B \pmod{m}$ for any $\emptyset \neq \mathcal{F}_0 \subset \mathcal{F}$.

3.2. **Relaxed Weighted Davenport Constants.**

Let $(G, +)$ be a nontrivial finite commutative group. The **Davenport constant** $D(G)$ is the least number n such that for any sequence $\{g_i\}_{i=1}^n$ in G, there is a nonempty subset $J \subset \{1, \ldots, n\}$ such that $\sum_{i \in J} g_i = 0$. There are unique integers $1 < n_1 \mid n_2 \ldots \mid n_r$ such that

$$G \cong \bigoplus_{i=1}^r \mathbb{Z}/n_i\mathbb{Z};$$

let us call r the **rank** of G. The pigeonhole principle implies

$$D(G) \leq \#G.$$

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

$$D(G) \geq 1 + \sum_{i=1}^{r} (n_i - 1) =: D^*(G), \tag{5}$$

as observed by van Emde Boas and D. Kruyswijk [EBK69, Thm. 5]. For surveys of classical work on the Davenport constant, see [GHK, Ch. 5] and [GG06]. For our purposes the most important result is the equality $D(G) = D^*(G)$ when G is a p-group [EBK69], [O69a]. In fact, as first observed by Schanuel [Sc74], for a p-group G the Davenport constant can be expressed in terms of systems of congruences modulo powers of p with solutions in $A_i = \{0, 1\}$. (We will shortly encounter a generalization of this.)

Let G be a finite commutative group of exponent e, and let $\mathbf{A} = \{A_i\}_{i=1}^{\infty}$ be a sequence of finite, nonempty subsets of $\mathbb{Z}$. Then given a finite sequence $\mathbf{g} = \{g_i\}_{i=1}^{n}$ in G we may associate an **A-weighted subsequence** $\{a_i g_i\}_{i=1}^{n}$ by selecting $a_i \in A_i$ for $1 \leq i \leq n$. An $\mathbf{A}$-weighted subsequence is **empty** if $a_i = 0 \in A_i$ for each i.

When each A_i contains 0 and at least one other element, we define the **weighted Davenport constant** $D_{\mathbf{A}}(G)$ as the least n such that every sequence $\{g_i\}_{i=1}^{n}$ in G has a nonempty $\mathbf{A}$-weighted zero-sum subsequence: i.e., there are $a_1 \in A_1, \ldots, a_n \in A_n$, not all 0, such that $\sum_{i=1}^{n} a_i g_i = 0$. Let $\{g_i\}_{i=1}^{D(G)}$ be a sequence in G, and for each $1 \leq i \leq D(G)$, let $a_i \in A_i \setminus \{0\}$. By definition of $D(G)$, there is a nonempty subset $J \subset \{1, \ldots, D(G)\}$ such that $\sum_{i \in J} a_i g_i = 0$. For $1 \leq i \leq D(G)$, let

$$b_i := \begin{cases} a_i & i \in J \\ 0 & i \notin J \end{cases}.$$

Then $\{b_i g_i\}_{i=1}^{D(G)}$ is an $\mathbf{A}$-weighted zero-sum subsequence. Thus we have

$$D_{\mathbf{A}}(G) \leq D(G) \leq \#G.$$

Theorem 3.3. *(Troi-Zannier* [TZ97]*, Brink* [Br11]*) Let $G \cong \bigoplus_{i=1}^{r} \mathbb{Z}/p^{v_i}$ be a p-group of exponent p^v. Let $n \in \mathbb{Z}^+$, and let $\mathbf{A} = (A_1, \ldots, A_n)$ with each $A_i \subset \mathbb{Z}$ nonempty, containing* 0*, and such that no two distinct elements are congruent modulo p. If*

$$\sum_{i=1}^{n} (\#A_i - 1) > \sum_{j=1}^{r} (p^{v_i} - 1) = D^*(G) - 1,$$

every sequence of length n in G has a nonempty $\mathbf{A}$-weighted zero-sum subsequence.

Troi-Zannier's proof uses group ring methods. They remark on their inability to push through a Chevalley-Warning style proof in the general case; this is what Brink does using the Schauz-Wilson-Brink Theorem.

When $A_1 = \ldots = A_n = A$, we write $D_A(G)$ for $D_{(A_1,\ldots,A_n)}(G)$. This version of the weighted Davenport constant was introduced by Adhikari-Rath [AR06]. In this case, Theorem 3.3 becomes the upper bound

$$\text{For all } p\text{-groups } G,\ D_A(G) \leq \left\lceil \frac{D^*(G)}{\#A - 1} \right\rceil. \tag{6}$$

Thangadurai gives some evaluations of $D_A(G)$ when $G = \mathbb{Z}/p\mathbb{Z}$ using elementary methods [Th07, Thm. 2] and when $G = \bigoplus_{i=1}^r \mathbb{Z}/p\mathbb{Z}$ using (6) [Th07, Cor. 1.2]. For more information on a (not identical, but closely related) weighted Davenport constant, see [G, Ch. 14-16]. For a recent arithmetic interpretation of weighted Davenport constants, see [HK14].

