Generalisations of Roth's theorem on finite abelian groups

by

Cassandra Naymie

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Pure Mathematics

Waterloo, Ontario, Canada, 2012

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

Roth's theorem, proved by Roth in 1953, states that when $A \subseteq [1, N]$ with A dense enough, A has a three term arithmetic progression (3-AP). Since then the bound originally given by Roth has been improved upon by number theorists several times. The theorem can also be generalized to finite abelian groups. In 1994 Meshulam worked on finding an upper bound for subsets containing only trivial 3-APs based on the number of components in a finite abelian group. Meshulams bound holds for finite abelian groups of odd order. In 2003 Lev generalised Meshulams result for almost all finite abelian groups. In 2009 Liu and Spencer generalised the concept of a 3-AP to a linear equation and obtained a similar bound depending on the number of components of the group. In 2011, Liu, Spencer and Zhao generalised the 3-AP to a system of linear equations. This thesis is an overview of these results.

Acknowledgements

First and foremost I would like to thank my supervisors, Yu-Ru Liu and Wentang Kuo, for their excellent guidance. I've learned so much from them over this past year, and it has made me a better mathematician. I feel so lucky that I had such caring and thoughtful supervisors.

I would like to thank my readers, Nico Spronk and Mike Rubinstein, for their generous and insightful feedback on this thesis.

I would like to thank Nancy Maloney for being patient with me and my frequent questions regarding the administrative side of my degree. Without her help, I doubt I would be graduating.

I am grateful for the mentorship I received throughout my Master's from Yu-Ru Liu, Kathryn Hare, and Nico Spronk. They inspired and encouraged me to pursue doctoral studies, and gave me invaluable advice concerning my future in mathematics.

Finally, I would like to thank the pure math department for cultivating my love and skill for mathematics during my undergraduate and graduate degrees.

Table of Contents

Chapter 1

Introduction

1.1 Main results

This thesis is a collection of research done over the last twenty years on generalizing Roth's theorem on finite abelian groups. This introduction includes content which will be repeated later on, so that each chapter may be read independently from the others with relative ease.

Definition 1.1.1. Let G be an abelian group. *A three term arithmetic progression (or 3-AP)* is a subset $\{x, y, z\} \subseteq G$ with $x + z = 2y$. If $x = z$, we say that the 3-AP is trivial, and that it is non-trivial otherwise.

For $k \in \mathbb{N} = \{0, 1, 2, ...\}$, let $\mathbb{Z}_k$ denote the cyclic group of order k. Let G be a finite abelian group with

$$G = \mathbb{Z}_{k_1} \oplus \mathbb{Z}_{k_2} \oplus \cdots \oplus \mathbb{Z}_{k_n},$$

where $k_i \in \mathbb{N}$, $k_i \geq 2$ for $i \in \{1, \ldots, n\}$ and $k_1 \mid k_2 \mid \cdots \mid k_n$. Each finite abelian group can be decomposed uniquely in this form [4]. We denote the number of components of G by $c(G)$, thus, here $c(G) = n$.

Definition 1.1.2. Let G be a finite abelian group. Define

$$D(G) = \sup_{\substack{A \subset G \\ A \text{ contains no} \\ \text{non-trivial 3-APs}}} |A|.$$

Definition 1.1.3. Given non-negative functions $f(x), g(x)$ defined on a subset of the real numbers, we say that

$$f(x) = O(g(x)) \quad \text{or} \quad f(x) \ll g(x),$$

if there is some $C > 0$ and $x_0 > 0$ with $f(x) \leq Cg(x)$ for each $x \geq x_0$. We say that

$$f(x) = o(g(x))$$

if for any $\varepsilon > 0$, there exists $x_1 > 0$ with $f(x) \leq \varepsilon g(x)$ for each $x \geq x_1$.

In 1953 Roth [9] proved that $D(\mathbb{Z}_m) = O(m/\log\log m)$. From Heath-Brown's [3] work in 1987 and Szemeredi's [11] work in 1990 this bound was improved to $D(\mathbb{Z}_m) = O(m/(\log m)^\alpha)$ for any fixed α with $0 < \alpha < \frac{1}{20}$. The best current bound on Roth's theorem is by Tom Sanders, and gives $D(\mathbb{Z}_m) = O(m(\log\log m)^5/\log m)$. It has also been shown by Brown and Buhler [1] and Frankl, Graham and Rodl [2] that when G is any finite abelian group of odd order that $D(G) = o(|G|)$.

In 1994 Meshulam [8] used his result bounding $D(G)$ by the number of components of a finite abelian group G with odd order to improve the asymptotic bound on $D(G)$. Intuitively, it seems that $D(G)$ depends on the size of G and also the number of components of G, with a large number of components decreasing the size of $D(G)$. Indeed, consider the two finite abelian groups $\mathbb{Z}_{81}$ and $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$. These two groups have the same size, but the latter gives us very little room to build subsets while avoiding non-trivial 3-APs. Meshulam's result gives us a formal verification of this intuition. In 1994 Meshulam [8] proved the following.

Theorem 1.1.1. *Let $n \in \mathbb{N}$ and define*

$$d(n) = \sup_{\substack{c(G) \geq n \\ |G| \text{ odd}}} \frac{D(G)}{|G|}.$$

Let $n \in \mathbb{N}$. We have

$$d(n) \leq \frac{2}{n}.$$

By definition we see that $d(n) \leq d(n-1)$ for each n. Meshulam's proof uses induction on $d(n)$. It shows that if G is a finite abelian group with odd order and $c(G) \geq n$, and $A \subseteq G$ with no non-trivial 3-APs, then $|A|/|G|$ is bounded above by $2/n$. Notice that this theorem only holds for groups which have odd order. Indeed, for Meshulam's proof to work, we require that the finite abelian group G has odd order (in particular we need that $2a = 2b$ implies $a = b$). In 2003 Lev [5] adapted Meshulam's proof for finite abelian groups with the condition that $2G = \{g + g : g \in G\}$ is non-trivial, i.e. G is not a direct sum of $\mathbb{Z}_2$.

Before stating Lev's result, we need to re-examine our definition of a non-trivial 3-AP. Previously, we called a subset $\{a, b, c\} \subseteq G$ a 3-AP if $a + c = 2b$. It was a trivial 3-AP if $a = c$ and a non-trivial 3-AP otherwise. When G has odd order, the condition that $a = c$

implies that $a = b = c$, so that each 3-AP is a set of either 1 or 3 elements. When G has elements of order 2, this distinction becomes more subtle. For example, in $\mathbb{Z}_{10}$, the subset $\{1, 6\}$ is a 3-AP since $6 + 6 = 2 \cdot 1$ and $1 + 1 = 2 \cdot 6$. This 3-AP is not necessarily trivial since it consists of two different elements, but it does not consist of three distinct elements. Notice that if we define $\phi : G \to 2G$ by $\phi(g) = 2g$, then when $G = \mathbb{Z}_{10}, \phi(6 - 1) = 0$. In general, if $a - b \in \ker \phi$, then $a + a = 2b$ and so $\{a, b\}$ is a 3-AP. The choice of defining a trivial 3-AP as one in which $a = c$ was motivated by this. When $a \neq c$, this implies that the 3-AP has 3 distinct elements. Lev's generalization of Meshulam's result is below.

Theorem 1.1.2. *Let G be a finite abelian group so that the group $2G = \{g + g : g \in G\}$ is non-trivial. Then we have that*

$$D(G) \leq \frac{2|G|}{c(2G)}.$$

For $n \in \mathbb{N}$ define

$$d(n) = \sup_{c(2G) \geq n} \frac{D(G)}{|G|},$$

so that we may equivalently state,

$$d(n) \leq \frac{2}{n}.$$

When G has odd order, $2G = G$ and thus $c(2G) = c(G)$. In this case Lev's result reduces to $D(G) < \frac{2|G|}{c(G)}$, which is exactly Meshulam's result.

Lev's result gives a very good bound on sizes of subsets containing only trivial 3-APs for most finite abelain groups. The subsequent research looked at generalizing the concept of a 3-AP. In 2009 Liu and Spencer [6] generalized Meshulam's result to subsets which contain no trivial solutions to a linear equation.

Let $s \in \mathbb{N}$ with $s \geq 3$. Let $\mathbf{r} = (r_1, r_2, \ldots, r_s) \in (\mathbb{Z} \setminus \{0\})^s$ be a vector satisfying $r_1 + r_2 + \cdots + r_s = 0$. Given a finite abelian group G,

$$G \cong \mathbb{Z}_{k_1} \oplus \mathbb{Z}_{k_2} \oplus \cdots \oplus \mathbb{Z}_{k_n}$$

with $k_i \in \{2, 3, \ldots\}$ for each $i \in \{1, \ldots, n\}$ and $k_i | k_{i+1}$ for $i \in \{1, \ldots, n - 1\}$. We say G has n constituents, and denote this by $c(G) = n$. We let $|G|$ denote the cardinality of G. We say that G is *coprime* to $\mathbf{r}$ if $\gcd(r_i, |G|) = 1$ for each $i \in \{1, \ldots, s\}$.

Here, we have that a 3-AP $\{a, b, c\} \subseteq G$ is generalized to a solution to the linear equation $\mathbf{r}$.

Definition 1.1.4. Let $\mathbf{x} = (x_1, \ldots, x_s) \in G^s$. We say $\mathbf{x}$ is a *solution* to $\mathbf{r}$ if $r_1 x_1 + \cdots r_s x_s = 0$. A solution $\mathbf{x} \in G^s$ is *trivial* if there is some subset $\{j_1, \ldots, j_l\} \subseteq \{1, \ldots, s\}$ with $x_{j_1} = \cdots = x_{j_l}$ and $r_{j_1} + \cdots + r_{j_l} = 0$. Otherwise we say a solution $\mathbf{x} \in G^s$ is *non-trivial*.

Theorem 1.1.3. *Let $\mathbf{r} = (r_1, \ldots, r_s) \in (\mathbb{Z} \setminus \{0\})^s$ so that $r_1 + \cdots + r_s = 0$, with G a finite abelian group coprime to $\mathbf{r}$, and let $A \subseteq G$. If every solution $\mathbf{x} \in A^s$ is trivial, we say that A is free of non-trivial solutions and write $A \in NTSF_{\mathbf{r}}$ (non-trivial solution free subsets). Define*

$$D_{\mathbf{r}}(G) = \max_{\substack{A \subseteq G \\ A \in NTSF_{\mathbf{r}}}} |A|$$

and

$$d_{\mathbf{r}}(n) = \sup_{\substack{G \text{ coprime to } \mathbf{r} \\ c(G) \geq n}} \frac{D_{\mathbf{r}}(G)}{|G|}.$$

Then there exists a constant $C = C(\mathbf{r}) > 0$ such that

$$d_{\mathbf{r}}(n) \leq \frac{C(\mathbf{r})^{s-2}}{n^{s-2}}.$$

This indeed generalizes Meshulam's result. If we let $\mathbf{r} = (1, -2, 1)$, then a non-trivial solution is a 3-AP, and $C(\mathbf{r}) = 2$. Note however, that this does not generalize Lev's result. A group which has even order is not coprime to $\mathbf{r} = (1, -2, 1)$. Similar to the proofs written by Meshulam and Lev, the proof of this result uses induction on $d_{\mathbf{r}}(n)$ and a bound on $|A|/|G|$, where $A \subseteq G$ contains only trivial solutions.

The final result this thesis examines generalizes the previous result from bounds on sets containing no solutions to a linear equation to bounds on sets containing no solutions to systems of linear equations. This bound, depending of course on the system of linear equations being considered, was found in 2011 by Liu, Spencer and Zhao [7]. It is necessary to re-define a trivial solution, and to find a requirement on G similar to that of it being coprime. Below the result is outlined in all its technicality.

Definition 1.1.5. Let $R, S \in \mathbb{N}$ such that $S \geq 2R + 1$. Let $Y = (y_{i,j}) \in \mathbb{Z}^{R \times S}$ be a matrix satisfying $y_{i,1} + y_{i,2} + \cdots + y_{i,S} = 0$ for each $i \in \{1, \ldots, R\}$. Let $L \in \mathbb{N}$ with $R \leq L \leq S - R - 1$. Let G be a finite abelian group.

Then we say G is *L-coprime* to Y if there exists L columns of Y satisfying the following conditions:

- Upon choosing any R of these L columns, we obtain an $R \times R$ matrix $Z \in \mathbb{Z}^{R \times R}$ with $\gcd(\det(Z), |G|) = 1$, where $\det(Z)$ denotes the determinant of Z.
- Upon removing any $L - R + 1$ of these L columns from Y, there exist within the remaining columns two disjoint sets of R columns which form $R \times R$ matrices $Z_1, Z_2 \in \mathbb{Z}^{R \times R}$ with
$$\gcd(\det(Z_1), |G|) = \gcd(\det(Z_2), |G|) = 1.$$

When a matrix G is L-coprime to $Y \in \mathbb{Z}^{R\times S}$, the indices of the L columns satisfying the above conditions are denoted by $l_Y(G;L)$, i.e. if the L columns of Y satisfying the conditions of L-coprimality are

$$\left\{ \begin{pmatrix} y_{1,j_1} \\ y_{2,j_1} \\ \vdots \\ y_{R,j_1} \end{pmatrix}, \begin{pmatrix} y_{1,j_2} \\ y_{2,j_2} \\ \vdots \\ y_{R,j_2} \end{pmatrix}, \cdots, \begin{pmatrix} y_{1,j_L} \\ y_{2,j_L} \\ \vdots \\ y_{R,j_L} \end{pmatrix} \right\},$$

then $l_Y(G;L) = \{j_1, j_2, \ldots, j_L\}$.

Definition 1.1.6. Let $R, S \in \mathbb{N}$, and $Y \in \mathbb{Z}^{R\times S}$ be defined as above. Let G be a finite abelian group. We say that $\overline{x} = (x_1, \ldots, x_s) \in G^S$ is a solution to Y if $Y\overline{x} = 0$, i.e. $\overline{x} = (x_1, \ldots, x_S)$ is a solution if

$$\begin{pmatrix} y_{1,1}x_1 + y_{1,2}x_2 + \cdots + y_{1,S}x_S \\ y_{2,1}x_1 + y_{2,2}x_2 + \cdots + y_{2,S}x_S \\ \vdots \\ y_{R,1}x_1 + y_{R,2}x_2 + \cdots + y_{R,S}x_S \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

We say that a solution $\overline{x} \in G^S$ is *trivial* if there are $i \neq j$, $i, j \in \{1, \ldots, S\}$, with $x_i = x_j$. Otherwise, when each x_i is distinct, we say that $\overline{x}$ is a *non-trivial solution.*

Definition 1.1.7. Let $R, S \in \mathbb{N}$, $L \in \mathbb{N}$, and $Y \in \mathbb{Z}^{R\times S}$ be defined as in Definition 5.1.1. Let G be a finite abelian group which is L-coprime to Y, and let $A \subseteq G$. If every solution $\overline{x} \in A^S$ to the equation $Y\overline{x} = 0$ is trivial, we say that A *contains only trivial solutions to* Y, and write $A \in TRIV_Y$. Define

$$D_Y(G) = \max_{\substack{A\subseteq G \\ A\in TRIV_Y}} |A|$$

and

$$d_Y(N;L) = \sup_{\substack{G \text{ is } L\text{-coprime to } Y \\ c(G)\geq N}} \frac{D_Y(G)}{|G|}.$$

Theorem 1.1.4. *Let $R, S \in \mathbb{N}$ such that $S \geq 2R+1$. Let $Y = (y_{i,j}) \in \mathbb{Z}^{R\times S}$ be a matrix satisfying $y_{i,1} + y_{i,2} + \cdots + y_{i,S} = 0$ for each $i \in \{1, \ldots, R\}$. Let $L \in \mathbb{N}$ with $R \leq L \leq S - R - 1$. Then there exists a constant $C = C(Y;L) > 1$ such that, for any $N \in \mathbb{N}$,*

$$d_Y(N;L) \leq \left(\frac{C}{N}\right)^{\frac{L-R+1}{R}}.$$

1.2 Fourier Analysis Preliminaries

The proofs explained in this thesis use a substantial amount of Fourier analysis on finite abelian groups. Proposition 1.2.3 is particularly useful. Assume that G is a finite abelian group. This section contains results on the Fourier analysis of G which are relevant throughout the thesis.

Definition 1.2.1. Let $\widehat{G}$ denote the *character group*, or *dual group*, of G, i.e.

$$\widehat{G} = \big\{\gamma : G \to \mathbb{C} \mid |\gamma(x)| = 1 \ \forall x \in G, \gamma(x+y) = \gamma(x)\gamma(y) \ \forall x, y \in G\big\}.$$

We call elements of $\widehat{G}$ *characters on* G.