Here is a further generalization of the Davenport constant. We give ourselves:
- A positive integer r.
- A finite group $G = \bigoplus_{i=1}^r \mathbb{Z}/n_i\mathbb{Z}$ with $1 < n_1 \mid \ldots \mid n_r$.
- A sequence $\mathbf{A} = \{A_i\}_{i=1}^\infty$ of nonempty finite subsets of $\mathbb{Z}$.
- A nonempty subset $B \subset G$.

We put

$$N_{\mathbf{A}}^B(\mathbf{g}) = \#\{a \in \prod_{i=1}^n A_i \mid \sum_{i=1}^n a_i g_i \in B\},$$

i.e., the number of $\mathbf{A}$-weighted subsequences of $\mathbf{g}$ with sum in B. For $b \in B$, we put $N_{\mathbf{A}}^b(\mathbf{g}) = N_{\mathbf{A}}^{\{b\}}(\mathbf{g})$.

Henceforth we suppose that each A_i and B contains 0 and that $\#A_i \geq 2$ for all i. We define the **relaxed weighted Davenport constant** $D_{\mathbf{A}}^B(G)$ as the least $n \in \mathbb{Z}^+$ such that every length n sequence in G has a nonzero $\mathbf{A}$-weighted subsequence with sum in B. We have

$$D_{\mathbf{A}}^B(G) \leq D_{\mathbf{A}}(G) \leq D(G).$$

We write $D^B(G)$ for $D_{\{0,1\}}^B$. It would be interesting to give upper bounds on $N^B(\mathbf{g})$ depending only on $\#B$ and n (the length of $\mathbf{g}$).

For a length n sequence $\mathbf{g} = \{g_i\}_{i=1}^n \in G$, let

$$\Sigma(\mathbf{g}) = \left\{ \sum_{i \in J} g_i \mid J \subset \{1, \ldots, n\} \right\} \subset G$$

be the set of all subsequence sums of $\mathbf{g}$.

For a general group G we have little insight into the quantity $D_{\mathbf{A}}^B(G)$, and we will content ourselves here with a few observations.

Theorem 3.4.
Let $(G, +)$ be a finite commutative group, and let $\mathbf{g} = \{g_i\}_{i=1}^n$ be a sequence in G.
a) ([Ol69b, Thm. 2]*) We have $N^0(\mathbf{g}) = \max\{1, 2^{n+1-D(G)}\}$.*
b) ([CCQWZ11, Thm. 2]*) For all $x \in \Sigma(\mathbf{g})$, we have $N^x(\mathbf{g}) \geq 2^{n+1-D(G)}$.*
c) ([CCQWZ11, Prop. 4]*) If for some $y \in G$ we have $N^y(\mathbf{g}) = 2^{n+1-D(G)}$, then $N^x(\mathbf{g}) \geq 2^{n+1-D(G)}$ for all $x \in G$.*

Corollary 3.5. *Let $\mathbf{g}$ be a sequence of length n in G, and let $\{0\} \subsetneq B \subset G$. Then:*
a) We have $N^B(\mathbf{g}) \geq (\#(\sum(\mathbf{g}) \cap B)) \cdot 2^{n+1-D(G)}$.
b) We have that $N^B(\mathbf{g})$ is 0 or is at least $2^{n+1-D(G)} + 1$.

Proof. a) By Theorem 3.4b), each $b \in B$ which occurs as a subsequential sum of $\mathbf{g}$ must occur at least $2^{n+1-D(G)}$ times.

b) We have $N^B(\mathbf{g}) = 0$ iff $\sum(\mathbf{g}) \cap B = \varnothing$. We may assume this is not the case: there is $y \in \sum(\mathbf{g}) \cap B$, and then part a) gives $N^B(\mathbf{g}) \geq 2^{n+1-D(G)}$. Certainly $N^B(\mathbf{g}) \geq N^y(\mathbf{g})$, and by Theorem 3.4c), if $N^y(\mathbf{g}) = 2^{n+1-D(G)}$, then

$$N^B(\mathbf{g}) \geq (\#B)2^{n+1-D(G)} > 2^{n+1-D(G)}. \qquad \square$$

Remark 3.6. *Suppose* $0 \in B$ *and* B *is a large subset of* G*. When* $\sum(\mathbf{g}) \cap B$ *is large, Corollary 3.5a) gives a good lower bound on* $N^B(\mathbf{g})$*. When* $\sum(\mathbf{g}) \cap B$ *is small, then there ought to be significantly more than* $2^{n+1-D(G)}$ *zero-sum subsequences.*

Remark 3.7. *If* B *is a subgroup of* G*, then* $D^B_{\mathbf{A}}(G) = D_{\mathbf{A}}(G/B)$*.*

However, when G is a p-group, our Main Theorem can be applied.