Given γ a character on G, for each x in G,

$$\gamma(x) = \gamma(x+0) = \gamma(x)\gamma(0)$$

so that $\gamma(0) = 1$. Consider

$$\gamma(x)\gamma(-x) = \gamma(x-x) = \gamma(0) = 1,$$

so that $\gamma(x)^{-1} = \gamma(-x)$. Since $\gamma(x)$ is on the unit circle in $\mathbb{C}$,

$$\overline{\gamma(x)} = \frac{1}{\gamma(x)} = \gamma(x)^{-1}.$$

Together this means

$$\overline{\gamma(x)} = \gamma(-x).$$

Proposition 1.2.1. *Let G be a finite abelian group. Then $G \cong \widehat{G}$.*

Proof. Let G be a finite abelian group with

$$G = \mathbb{Z}_{k_1} \oplus \mathbb{Z}_{k_2} \oplus \cdots \oplus \mathbb{Z}_{k_n},$$

where $k_i \in \mathbb{N}$, $k_i \geq 2$ for $i \in \{1, \ldots, n\}$ and $k_1 \mid k_2 \mid \cdots \mid k_n$. Let $a = (a_1, \ldots, a_n) \in G$ and $x = (x_1, \ldots, x_n) \in G$, and define

$$\begin{array}{rcl} \Phi : G & \to \widehat{G} \\ a & \mapsto \gamma_a \end{array} \qquad \text{where} \qquad \begin{array}{rcl} \gamma_a : G & \to \mathbb{C} \\ x & \mapsto e^{2\pi i\left(\frac{a_1}{k_1}x_1 + \cdots + \frac{a_n}{k_n}x_n\right)}. \end{array}$$

Note that γ_a is indeed a character on G, since

$$\gamma_a(x+y) = e^{2\pi i\left(\frac{a_1}{k_1}(x_1+y_1) + \cdots + \frac{a_n}{k_n}(x_n+y_n)\right)} = e^{2\pi i\left(\frac{a_1}{k_1}x_1 + \cdots + \frac{a_n}{k_n}x_n\right)} e^{2\pi i\left(\frac{a_1}{k_1}y_1 + \cdots + \frac{a_n}{k_n}y_n\right)} = \gamma_a(x)\gamma_a(y).$$

Suppose that $\gamma_a = \gamma_b$. Then

$$e^{2\pi i \frac{a_1}{k_1}} = \gamma_a(1, 0, \ldots, 0) = \gamma_b(1, 0, \ldots, 0) = e^{2\pi i \frac{b_1}{k_1}}$$

so that $a_1 = b_1 \mod k_1$. Similarly, $a_i = b_i \mod k_i$ for each $i \in \{1, \ldots, n\}$, and Φ is one to one. To check Φ is onto, let $\gamma \in \widehat{G}$. Then $\gamma(1, 0, \ldots, 0) = e^{2\pi i z}$ for some $z \in [0, 1]$. Let $a_1 = zk_1$. Since $\gamma(0) = 1$, we have that

$$1 = \gamma(k_1, 0, \ldots, 0) = e^{2\pi i k_1 z}$$

so that $a_1 = k_1 z \in \mathbb{Z}_{k_1}$. We can similarly define $a_2, \ldots, a_n$, and it is clear that $\gamma = \gamma_{(a_1,\ldots,a_n)}$. As such, $G \cong \widehat{G}$. □

Definition 1.2.2. Let $f : G \to \mathbb{C}$. Define the *Fourier transform of* f as

$$\begin{aligned} \hat{f} : \widehat{G} &\to \mathbb{C} \\ \gamma &\mapsto \sum_{x \in G} f(x)\gamma(-x). \end{aligned}$$

Definition 1.2.3. Let $f, g : G \to \mathbb{C}$. Define the *convolution of* f *and* g as

$$f * g(x) = \sum_{y \in G} f(y)g(x - y)$$

for x an element of G, and denote $f * f * \cdots * f$ where f is convoluted with itself k times by f^{*^k}.

Proposition 1.2.2. *Let* f *and* g *be functions from* G *to* $\mathbb{C}$ *and* γ *be a character on* G. *Then* $\widehat{f * g}(\gamma) = \hat{f}(\gamma)\hat{g}(\gamma)$.

Proof. From the definition,

$$\begin{aligned} \widehat{f * g}(\gamma) &= \sum_{x \in G} (f * g)(x)\gamma(-x) \\ &= \sum_{x \in G} (\sum_{y \in G} f(y)g(x - y))\gamma(-x). \end{aligned}$$

Since γ is a character,

$$\gamma(-x) = \gamma(-x - y + y) = \gamma(-y)\gamma(-x + y),$$

which produces

$$\begin{aligned}\widehat{f * g}(\gamma) &= \sum_{x\in G}\sum_{y\in G} f(y)g(x-y)\gamma(-y)\gamma(-x+y) \\ &= \sum_{y\in G} f(y)\gamma(-y)\sum_{x\in G} g(x-y)\gamma(-x+y).\end{aligned}$$

From the definition of the Fourier transform,

$$\widehat{f * g}(\gamma) = \hat{f}(\gamma)\hat{g}(\gamma).$$

□

Definition 1.2.4. Let $A \subseteq G$. Define

$$\chi_A(x) = \begin{cases} 1, & \text{if } x \in A, \\ 0, & \text{otherwise.} \end{cases}$$

If $\gamma(x) = 1$ for all $x \in G$ we denote γ by e.

Definition 1.2.5. Let $\delta : \widehat{G} \to \mathbb{C}$ be defined as

$$\delta(\gamma) = \begin{cases} 1, & \text{if } \gamma = e, \\ 0, & \text{otherwise.} \end{cases}$$

Proposition 1.2.3. *(Orthogonality) (1) Let γ be a character on G. Then*

$$\sum_{x\in G}\gamma(x) = \begin{cases} |G|, & \textit{if } \gamma = e, \\ 0, & \textit{otherwise.} \end{cases}$$

(2) Let x be an element of G. Then

$$\sum_{\gamma\in\widehat{G}}\gamma(x) = \begin{cases} |\widehat{G}| = |G|, & \textit{if } x = 0, \\ 0, & \textit{otherwise.} \end{cases}$$

Proof. (1) When $\gamma = e$ the above equality is clear. When $\gamma \neq e$ then there is some $y \in G$ with $\gamma(y) \neq 1$. Consider

$$\sum_{x\in G}\gamma(x) = \sum_{x\in G}\gamma(x-y+y) = \sum_{x\in G}\gamma(x-y)\gamma(y) = \gamma(y)\sum_{x\in G}\gamma(x-y) = \gamma(y)\sum_{x\in G}\gamma(x).$$

Since $\gamma(y) \neq 1$, the above equality holds if and only if $\sum_{x\in G}\gamma(x) = 0$.

(2) When $x = 0, \gamma(x) = 1$ for each γ in the dual group. Therefore

$$\sum_{\gamma \in \widehat{G}} \gamma(0) = |\widehat{G}| = |G|.$$

When $x \neq 0$, there exists some γ_0 in the dual group with $\gamma_0(x) \neq 1$. Then

$$\sum_{\gamma \in \widehat{G}} \gamma(x) = \sum_{\gamma \in \widehat{G}} \gamma_0(x - x)\gamma(x) = \gamma_0(x) \sum_{\gamma \in \widehat{G}} \gamma_0(-x)\gamma(x).$$

Recall that for characters on G, $\gamma(-x) = \gamma^{-1}(x)$, and that the group operation of $\widehat{G}$ is pointwise multiplication. This means

$$\sum_{\gamma \in \widehat{G}} \gamma(x) = \gamma_0(x) \sum_{\gamma \in \widehat{G}} \gamma_0^{-1}\gamma(x) = \gamma_0(x) \sum_{\gamma \in \widehat{G}} \gamma(x).$$

Since $\gamma_0(x) \neq 1$, the above equality holds if and only if

$$\sum_{\gamma \in \widehat{G}} \gamma(x) = 0.$$

□

Proposition 1.2.4. *If $f(x) = 1$ for all $x \in G$ then $\hat{f}(\gamma) = |G|\delta(\gamma)$.*

Proof. By Proposition 1.2.3(2), if $f(x) = 1$ for all $x \in G$ then

$$\hat{f}(\gamma) \quad = \quad \sum_{x \in G} 1(x)\gamma(-x) = \sum_{x \in G} \gamma(x) = \begin{cases} |G|, & \text{if } \gamma = e, \\ 0, & \text{otherwise} \end{cases}$$

so that $\hat{f}(\gamma) = |G|\delta(\gamma)$.

□

Proposition 1.2.5. *(Parseval's Identity) Let $\rho : G \to \mathbb{C}$. Then*

$$\sum_{\gamma \in \widehat{G}} |\hat{\rho}(\gamma)|^2 = |G| \sum_{x \in G} |\rho(x)|^2.$$

Proof. We first expand the Fourier transform of ρ:

$$\sum_{\gamma \in \widehat{G}} |\hat{\rho}(\gamma)|^2 = \sum_{\gamma \in \widehat{G}} \left| \sum_{x \in G} \rho(x)\gamma(-x) \right|^2.$$

The square of the absolute value of the Fourier transform of ρ on γ can also be expressed as an inner product:

$$\begin{aligned}\sum_{\gamma\in\widehat{G}}|\hat{\rho}(\gamma)|^2 &= \sum_{\gamma\in\widehat{G}}\left\langle\sum_{x\in G}\rho(x)\gamma(-x),\sum_{y\in G}\rho(y)\gamma(-y)\right\rangle \\ &= \sum_{\gamma\in\widehat{G}}\sum_{x\in G}\sum_{y\in G}\langle\rho(x)\gamma(-x),\rho(y)\gamma(-y)\rangle \\ &= \sum_{\gamma\in\widehat{G}}\sum_{x\in G}\sum_{y\in G}(\rho(x)\gamma(-x))\left(\overline{\rho(y)\gamma(-y)}\right).\end{aligned}$$

Recalling that $\overline{\gamma(-y)}=\gamma(y)$ and rearranging the sums produces

$$\begin{aligned}\sum_{\gamma\in\widehat{G}}|\hat{\rho}(\gamma)|^2 &= \sum_{x\in G}\sum_{y\in G}\rho(x)\overline{\rho(y)}\sum_{\gamma\in\widehat{G}}\gamma(-x)\gamma(y) \\ &= \sum_{x\in G}\sum_{y\in G}\rho(x)\overline{\rho(y)}\sum_{\gamma\in\widehat{G}}\gamma(y-x).\end{aligned}$$

By Proposition 1.2.3(2)

$$\sum_{\gamma\in\widehat{G}}\gamma(z)=\begin{cases}|G|, & \text{if } z=0,\\ 0, & \text{otherwise.}\end{cases}$$

In the above case the sum is only non-zero when $x=y$, resulting in

$$\sum_{\gamma\in\widehat{G}}|\hat{\rho}(\gamma)|^2=\sum_{x\in G}\rho(x)\overline{\rho(x)}|G|=|G|\sum_{x\in G}|\rho(x)|^2.$$

□

Chapter 2

3-APs on Finite Abelian Groups of Odd Order

2.1 Introduction

Definition 2.1.1. Let G be an abelian group. *A three term arithmetic progression (or 3-AP)* is a subset $\{x, y, z\} \subseteq G$ with $x + z = 2y$. If $x = y = z$, we say that the 3-AP is trivial, and that it is non-trivial otherwise.

For $k \in \mathbb{N} = \{0, 1, 2, ...\}$, let $\mathbb{Z}_k$ denote the cyclic group of order k. Let G be a finite abelian group with

$$G = \mathbb{Z}_{k_1} \oplus \mathbb{Z}_{k_2} \oplus \cdots \oplus \mathbb{Z}_{k_n},$$

where $k_i \in \mathbb{N}$, $k_i \geq 2$ for $i \in \{1, \ldots, n\}$ and $k_1 \mid k_2 \mid \cdots \mid k_n$. Each finite abelian group can be decomposed uniquely in this form [4]. We denote the number of components of G by $c(G)$, thus, here $c(G) = n$.

Definition 2.1.2. Let G be a finite abelian group of odd order. Define

$$D(G) = \sup_{\substack{A \subset G \\ A \text{ contains no} \\ \text{non-trivial 3-APs}}} |A|.$$

In 1994 Meshulam [8] used his result bounding $D(G)$ by the number of components of a finite abelian group G with odd order to improve the asymptotic bound on $D(G)$.

Definition 2.1.3. Let $n \in \mathbb{N}$ and define

$$d(n) = \sup_{\substack{c(G) \geq n \\ |G| \text{ odd}}} \frac{D(G)}{|G|}.$$

By definition we see that $d(n) \leq d(n-1)$ for each n. In 1994 Meshulam [8] proved the following.

Theorem 2.1.1. *Let $n \in \mathbb{N}$. We have*

$$d(n) \leq \frac{2}{n}.$$

2.2 Proof of Meshulam's Theorem

Meshulam's proof is inductive on $d(n)$. The base case is trivial since $D(G) \leq |G|$ always holds. Therefore

$$d(1) = \sup_{c(G)\geq 1} \frac{D(G)}{|G|} \leq 1 < 2.$$

Suppose that G is a finite abelian group with odd order with more than n components so that $c(G) \geq n \geq 2$. Let $A \subseteq G$ contain no 3-APs. Let $B = -2A = \{-2a : a \in A\}$. Define $f, g, h : \widehat{G} \to \mathbb{C}$ as follows:

1. $f(\gamma) = \widehat{\chi_A}(\gamma)$
2. $g(\gamma) = \widehat{\chi_B}(\gamma)$
3. $h(\gamma) = d(n-1)|G|\delta(\gamma)$

and let $u : G \to \mathbb{C}$ be defined by $u(x) = d(n-1) - \chi_B(x)$. We remark that

$$\begin{aligned}
\hat{u}(\gamma) &= \sum_{x\in G} u(x)\gamma(-x) \\
&= d(n-1)\sum_{x\in G}\gamma(-x) - \sum_{x\in G}\chi_B(x)\gamma(-x) \\
&= d(n-1)|G|\delta(\gamma) - \sum_{x\in G}\chi_B(x)\gamma(-x) \\
&= h(\gamma) - g(\gamma).
\end{aligned}$$

Proposition 2.2.1.

$$\max_{\gamma\in\hat{G}} |\hat{u}(\gamma)| = d(n-1)|G| - |A|.$$

Proof. Let $\gamma \in \hat{G}$ be arbitrary, and let W denote the kernel of γ. Note that since the image of γ is on the unit disc, it is cyclic, and

$$c(W) \geq c(G) - 1 = n - 1.$$

Let $x \in G$, and suppose that $W \cap (x - B)$ has a 3-AP. Then $\{x - 2a_1, x - 2a_2, x - 2a_3\}$ is a 3-AP, which gives us that

$$x - 2a_1 + x - 2a_3 = 2x - 4a_2$$

so that

$$2a_1 + 2a_3 = 4a_2.$$

Since G has odd order, we can reduce this to

$$a_1 + a_3 = 2a_2.$$

Therefore $\{a_1, a_2, a_3\} \subseteq A$ is a 3-AP, which only contains the trivial 3-AP. Therefore $a_1 = a_2 = a_3$, and our 3-AP from $W \cap (x - B)$ is also trivial. From the definition of $d(n)$ we see that

$$|W \cap (x - B)| \leq |W| d(c(W)) \leq |W| d(n - 1).$$

In particular

$$|W| d(n - 1) - |W \cap (x - B)| \geq 0.$$

We will use this fact to show that $\chi_W * u(x) \geq 0$ for each $x \in G$:

$$\chi_W * u(x) = \sum_{y \in G} \chi_W(y) u(x - y) = \sum_{w \in W} u(x - w).$$

Expanding the definition of $u(x) = d(n - 1) - \chi_B(x)$ we see that

$$\chi_W * u(x) = \sum_{w \in W} \Big(d(n - 1) - \chi_B(x - w) \Big) = |W| d(n - 1) - |B \cap (x - W)|.$$

Note that y is an element of $B \cap (x - W)$ if and only if $x - y$ is an element of $W \cap (x - B)$. These sets have the same size, i.e. $|B \cap (x - W)| = |W \cap (x - B)|$. Therefore

$$\chi_W * u(x) = |W| d(n - 1) - |W \cap (x - B)| \geq 0.$$

Recall that W is the kernel of γ, which gives us

$$\widehat{\chi_W}(\gamma) = \sum_{w \in W} \gamma(-w) = \sum_{w \in W} 1 = |W|.$$

This guarantees that

$$|\widehat{\chi_W * u}(\gamma)| = |\widehat{\chi_W}(\gamma)| |\hat{u}(\gamma)| = |W| |\hat{u}(\gamma)|.$$

By expanding the Fourier transform of $\chi_W * u$, and recalling that $\gamma \in \widehat{G}$ has magnitude $|\gamma(x)| = 1$ for each $x \in G$, we get the following:

$$|\widehat{\chi_W * u}(\gamma)| = \left| \sum_{x \in G} \chi_W * u(x) \gamma(-x) \right| \leq \left| \sum_{x \in G} \chi_W * u(x) \right|.$$

Earlier we found an expression for $\chi_W * u$ which showed that $\chi_W * u(x) \geq 0$ for each $x \in G$. As such, we can remove the absolute values:

$$\begin{aligned} |\widehat{\chi_W * u}(\gamma)| &\leq \sum_{x \in G} \chi_W * u(x) \\ &= \sum_{x \in G} |W| d(n-1) - |B \cap (x - W)| \\ &= |G||W| d(n-1) - \sum_{x \in G} |B \cap (x - W)| \end{aligned}$$

Given $b \in B$ and $w \in W$, there is a unique $x \in G$ with $b = x - w$. This justifies the equality $\sum_{x \in G} |B \cap (x - W)| = |B||W|$, giving us

$$|\widehat{\chi_W * u}(\gamma)| \leq |G||W| d(n-1) - |B||W|.$$

Putting it all together we get that

$$|W||\hat{u}(\gamma)| = |\widehat{\chi_W * u}(\gamma)| \leq |G||W| d(n-1) - |B||W|$$

so that

$$|\hat{u}(\gamma)| \leq |G| d(n-1) - |B|.$$

We will check that $|B| = |A|$. Clearly $|B| \leq |A|$. Suppose that $-2a_1 = -2a_2$ so that $2(a_1 - a_2) = 0$. Since G has odd order $a_1 = a_2$, giving us $|B| = |A|$. Our above inequality becomes

$$|\hat{u}(\gamma)| \leq |G| d(n-1) - |A|.$$

Now we will check that the maximum is indeed attained by picking $\gamma = e$. Indeed

$$\begin{aligned}\hat{u}(e) &= h(e) - g(e) \\ &= |G|d(n-1)\delta(e) - \widehat{\chi_B}(e) \\ &= |G|d(n-1) - \sum_{x\in G}\chi_B(x)e(-x) \\ &= |G|d(n-1) - |B| \\ &= |G|d(n-1) - |A|.\end{aligned}$$

This completes the proof of the proposition. □

Lemma 1. *The following equalities hold.*

1. $\chi_A^{*^2} * \chi_B(0) = |A|$.
2. $\sum_{\gamma\in\widehat{G}} f(\gamma)^2 g(\gamma) = |G||A|$.
3. $\sum_{\gamma\in\widehat{G}} f(\gamma)^2 h(\gamma) = |A|^2|G|d(n-1)$.