Theorem 3.8. *Let* p *be a prime; let* $1 \leq v_1 \leq \ldots \leq v_r$*, and let* $G = \bigoplus_{j=1}^r \mathbb{Z}/p^{v_j}\mathbb{Z}$*. Let* $\{A_i\}_{i=1}^\infty$ *be a sequence of subsets of* $\mathbb{Z}$*, and for* $1 \leq j \leq r$ *let* $B_j \subset \mathbb{Z}$*. Suppose each* A_i *and* B_j *is nonempty and has no two distinct elements congruent modulo* p*. Let* $B = \prod_{j=1}^r B_j$ *and let* $\overline{B}$ *be the image of* B *under the natural homomorphism* $\mathbb{Z}^r \to G$*. Let* $\mathbf{g} = \{g_i\}_{i=1}^n$ *be a sequence in* G*.*
a) The number of $\mathbf{A}$*-weighted subsequences of* $\mathbf{g}$ *with* $\sum_{i=1}^n a_i g_i \in \overline{B}$ *is either* 0 *or at least*

$$\mathfrak{m}\left(\#A_1, \ldots, \#A_n; \sum_{i=1}^n \#A_i - \sum_{j=1}^r (p^{v_j} - \#B_j)\right).$$

b) If 0 *lies in each* A_i *and* B_j*, then there is a nonempty* $\mathbf{A}$*-weighted subsequence of* $\mathbf{g}$ *with sum* $\sum_{i=1}^n a_i g_i \in \overline{B}$ *if*

$$\sum_{i=1}^n (\#A_i - 1) > \sum_{j=1}^r (p^{v_j} - \#B_j). \tag{7}$$

Proof. a) Let $\tilde{\mathbf{g}}$ be a length n sequence in $\mathbb{Z}^r$ that maps to $\mathbf{g}$ under the homomorphism $\mathbb{Z}^r \to G$. Write $\tilde{\mathbf{g}}_i = (\tilde{a}_1^{(i)}, \ldots, \tilde{a}_r^{(i)})$, and for all $1 \leq j \leq r$, put

$$f_j(\mathbf{t}) := \sum_{i=1}^n \tilde{a}_j^{(i)} t_i.$$

Now apply Theorem 1.4. b) Apply part a) and (1). □

Remark 3.9. *Taking* $B = \{0\}$ *gives* [CFS14, Thm. 4.6]*. The latter implies Corollary 3.3, which implies the result of van Emde Boas-Kruyswijk and Olson that* $D(G) = D^*(G)$ *for* p*-groups.*

The following result is the generalization of Theorem [CFS14, Thm. 4.11] obtained by applying the Main Theorem. The proof carries over immediately and is omitted.

Theorem 3.10. *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* $A_1, \ldots, A_n, B_1, \ldots, B_r$ *be subsets of* $\mathbb{Z}$*, each nonempty with distinct elements pairwise incongruent modulo* p *and with* $0 \in A_i$ *for all* i*. Put*

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

For $1 \leq i \leq r$, let $\overline{B_i}$ be the image of B under the natural map $\mathbb{Z} \to \mathbb{Z}/p^{v_i}\mathbb{Z}$. For $x \in G$, let $\operatorname{EGZ}_{A,k}(B)$ be the number of $(a_1, \ldots, a_n) \in A$ such that

$$a_1x_1 + \ldots + a_nx_n \in \prod_{j=1}^{r} \overline{B_j} \text{ and } p^k \mid \#\{1 \leq i \leq n \mid a_i \neq 0\}.$$

Then either $\operatorname{EGZ}_{A,k}(B) = 0$ or

$$\operatorname{EGZ}_{A,k}(B) \geq \mathfrak{m}(\#A_1, \ldots, \#A_n; \#A_1 + \ldots + \#A_n - \sum_{j=1}^{r}(p^{v_j} - \#B_j) - (a_M - 1)(p^k - 1)).$$

3.3. Divisible Subgraphs.

Here, a **graph** G is a relation $\sim$ – called *incidence* – between two finite sets $V(G)$ and $E(G)$ such that every $e \in E(G)$ is incident to exactly two elements of $V(G)$. If $\#V(G) = r$ we will identify $V(G)$ with $\{1, \ldots, r\}$. The degree of $x \in V(G)$ is $\#\{e \in E(G) \mid x \sim e\}$. A subgraph is induced by restricting the incidence relation to a subset $E' \subset E$. We say a graph is empty if $E = \varnothing$. For $q \in \mathbb{Z}^+$, a graph $\mathcal{G} = (V(\mathcal{G}), E(\mathcal{G}))$ is **q-divisible** if for all $x \in V(G)$, $q \mid \deg x$ [AFK84]. An empty graph is q-divisible for all q. We say a graph is **q-atomic** if it admits no nonempty q-divisible subgraph.

For $r \geq 2$ and $q \in \mathbb{Z}^+$, let $E(r, q)$ be the least $n \in \mathbb{Z}^+$ such that every graph with r vertices and n edges admits a nonempty q-divisible subgraph. We have $E(2, q) = q$ for all q; henceforth we suppose $r \geq 3$.

Theorem 3.11. ([AFK84]) *For $r \geq 3$ and $q \in \mathbb{Z}^+$, we put*

$$\mathcal{E}(r, q) := \begin{cases} (q-1)r + 1 & q \text{ odd} \\ (q-1)r - \frac{q}{2} + 1 & q \text{ even} \end{cases}.$$

a) We have $\mathcal{E}(r, q) \leq E(r, q)$.
b) We have $\mathcal{E}(r, q) = E(r, q)$ if q is a prime power.

The proof of part a) is by a simple direct construction of q-atomic graphs that we do not revisit here. The proof of part b) is by connection with the Davenport constant.[3] By making this connection explicit we can slightly sharpen their results.

Theorem 3.12. *For $r \geq 3$, $q \in \mathbb{Z}^+$, we put*

$$G(r, q) := \begin{cases} \bigoplus_{i=1}^{r} \mathbb{Z}/q\mathbb{Z} & q \text{ odd} \\ \bigoplus_{i=1}^{r-1} \mathbb{Z}/q\mathbb{Z} \oplus \mathbb{Z}/\frac{q}{2}\mathbb{Z} & q \text{ even} \end{cases}$$

and

$$D(r, q) := D(G(r, q)).$$

a) We have (cf. (5))

$$D^*(G(r, q)) = \mathcal{E}(r, q) \leq E(r, q) \leq D(r, q). \tag{8}$$

b) A graph with r vertices and n edges has at least $2^{n+1-D(r,q)}$ q-divisible subgraphs.
c) [AFK84, Thm. 3.5] *If q is a prime power, then $E(r, q) = \mathcal{E}(r, q)$ and a graph with r vertices and n edges has at least $2^{n+1-\mathcal{E}(r,q)}$ q-divisible subgraphs.*

[3] Essentially. The term "Davenport constant" does not appear in [AFK84].

Proof. a) The equality $D^*(G(r,q)) = \mathcal{E}(r,q)$ is immediate, and $\mathcal{E}(r,q) \leq E(r,q)$ is Theorem 3.11a). Let $\mathcal{G}$ be a graph with r vertices and n edges, and let

$$A := (a_j^{(i)})_{1 \leq i \leq n,\ 1 \leq j \leq r}$$

be its incidence matrix. Then

$$I \subset \{1, \ldots, n\} \mapsto x^I \in \{0,1\}^n,\ x_i^I = \begin{cases} 1 & i \in I \\ 0 & i \notin I \end{cases}$$

induces a bijection between the q-divisible subgraphs of $\mathcal{G}$ and the solutions $x \in \{0,1\}^n$ to the system of linear congruences

$$\forall 1 \leq j \leq r,\ \sum_{i=1}^n t_j a_j^{(i)} \equiv 0 \pmod q$$

and thus to zero-sum subsequences of $\mathbf{a} = \{a^{(i)}\}_{i=1}^n$ in $\bigoplus_{j=1}^r \mathbb{Z}/q\mathbb{Z}$. Thus

$$E(r,q) \leq D(\bigoplus_{j=1}^r \mathbb{Z}/q\mathbb{Z}).$$

When q is odd, $D(r,q) = D(G(r,q))$. When q is even, the fact that every edge is incident to precisely two vertices can be exploited to improve the bound:

$$\forall 1 \leq i \leq e,\ \sum_{j=1}^n a_j^{(i)} = 2 \equiv 0 \pmod 2. \tag{9}$$

In group-theoretic terms, (9) means that the terms of $\mathbf{a}$ lie in the subgroup

$$G' = \{(x_1, \ldots, x_n) \in \bigoplus_{i=1}^n \mathbb{Z}/q\mathbb{Z} \mid \sum_j x_j \equiv 0 \pmod 2\} \cong G(r,q).$$