Proof. 1. Following the definition of convolution gives us

$$\begin{aligned}\chi_A^{*^2} * \chi_B(0) &= \sum_{x\in G}\chi_A(x)(\chi_A * \chi_B(-x)) \\ &= \sum_{x\in G}\chi_A(x)\sum_{y\in G}\chi_A(y)\chi_B(-x-y).\end{aligned}$$

Suppose $x, y \in A$ and $-x - y = -2a \in B$ for some $a \in A$. Then we have that $x + y = 2a$. Since A has no 3-APs this only happens when $x = y = a$. Therefore

$$\sum_{x\in G}\chi_A(x)\sum_{y\in G}\chi_A(y)\chi_B(-x-y) = \sum_{x\in G}\chi_A(x)\chi_A(x)\chi_B(-2x) = |A|.$$

2. Recall the orthogonality property of the dual group, so that

$$\sum_{\gamma\in\widehat{G}}\gamma(-x) = \begin{cases} |G|, & \text{if } x = 0, \\ 0, & \text{otherwise.}\end{cases}$$

From expanding the definition of f and g and using the commutativity of the Fourier transform on convolutions, we see that

$$\sum_{\gamma\in\widehat{G}} f(\gamma)^2 g(\gamma) = \sum_{\gamma\in\widehat{G}}\widehat{\chi_A}(\gamma)^2\widehat{\chi_B}(\gamma) = \sum_{\gamma\in\widehat{G}}\widehat{\chi_A^{*^2} * \chi_B}(\gamma).$$

From the defintion of convolution,

$$\begin{aligned}\sum_{\gamma\in\widehat{G}} f(\gamma)^2 g(\gamma) &= \sum_{\gamma\in\widehat{G}}\sum_{x\in G} \chi_A^{*^2} * \chi_B(x)\gamma(-x) \\ &= \sum_{x\in G} \chi_A^{*^2} * \chi_B(x) \sum_{\gamma\in\widehat{G}} \gamma(-x).\end{aligned}$$

Using the orthogonality property of the dual group along with the first result of this lemma shows us that

$$\sum_{\gamma\in\widehat{G}} f(\gamma)^2 g(\gamma) = |G|\chi_A^{*^2} * \chi_B(0) = |G||A|.$$

3. Note that

$$\widehat{\chi_A}(e) = \sum_{x\in G} \chi_A(x)e(-x) = |A|.$$

Thus when we expand the definitions of f and h,

$$\begin{aligned}\sum_{\gamma\in\widehat{G}} f(\gamma)^2 h(\gamma) &= \sum_{\gamma\in\widehat{G}} f(\gamma)^2 |G| d(n-1)\delta(\gamma) \\ &= f(e)^2 |G| d(n-1) \\ &= \widehat{\chi_A}(e)^2 |G| d(n-1) \\ &= |A|^2 |G| d(n-1).\end{aligned}$$

□

Proposition 2.2.2.

$$|d(n-1)|A| - 1| \leq d(n-1)|G| - |A|$$

Proof. We start by multiplying $|d(n-1)|A| - 1|$ by $|G||A|$ and using the previous lemma:

$$\begin{aligned}|G||A||d(n-1)|A| - 1| &= |d(n-1)|G||A|^2 - |G||A|| \\ &= \left|\sum_{\gamma\in\widehat{G}} f(\gamma)^2 h(\gamma) - \sum_{\gamma\in\widehat{G}} f(\gamma)^2 g(\gamma)\right| \\ &= \left|\sum_{\gamma\in\widehat{G}} f(\gamma)^2 (h(\gamma) - g(\gamma))\right|.\end{aligned}$$

It was noted earlier that $h - g = \hat{u}$, so that

$$|G||A||d(n-1)|A| - 1| = \left| \sum_{\gamma \in \widehat{G}} f(\gamma)^2 \hat{u}(\gamma) \right| \leq \sum_{\gamma \in \widehat{G}} |f(\gamma)|^2 (\max |\hat{u}(\gamma)|).$$

Using Proposition 2.2.1, expanding the defintion of f, and by Proposition 1.2.5 we have that

$$\begin{aligned} |G||A||d(n-1)|A| - 1| &\leq (|G|d(n-1) - |A|) \sum_{\gamma \in \widehat{G}} |\widehat{\chi_A}(\gamma)|^2 \\ &= (|G|d(n-1) - |A|)|G| \sum_{x \in G} |\chi_A(x)|^2 \\ &= (|G|d(n-1) - |A|)|G||A|. \end{aligned}$$

The inequality $|G||A||d(n-1)|A| - 1| \leq (|G|d(n-1) - |A|)|G||A|$ reduces to

$$|d(n-1)|A| - 1| \leq d(n-1)|G| - |A|,$$

finishing the proof. □

Recall that G is a finite abelian group of odd order with n components. We chose A as a subset of G with no 3-APs. Our goal is to show that $d(n) \leq 2/n$, where $d(n) = \sup \frac{D(G)}{|G|}$, and $D(G)$ is the largest size of a subset of G with no 3-APs. If we can bound $|A|/|G|$ by $2/n$ then we have finished the proof of Meshulam's result. By Proposition 2.2.2,

$$d(n-1)|A| - 1 \leq d(n-1)|G||A|.$$

We can rearrange these terms so that

$$\frac{|A|}{|G|} \leq \frac{|G|^{-1} + d(n-1)}{1 + d(n-1)}.$$

Here we note that $d(n-1) \leq \frac{2}{n-1}$ from our induction hypothesis. We can also bound $|G|^{-1}$. We know that G is a finite abelian group of odd order with n components. The smallest such group is $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \cdots \oplus \mathbb{Z}_3$, n copies of $\mathbb{Z}_3$, and it has size 3^n. Therefore $|G|^{-1} \leq 3^{-n}$. Putting it together, we get that

$$\begin{aligned}\frac{|A|}{|G|} &\leq \frac{|G|^{-1}+d(n-1)}{1+d(n-1)} \\ &\leq \frac{3^{-n}+d(n-1)}{1+d(n-1)} \\ &\leq \frac{3^{-n}+\frac{2}{n-1}}{1+\frac{2}{n-1}} \\ &\leq \frac{2}{n}.\end{aligned}$$

2.3 Corollaries

In 1990 Szemeredi and Heath-Brown showed that there exists some $\alpha > 0$ with $0 < \alpha < \frac{1}{20}$ such that $D(\mathbb{Z}_m) = O(m/(\log m)^\alpha)$. Meshulam combined his above result with this bound to acquire the following corollary.

Corollary 2.3.1. *For any $\beta > 0$ with $0 < \beta < \frac{1}{21}$ and any group G which is finite, abelian and of odd order*

$$D(G) = O\left(\frac{|G|}{(\log|G|)^\beta}\right).$$

Proof. Let $\beta = \frac{\alpha}{\alpha+1}$. If $c(G) > (\log|G|)^\beta$ then we are done, since Meshulam's result

$$D(G) \leq \frac{2|G|}{c(G)}$$

implies

$$D(G) \leq \frac{2|G|}{(\log|G|)^\beta}.$$

Now we consider the case when $t = c(G) \leq (\log|G|)^\beta$. Choose $A \subseteq G$ so that A contains no 3-APs. By the pigeonhole principle we can also choose a cyclic subgroup of $H \leq G$ (H may be one of the components of G) with $|H| \geq |G|^{1/t}$. We know that G/H has $\frac{|G|}{|H|}$ cosets. Again we can use the pigeonhole principle to guarantee a coset $x + H$ so that

$$|A \cap (x+H)|\frac{|G|}{|H|} \geq |A|$$

or

$$|A \cap (x+H)| \geq |A|\frac{|H|}{|G|}.$$

Szemeredi and Heath-Brown's result gives us $|A \cap x + H| = O(|H|/(\log |H|)^\alpha)$ so that

$$|A| \ll \frac{|G|}{(\log |H|)^\alpha} \ll \frac{|G|}{(\log |G|^{\frac{1}{t}})^\alpha} \ll \frac{|G|t^\alpha}{(\log |G|)^\alpha}.$$

Since $t \leq (log|G|)^\beta$,

$$|A| \ll \frac{|G|((\log |G|)^\beta)^\alpha}{(\log |G|)^\alpha} = |G|((\log |G|)^{\beta-1})^\alpha = |G|((\log |G|)^{\frac{-1}{\alpha+1}})^\alpha = \frac{|G|}{(\log |G|)^\beta}.$$

□

In 2011, Tom Sanders [10] gave the most recent bound for Roth's Theorem. He showed that for $m \in \mathbb{N}$,

$$D(\mathbb{Z}_m) = O\left(\frac{m(\log\log m)^5}{\log m}\right).$$

Using a similar technique as in Corollary 2.3.1, we achieve the following Corollary.

Corollary 2.3.2. *Let G be a finite abelian group of odd order, and let $D(G)$ denote the largest cardinality of a subset which contains no three term arithmetic progressions. It holds that*

$$D(G) = O\left(\frac{|G|(\log\log |G|)^{\frac{5}{2}}}{(\log |G|)^{\frac{1}{2}}}\right).$$

Proof. Fix a finite abelian group of odd order G, let $A \subseteq G$ so that A contains no 3-APs, and let $t = c(G)$.

Case I: Suppose that

$$t > \frac{(\ln |G|)^{\frac{1}{2}}}{(\ln\ln |G|)^{\frac{5}{2}}}.$$

In this case, we see by Theorem 2.1.1 that

$$D(G) \leq \frac{2|G|}{t} \ll \frac{|G|}{t} \ll \frac{|G|(\log\log |G|)^{\frac{5}{2}}}{(\log |G|)^{\frac{1}{2}}},$$

as desired.

Case II: Suppose that

$$t \leq \frac{(\log |G|)^{\frac{1}{2}}}{(\log\log |G|)^{\frac{5}{2}}}.$$

Applying the pigeonhole principle, we can find a cyclic subgroup H of G so that $|H| \geq |G|^{\frac{1}{t}}$. Applying the pigeonhole principle for a second time, we can find a coset $x + H$ of G/H so that

$$\frac{|A||H|}{|G|} \leq |A \cap (x + H)| = |(A - x) \cap H|.$$

Note that $(A - x) \cap H \subseteq H$ contains no 3-APs. By Sanders's bound, it holds that

$$\begin{aligned} |A| &\leq \frac{|G||(A-x)\cap H|}{|H|} \\ &\ll \frac{|H||G|(\log\log|H|)^5}{|H|(\log|H|)} \\ &\ll \frac{|G|(\log\log|H|)^5}{(\log|G|^{\frac{1}{t}})} \\ &\ll \frac{|G|(\log\log|G|)^5 t}{(\log|G|)} \\ &\ll \frac{|G|(\log\log|G|)^{\frac{5}{2}}}{(\log|G|)^{\frac{1}{2}}}. \end{aligned}$$

□

Chapter 3

3-APs on Finite Abelian Groups of Even Order

3.1 Introduction

In the previous chapter we saw how Meshulam bounded the size of a subset free of 3-APs for a finite abelian group. For his proof to work, we require that the finite abelian group G has odd order (in particular we need that $2a = 2b$ implies $a = b$). In 2003 Lev [5] adapted Meshulam's proof for finite abelian groups with the condition that $2G = \{g + g : g \in G\}$ is non-trivial, i.e. G is not a direct sum of $\mathbb{Z}_2$. For the remainder of this chapter, assume that G is a finite abelian group which is not a direct sum of $\mathbb{Z}_2$.

Before stating Lev's result, we need to refine our definition of a non-trivial 3-AP. Previously, we called a subset $\{a, b, c\} \subseteq G$ a 3-AP if $a + c = 2b$. It was a trivial 3-AP if $a = b = c$ and a non-trivial 3-AP otherwise. When G has elements of order 2, this distinction becomes more subtle. For example, in $\mathbb{Z}_{10}$, the subset $\{1, 6\}$ is a 3-AP since $6 + 6 = 2 \cdot 1$ and $1 + 1 = 2 \cdot 6$. This 3-AP is not necessarily trivial since it consists of two different elements, but it does not consist of three distinct elements. Notice that if we define $\phi : G \to 2G$ by $\phi(g) = 2g$, then when $G = \mathbb{Z}_{10}, \phi(6 - 1) = 0$. In general, if $a - b \in \ker \phi$, then $a + a = 2b$ and so $\{a, b\}$ is a 3-AP. When G has odd order, $\ker \phi$ is trivial, so every 3-AP consists of either 1 element (when it is trivial) or 3 elements (when it is non-trivial).

Definition 3.1.1. Let G be a finite abelian group. We say that $\{a, b, c\} \subseteq G$ is a *3-AP* when $a + c = 2b$. If a, b and c are all distinct, we say that $\{a, b, c\}$ is a *true 3-AP*.

Remark that in the above definition, requiring a, b and c to be all distinct is equivalent to requiring $a \neq c$.

We also need to redefine $D(G)$ to address the subtlety of 3-APs in groups with even order.

Definition 3.1.2. Let $A \subseteq G$ be free of true 3-APs, i.e. if $\{a, b, c\} \subseteq A$ with $a + c = 2b$, then $a = c$. We denote the set of all such $A \subseteq G$ by $PF[G]$ (progression free subsets of G). Then

$$D(G) = \sup_{A \subseteq G, A \in PF[G]} |A|.$$

Definition 3.1.3. For $n \in \mathbb{N}$ define

$$d(n) = \sup_{c(2G) \geq n} \frac{D(G)}{|G|}.$$

Lev's generalization of Meshulam's result is below.

Theorem 3.1.1. *Let G be a finite abelian group so that the group $2G = \{g + g : g \in G\}$ is non-trivial. Then we have that*

$$D(G) \leq \frac{2|G|}{c(2G)}.$$

Note that Theorem 3.1.1 is equivalent to

$$d(n) \leq \frac{2}{n}.$$

When G has odd order, $2G = G$ and thus $c(2G) = c(G)$. The result of Theorem 3.1.1 reduces to $D(G) < \frac{2|G|}{c(G)}$, which is exactly Meshulam's result.

3.2 Proof of Lev's Result

The proof of Theorem 3.1.1 is inductive on $c(2G)$. The base case is trivial, since when $c(2G) = 1$ we require that $D(G) < 2|G|$ which always holds since $D(G) \leq |G|$ for all G. Fix a finite abelian group G and suppose that $c(2G) = n \geq 2$, and that $A \subseteq G$ is free of true 3-APs. Showing that $|A| \leq \frac{2|G|}{n}$ is enough to prove Theorem 3.1.1.

Let G be in the canonical form for finite abelian groups. As such, G can be expressed as

$$G = \mathbb{Z}_{k_1} \oplus \mathbb{Z}_{k_2} \oplus \cdots \oplus \mathbb{Z}_{k_r}$$

with $k_i \in \mathbb{N}$ for each $i \in \{1, \ldots, r\}$ and $k_{i-1} | k_i$ for each $i \in \{2, \ldots, r\}$. Since $n \leq c(2G) \leq c(G) = r$, we have $r \geq n$.

Let $\phi : G \to 2G$ with $\phi(g) = 2g$. We let G_0 denote $\ker \phi = \{g \in G : 2g = 0\}$, so that $G/G_0 \cong 2G$. Let $s := |G_0|$ and $t := |2G|$ so that $st = |G|$. Let

$$G/G_0 = \{x_1 + G_0, x_2 + G_0, \ldots, x_t + G_0\}.$$

For each $1 \leq i \leq t$, let

$$n_i = \big|\{a \in A : a - x_i \in G_0\}\big|$$

so that $0 \leq n_i \leq |G_0|$ for each $1 \leq i \leq t$ and $|A| = n_1 + n_2 + \cdots + n_t$.