Thus again we find $E(r,q) \leq D(r,q)$.
b) We have seen that q-divisible subgraphs correspond bijectively to zero-sum subsequences of a sequence $\mathbf{a}$ in a group isomorphic to $G(r,q)$. Apply Theorem 3.4b).
c) Since q is a prime power, $G(r,q)$ is a p-group and thus

$$D(G(r,q)) = D^*(G(r,q)) = \mathcal{E}(r,q).$$

The result now follows from parts a) and b). □

Remark 3.13. *Alon-Friedland-Kalai conjecture that $E(r,q) \leq (q-1)r + 1$ for all $q \in \mathbb{Z}^+$* [AFK84, Conj. 3.7]. *This would follow if $D^*(G) = D(G)$ for all direct sums of copies of one finite cyclic group (an important open problem in the area). When q is odd, this conjecture is equivalent to $E(r,q) = \mathcal{E}(r,q)$; when q is even it gives*

$$(q-1)r - \frac{q}{2} + 1 \leq E(r,q) \leq (q-1)r + 1.$$

Again $E(r,q) = \mathcal{E}(r,q)$ would follow from $D^*(G(r,q)) = D(G(r,q))$. To the best of my knowledge, whether this equality holds for all even q is also open.

Remark 3.14. *We have allowed graphs with multiple edges, and in fact the graphs used in the proof of Theorem 3.11a) have multiple edges. We have not allowed loops, but we could have, as we now discuss. There are two possible conventions on how loops contribute to the incidence matrix (equivalently, the degree of a vertex).*

- *If we take the **topologist's convention** that placing a loop at a vertex increases its degree by 2, then Theorem 3.12 holds verbatim for graphs with loops.*

• *If we take the* ***algebraist's convention*** *that placing a loop at a vertex increases its degree by* 1*, then the parity phenomenon of (9) is lost, and for even q as well as odd we get $E(r,q) \leq D(\bigoplus_{i=1}^r \mathbb{Z}/q\mathbb{Z})$. In this case, the graph with $q-1$ loops placed at every vertex is q-atomic and shows*

$$D^*(\bigoplus_{i=1}^r \mathbb{Z}/q\mathbb{Z}) = (q-1)r + 1 \leq E(r,q).$$

When q is a prime power we get $E(r,q) = (q-1)r+1$ whether q is even or odd.

The connection with Davenport constants motivates us to explore a more general graph-theoretic setup. We first present a generalization which gives a graph-theoretic interpretation to the Davenport constant of any finite commutative group. The proofs are quite similar to those given above and are left to the reader.

Let $\mathbf{q} = (q_1, \ldots, q_r) \in (\mathbb{Z}^+)^r$ with $1 < q_1 \mid q_2 \mid \ldots q_r$ and put

$$G(\mathbf{q}) = \bigoplus_{i=1}^r \mathbb{Z}/q_i\mathbb{Z}.$$

When q_1 is even, there is a surjective group homomorphism

$$\Phi : G(\mathbf{q}) \to \mathbb{Z}/2\mathbb{Z},\ (x^{(1)}, \ldots, x^{(r)}) \mapsto \sum_{j=1}^r x^{(j)} \pmod 2.$$

Thus $G'(\mathbf{q}) := \operatorname{Ker} \Phi$ is an index 2 subgroup of $G(\mathbf{q})$. In this case we set $\mathbf{q}' = (\frac{q_1}{2}, q_2, \ldots, q_r)$.

Lemma 3.15. *If q_1 is even, then*

$$G'(\mathbf{q}) \cong G(\mathbf{q}').$$

If q_1 is odd, we put $G'(\mathbf{q}) = G(\mathbf{q})$.

Let $\mathcal{G} = (V,E)$ be a finite graph with $V = \{1, \ldots, r\}$. A subgraph $\mathcal{G}' = (V, E')$ is **q-divisible** if for all $1 \leq j \leq r$, $q_j \mid \deg j$. More generally, for $g = (g^{(j)})_{j=1}^r \in G(\mathbf{q})$, a subgraph $\mathcal{G}'$ is **of type** $(\mathbf{q}, g)$ if for all $1 \leq j \leq r$ we have

$$\deg j \equiv g^{(j)} \pmod{q_j}.$$

We then get the following generalization of Theorem 3.12.