Recall from the previous chapter that for $\gamma \in \widehat{G}$,

$$\widehat{\chi_A}(\gamma) = \sum_{x \in G} \chi_A(x)\overline{\gamma}(x) = \sum_{a \in A} \overline{\gamma}(a).$$

It is useful to note that

$$|\widehat{\chi_A}(\gamma)|^2 \;=\; \sum_{a,b \in A} \overline{\gamma}(a)\gamma(b).$$

Since γ is in the dual group, it holds that $\overline{\gamma}(x) = \gamma(-x)$ and $\gamma(c+d) = \gamma(c)\gamma(d)$. Therefore

$$|\widehat{\chi_A}(\gamma)|^2 = \sum_{a,b \in A} \gamma(-a)\gamma(b) = \sum_{a,b \in A} \gamma(b-a). \tag{3.1}$$

Lemma 2. *We have*

$$\sum_{\gamma \in \widehat{G}} (\widehat{\chi_A}(\gamma))^2 \widehat{\chi_A}(\overline{\gamma}^2) \leq |G||A||G_0|.$$

Proof. Since γ is in the dual group

$$(\widehat{\chi_A}(\gamma))^2 = \left(\sum_{a \in A} \overline{\gamma}(a)\right)\left(\sum_{c \in A} \overline{\gamma}(c)\right) = \left(\sum_{a \in A} \gamma(-a)\right)\left(\sum_{c \in A} \gamma(-c)\right) = \sum_{a,c \in A} \gamma(-a-c).$$

It follows that

$$\begin{aligned}
\sum_{\gamma \in \widehat{G}} (\widehat{\chi_A}(\gamma))^2 \widehat{\chi_A}(\overline{\gamma}^2) &= \sum_{\gamma \in \widehat{G}} \left(\sum_{a,c \in A} \gamma(-a-c)\right)\left(\sum_{b \in A} \gamma^2(b)\right) \\
&= \sum_{\gamma \in \widehat{G}} \sum_{a,b,c \in A} \gamma(-a-c+2b) \\
&= \sum_{a,b,c \in A} \sum_{\gamma \in \widehat{G}} \gamma(-a-c+2b).
\end{aligned}$$

By Proposition 1.2.3 (2), we have that for fixed $a, b, c \in A$

$$\sum_{\gamma \in \widehat{G}} \gamma(-a-c+2b) = \begin{cases} |G|, & \text{if } -a-c+2b=0, \\ 0, & \text{otherwise.} \end{cases}$$

Therefore

$$\sum_{\gamma \in \widehat{G}} (\widehat{\chi_A}(\gamma))^2 \widehat{\chi_A}(\overline{\gamma}^2) = |G| \# \{(a,b,c) \in A^3 : a+c=2b\}.$$

Since $A \in PF[G], a = c$ and

$$\begin{aligned} \sum_{\gamma \in \widehat{G}} (\widehat{\chi_A}(\gamma))^2 \widehat{\chi_A}(\overline{\gamma}^2) &= |G| \# \{(a,b,c) \in A^3 : 2a=2b\} \\ &= |G| \# \{(a,b) \in A^2 : a-b \in G_0\}. \end{aligned}$$

Without loss of generality assume that $a \in x_1 + G_0$. This gives us n_1 ways to pick $a \in A$. Since we require that $a - b \in G_0$, we also have $b \in x_1 + G_0$. As such, there are n_1 ways to pick $b \in A$ once we have chosen a. There are n_1^2 ways to choose $(a,b) \in A^2$ with $a - b \in G_0$ and $a \in x_1 + G_0$. Similarly, there are n_i^2 ways to choose $(a,b) \in A^2$ with $a - b \in G_0$ and $a \in x_i + G_0$ for each $1 \leq i \leq t$. Since $|A| = n_1 + \cdots + n_t$ and $n_i \leq |G_0|$ for each $i \in \{1, \ldots, t\}$, this means

$$\begin{aligned} \sum_{\gamma \in \widehat{G}} (\widehat{\chi_A}(\gamma))^2 \widehat{\chi_A}(\overline{\gamma}^2) &= |G|(n_1^2 + n_2^2 + \cdots + n_t^2) \\ &\leq |G|(n_1 + n_2 + \cdots + n_t) \max_{1 \leq i \leq t} n_i \\ &\leq |G||A||G_0|. \end{aligned}$$

□

A character γ is called a *real character* if $\gamma(x) \in \mathbb{R}$ for each $x \in G$, and $\overline{\gamma} = \gamma$. We now split up the sum in Lemma 2 according to whether or not γ is a real character. We note that since $|\gamma(x)| = 1$ for each $x \in G$, if γ is a real character then $\gamma(x) \in \{1, -1\}$ for each $x \in G$, so that γ is a real character if and only if $\gamma^2 = e$.

Lemma 3. *Let*

$$S := \sum_{\gamma \in \widehat{G}, \gamma^2 = e} (\widehat{\chi_A}(\gamma))^2$$

and let

$$M := \max_{\gamma \in \widehat{G}, \gamma^2 \neq e} |\widehat{\chi_A}(\overline{\gamma}^2)|.$$

Then

$$|A|S - |G||A||G_0| \leq M(|A||G| - S).$$

Proof. The inequality from Lemma 2 can be written as

$$\sum_{\gamma \in \widehat{G}, \gamma^2 = e} (\widehat{\chi_A}(\gamma))^2 \widehat{\chi_A}(\overline{\gamma}^2) + \sum_{\gamma \in \widehat{G}, \gamma^2 \neq e} (\widehat{\chi_A}(\gamma))^2 \widehat{\chi_A}(\overline{\gamma}^2) \leq |G||A||G_0|,$$

which implies that

$$- \sum_{\gamma \in \widehat{G}, \gamma^2 \neq e} (\widehat{\chi_A}(\gamma))^2 \widehat{\chi_A}(\overline{\gamma}^2) \geq \sum_{\gamma \in \widehat{G}, \gamma^2 = e} (\widehat{\chi_A}(\gamma))^2 \widehat{\chi_A}(\overline{\gamma}^2) - |G||A||G_0|.$$

When $\gamma^2 = e$,

$$\widehat{\chi_A}(\overline{\gamma}^2) = \sum_{a \in A} 1 = |A|,$$

so that

$$\begin{aligned} - \sum_{\gamma \in \widehat{G}, \gamma^2 \neq e} (\widehat{\chi_A}(\gamma))^2 \widehat{\chi_A}(\overline{\gamma}^2) &\geq |A| \sum_{\gamma \in \widehat{G}, \gamma^2 = e} (\widehat{\chi_A}(\gamma))^2 - |G||A||G_0| \\ &= |A|S - |G||A||G_0|. \end{aligned}$$

We have

$$\begin{aligned} |A|S - |G||A||G_0| &\leq - \sum_{\gamma \in \widehat{G}, \gamma^2 \neq e} (\widehat{\chi_A}(\gamma))^2 \widehat{\chi_A}(\overline{\gamma}^2) \\ &\leq \left| \sum_{\gamma \in \widehat{G}, \gamma^2 \neq e} (\widehat{\chi_A}(\gamma))^2 \widehat{\chi_A}(\overline{\gamma}^2) \right| \\ &\leq \sum_{\gamma \in \widehat{G}, \gamma^2 \neq e} |(\widehat{\chi_A}(\gamma))|^2 |\widehat{\chi_A}(\overline{\gamma}^2)| \\ &\leq M \sum_{\gamma \in \widehat{G}, \gamma^2 \neq e} |(\widehat{\chi_A}(\gamma))|^2. \end{aligned}$$

When γ is a real character, we see that

$$\widehat{\chi_A}(\gamma) = \sum_{a \in A} \overline{\gamma}(a)$$

is a real number since it is a sum consisting of 1s and -1s. As such $\widehat{\chi_A}(\gamma)^2 = |\widehat{\chi_A}(\gamma)|^2$, and

$$S = \sum_{\gamma \in \widehat{G}, \gamma^2 = e} (\widehat{\chi_A}(\gamma))^2 = \sum_{\gamma \in \widehat{G}, \gamma^2 = e} |(\widehat{\chi_A}(\gamma))|^2.$$

This means that

$$|A|S - |G||A||G_0| \leq M \left(\sum_{\gamma \in \widehat{G}} |(\widehat{\chi_A}(\gamma))|^2 - S \right).$$

By Proposition 1.2.5, we have

$$\sum_{\gamma \in \widehat{G}} |(\widehat{\chi_A}(\gamma))|^2 = |G| \sum_{x \in G} \chi_A(x) = |G||A|.$$

We can conclude that

$$|A|S - |G||A||G_0| \leq M(|A||G| - S).$$

□

By the definition of M, there exists a character γ_0 with $\gamma_0^2 \neq e$ and $M = |\widehat{\chi_A}(\overline{\gamma_0}^2)|$. The kernel of γ_0^2 is a subgroup of G that we will call W, i.e.

$$W = \{g \in G : \gamma_0^2(g) = 1\}.$$

We wish to calculate

$$\widehat{\chi_A}(\overline{\gamma_0}^2) = \sum_{a \in A} \gamma_0^2(a).$$

For $a \in A$ and $g \in G$, notice that $\gamma_0^2(g) = \gamma_0^2(a)$ if and only if $a - g \in W$. Therefore $g \in G$ is counted for each $a \in A$ in the same coset as g. For a fixed $a \in A$, the number of $g \in G$ with $a - g \in W$ is $|W|$. Therefore

$$\begin{aligned} \sum_{a \in A} \gamma_0^2(a) &= \sum_{a \in A} \sum_{\substack{g \in G \\ a-g \in W}} \frac{\gamma_0^2(g)}{|W|} \\ &= \frac{1}{|W|} \sum_{g \in G} \sum_{\substack{a \in A \\ a-g \in W}} \gamma_0^2(g) \\ &= \frac{1}{|W|} \sum_{g \in G} \gamma_0^2(g) |(A - g) \cap W|. \end{aligned}$$

Since $\gamma_0^2 \neq e$, By Proposition 1.2.3 (1), we have

$$0 = \frac{D(W)}{|W|} \sum_{g \in G} \gamma_0^2(g).$$

It follows that

$$\frac{1}{|W|} \sum_{g \in G} \gamma_0^2(g) |(A-g) \cap W| = \frac{1}{|W|} \sum_{g \in G} (-\gamma_0^2(g))(D(W) - |(A-g) \cap W|).$$

Thus, we have

$$\widehat{\chi_A}(\overline{\gamma_0}^2) = \frac{1}{|W|} \sum_{g \in G} (-\gamma_0^2(g))(D(W) - |(A-g) \cap W|).$$

Suppose that $\{x, y, z\}$ is a 3-AP inside of $(A-g) \cap W$. Then $\{x+g, y+g, z+g\}$ is a 3-AP inside of A. Since A contains no true 3-AP, $x = z$ and $(A-g) \cap W$ is free of true 3-APs. Therefore $D(W) - |(A-g) \cap W| \geq 0$ for each $g \in G$. We have

$$M = |\widehat{\chi_A}(\overline{\gamma_0}^2)| = \left| \frac{1}{|W|} \sum_{g \in G} (-\gamma_0^2(g))(D(W) - |(A-g) \cap W|) \right|$$

so that

$$\begin{aligned} M &\leq \frac{1}{|W|} \sum_{g \in G} |(-\gamma_0^2(g))(D(W) - |(A-g) \cap W|)| \\ &= \frac{1}{|W|} \sum_{g \in G} D(W) - |(A-g) \cap W| \\ &= \frac{D(W)}{|W|} |G| - \frac{1}{|W|} \sum_{g \in G} |(A-g) \cap W|. \end{aligned}$$

Notice that for a fixed $g \in G$,

$$|(A-g) \cap W| = \#\{(a, w) \in A \times W : g = a - w\}.$$

We have

$$\sum_{g \in G} |(A-g) \cap W| = \sum_{g \in G} \#\{(a, w) \in A \times W : g = a - w\}| = |A||W|.$$

Therefore

$$\frac{1}{|W|}\sum_{g\in G}|(A-g)\cap W| = |A|.$$

If we let $k = D(W)/|W|$, we have

$$M \leq k|G| - |A|.$$

Combining the above inequality with Lemma 3, we see that

$$|A|S - |G||A||G_0| \leq (|A||G| - S)(k|G| - |A|) = k|A||G|^2 - |A|^2|G| - Sk|G| + |A|S.$$

Rearranging terms and dividing by $|G|$ results in

$$Sk + |A|^2 \leq k|A||G| + |G_0||A|. \tag{3.2}$$

Lemma 4. *Let S be defined as in Lemma 3. We have*

$$S \geq |A|^2.$$

Proof. Recall that $G/2G \cong G_0$, and $|G_0| = s$. Write

$$G_0 \cong G/2G = \{y_1 + 2G, y_2 + 2G, \ldots, y_s + 2G\}.$$

Let

$$m_i = \big|\{a \in A : a - y_i \in 2G\}\big|$$

so that $m_i \leq |2G| = t$ and $|A| = m_1 + m_2 + \cdots + m_s$. It is useful to note that for $\gamma \in \widehat{G}$ with $\gamma^2 = e$, $|\widehat{\chi_A}(\gamma)|^2 = (\widehat{\chi_A}(\gamma))^2$. This holds since $\gamma(a)$ is real for each $a \in A$.

By Proposition 1.2.3 we have

$$\begin{aligned} S &= \sum_{\gamma\in\widehat{G}}\left(\frac{1}{|G|}\sum_{g\in G}\gamma^2(g)\right)|\widehat{\chi_A}(\gamma)|^2 \\ &= \frac{1}{|G|}\sum_{g\in G}\sum_{\gamma\in\widehat{G}}\gamma^2(g)|\widehat{\chi_A}(\gamma)|^2. \end{aligned}$$

For a fixed $g \in G$, consider the above inner sum. By (3.1), we have

$$\begin{aligned}\sum_{\gamma\in\widehat{G}}\gamma^2(g)|\widehat{\chi_A}(\gamma)|^2 &= \sum_{\gamma\in\widehat{G}}\gamma^2(g)\sum_{a,b\in A}\gamma(b-a)\\ &= \sum_{a,b\in A}\sum_{\gamma\in\widehat{G}}\gamma(2g+b-a).\end{aligned}$$

By Proposition 1.2.3,

$$\sum_{\gamma\in\widehat{G}}\gamma(2g+b-a)=\begin{cases}|G|, & \text{if } 2g=a-b,\\ 0, & \text{otherwise.}\end{cases}$$

Therefore

$$\sum_{a,b\in A}\sum_{\gamma\in\widehat{G}}\gamma(2g+b-a)=|G|\#\{(a,b)\in A^2 : a-b=2g\}.$$

Putting it together

$$\begin{aligned}S &= \frac{1}{|G|}\sum_{g\in G}\sum_{\gamma\in\widehat{G}}\gamma^2(g)|\widehat{\chi_A}(\gamma)|^2\\ &= \frac{1}{|G|}\sum_{g\in G}\sum_{a,b\in A}\sum_{\gamma\in\widehat{G}}\gamma(2g+b-a)\\ &= \sum_{g\in G}\#\{(a,b)\in A^2 : a-b=2g\}.\end{aligned}$$

Given a pair $(a,b)\in A^2$, it is counted in $\#\{(a,b)\in A^2 : a-b=2g\}$ if and only if $a-b\in 2G$. When $a-b\in 2G$, since $G/2G\cong G_0$, there are $|G_0|$ different $g\in G$ with $a-b=2g$. Therefore each pair $(a,b)\in A^2$ which is counted in the above sum is counted $|G_0|$ times, giving us

$$S=|G_0|\#\{(a,b)\in A^2 : a-b\in 2G\}.$$

Recall we had

$$G_0\cong G/2G=\{y_1+2G, y_2+2G,\ldots,y_s+2G\}$$

and $m_i=|\{a\in A : a-y_i\in 2G\}|$. To calculate $\#\{(a,b)\in A^2 : a-b\in 2G\}$ suppose, without loss of generality, that $a-y_1\in 2G$. We must also have that $b-y_1\in 2G$. There are m_1 ways to choose such an $a\in A$ and m_1 ways to choose such a $b\in A$. As such, there are m_1^2 pairs $(a,b)\in A^2$ with $b-a\in 2G$ and $a-y_1\in 2G$. Similarly, there are m_i^2 pairs

$(a,b) \in A^2$ with $a - b \in 2G$ and $a - y_i \in 2G$ for $i \in \{1, \ldots, s\}$. We have

$$\begin{aligned} S &= |G_0|(m_1^2 + m_2^2 + \cdots + m_s^2) \\ &\geq |G_0|\frac{1}{s}\left(\sum_{i=1}^{s} m_i\right)^2 \\ &= |A|^2 \end{aligned}$$

since $|G_0| = s$ and $|A| = m_1 + \cdots + m_s$. This completes our proof. □

By Lemma 4 and (3.2),we see that

$$k|A|^2 + |A|^2 \leq |A||G_0| + k|A||G|,$$

which in turn reduces to

$$|A| \leq k(|G| - |A|) + |G_0|.$$

Now it is time to apply the induction hypothesis to find an upper bound on $k = \frac{D(W)}{|W|}$. For a function f defined on a set X, and $Y \subseteq X$ a subset, we let $f|_Y$ denote the restriction of f to Y. Recall that W was chosen as the kernel of γ_0^2. Let $\gamma_1 = \gamma_0|_{2G} \in \widehat{2G}$. Since γ_1 is in the dual group of $2G$, we have $|\gamma_1| = 1$ which means that the image of γ_1 is a subgroup of the multiplicative group of the field of complex numbers. Since $G = \mathbb{Z}_{k_1} \oplus \mathbb{Z}_{k_2} \oplus \cdots \oplus \mathbb{Z}_{k_r}$ with $k_i | k_r$ for each $1 \leq i \leq r$, it must hold that the image of γ_0 consists of k_r^{th} roots of unity. The image of γ_1 is a subgroup of the image of γ_0, so it too is a cyclic group. Since $\gamma_0^2 \neq e$, the image of γ_1 is non-trivial. Note that

$$\gamma_1(2g) = 0 \iff \gamma_0(2g) = 0 \iff \gamma_0^2(g) = 0.$$

We defined W as the kernel of γ_0^2. Thus

$$\gamma_1(2g) = 0 \iff g \in W \iff 2g \in 2W$$

and $\ker(\gamma_1) = 2W$. Therefore $\mathrm{im}(\gamma_1) \cong 2G/2W$ means that $2G/2W$ is either cyclic or trivial. As such, $2G$ has one more component than $2W$, so that $c(2W) \geq n - 1$. By the induction hypothesis $k = D(W)/|W| \leq d(n-1) \leq 2/(n-1)$. We have

$$\begin{aligned} |A| &\leq k(|G| - |A|) + |G_0| \\ &\leq \frac{2|G|}{n-1} - \frac{2|A|}{n-1} + |G_0|. \end{aligned}$$

We use this to bound $|A|$ so that

$$|A| \leq \frac{|G|}{1+\frac{2}{n-1}} \left(\frac{2}{n-1} + \frac{|G_0|}{|G|} \right).$$

We now need to consider the size of $|G_0|/|G|$. Recall that $G_0 = \{x \in G : 2x = 0\}$, and also that

$$G = \mathbb{Z}_{k_1} \oplus \mathbb{Z}_{k_2} \oplus \cdots \oplus \mathbb{Z}_{k_r}$$

with $k_{i-1}|k_i$ for each $2 \leq i \leq r$. Let $l = \max\{i \in \{1, \ldots, r-1\} : k_i = 2\}$. If $k_i \geq 3$ for each $1 \leq i \leq r$ then we let $l = 0$. Let

$$G_1 = \bigoplus_{i=1}^{l} \mathbb{Z}_{k_i} \quad \text{and} \quad G_2 = \bigoplus_{i=l+1}^{r} \mathbb{Z}_{k_i}$$

so that $G = G_1 \oplus G_2$. It holds that $c(2G) = c(G_2)$.