Theorem 3.16. *Let $\mathbf{q} \in (\mathbb{Z}^+)^n$, and let $\mathcal{G}$ be a finite graph with vertex set $V = \{1, \ldots, r\}$ and n edges, and let $g \in G(\mathbf{q})$. Let $\mathbf{a}$ be the incidence matrix of $\mathcal{G}$, regarded as a sequence of length n in $G'(\mathbf{q})$. Then the number of subgraphs of $\mathcal{G}$ of type $(\mathbf{q}, g)$ is $N^g(G'(\mathbf{a}))$, hence is 0 or at least $2^{n+1-D(G'(\mathbf{q}))}$.*

3.4. **Divisibility in Weighted Graphs.**

Let $G = G(\mathbf{q}) = \bigoplus_{i=1}^r \mathbb{Z}/q_i\mathbb{Z}$ be an (arbitrary) finite commutative p-group. We give ourselves a sequence $\mathbf{A} = \{A_i\}_{i=1}^\infty$ of finite nonempty subsets of $\mathbb{Z}$. For $1 \leq j \leq r$, let $B_j \subset \mathbb{Z}/q_j\mathbb{Z}$ be nonempty subsets, and put $B = \prod_{i=1}^r B_j$, viewed as a subset of G. We will give a graph theoretic application of the quantities $D_{\mathbf{A}}^B(G)$ and $N_{\mathbf{A}}^B(G,n)$ which further generalizes the results of the previous section.

Let $\mathcal{G}$ be a finite graph with vertex set $V = \{1, \ldots, r\}$ and edge set $E = \{1, \ldots, n\}$. An element $a \in \prod_{i=1}^n A_i$ may be viewed as giving an integer weight a_i to each edge i of $\mathcal{G}$: we call this data an **A-weighted subgraph** of $\mathcal{G}$. (The case $A_i = \{0, 1\}$ for all i recovers the usual notion of a subgraph.) For a weighted subgraph $(\mathcal{G}, a)$ and a vertex $j \in V$, the **weighted degree** of j is

$$d_{\mathbf{A}}(j) \coloneqq \sum_{i \sim j} a_i,$$

that is, the sum of the weights of the edges incident to j. A weighted subgraph $(\mathcal{G}, a)$ is B-**divisible** if for all $1 \leq j \leq r$, we have $d_{\mathbf{A}}(j) \in B_j \pmod{\mathbb{Z}/q_j\mathbb{Z}}$.

This setup is designed so that the number of $\mathbf{A}$-weighted B-divisible subgraphs is equal to the number of $\mathbf{A}$-weighted B-sum subsequences of the sequence $\mathbf{a}$ in $G'(\mathbf{q})$ corresponding to the incidence matrix. Thus we may apply the results of §3.2 to deduce the following result.

Theorem 3.17. *a) Let $G(\mathbf{q})$, $\mathbf{A} = \{A_i\}_{i=1}^\infty$, $B = \prod_{j=1}^r B_j$ be as above, and let $\mathcal{G}$ be a finite graph with vertex set $V = \{1, \ldots, r\}$ and edge set $E = \{1, \ldots, n\}$. Let $\mathbf{a}$ be the incidence matrix of $\mathcal{G}$, viewed as a sequence of length n in $G'(\mathbf{q})$. Then the number of B-divisible $\mathbf{A}$-weighted subgraphs of $\mathcal{G}$ is $N_{\mathbf{A}}^B(\mathbf{a})$.*
b) If each A_i contains 0 and at least one element not divisible by $q_r = \exp G(\mathbf{q})$ and each B_j contains 0, then there is a nonempty $\mathbf{A}$-weighted B-divisible subgraph of $\mathcal{G}$ whenever $n \geq D_{\mathbf{A}}^B(G'(\mathbf{q}))$.
c) Let p be a prime, let $1 \leq v_1 \leq \ldots \leq v_r \in \mathbb{Z}$ and put $\mathbf{q} = (p^{v_1}, \ldots, p^{v_r})$. Let $A_1, \ldots, A_n, B_1, \ldots, B_r$ each have the property that no two distinct elements are congruent modulo p. Then:
(i) the number of $\mathbf{A}$-weighted B-divisible subgraphs of $\mathcal{G}$ is either 0 or at least

$$\mathfrak{m}\left(\#A_1, \ldots, \#A_n; \sum_{i=1}^n \#A_i - \sum_{j=1}^r (p^{v_j} - \#B_j)\right).$$

(ii) Suppose that 0 lies in A_i for all $1 \leq i \leq n$ and 0 lies in B_j for all $1 \leq j \leq r$. Then there is a nonempty $\mathbf{A}$-weighted B-divisible subgraph if

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

Remark 3.18. *Theorem 3.17c)(ii) with $A_i = \{0, 1\}$ recovers* [AFK84, Thm. A.4].

3.5. **Polynomial Interpolation With Relaxed Targets.**

Our final application of the Main Theorem lies not in combinatorics but in algebra, specifically the problem of polynomial interpolation in commutative rings.