Our proof now splits in two cases. In the first case, $G_1 = \emptyset$, so that $c(2G) = c(G_2) = c(G) \geq n$. We have

$$\frac{|G_0|}{|G|} = \frac{1}{|2G|} = \prod_{i \in [1,r]: k_i \text{ is odd}} \frac{1}{k_i} \prod_{i \in [1,r]: k_i \text{ is even}} \frac{2}{k_i} \leq \frac{1}{2^r} \leq \frac{1}{2^n} < \frac{2}{n(n-1)}.$$

Note that we require $G_2 = G$ for the first inequality: Since each even k_i satisfies $k_i \geq 4$ if and only if $G_2 = G$, it is certain that $\frac{2}{k_i} \leq \frac{1}{2}$. This upper bound on $\frac{|G_0|}{|G|}$ means that

$$|A| \leq \frac{|G|}{1+\frac{2}{n-1}} \left(\frac{2}{n-1} + \frac{2}{n(n-1)} \right) = \frac{|G|(n-1)}{n+1} \cdot \frac{2}{n-1} \cdot \frac{n+1}{n} = \frac{2|G|}{n}.$$

For the second case assume that G_1 is non-empty, and suppose that $B \subseteq G$ with $|B| > |G_1|D(G_2)$. We claim that $B \in PF[G]$. Consider the elements of B inside the quotient group $G/G_2 \cong G_1$. There exists some coset $g_0 + G_2$ so that $|B \cap (g_0 + G_2)| > D(G_2)$. This is true since there are $|G_1|$ cosets in G/G_2, and assuming that $|B \cap (g + G_2)| \leq D(G_2)$ for each coset $g + G_2$ means that $|B| \leq |G_1|D(G_2)$, producing a contradiction.

Given that

$$|(B - g_0) \cap G_2| = |B \cap (g_0 + G_2)| > D(G_2),$$

there exists a true 3-AP inside of $(B - g_0) \cap G_2$, say $\{b_1 - g_0, b_2 - g_0, b_3 - g_0\}$ with each element distinct and $b_1 - g_0 + b_3 - g_0 = 2(b_2 - g_0)$. Then $\{b_1, b_2, b_3\}$ is a true 3-AP in B. Since B was chosen arbitrarily as a subset greater than $|G_1|D(G_2)$, we have $D(G) \leq |G_1|D(G_2)$. Notice that G_2 was chosen so that $c(2G_2) = c(G_2) = c(2G) \geq n$, so as a group G_2 falls

into the first case from above, i.e. we have $D(G_2) \leq 2|G_2|/n$. Since $|G| = |G_1||G_2|$,

$$D(G) \leq |G_1|D(G_2) < |G_1|\frac{2|G_2|}{n} = \frac{2|G|}{n}$$

as desired. This completes the proof of Lev's result. Recall that with Meshulam's result, we were able to produce Corollary 2.3.2 which gave a bound for $D(G)$ depending only on $|G|$ where G is a finite abelian group of odd order. The following Corollary uses Lev's result to achieve the same bound for a larger class of finite abelian groups. The proof is similar to the one outlined for Corollary 2.3.2. We simply modify the first case by using Theorem 3.1.1 instead of Theorem 2.1.1.

Corollary 3.2.1. *Let G be a finite abelian group so that $c(G) = c(2G)$, and let $D(G)$ denote the largest cardinality of a subset which contains no non-trivial three term arithmetic progressions. It holds that*

$$D(G) = O\left(\frac{|G|(\log\log|G|)^{\frac{5}{2}}}{(\log|G|)^{\frac{1}{2}}}\right).$$

Chapter 4

Solutions to Linear Equations on Finite Abelian Groups

4.1 Introduction

In the two previous chapters we outlined results by Meshulam and Lev which bounded the size of subsets that are free of 3-APs. In 2009 Liu and Spencer [6] generalized Meshulam's result to subsets which contain no trivial solutions to a linear equation.

Let $s \in \mathbb{N}$ with $s \geq 3$. Let $\mathbf{r} = (r_1, r_2, \ldots, r_s) \in (\mathbb{Z} \setminus \{0\})^s$ be a vector satisfying $r_1 + r_2 + \cdots + r_s = 0$. Given a finite abelian group G,

$$G \cong \mathbb{Z}_{k_1} \oplus \mathbb{Z}_{k_2} \oplus \cdots \oplus \mathbb{Z}_{k_n}$$

with $k_i \in \{2, 3, \ldots\}$ for each $i \in \{1, \ldots, n\}$ and $k_i | k_{i+1}$ for $i \in \{1, \ldots, n-1\}$. We say G has n constituents, and denote this by $c(G) = n$. We let $|G|$ denote the cardinality of G.

Definition 4.1.1. Let $\mathbf{r}$ and G be defined as above. We say that G is *coprime* to $\mathbf{r}$ if $\gcd(r_i, |G|) = 1$ for each $i \in \{1, \ldots, s\}$.

Definition 4.1.2. Let $\mathbf{x} = (x_1, \ldots, x_s) \in G^s$. We say $\mathbf{x}$ is a *solution* to $\mathbf{r}$ if $r_1 x_1 + \cdots r_s x_s = 0$. A solution $\mathbf{x} \in G^s$ is *trivial* if there is some subset $\{j_1, \ldots, j_l\} \subseteq \{1, \ldots, s\}$ with $x_{j_1} = \cdots = x_{j_l}$ and $r_{j_1} + \cdots + r_{j_l} = 0$. Otherwise we say a solution $\mathbf{x} \in G^s$ is *non-trivial*.

Definition 4.1.3. Let $\mathbf{r}$ and G be defined as above, with G coprime to $\mathbf{r}$, and let $A \subseteq G$. If every solution $\mathbf{x} \in A^s$ is trivial, we say that A is free of non-trivial solutions and write $A \in NTSF_{\mathbf{r}}$ (non-trivial solution free subsets). Define

$$D_{\mathbf{r}}(G) = \max_{\substack{A \subseteq G \\ A \in NTSF_{\mathbf{r}}}} |A|$$

and

$$d_{\mathbf{r}}(n) = \sup_{\substack{G \text{ coprime to } \mathbf{r} \\ c(G) \geq n}} \frac{D_{\mathbf{r}}(G)}{|G|}.$$

For simplicity we write $D(G)$ for $D_{\mathbf{r}}(G)$ and $d(n)$ for $d_{\mathbf{r}}(n)$ when $\mathbf{r}$ is clear from the context.

Theorem 4.1.1. *Let $\mathbf{r} = (r_1, \dots, r_s) \in (\mathbb{Z} \setminus \{0\})^s$ so that $r_1 + \cdots + r_s = 0$. Then there exists a constant $C = C(\mathbf{r}) > 0$ such that*

$$d_{\mathbf{r}}(n) \leq \frac{C(\mathbf{r})^{s-2}}{n^{s-2}}.$$

4.2 Preliminaries

Fix $\mathbf{r} \in (\mathbb{Z} \setminus \{0\})^s$ with $r_1 + \cdots + r_s = 0$, let $n \in \mathbb{N}$, and fix a finite abelian group G that is coprime to $\mathbf{r}$ with $c(G) \geq n$. Fix $A \subseteq G$ so that A is free of non-trivial solutions to $\mathbf{r}$. We let $T(A)$ denote the number of solutions to $\mathbf{r}$ inside A. Let $r_i A = \{r_i a : a \in A\}$ and

$$\chi_{r_i A}(x) = \begin{cases} 1, & \text{if } x \in r_i A, \\ 0, & \text{otherwise.} \end{cases}$$

By Proposition 1.2.3,

$$\begin{aligned} \sum_{\gamma \in \widehat{G}} \widehat{\chi_{r_1 A}}(\gamma)\widehat{\chi_{r_2 A}}(\gamma) \cdots \widehat{\chi_{r_s A}}(\gamma) &= \sum_{\gamma \in \widehat{G}} \left(\sum_{x \in A} \gamma(-r_1 x) \right) \left(\sum_{x \in A} \gamma(-r_2 x) \right) \cdots \left(\sum_{x \in A} \gamma(-r_s x) \right) \\ &= \sum_{x_1 \in A} \sum_{x_2 \in A} \cdots \sum_{x_s \in A} \sum_{\gamma \in \widehat{G}} \gamma(-(r_1 x_1 + r_2 x_2 + \cdots + r_s x_s)) \\ &= |G| T(A). \end{aligned}$$

Recall from previous chapters that

$$\delta(\gamma) = \begin{cases} 1, & \text{if } \gamma = e, \\ 0, & \text{otherwise.} \end{cases}$$

Lemma 5. *Let G be a finite abelian group coprime to $\mathbf{r}$ with $c(G) \geq n$. Suppose that $A \subseteq G$ contains no non-trivial solutions to $\mathbf{r}$. Let $W \subseteq G$ be a subgroup. Then for each $i \in \{1, \dots, s\}$ and for each $x \in G$, $W \cap (x - r_i A)$ contains no non-trivial solutions to $\mathbf{r}$, so that*

$$|W \cap (x - r_i A)| \leq D(W).$$

Proof. First note that since $W \subseteq G$ is a subgroup of G, we have that $|W|$ divides $|G|$. Since $\gcd(r_i, |G|) = 1$ for each $i \in \{1, \ldots, s\}$, it follows that $\gcd(r_i, |W|) = 1$ for each $i \in \{1, \ldots, s\}$, and W is coprime to $\mathbf{r}$. As such, $D(W) = D_{\mathbf{r}}(W)$ is indeed well defined.

Consider a solution $(w_1, \ldots, w_s) = (x - r_i a_1, x - r_i a_2, \ldots, x - r_i a_s)$ so that

$$\begin{aligned} 0 &= r_1(x - r_i a_1) + r_2(x - r_i a_2) + \cdots + r_s(x - r_i a_s) \\ &= x(r_1 + r_2 + \cdots + r_s) - r_i(r_1 a_1 + r_2 a_2 + \cdots + r_s a_s). \end{aligned}$$

Recall that $r_1 + r_2 + \cdots + r_s = 0$, so that the above equation reduces to

$$0 = r_i(r_1 a_1 + r_2 a_2 + \cdots + r_s a_s).$$

Here we use the fact that G is coprime to $\mathbf{r}$, (note that the 0 above is $0 \in G$, not $0 \in \mathbb{Z}$). Since $|G|$ is coprime to r_i for each $i \in \{1, \ldots, s\}$, G contains no elements of order r_i except 0. Therefore $r_1 a_1 + r_2 a_2 + \cdots + r_s a_s = 0$, which means that $(a_1, a_2, \ldots, a_s)$ is a solution to $\mathbf{r}$. We chose A so that it only contains trivial solutions to $\mathbf{r}$. As such, $(w_1, \ldots, w_s) = (x - r_i a_1, x - r_i a_2, \ldots, x - r_i a_s)$ is also a trivial solution. Since $(w_1, \ldots, w_s)$ was chosen arbitrarily, we know that $W \cap (x - r_i A) \subseteq W$ contains no non-trivial solutions to $\mathbf{r}$. □

Lemma 6. *Let G be a finite abelian group coprime to $\mathbf{r}$ with $c(G) \geq n$. Suppose that $A \subseteq G$ contains no non-trivial solutions to $\mathbf{r}$. Then for each $i \in \{1, \ldots, s\}$,*

$$\sup_{\gamma \in \widehat{G}} ||G| d(n-1)\delta(\gamma) - \widehat{\chi_{r_i A}}(\gamma)| = d(n-1)|G| - |A|.$$

In particular, since $|G| d(n-1)\delta(\gamma) = 0$ when $\gamma \neq e$, it follows that

$$\sup_{\gamma \neq e} |\widehat{\chi_{r_i A}}(\gamma)| = d(n-1)|G| - |A|.$$

Proof. Let $\gamma \in \widehat{G}$ and let $W = \ker(\gamma)$. Since $\gamma(G)$ is a cyclic group and $\gamma(G) \cong G/W$, we have that $c(W) \geq c(G) - 1 \geq n - 1$. Note that

$$|W| \left| |G| d(n-1)\delta(\gamma) - \widehat{\chi_{r_i A}}(\gamma) \right| = \left| \sum_{y \in W} \sum_{x \in G} d(n-1)\gamma(-x) - \sum_{y \in W} \sum_{x \in G} \chi_{r_i A}(x)\gamma(-x) \right|.$$

For any $y \in W = \ker(\gamma)$, we have $\gamma(-x) = \gamma(-x - y)$, and

$$\sum_{x \in G} \chi_{r_i A}(x)\gamma(-x) = \sum_{x \in G} \chi_{r_i A}(x)\gamma(-x - y) = \sum_{x \in G} \chi_{r_i A}(x - y)\gamma(-x).$$

Therefore

$$\begin{aligned} |W|\big||G|d(n-1)\delta(\gamma) - \widehat{\chi_{r_iA}}(\gamma)\big| &= \left|\sum_{x\in G}\left(\sum_{y\in W} d(n-1) - \sum_{y\in W}\chi_{r_iA}(x-y)\right)\gamma(-x)\right| \\ &\leq \sum_{x\in G}\left|\sum_{y\in W} d(n-1) - \sum_{y\in W}\chi_{r_iA}(x-y)\right|. \end{aligned}$$

Since

$$\chi_{r_iA}(x-y) = \begin{cases} 1, & \text{if } x-y \in r_iA, \\ 0, & \text{otherwise,} \end{cases}$$

we have that

$$\sum_{y\in W}\chi_{r_iA}(x-y) = |(x-W)\cap r_iA| = |W\cap(x-r_iA)|.$$

By Proposition 1.2.3, it holds that $W\cap(x-r_iA)\subseteq W$ contains no non-trivial solutions to $\mathbf{r}$. By the definition of $d(n-1)$,

$$d(n-1) \geq \frac{|W\cap(x-r_iA)|}{|W|}$$

and

$$\begin{aligned} |W|\big||G|d(n-1)\delta(\gamma) - \widehat{\chi_{r_iA}}(\gamma)\big| &\leq \sum_{x\in G}\left|\sum_{y\in W} d(n-1) - \sum_{y\in W}\chi_{r_iA}(x-y)\right|. \\ &= \sum_{x\in G}||W|d(n-1) - |W\cap(x-r_iA)|| \\ &= \sum_{x\in G}|W|d(n-1) - |W\cap(x-r_iA)|. \end{aligned}$$

To compute $\sum_{x\in G}|W\cap(x-r_iA)|$ notice that for a fixed $r_ia\in r_iA$, there are $|W|$ different $x\in G$ with $x-r_ia\in W$. Since G is coprime to $\mathbf{r}$, the function $g\mapsto r_ig$ is a bijection on G and $r_iG=G$, with $|r_iA|=|A|$ for any subset $A\subseteq G$. Therefore

$$\sum_{x\in G}|W\cap(x-r_iA)| = |r_iA||W| = |A||W|.$$

It holds that

$$\sum_{x\in G}|W|d(n-1) = |G||W|d(n-1),$$

which results in

$$|W|\big||G|d(n-1)\delta(\gamma) - \widehat{\chi_{r_iA}}(\gamma)\big| \leq |G||W|d(n-1) - |A||W|.$$

Therefore, for each $\gamma \in \widehat{G}$,

$$\big||G|d(n-1)\delta(\gamma) - \widehat{\chi_{r_iA}}(\gamma)\big| \leq |G|d(n-1) - |A|,$$

so that

$$\sup_{\gamma\in\widehat{G}} ||G|d(n-1)\delta(\gamma) - \widehat{\chi_{r_iA}}(\gamma)| \leq d(n-1)|G| - |A|.$$

Equality holds since

$$\begin{aligned}\big||G|d(n-1)\delta(e) - \widehat{\chi_{r_iA}}(e)\big| &= |G|d(n-1) - \sum_{x\in r_iA} 1 \\ &= |G|d(n-1) - |A|.\end{aligned}$$

This concludes the proof. □

Lemma 7. *Let G be a finite abelian group coprime to $\mathbf{r}$ with $c(G) \geq n$. Suppose that $A \subseteq G$ contains no non-trivial solutions to $\mathbf{r}$. Let $B_{\mathbf{r}} = B$ denote the number of different subsets $\emptyset \neq \{r_{j_1}, \ldots, r_{j_l}\} \subseteq \{r_1, \ldots, r_s\}$ with $r_{j_1} + \cdots + r_{j_l} = 0$. Let $d^*(n) = d^*(n; A, G) = |A|/|G|$. Then*

$$d^*(n)^s - d^*(n)(d(n-1) - d^*(n))^{s-2} - \frac{Bd^*(n)^{s-2}}{|G|} \leq 0.$$

Proof. We saw in the beginning of this section that

$$\begin{aligned}|G|T(A) &= \sum_{\gamma\in\widehat{G}} \widehat{\chi_{r_1A}}(\gamma)\widehat{\chi_{r_2A}}(\gamma)\cdots\widehat{\chi_{r_sA}}(\gamma) \\ &= \widehat{\chi_{r_1A}}(e)\widehat{\chi_{r_2A}}(e)\cdots\widehat{\chi_{r_sA}}(e) + \sum_{\gamma\in\widehat{G},\gamma\neq e} \widehat{\chi_{r_1A}}(\gamma)\widehat{\chi_{r_2A}}(\gamma)\cdots\widehat{\chi_{r_sA}}(\gamma).\end{aligned}$$

For each $i \in \{1, \ldots, s\}$,

$$\widehat{\chi_{r_iA}}(e) = \sum_{x\in G} \chi_{r_iA}(x)e(-x) = \sum_{x\in r_iA} 1 = |r_iA| = |A|,$$

and we have

$$\widehat{\chi_{r_1A}}(e)\widehat{\chi_{r_2A}}(e)\cdots\widehat{\chi_{r_sA}}(e) = |A|^s = d^*(n)^s|G|^s.$$