Theorem 3.19. *Let $(\mathfrak{r}, \mathfrak{p})$ be a finite, local principal ring with residue field $\mathbb{F}_q$ and length v. Let $f_1, \ldots, f_n \in \mathfrak{r}[t_1, \ldots, t_N]$ be $\mathfrak{r}$-linearly independent, and let $V = \langle f_1, \ldots, f_n \rangle$ be the $\mathfrak{r}$-module spanned by $f_1, \ldots, f_n$, so that every $f \in V$ may be uniquely written as*

$$f = \sum_{i=1}^n c_i(f) f_i, \;\; c_i(f) \in \mathfrak{r}.$$

Let $X = \{x_j\}_{j=1}^r \subset \mathfrak{r}^N$ be finite of cardinality r. Let $A_1, \ldots, A_n, B_1, \ldots, B_r \subset \mathfrak{r}$ satisfy Condition (F). For $1 \leq j \leq r$, let $1 \leq v_j \leq v$.
a) Let $\mathcal{S}$ be the set of $f \in V$ such that
(i) $c_i(f) \in A_i$ for all $1 \leq i \leq n$ and
(ii) $f(x_j) \in B_j \pmod{\mathfrak{p}^{v_j}}$ for all $1 \leq j \leq n$.
Then $\#\mathcal{S} = 0$ or

$$\#\mathcal{S} \geq \mathfrak{m}(\#A_1, \ldots, \#A_n; \sum_{i=1}^n \#A_i - \sum_{j=1}^r (q^{v_j} - \#B_j)).$$

b) Suppose that 0 is an element of each A_i and B_j and that

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

Then there is $0 \neq f \in \mathcal{S}$.

Proof. a) For $1 \leq j \leq r$, let $L_j : \mathfrak{r}[t_1, \ldots, t_N] \to \mathfrak{r}$ by $f \mapsto f(x_j)$; this is an $\mathfrak{r}$-linear map, hence so is its restriction to the $\mathfrak{r}$-submodule V. The basis $f_1, \ldots, f_n$ gives us an identification of V with $\mathfrak{r}^n$ under which $f = \sum_{i=1}^n c_i(f) f_i$ corresponds to $(c_1(f), \ldots, c_n(f)) \in \mathfrak{r}^n$. In this way we may view each L_j as a linear polynomial on $\mathfrak{r}^n$. For $f = (c_1(f), \ldots, c_n(f)) \in \mathfrak{r}^n$ the condition $L_j(f) \in B_j \pmod{\mathfrak{p}^{v_j}}$ corresponds to $f(x_j) \in B_j \pmod{\mathfrak{p}^{v_j}}$. So Theorem 1.6 applies.
b) The hypotheses imply that $0 \in \mathcal{S}$ and
$\mathfrak{m}(\#A_1, \ldots, \#A_n; \sum_{i=1}^n \#A_i - \sum_{j=1}^r (q^{v_j} - \#B_j)) \geq 2$. □

Corollary 3.20. *For each $x \in \mathbb{F}_q^\times$, let B_x be a subset of $\mathbb{F}_q$ containing 0. There is a nonzero polynomial $f \in \mathbb{F}_q[t]$ of degree at most n such that $f(0) = 0$, $f(x) \in B_x$ for all $x \in \mathbb{F}_q^\times$ if*

$$n > q - \frac{\sum_{x \in \mathbb{F}_q^\times} \#B_x}{q-1}.$$

Proof. Order the elements of $\mathbb{F}_q$ as $x_1 = 0, x_2, \ldots, x_q$. We apply Theorem 3.19b) with $n+1$ in place of n, $\mathfrak{r} = \mathbb{F}_q$, $N = 1$, $f_1 = 1, f_2 = t_1, \ldots, f_{n+1} = t_1^n$, $X = \mathbb{F}_q$, $A_1 = \ldots = A_{n+1} = \mathbb{F}_q$, $B_1 = \{0\}$, $B_j = B_{x_j}$ for $2 \leq j \leq q$, $v_1 = \ldots = v_r = 1$: there is a nonzero polynomial of degree at most n with $f(0) = 0$ and $f(x) \in S_x$ for all $x \in \mathbb{F}_q^\times$ if

$$n + 1 < \sum_{i=1}^{n+1} \#A_i - \sum_{j=1}^q (q - \#B_j) = (n+1)q - (q-1) - q(q-1) + \sum_{x \in \mathbb{F}_q^\times} \#B_x,$$

which is equivalent to

$$n > q - \frac{\sum_{x \in \mathbb{F}_q^\times} \#B_x}{q-1}. \qquad \square$$

Corollary 3.20 is due to Troi and Zannier when $q = p$ is a prime [TZ97, Thm. 2]. Their proof is quite different: it uses Theorem 3.3 and an auxiliary result involving integer-valued polynomials. It does not seem to carry over to $\mathbb{F}_q$.

References

[AF93] N. Alon and Z. Füredi, *Covering the cube by affine hyperplanes.* Eur. J. Comb. 14 (1993), 79-83.

[AFK84] N. Alon, S. Friedland and G. Kalai, *Regular subgraphs of almost regular graphs.* J. Combin. Theory Ser. B 37 (1984), 79-91.

[AKLMRS] 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.

[Al99] N. Alon, *Combinatorial Nullstellensatz.* Recent trends in combinatorics (Mátraháza, 1995). Combin. Probab. Comput. 8 (1999), 7-29.

[AR06] S.D. Adhikari and P. Rath, *Davenport constant with weights and some related questions.* Integers 6 (2006), A30, 6 pp.

[Ax64] J. Ax, *Zeroes of polynomials over finite fields.* Amer. J. Math. 86 (1964), 255-261.

[BC15] A. Brunyate and P.L. Clark, *Extending the Zolotarev-Frobenius approach to quadratic reciprocity* Ramanujan J. 37 (2015), 25-50.

[Br11] D. Brink, *Chevalley's theorem with restricted variables.* Combinatorica 31 (2011), 127-130.

[BS80] R.C. Baker and W.M. Schmidt, *Diophantine problems in variables restricted to the values* 0 *and* 1. J. Number Theory 12 (1980), 460–486.

[BS09] S. Ball and O. Serra, *Punctured combinatorial Nullstellensätze.* Combinatorica 29 (2009), 511–522.

[CCQWZ11] 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), no. 1, Paper 133, 10 pp.

[CFS14] P.L. Clark, A. Forrow and J.R. Schmitt, *Warning's second theorem with restricted variables.* Combinatorica 37 (2017), 397–417.

[Ch35] C. Chevalley, *Démonstration d'une hypothèse de M. Artin.* Abh. Math. Sem. Univ. Hamburg 11 (1935), 73–75.

[Cl14] P.L. Clark, *The Combinatorial Nullstellensätze Revisited.* Electronic Journal of Combinatorics. Volume 21, Issue 4 (2014). Paper #P4.15

[DAGS12] S. Das Adhikari, D.J. Grynkiewicz and Z.-W. Sun, *On weighted zero-sum sequences.* Adv. in Appl. Math. 48 (2012), 506–527.

[EBK69] P. van Emde Boas and D. Kruyswijk, *A combinatorial problem on finite abelian groups, III*, Report ZW- 1969-008, Math. Centre, Amsterdam, 1969.

[EGZ61] P. Erdős, A. Ginzburg and A. Ziv, *Theorem in the additive number theory.* Bull. Research Council Israel 10F (1961), 41–43.

[G] D.J. Grynkiewicz, *Structural Additive Theory*, Developments in Mathematics, Springer, 2013.

[GG06] W. Gao and A. Geroldinger, *Zero-sum problems in finite abelian groups: a survey.* Expo. Math. 24 (2006), no. 4, 337369.

[GHK] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations. Algebraic, combinatorial and analytic theory.* Pure and Applied Mathematics (Boca Raton), 278. Chapman & Hall/CRC, Boca Raton, FL, 2006.

[HB11] D.R. Heath-Brown, *On Chevalley-Warning theorems.* (Russian. Russian summary) Uspekhi Mat. Nauk 66 (2011), no. 2(398), 223–232; translation in Russian Math. Surveys 66 (2011), no. 2, 427–436.

[HK14] F. Halter-Koch, *Arithmetical interpretation of weighted Davenport constants.* Arch. Math. 103 (2014), 125–131.

[Hu68] T.W. Hungerford, *On the structure of principal ideal rings.* Pacific J. of Math. 25 (1968), 543–547.

[Ne71] A.A. Nečaev, *The structure of finite commutative rings with unity.* Mat. Zametki 10 (1971), 679–688.

[O69a] J.E. Olson, *A combinatorial problem on finite Abelian groups.* I. J. Number Theory 1 (1969), 8–10.

[Ol69b] J.E. Olson, *A combinatorial problem on finite Abelian groups. II.* J. Number Theory 1 (1969), 195–199.

[Sc74] S.H. Schanuel, *An extension of Chevalley's theorem to congruences modulo prime powers.* J. Number Theory 6 (1974), 284–290.

[Sc08] U. Schauz, *Algebraically solvable problems: describing polynomials as equivalent to explicit solutions*. Electron. J. Combin. 15 (2008), no. 1, Research Paper 10, 35 pp.

[Th07] R. Thangadurai, *A variant of Davenport's constant*. Proc. Indian Acad. Sci. Math. Sci. 117 (2007), 147–158.

[TZ97] 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.

[Wa35] E. Warning, *Bemerkung zur vorstehenden Arbeit von Herrn Chevalley*. Abh. Math. Sem. Hamburg 11 (1935), 76–83.

[Wi06] R.M. Wilson, *Some applications of polynomials in combinatorics*. IPM Lectures, May, 2006.