By Cauchy's inequality,

$$\begin{aligned}
&\left|\sum_{\gamma\in\widehat{G},\gamma\neq e}\widehat{\chi_{r_1A}}(\gamma)\widehat{\chi_{r_2A}}(\gamma)\cdots\widehat{\chi_{r_sA}}(\gamma)\right| \\
&\leq \max_{\gamma\in\widehat{G},\gamma\neq e}|\widehat{\chi_{r_3A}}(\gamma)\cdots\widehat{\chi_{r_sA}}(\gamma)|\left(\sum_{\gamma\in\widehat{G},\gamma\neq e}\widehat{\chi_{r_1A}}(\gamma)\widehat{\chi_{r_2A}}(\gamma)\right) \\
&\leq \max_{\gamma\in\widehat{G},\gamma\neq e}|\widehat{\chi_{r_3A}}(\gamma)\cdots\widehat{\chi_{r_sA}}(\gamma)|\left(\sum_{\gamma\in\widehat{G},\gamma\neq e}|\widehat{\chi_{r_1A}}(\gamma)|^2\right)^{\frac{1}{2}}\left(\sum_{\gamma\in\widehat{G}}|\widehat{\chi_{r_2A}}(\gamma)|^2\right)^{\frac{1}{2}}.
\end{aligned}$$

By Proposition 1.2.5, for $i\in\{1,2\}$,

$$\sum_{\gamma\in\widehat{G},\gamma\neq e}|\widehat{\chi_{r_iA}}(\gamma)|^2\leq|G|\sum_{x\in G}|\chi_{r_iA}(x)|^2=|G|\sum_{x\in r_iA}1=|G||A|,$$

and by Lemma 6

$$\max_{\gamma\in\widehat{G},\gamma\neq e}|\widehat{\chi_{r_iA}}(\gamma)|\leq|G|d(n-1)-|A|.$$

It follows that

$$\begin{aligned}
\left|\sum_{\gamma\in\widehat{G},\gamma\neq e}\widehat{\chi_{r_1A}}(\gamma)\widehat{\chi_{r_2A}}(\gamma)\cdots\widehat{\chi_{r_sA}}(\gamma)\right| &\leq (|G|d(n-1)-|A|)^{s-2}|G||A| \\
&= |G|^{s-2}(d(n-1)-d^*(n))^{s-2}|G||A| \\
&= |G|d^*(n)(d(n-1)-d^*(n))^{s-2}.
\end{aligned}$$

We have

$$\begin{aligned}
|G|T(A) &= \widehat{\chi_{r_1A}}(e)\widehat{\chi_{r_2A}}(e)\cdots\widehat{\chi_{r_sA}}(e)+\sum_{\gamma\in\widehat{G},\gamma\neq e}\widehat{\chi_{r_1A}}(\gamma)\widehat{\chi_{r_2A}}(\gamma)\cdots\widehat{\chi_{r_sA}}(\gamma) \\
&\geq \widehat{\chi_{r_1A}}(e)\widehat{\chi_{r_2A}}(e)\cdots\widehat{\chi_{r_sA}}(e)-\left|\sum_{\gamma\in\widehat{G},\gamma\neq e}\widehat{\chi_{r_1A}}(\gamma)\widehat{\chi_{r_2A}}(\gamma)\cdots\widehat{\chi_{r_sA}}(\gamma)\right| \\
&\geq d^*(n)^s|G|^s-|G|^sd^*(n)(d(n-1)-d^*(n))^{s-2}.
\end{aligned}$$

This implies a lower bound on $T(A)$, specifically

$$T(A)\geq|G|^{s-1}\left(d^*(n)^s-d^*(n)(d(n-1)-d^*(n))^{s-2}\right).$$

Since A contains no non-trivial solutions to $\mathbf{r}$, if $r_1a_1+\cdots+r_sa_s=0$, then there is some $\emptyset \neq \{r_{j_1},\ldots,r_{j_l}\} \subseteq \{r_1,\ldots,r_s\}$ with $r_{j_1}+\cdots+r_{j_s}=0$ and $a_{j_1}=\cdots=a_{j_l}$. There are B ways to fix indices $\{j_1,\ldots,j_l\}$ with $r_{j_1}+\cdots+r_{j_l}=0$. We can assume without loss of generality that $\{j_1,\ldots,j_l\}=\{s-l+1,\ldots,s\}$ so that $\{1,\ldots,s\}\setminus\{j_1,\ldots,j_l\}=\{1,2,\ldots,s-l\}$. Notice that since $\mathbf{r}$ consists of non-zero integers, $l\geq 2$ and $s-l\leq s-2$.

Consider the number of solutions in A with $a_{j_1}=\cdots=a_{j_l}$. There are $|A|$ different ways to pick a_{j_1}, and since $a_{j_1}=\cdots=a_{j_l}$, this fixes each a_{j_i}. Consider the indices $\{1,\ldots,s\}\setminus\{j_1,\ldots,j_l\}=\{1,2,\ldots,s-l\}$. There are $|A|$ different ways to pick a_1. Similarly, there are $|A|$ different ways to pick a_i for $i\in\{1,2,\ldots,s-l-1\}$. Since

$$r_1a_1+r_2a_2+\cdots+r_{s-l}a_{s-l}=r_1a_1+\cdots r_sa_s-(r_{j_1}a_{j_1}+\cdots r_{j_l}a_{j_l})=0-0=0,$$

it holds that

$$r_{s-l}a_{s-l}=-(r_1a_1+r_2a_2+\cdots+r_{s-l-1}a_{s-l-1}).$$

This means that either a_{s-l} is determined by the choices for $a_1,\ldots,a_{s-l-1}$ or there is no valid choice for $a_{s-l}\in A$. Therefore, given $\emptyset\neq\{r_{j_1},\ldots,r_{j_l}\}\subseteq\{r_1,\ldots,r_s\}$ with $r_{j_1}+\cdots r_{j_s}=0$, there are at most $|A||A|^{s-l-1}=|A|^{s-l}\leq|A|^{s-2}$ different solutions in A with $a_{j_1}=\cdots=a_{j_l}$. We then have

$$T(A)\leq B|A|^{s-2}=Bd^*(n)^{s-2}|G|^{s-2}.$$

Putting together the bounds on $T(A)$, we see that

$$|G|^{s-1}(d^*(n)^s-d^*(n)(d(n-1)-d^*(n))^{s-2})\leq Bd^*(n)^{s-2}|G|^{s-2},$$

so that

$$d^*(n)^s-d^*(n)(d(n-1)-d^*(n))^{s-2}-\frac{Bd^*(n)^{s-2}}{|G|}\leq 0.$$

□

4.3 Proof of Theorem 4.1.1

Let $\mathbf{r}=(r_1,\ldots,r_s)\in(\mathbb{Z}\setminus\{0\})^s$ so that $r_1+\cdots+r_s=0$, and let $B_{\mathbf{r}}=B$ denote the number of different subsets $\emptyset\neq\{r_{j_1},\ldots,r_{j_l}\}\subseteq\{r_1,\ldots,r_s\}$ with $r_{j_1}+\cdots+r_{j_l}=0$. Let G be a finite abelian group coprime to $\mathbf{r}$ with $c(G)\geq n$. Suppose that $A\subseteq G$ contains no non-trivial solutions to $\mathbf{r}$. Let $d^*(n)=d^*(n;A,G)=|A|/|G|$. The proof of Theorem 4.1.1 is inductive on n. First pick $F\in\mathbb{R}$ with $F>1$. Let

$$E=\sqrt[s-2]{1-\frac{1}{F}},$$

and let

$$C = \max\left\{(BF)^{\frac{1}{2s-4}}\left(\frac{2s-4}{e\ln 2}\right), \frac{(E+1)^{\frac{1}{s-2}}}{(E+1)^{\frac{1}{s-2}}-1}\right\}.$$

We claim that this C satisfies

$$d(n) \leq \frac{C^{s-2}}{n^{s-2}}.$$

To show that $d(n) \leq \frac{C^{s-2}}{n^{s-2}}$ it is enough to show $d^*(n) \leq \frac{C^{s-2}}{n^{s-2}}$. To verify the base case recall that $D(G) \leq |G|$ for every finite abelian group G, and

$$d(1) = \sup_{\substack{G \text{ coprime to } \mathbf{r} \\ c(G)\geq 1}} \frac{D(G)}{|G|} \leq 1.$$

It holds that

$$1 \leq \frac{(E+1)^{\frac{1}{s-2}}}{(E+1)^{\frac{1}{s-2}}-1} \leq C \leq C^{s-2},$$

so that $d(1) \leq C^{s-2}$, as desired. Assume that

$$d(n-1) \leq \frac{C^{s-2}}{(n-1)^{s-2}}.$$

By its definition, $d(n) \leq 1$, so when $n \leq C$ the proof holds trivially. Assume that $n > C$, and consider the following two cases:

Case I: Suppose that

$$d^*(n)^2 \leq \frac{FB}{|G|}.$$

Since G is a finite abelian group with at least n constituents, it holds that $|G| \geq 2^n$. Therefore

$$d^*(n) \leq \left(\frac{FB}{|G|}\right)^{\frac{1}{2}} \leq \left(\frac{FB}{2^n}\right)^{\frac{1}{2}},$$

and

$$d^*(n)n^{s-2} \leq \left(\frac{FB}{2^n}\right)^{\frac{1}{2}} n^{s-2}.$$

Define

$$f(x) = \frac{x^{s-2}}{2^{\frac{x}{2}}},$$

so that the above inequality can be written as

$$d^*(n)n^{s-2} \leq (FB)^{\frac{1}{2}} f(n).$$

Since $f(0) = 0$ and $\lim_{x\to\infty} f(x) = 0$, f attains a maximum value on $[0, \infty)$. We have

$$f'(x) = \frac{x^{s-2}(s-2)}{x2^{\frac{x}{2}}} - \frac{1}{2}\frac{x^{s-2}\ln(2)}{x2^{\frac{x}{2}}}$$

so that the only zero of $f'(x)$ is $x = (2s-4)/\ln(2)$. Therefore, for each positive $x \in \mathbb{R}$,

$$f(x) \leq f\left(\frac{2s-4}{\ln(2)}\right) = \left(\frac{2s-4}{e\ln 2}\right)^{s-2}.$$

By the definition of C,

$$C^{s-2} \geq (BF)^{\frac{1}{2}}\left(\frac{2s-4}{e\ln 2}\right)^{s-2},$$

so that

$$d^*(n)n^{s-2} \leq (FB)^{\frac{1}{2}}f(n) \leq (FB)^{\frac{1}{2}}\left(\frac{2s-4}{e\ln 2}\right)^{s-2} \leq C^{s-2},$$

and

$$d^*(n) \leq \frac{C^{s-2}}{n^{s-2}}$$

as desired.

Case II: Suppose that

$$d^*(n)^2 > \frac{FB}{|G|}.$$

After multiplying both sides by $d^*(n)^{s-2}$ and doing some rearranging, this implies

$$\frac{d^*(n)^s}{F} > \frac{Bd^*(n)^{s-2}}{|G|}.$$

We have seen in Lemma 7

$$d^*(n)^s - d^*(n)(d(n-1) - d^*(n))^{s-2} - Bd^*(n)^{s-2} \leq 0.$$

Therefore

$$\frac{d^*(n)^s}{F} + \left(1 - \frac{1}{F}\right)d^*(n)^s = d^*(n)^s < d^*(n)(d(n-1) - d^*(n))^{s-2} + \frac{Bd^*(n)^{s-2}}{|G|}$$

and

$$\left(1 - \frac{1}{F}\right)d^*(n)^s < d^*(n)(d(n-1) - d^*(n))^{s-2} + \frac{Bd^*(n)^{s-2}}{|G|} - \frac{d^*(n)^s}{F}.$$

Since

$$\frac{Bd^*(n)^{s-2}}{|G|} - \frac{d^*(n)^s}{F} < 0,$$

we have

$$E^{s-2}d^*(n)^s = \left(1 - \frac{1}{F}\right) d^*(n)^s < d^*(n)(d(n-1) - d^*(n))^{s-2}. \tag{4.1}$$

This gives us

$$E^{s-2}d^*(n)^{s-1} < (d(n-1) - d^*(n))^{s-2},$$

so that

$$Ed^*(n)^{\frac{s-1}{s-2}} + d^*(n) < d(n-1) \leq \frac{C^{s-2}}{(n-1)^{s-2}}.$$

Notice that $Ex^{\frac{s-1}{s-2}} + x$ is an increasing function of x. As such, if

$$Ed^*(n)^{\frac{s-1}{s-2}} + d^*(n) \leq E\left(\frac{C^{s-2}}{n^{s-2}}\right)^{\frac{s-1}{s-2}} + \frac{C^{s-2}}{n^{s-2}},$$

then it follows that $d^*(n) \leq \frac{C^{s-2}}{n^{s-2}}$. By the definition of C, it holds that

$$C \geq \frac{(E+1)^{\frac{1}{s-2}}}{(E+1)^{\frac{1}{s-2}} - 1},$$

which leads to the following inequalities:

$$\begin{aligned}
& C \geq \frac{1}{(E+1)^{\frac{1}{s-2}} - 1} + 1 \\
\iff \quad & \frac{1}{C-1} \leq (E+1)^{\frac{1}{s-2}} - 1 \\
\iff \quad & \frac{C}{C-1} \leq (E+1)^{\frac{1}{s-2}} \\
\iff \quad & \left(\frac{C}{C-1}\right)^{s-2} \leq E+1 \\
\iff \quad & \frac{C^{s-1}}{(C-1)^{s-2}} \leq C(E+1) \\
\iff \quad & \frac{C^{s-1}}{(C-1)^{s-2}} - C \leq CE.
\end{aligned}$$

Define, for $x \in \mathbb{R}$ with $x > 1$,

$$g(x) = \frac{x^{s-1}}{(x-1)^{s-2}} - x.$$

Then we have

$$\begin{aligned} g(x) &= (x-1)\left(1+\frac{1}{x-1}\right)^{s-1} - x \\ &= (x-1)\sum_{k=0}^{s-1}\binom{s-1}{k}\frac{1}{(x-1)^k} - x \\ &= \sum_{k=0}^{s-1}\binom{s-1}{k}(x-1)^{1-k} - x. \end{aligned}$$

Therefore

$$\begin{aligned} g'(x) &= \sum_{k=0}^{s-1}(1-k)\binom{s-1}{k}(x-1)^{-k} - 1 \\ &= 1 + 0 + \sum_{k=2}^{s-1}(1-k)\binom{s-1}{k}(x-1)^{-k} - 1 \\ &= \sum_{k=2}^{s-1}(1-k)\binom{s-1}{k}(x-1)^{-k}. \end{aligned}$$

We have that $1-k<0$ for $k\geq 2$, $\binom{s-1}{k}>0$ for $k\in\{2,\ldots,s-1\}$, and $(x-1)^{-k}>0$ for $x>1$, so that $g'(x)<0$ and $g(x)$ is a decreasing function. Since we are considering $n>C$, we have

$$\frac{n^{s-1}}{(n-1)^{s-2}} - n \leq \frac{C^{s-1}}{(C-1)^{s-2}} - C \leq CE.$$

This leads to the following inequalities:

$$\begin{aligned} & \frac{n^{s-1}}{(n-1)^{s-2}} - n \leq CE \\ \iff & \frac{1}{(n-1)^{s-2}} - \frac{1}{n^{s-2}} \leq \frac{EC}{n^{s-1}} \\ \iff & \frac{1}{(n-1)^{s-2}} \leq \frac{EC}{n^{s-1}} + \frac{1}{n^{s-2}} \\ \iff & \frac{C^{s-2}}{(n-1)^{s-2}} \leq \frac{EC^{s-1}}{n^{s-1}} + \frac{C^{s-2}}{n^{s-2}} \\ \iff & \frac{C^{s-2}}{(n-1)^{s-2}} \leq E\left(\frac{C^{s-2}}{n^{s-2}}\right)^{\frac{s-1}{s-2}} + \frac{C^{s-2}}{n^{s-2}}. \end{aligned}$$

Therefore

$$Ed^*(n)^{\frac{s-1}{s-2}} + d^*(n) < d(n-1) \leq \frac{C^{s-2}}{(n-1)^{s-2}} \leq E\left(\frac{C^{s-2}}{n^{s-2}}\right)^{\frac{s-1}{s-2}} + \frac{C^{s-2}}{n^{s-2}}$$

and we can conclude that

$$d^*(n) \leq \frac{C^{s-2}}{n^{s-2}}.$$

This completes the proof of Theorem 4.1.1.

4.4 Additional remarks

Remark 1. Minimizing $C(\mathbf{r})$

Fix $\mathbf{r} = (r_1, \ldots, r_s)$, and notice that $C(\mathbf{r})$ worked for any value of $F > 1$. Recall that

$$E = \sqrt[s-2]{1 - \frac{1}{F}}.$$

Therefore given any $E \in (0,1)$, we can find $F > 1$ so that $E = \sqrt[s-2]{1 - \frac{1}{F}}$. Remark also that

$$(BF)^{\frac{1}{2s-4}} = \left(\frac{B}{1 - E^{s-2}}\right)^{\frac{1}{2s-4}}$$

so that

$$C = \max\left\{\left(\frac{B}{1 - E^{s-2}}\right)^{\frac{1}{2s-4}}\left(\frac{2s-4}{e\ln 2}\right), \frac{(E+1)^{\frac{1}{s-2}}}{(E+1)^{\frac{1}{s-2}} - 1}\right\}.$$

When we consider

$$\left(\frac{B}{1 - E^{s-2}}\right)^{\frac{1}{2s-4}}\left(\frac{2s-4}{e\ln 2}\right)$$

as a function of E defined on $(0,1)$, it is increasing. Indeed, B and $\frac{2s-4}{e\ln 2}$ are positive constants depending only on $\mathbf{r}$, and $\frac{1}{1-E^{s-2}}$ is increasing on $(0,1)$. When we consider

$$\frac{(E+1)^{\frac{1}{s-2}}}{(E+1)^{\frac{1}{s-2}} - 1}$$

as a function of E defined on $(0,1)$, it is decreasing. Indeed, the function $(E+1)^{\frac{1}{s-2}}$ is increasing for $E \in (0,1)$ and gives values in $(1, 2^{\frac{1}{s-2}})$. The function $\frac{x}{x-1}$ is decreasing for $x > 1$. Composing these two functions verifies that our function is decreasing on $(0,1)$. As

such, to minimize our value of C, we may choose a value of E such that

$$\left(\frac{B}{1-E^{s-2}}\right)^{\frac{1}{2s-4}}\left(\frac{2s-4}{e\ln 2}\right)=\frac{(E+1)^{\frac{1}{s-2}}}{(E+1)^{\frac{1}{s-2}}-1}.$$

Since

$$\lim_{E\to 1^-}\left(\frac{B}{1-E^{s-2}}\right)^{\frac{1}{2s-4}}\left(\frac{2s-4}{e\ln 2}\right)=\infty$$

and

$$\lim_{E\to 0^+}\frac{(E+1)^{\frac{1}{s-2}}}{(E+1)^{\frac{1}{s-2}}-1}=\infty,$$

we are guaranteed the existence of such an $E\in(0,1)$. We saw earlier that the above functions are increasing and decreasing, respectively, which tells us that this value of $E\in(0,1)$ is unique.

Consider now the case when $\mathbf{r}=(1,-2,1)$. We have G is coprime to $\mathbf{r}$ exactly when $|G|$ is odd. We also have that a solution $(x_1,x_2,x_3)\subseteq G$ is a three term arithmetic progression. This is the case we examined in Chapter 1, where we saw that given $n\in\mathbb{N}$,

$$d_{(1,-2,1)}(n)\leq\frac{2}{n}.$$

To apply Theorem 4.1.1 to $\mathbf{r}=(1,-2,1)$, we have $s=3$ and notice that $B(\mathbf{r})=1$, since the only subset of $\{1,-2,1\}$ which sums to 0 is $\{1,-2,1\}$. We therefore have

$$d_{(1,-2,1)}(n)\leq\frac{C(\mathbf{r})}{n}$$

with

$$C(\mathbf{r})=\max\left\{\left(\frac{1}{1-E}\right)^{\frac{1}{2}}\left(\frac{2}{e\ln 2}\right),\frac{E+1}{E}\right\}.$$

Let $C_1=\frac{2}{e\ln 2}\approx 0.39049508$, so that $C(\mathbf{r})$ is minimized when

$$\begin{aligned}
&\left(\frac{C_1^2}{1-E}\right)^{\frac{1}{2}} &&= &&\frac{E+1}{E}\\
\iff\quad &\frac{C_1^2}{1-E} &&= &&\frac{(E+1)^2}{E^2}\\
\iff\quad &C_1^2E &&= &&-E^3-E^2+E+1\\
\iff\quad &E^3+(C_1^2+1)E^2-E-1 &&= &&0.
\end{aligned}$$

Solving the cubic equation gives us a unique zero at $E\approx 0.9632906555864345$. This mini-

mizes $C(\mathbf{r})$ at 2.03810827418. Unfortunately, this is slightly larger than the constant given in Meshulam's bound in Theorem 2.1.1. We will address this in subsequent remarks.

Remark 2. Minimizing $C(\mathbf{r})$ in special cases

The very general result of Theorem 4.1.1 can be adapted for more specific cases by mimicking the proof of Theorem 4.1.1. For example, consider the cases where $\mathbf{r} = (r_1, \ldots, r_s)$ has only one subset $\{r_{j_1}, \ldots, r_{j_l}\} \subseteq \{r_1, \ldots, r_s\}$ with $r_{j_1} + \cdots + r_{j_l} = 0$, namely the subset $\{r_{j_1}, \ldots, r_{j_l}\} = \{r_1, \ldots, r_s\}$. In this case, we have $T(A) = |A|$ where $A \subseteq G$ is free of non-trivial solutions to $\mathbf{r}$. We use this information to alter the general result of Lemma 7, where we devised an inequality from two bounds on $T(A)$. We previously had an upper bound of

$$T(A) \leq B(\mathbf{r}) d^*(n) |G|^{s-2}$$

and a lower bound of

$$T(A) \geq |G|^{s-1}\big(d^*(n)^s - d^*(n)(d(n-1) - d^*(n))^{s-2}\big).$$

We can now write

$$|A| \geq |G|^{s-1}\big(d^*(n)^s - d^*(n)(d(n-1) - d^*(n))^{s-2}\big)$$

with

$$\begin{aligned} 0 &\geq |G|^{s-1}\big(d^*(n)^s - d^*(n)(d(n-1) - d^*(n))^{s-2}\big) - d^*(n)|G| \\ &= d^*(n)^s - d^*(n)(d(n-1) - d^*(n))^{s-2} - \frac{d^*(n)}{|G|^{s-2}}. \end{aligned}$$

This leads to the following result:

Corollary 4.4.1. *Let $\mathbf{r} = (r_1, \ldots, r_s) \in \mathbb{Z}^s$ with $r_1 + \cdots + r_s = 0$ and for any $\{r_{j_1}, \ldots, r_{j_l}\} \subsetneq \{r_1, \ldots, r_s\}$, we have $r_{j_1} + \cdots + r_{j_l} \neq 0$. Let*

$$C = \max\left\{ F^{\frac{1}{(s-1)(s-2)}} \left(\frac{s-1}{e \ln 2}\right), \frac{(E+1)^{\frac{1}{s-2}}}{(E+1)^{\frac{1}{s-2}} - 1} \right\},$$

where F is any real number with $F > 1$ and $E = (1 - F^{-1})^{\frac{1}{s-2}}$ (so that $F = \frac{1}{1-E^{s-2}}$). It therefore holds that

$$d_{\mathbf{r}}(n) \leq \frac{C^{s-2}}{n^{s-2}}.$$

Proof. Case I: Suppose

$$d^*(n)^{s-1} \leq \frac{F}{|G|^{s-2}}.$$

Since G has at least n components, we have

$$d^*(n) \leq \left(\frac{F}{|G|^{s-2}}\right)^{\frac{1}{s-1}} \leq \left(\frac{F}{(2^n)^{s-2}}\right)^{\frac{1}{s-1}},$$

so that

$$d^*(n)n^{s-2} \leq \left(\frac{F}{(2^n)^{s-2}}\right)^{\frac{1}{s-1}} n^{s-2} = \left(\frac{F^{\frac{1}{(s-1)(s-2)}}n}{2^{\frac{n}{s-1}}}\right)^{s-2}.$$

We will verify that

$$\frac{F^{\frac{1}{(s-1)(s-2)}}n}{2^{\frac{n}{s-1}}} \leq C,$$

so that we may conclude

$$d^*(n) \leq \left(\frac{C}{n}\right)^{s-2}.$$

For non-negative $x \in \mathbb{R}$, define

$$f(x) = \frac{x}{2^{\frac{x}{s-1}}}.$$

We have that $f(0) = 0$ and $\lim_{x\to\infty} f(x) = 0$, so that f attains its maximum value on $[0, \infty)$. Notice that

$$f'(x) = \frac{1}{2^{\frac{x}{s-1}}} - \frac{x}{s-1}\frac{\ln(2)}{2^{\frac{x}{s-1}}} = \frac{1}{2^{\frac{x}{s-1}}}\left(1 - \frac{x\ln(2)}{s-1}\right).$$

It therefore holds that f contains only one critical point, and f attains its maximum at $x = \frac{s-1}{\ln(2)}$, where

$$f\left(\frac{s-1}{\ln(2)}\right) = \frac{s-1}{e\ln(2)}.$$

As such,

$$\frac{F^{\frac{1}{(s-1)(s-2)}}n}{2^{\frac{n}{s-1}}} = F^{\frac{1}{(s-1)(s-2)}} f(n) \leq F^{\frac{1}{(s-1)(s-2)}}\left(\frac{s-1}{e\ln(2)}\right) \leq C$$

finishing our first case.

Case II: Suppose

$$d^*(n)^{s-1} > \frac{F}{|G|^{s-2}}.$$

By our modified version of Lemma 7, we have

$$\frac{d^*(n)^s}{F} + \left(1 - \frac{1}{F}\right) d^*(n)^s = d^*(n)^s \leq d^*(n)\big(d(n-1) - d^*(n)\big)^{s-2} + \frac{d^*(n)}{|G|^{s-2}},$$

so that

$$\left(1 - \frac{1}{F}\right) d^*(n)^s \leq d^*(n)^s \leq d^*(n)\big(d(n-1) - d^*(n)\big)^{s-2} + \frac{d^*(n)}{|G|^{s-2}} - \frac{d^*(n)^s}{F}.$$

Since

$$\frac{d^*(n)}{|G|^{s-2}} - \frac{d^*(n)^s}{F} < 0,$$

we have

$$\left(1 - \frac{1}{F}\right) d^*(n)^s = E^{s-2} d^*(n)^s < d^*(n)\big(d(n-1) - d^*(n)\big)^{s-2},$$

which is identical to inequality 4.1. We saw in the proof of Theorem 4.1.1 that inequality 4.1, combined with the assumption that

$$C \geq \frac{(E+1)^{\frac{1}{s-2}}}{(E+1)^{\frac{1}{s-2}} - 1},$$

results in

$$d^*(n) \leq \left(\frac{C}{n}\right)^{s-2}.$$

This completes our proof. □

We notice, in a similar fashion to our observations on Theorem 4.1.1, that for any $E \in (0,1)$ we may write,

$$C = \max\left\{ \left(\frac{1}{1 - E^{s-2}}\right)^{\frac{1}{(s-1)(s-2)}} \left(\frac{s-1}{e \ln 2}\right), \frac{(E+1)^{\frac{1}{s-2}}}{(E+1)^{\frac{1}{s-2}} - 1} \right\}.$$

To minimize C, we again notice that

$$\lim_{E \to 1^-} \left(\frac{1}{1 - E^{s-2}}\right)^{\frac{1}{(s-1)(s-2)}} \left(\frac{s-1}{e \ln 2}\right) = \lim_{E \to 0^+} \frac{(E+1)^{\frac{1}{s-2}}}{(E+1)^{\frac{1}{s-2}} - 1} = \infty$$

with the two functions of $E \in (0,1)$ increasing and decreasing, respectively. Therefore C

is minimized when

$$\left(\frac{1}{1-E^{s-2}}\right)^{\frac{1}{(s-1)(s-2)}}\left(\frac{s-1}{e\ln 2}\right)=\frac{(E+1)^{\frac{1}{s-2}}}{(E+1)^{\frac{1}{s-2}}-1}.$$

In the case examined by Meshulam, where $\mathbf{r}=(1,-2,1)$ and $s=3$, the above equality reduces to

$$\left(\frac{1}{1-E}\right)^{\frac{1}{2}}\frac{2}{e\ln(2)}=\frac{E+1}{E}.$$

We solved this earlier in this section where $E\approx 0.9632906555864345$ gives us $C\approx 2.03810827418$. It should be expected that Corollary 4.4.1 does not alter the case when $s=3$: If $(r_1,r_2,r_3)\in(\mathbb{Z}\setminus\{0\})^3$, then $r_1+r_2=0$ implies $r_3=0$, contradicting our requirements for $\mathbf{r}$.

Remark 3. The case $\mathbf{r}=(1,-2,1)$

To obtain Meshulam's result, we can use the same modified version of Lemma 7 which was used in Corollary 4.4.1, which states

$$0\geq d^*(n)^s-d^*(n)(d(n-1)-d^*(n))^{s-2}-\frac{d^*(n)}{|G|^{s-2}}.$$

In the case where $\mathbf{r}=(1,-2,1)$, we have $s=3$ and G coprime to $\mathbf{r}$ if and only if $|G|$ is odd. Therefore

$$d^*(n)^3-\frac{d^*(n)}{|G|}\leq d^*(n)\big(d(n-1)-d^*(n)\big),$$

so that

$$d^*(n)^2+d^*(n)-\frac{1}{|G|}\leq d(n-1).$$

Since $c(G)\geq n$ and $|G|$ is odd, we have

$$d^*(n)^2+d^*(n)-\frac{1}{3^n}\leq d^*(n)^2+d^*(n)-\frac{1}{|G|}\leq d(n-1).$$

We can assume inductively that $d(n-1)\leq 2/(n-1)$. Notice that our base cases $n=1$ and $n=2$ are trivial since $d(n)\leq 1$ for each natural number n. Consider $n\geq 3$, and notice that

$$1\leq\frac{n-1}{n-2}\leq 2,$$

so that

$$\frac{n-1}{(n-2)3^n} \leq \frac{2}{3^n} \leq \frac{2}{n^2}.$$

We therefore have

$$\frac{n-1}{3^n} \leq \frac{2(n-2)}{n^2} = \frac{2n^2+2n-4}{n^2} - 2 = \frac{(2n+4)(n-1)}{n^2} - 2,$$

which implies that

$$\frac{2}{n-1} \leq \frac{2n+4}{n^2} - \frac{1}{3^n} = \left(\frac{2}{n}\right)^2 + \frac{2}{n} - \frac{1}{3^n}.$$

Therefore

$$d^*(n)^2 + d^*(n) - \frac{1}{3^n} \leq d(n-1) \leq \frac{2}{n-1} \leq \left(\frac{2}{n}\right)^2 + \frac{2}{n} - \frac{1}{3^n}.$$

For fixed n, the function $x^2 + x - \frac{1}{3^n}$ is increasing. As such, $d^*(n) \leq \frac{2}{n}$, which provides another proof of Theorem 2.1.1.

Chapter 5

Meshulam's Theorem on Systems of Linear Equations

5.1 Introduction

In the previous chapter, we saw a generalization of Meshulam's Theorem from 3-APs to linear equations, and outlined the proof of Liu and Spencer. In 2011, Liu, Spencer and Zhao [7] found a bound for sets containing only trivial solutions to a system of linear equations.

In their work, they consider matrices $Y = (y_{i,j}) \in \mathbb{Z}^{R\times S}$ satisfying $R, S \in \mathbb{N}$ with $S \geq 2R+1$ and $y_{i,1} + y_{i,2} + \cdots + y_{i,S} = 0$ for each $i \in \{1, \ldots, R\}$. Given such a matrix Y, we can distinguish a class of finite abelian groups G for which we can bound the size of a subset $A \subseteq G$ containing 'trivial' solutions to the equation $Yx = 0$, where $x \in A^S$.

Given a finite abelian group G, we can write

$$G \cong \mathbb{Z}_{k_1} \oplus \mathbb{Z}_{k_2} \oplus \cdots \oplus \mathbb{Z}_{k_n}$$

with $k_i \in \{2, 3, \ldots\}$ for each $i \in \{1, \ldots, n\}$ and $k_i | k_{i+1}$ for $i \in \{1, \ldots, n-1\}$. We say G has n constituents, and denote this by $c(G) = n$. We denote by $|G|$ the cardinality of G.

Definition 5.1.1. Let $R, S \in \mathbb{N}$ such that $S \geq 2R+1$. Let $Y = (y_{i,j}) \in \mathbb{Z}^{R\times S}$ be a matrix satisfying $y_{i,1} + y_{i,2} + \cdots + y_{i,S} = 0$ for each $i \in \{1, \ldots, R\}$. Let $L \in \mathbb{N}$ with $R \leq L \leq S - R - 1$. Let G be a finite abelian group.

Then we say G is *L-coprime* to Y if there exists L columns of Y satisfying the following conditions:

- Upon choosing any R of these L columns, we obtain an $R \times R$ matrix $Z \in \mathbb{Z}^{R\times R}$ with $\gcd(\det(Z), |G|) = 1$, where $\det(Z)$ denotes the determinant of Z.

- Upon removing any $L - R + 1$ of these L columns from Y, there exist within the remaining columns two disjoint sets of R columns which form $R \times R$ matrices $Z_1, Z_2 \in \mathbb{Z}^{R\times R}$ with
$$\gcd(\det(Z_1), |G|) = \gcd(\det(Z_2), |G|) = 1.$$

When a matrix G is L-coprime to $Y \in \mathbb{Z}^{R\times S}$, the indices of the L columns satisfying the above conditions are denoted by $l_Y(G; L)$, i.e. if the L columns of Y satisfying the conditions of L-coprimality are

$$\left\{ \begin{pmatrix} y_{1,j_1} \\ y_{2,j_1} \\ \vdots \\ y_{R,j_1} \end{pmatrix}, \begin{pmatrix} y_{1,j_2} \\ y_{2,j_2} \\ \vdots \\ y_{R,j_2} \end{pmatrix}, \cdots, \begin{pmatrix} y_{1,j_L} \\ y_{2,j_L} \\ \vdots \\ y_{R,j_L} \end{pmatrix} \right\},$$

then $l_Y(G; L) = \{j_1, j_2, \ldots, j_L\}$.

Definition 5.1.2. Let $R, S \in \mathbb{N}$, and $Y \in \mathbb{Z}^{R\times S}$ be defined as above. Let G be a finite abelian group. We say that $\overline{x} = (x_1, \ldots, x_s) \in G^S$ is a solution to Y if $Y\overline{x} = 0$, i.e. $\overline{x} = (x_1, \ldots, x_S)$ is a solution if

$$\begin{pmatrix} y_{1,1}x_1 + y_{1,2}x_2 + \cdots + y_{1,S}x_S \\ y_{2,1}x_1 + y_{2,2}x_2 + \cdots + y_{2,S}x_S \\ \vdots \\ y_{R,1}x_1 + y_{R,2}x_2 + \cdots + y_{R,S}x_S \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

We say that a solution $\overline{x} \in G^S$ is *trivial* if there are $i \neq j$, $i, j \in \{1, \ldots, S\}$, with $x_i = x_j$. Otherwise, when each x_i is distinct, we say that $\overline{x}$ is a *non-trivial solution.*

Definition 5.1.3. Let $R, S \in \mathbb{N}$, $L \in \mathbb{N}$, and $Y \in \mathbb{Z}^{R\times S}$ be defined as in Definition 5.1.1. Let G be a finite abelian group which is L-coprime to Y, and let $A \subseteq G$. If every solution $\overline{x} \in A^S$ to the equation $Y\overline{x} = 0$ is trivial, we say that A *contains only trivial solutions to* Y, and write $A \in TRIV_Y$. Define

$$D_Y(G) = \max_{\substack{A\subseteq G \\ A\in TRIV_Y}} |A|$$

and

$$d_Y(N; L) = \sup_{\substack{G \text{ is } L\text{-coprime to } Y \\ c(G)\geq N}} \frac{D_Y(G)}{|G|}.$$

Theorem 5.1.1. *Let $R, S \in \mathbb{N}$ such that $S \geq 2R + 1$. Let $Y = (y_{i,j}) \in \mathbb{Z}^{R\times S}$ be a matrix satisfying $y_{i,1} + y_{i,2} + \cdots + y_{i,S} = 0$ for each $i \in \{1, \ldots, R\}$. Let $L \in \mathbb{N}$ with*

$R \leq L \leq S - R - 1$. *Then there exists a constant* $C = C(Y; L) > 1$ *such that*

$$d_Y(N; L) \leq \left(\frac{C}{N}\right)^{\frac{L-R+1}{R}}$$

for any $N \in \mathbb{N}$.

5.2 Generalizations to several dimensions

Before proving Theorem 5.1.1, we will prove a variation of Proposition 1.2.3.

Proposition 5.2.1. *Let* G *be a finite abelian group, and let* $\widehat{G}$ *denote the character group as defined in Chapter 1. Then* $\widehat{G^R} \cong \widehat{G}^R$.

Proof. Let $\gamma \in \widehat{G^R}$ so that for $(g_1, g_2, \ldots, g_R), (h_1, h_2, \ldots, h_R) \in G^R$, we have

- $\gamma(g_1, g_2, \ldots, g_R) \in \mathbb{C}$
- $|\gamma(g_1, g_2, \ldots, g_R)| = 1$
- $\gamma(g_1 + h_1, g_2 + h_2, \ldots, g_R + h_R) = \gamma(g_1, g_2, \ldots, g_R)\gamma(h_1, h_2, \ldots, h_R)$

Define $\phi : \widehat{G^R} \mapsto \widehat{G}^R$ by $\phi(\gamma) = (\gamma_1, \gamma_2, \ldots, \gamma_R)$, where

$$\begin{aligned} \gamma_1(g) &= \gamma(g, 0, \ldots, 0) \\ \gamma_2(g) &= \gamma(0, g, \ldots, 0) \\ &\vdots \\ \gamma_R(g) &= \gamma(0, 0, \ldots, g) \end{aligned}$$

for any $g \in G$. Notice that γ_1 is indeed in the character group $\widehat{G}$ since

$$|\gamma_1(g)| = |\gamma(g, 0, \ldots, 0)| = 1,$$

and

$$\gamma_1(g + h) = \gamma(g + h, 0, \ldots, 0) = \gamma(g, 0 \ldots, 0)\gamma(h, 0, \ldots, 0) = \gamma_1(g)\gamma_1(h).$$

Similarly, $\gamma_i \in \widehat{G}$ for each $i \in \{1, \ldots, R\}$, so that $(\gamma_1, \gamma_2, \ldots, \gamma_R) \in \widehat{G}^R$. For $\gamma, \zeta \in \widehat{G^R}$,

$$\phi(\gamma\zeta) = ((\gamma\zeta)_1, (\gamma\zeta)_2, \ldots, (\gamma\zeta)_R)$$

where

$$(\gamma\zeta)_1(g) = \gamma\zeta(g,0,\ldots,0) = \gamma(g,0,\ldots,0)\zeta(g,0,\ldots,0) = \gamma_1(g)\zeta_1(g).$$

Similarly $(\gamma\zeta)_i = \gamma_i\zeta_i$ for each $i \in \{1,\ldots,R\}$, so that

$$\phi(\gamma\zeta) = ((\gamma\zeta)_1,(\gamma\zeta)_2,\ldots,(\gamma\zeta)_R) = (\gamma_1\zeta_1,\gamma_2\zeta_1,\ldots,\gamma_R\zeta_R) = \phi(\gamma)\phi(\zeta)$$

and ϕ is a group homomorphism. Notice that for $\gamma \in \widehat{G^R}$,

$$\gamma(g_1,g_2,\ldots,g_R) = \gamma(g_1,0,\ldots,0)\gamma(0,g_2,\ldots,0)\cdots\gamma(0,0,\ldots,g_R) = \gamma_1(g_1)\gamma_2(g_2)\cdots\gamma_R(g_R).$$

Suppose that $\phi(\gamma) = \phi(\zeta)$ so that $(\gamma_1,\gamma_2,\ldots,\gamma_R) = (\zeta_1,\zeta_2,\ldots,\zeta_R)$ for $\gamma,\zeta \in \widehat{G^R}$. We have for $(g_1,g_2,\ldots,g_R) \in G^R$

$$\begin{aligned}\gamma(g_1,g_2,\ldots,g_R) &= \gamma_1(g_1)\gamma_2(g_2)\cdots\gamma_R(g_R)\\ &= \zeta_1(g_1)\zeta_2(g_2)\cdots\zeta_R(g_R)\\ &= \zeta(g_1,g_2,\ldots,g_R),\end{aligned}$$

so that ϕ is injective. Let $(\gamma_1,\gamma_2,\ldots,\gamma_R) \in \widehat{G}^R$, and define γ from G^R to $\mathbb{C}$ by $\gamma(g_1,g_2,\ldots,g_R) = \gamma_1(g_1)\gamma(g_2)\cdots\gamma_R(g_R)$. We have that γ is indeed in $\widehat{G^R}$, since

$$|\gamma(g_1,g_2,\ldots,g_R)| = |\gamma_1(g_1)\gamma(g_2)\cdots\gamma_R(g_R)| = 1$$

and

$$\begin{aligned}\gamma(g_1+h_1,g_2+h_2,\ldots,g_R+h_R) &= \gamma_1(g_1+h_1)\gamma_2(g_2+h_2)\cdots\gamma_R(g_R+h_R)\\ &= \gamma_1(g_1)\gamma_1(h_1)\cdots\gamma_R(g_R)\gamma_R(h_R)\\ &= \gamma(g_1,g_2,\ldots,g_R)\gamma(h_1,h_2,\ldots,h_R).\end{aligned}$$

Let $\phi(\gamma) = (\zeta_1,\zeta_2,\ldots,\zeta_R) \in \widehat{G}^R$, with

$$\zeta_1(g) = \gamma(g,0,\ldots,0) = \gamma_1(g)\gamma_2(0)\cdots\gamma_R(0) = \gamma_1(g),$$

so that $\zeta_1 = \gamma_1$. Similarly, $\zeta_i = \gamma_i$ for each $i \in \{1,\ldots,R\}$. As such, $\phi(\gamma) = (\gamma_1,\gamma_2,\ldots,\gamma_R)$ and ϕ is surjective. Therefore $\widehat{G^R} \cong \widehat{G}^R$.

□

Proposition 5.2.2. *Let G be a finite abelian group, let $\widehat{G}$ denote the dual group of G, and*

let $R \in \mathbb{N}$. For $\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_R) \in \widehat{G}^R$ and $g = (g_1, g_2, \ldots, g_R) \in G^R$, we have

$$\frac{1}{|G|^R} \sum_{\gamma \in \widehat{G}^R} \gamma_1(g_1)\gamma_2(g_2)\cdots\gamma_R(g_R) = \begin{cases} 1, & \textit{if } (g_1, g_2, \ldots, g_R) = 0, \\ 0, & \textit{otherwise.} \end{cases}$$

Proof. It holds that

$$\frac{1}{|G|^R} \sum_{\gamma \in \widehat{G}^R} \gamma_1(g_1)\gamma_2(g_2)\cdots\gamma_R(g_R) = \prod_{i=1}^{R} \left(\frac{1}{|G|} \sum_{\gamma_i \in \widehat{G}} \gamma_i(g_i) \right).$$

By Proposition 1.2.3, for each $i \in \{1, \ldots, R\}$

$$\frac{1}{|G|} \sum_{\gamma_i \in \widehat{G}} \gamma_i(g_i) = \begin{cases} 1, & \text{if } g_i = 0, \\ 0, & \text{otherwise.} \end{cases}$$

Therefore

$$\frac{1}{|G|^R} \sum_{\gamma \in \widehat{G}^R} \gamma_1(g_1)\gamma_2(g_2)\cdots\gamma_R(g_R) = \begin{cases} 1, & \text{if } (g_1, g_2, \ldots, g_R) = 0, \\ 0, & \text{otherwise.} \end{cases}$$

□

We let e denote the trivial character of $\widehat{G}$, $\widehat{G^R}$ and $\widehat{G}^R$. The implied dual group will be clear from context. We let $\Gamma(G) = \widehat{G}^R \setminus \{e\}$.

Lemma 8. *Let G be a finite abelian group, and let $R \in \mathbb{N}$. Let $Z \in \mathbb{Z}^{R \times R}$ be a matrix satisfying* $\gcd(\det(Z), |G|) = 1$. *Then for $\overline{x} \in G^R$, we have $Z\overline{x} = 0$ if and only if $\overline{x} = 0$.*

Proof. We have

$$G \cong \mathbb{Z}_{k_1} \oplus \mathbb{Z}_{k_2} \oplus \cdots \oplus \mathbb{Z}_{k_M}$$

with $k_i \in \mathbb{N}$ and $k_i \geq 2$ for each $i \in \{1, \ldots, M\}$ and $k_i | k_{i+1}$ for each $i \in \{1, \ldots, M-1\}$. As such, for $\overline{x} \in G^R$,

$$\overline{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_R \end{pmatrix} = \begin{pmatrix} x_{1,1} \oplus x_{1,2} \oplus \cdots \oplus x_{1,M} \\ x_{2,1} \oplus x_{2,2} \oplus \cdots \oplus x_{2,M} \\ \vdots \\ x_{R,1} \oplus x_{R,2} \oplus \cdots \oplus x_{R,M} \end{pmatrix}$$

so that for each $i \in \{1, \ldots, M\}$,

$$\begin{pmatrix} x_{1,i} \\ x_{2,i} \\ \vdots \\ x_{R,i} \end{pmatrix} \in \mathbb{Z}_{k_i}^R.$$

We have that

$$Z \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_R \end{pmatrix} = 0$$

if and only if, for each $i \in \{1, \ldots, M\}$,

$$Z \begin{pmatrix} x_{1,i} \\ x_{2,i} \\ \vdots \\ x_{R,i} \end{pmatrix} = 0 \in \mathbb{Z}_{k_i}.$$

Given $i \in \{1, \ldots, M\}$, k_i divides $|G|$. Since $\gcd(\det(Z), |G|) = 1$, it also holds that $\gcd(\det(Z), k_i) = 1$ for each $i \in \{1, \ldots, M\}$. Therefore, for each $i \in \{1, \ldots, M\}$, Z is invertible over $\mathbb{Z}_{k_i}$, and

$$Z \begin{pmatrix} x_{1,i} \\ x_{2,i} \\ \vdots \\ x_{R,i} \end{pmatrix} = 0 \in \mathbb{Z}_{k_i}$$

if and only if

$$\begin{pmatrix} x_{1,i} \\ x_{2,i} \\ \vdots \\ x_{R,i} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

which holds if and only if $\overline{x} = 0 \in G^R$. Therefore, given $\overline{x} \in G^R$, $Z\overline{x} = 0$ if and only if $\overline{x} = 0$. □

5.3 Preliminary Lemmas

In this section we outline a series of results which contribute to the proof of Theorem 5.1.1. For the entirety of this section we fix $R, S, L \in \mathbb{N}$ with $S \geq 2R+1$ and $R \leq L \leq S-R-1$,

and $Y = (y_{i,j}) \in \mathbb{Z}^{R\times S}$ a matrix satisyfing $y_{i,1} + y_{i,2} + \cdots + y_{i,S} = 0$ for each $i \in \{1, \ldots, R\}$. Fix $N \in \mathbb{N}$. We subsequently fix G, a finite abelian group which is L-coprime to Y with $c(G) \geq N$, and $A \subseteq G$ so that A contains only trivial solutions to the matrix Y.

Lemma 9. *Let* $T(A) = |\{\overline{x} \in A^S : Y\overline{x} = 0\}|$. *Then*

$$T(A) \leq \binom{S}{2}|A|^{S-R-1}.$$

Proof. Suppose $\overline{x} \in A^S$ with $Y\overline{x} = 0$. Since A contains only trivial solutions to the matrix Y, we have that $\overline{x} = (x_1, x_2, \ldots, x_S)$ where $x_i = x_j$ for some $i, j \in \{1, \ldots, S\}$ with $i \neq j$. There are $\binom{S}{2}$ ways to fix two distinct elements i and j from $\{1, \ldots, S\}$. Having chosen $i, j \in \{1, \ldots, S\}$ with $i \neq j$, we consider

$$\big|\{\overline{x} \in A^S : x_i = x_j \text{ and } Y\overline{x} = 0\}\big|.$$

Suppose that $\{i, j\} \cap l_Y(G; L) = \emptyset$, i.e. neither i nor j indexes one of the L columns which satisfies G's L-coprimality with Y. Without loss of generality, suppose that these L columns are indexed by $\{1, 2, \ldots, L\}$. Then the $R \times R$ matrix $Z \in \mathbb{Z}^{R\times R}$ formed by the columns indexed by $\{1, \ldots, R\}$ has $\det(Z)$ coprime to $|G|$, by the definition of G being L-coprime to Y. Since $Y\overline{x} = 0$, we have

$$\begin{aligned}
Z\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_R \end{pmatrix} &= \begin{pmatrix} y_{1,1} & y_{1,2} & \cdots & y_{1,R} \\ y_{2,1} & y_{2,2} & \cdots & y_{2,R} \\ \vdots & \vdots & \ddots & \vdots \\ y_{R,1} & y_{R,2} & \cdots & y_{R,R} \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_R \end{pmatrix} \\
&= \begin{pmatrix} y_{1,1}x_1 + y_{1,2}x_2 + \cdots + y_{1,R}x_R \\ y_{2,1}x_1 + y_{2,2}x_2 + \cdots + y_{2,R}x_R \\ \vdots \\ y_{R,1}x_1 + y_{R,2}x_2 + \cdots + y_{R,R}x_R \end{pmatrix} \\
&= -\begin{pmatrix} y_{1,R+1}x_{R+1} + y_{1,R+2}x_{R+2} + \cdots + y_{1,S}x_S \\ y_{2,R+1}x_{R+1} + y_{2,R+2}x_{R+2} + \cdots + y_{2,S}x_S \\ \vdots \\ y_{R,R+1}x_{R+1} + y_{R,R+2}x_{R+2} + \cdots + y_{R,S}x_S \end{pmatrix}.
\end{aligned}$$

Within the set $\{x_{R+1}, x_{R+2}, \ldots, x_S\} \subseteq A$, there are $|A|$ ways to pick x_i, which fixes $x_j = x_i$. There are $|A|$ ways to pick the each of the remaining $S - R - 2$ elements, so that there are $|A|^{S-R-1}$ ways to determine the set $\{x_{R+1}, x_{R+2}, \ldots, x_S\} \subseteq A$. Since $\gcd(\det(Z), |G|) = 1$, we have by Lemma 8 that Z is invertible over G. As such, once $\{x_{R+1}, x_{R+2}, \ldots, x_S\} \subseteq A$ is fixed, the above equations determine the elements $\{x_1, x_2, \ldots, x_R\}$, which may or may

not be elements of A. Therefore the number of solutions of $Y\overline{x} = 0$ with $\overline{x} \in A^S$ and $x_i = x_j$ is bounded above by $|A|^{S-R-1}$.

Suppose now that $\{i, j\} \cap l_Y(G; L) \neq \emptyset$. Without loss of generality, assume that $j \in l_Y(G; L)$. Since G is L-coprime to Y, we can remove any $L - R + 1$ of the L columns indexed by $l_Y(G; L)$ and there exist within the remaining columns two disjoint sets of R columns forming matrices which have determinant coprime to $|G|$. By removing $L-R+1$ columns which include the j^{th} column, there exist two disjoint R-subsets of $\{1, \ldots, S\}\backslash\{j\}$, called U and V, which index columns forming $R \times R$ matrices with determinant coprime to $|G|$. We have that j is in neither U nor V, and that i is in at most one of U or V. Without loss of generality assume that $U \cap \{i, j\} = \emptyset$. Now our proof mirrors that of the first case:

Without loss of generality assume that $U = \{1, \ldots, R\}$. Within the set $\{x_{R+1}, x_{R+2}, \ldots, x_S\} \subseteq A$, there are $|A|$ ways to pick x_i, which fixes $x_j = x_i$. There are $|A|$ ways to pick the each of the remaining $S - R - 2$ elements, so that there are $|A|^{S-R-1}$ ways to determine the set $\{x_{R+1}, x_{R+2}, \ldots, x_S\} \subseteq A$. We have that the $R \times R$ matrix $Z \in \mathbb{Z}^{R\times R}$ formed by the columns indexed by $U = \{1, \ldots, R\}$ has $\det(Z)$ coprime to $|G|$, and it is invertible over G by Lemma 8. As such, once $\{x_{R+1}, x_{R+2}, \ldots, x_S\} \subseteq A$ is fixed, the invertibility of Z determines the elements $\{x_1, x_2, \ldots, x_R\} \subseteq G$, which may or may not be elements of A. Therefore the number of solutions of $Y\overline{x} = 0$ with $\overline{x} \in A^S$ and $x_i = x_j$ is bounded above by $|A|^{S-R-1}$.

Combining the two cases, we see that upon fixing distinct columns indexed by i and j, the number of solutions $\overline{x} \in A^S$ to $Y\overline{x} = 0$ is bounded above by $|A|^{S-R-1}$. Since there are $\binom{S}{2}$ ways to fix i and j, we have

$$T(A) \leq \binom{S}{2}|A|^{S-R-1}$$

as desired.

□

Lemma 10. *We have that*

$$\sup_{\substack{\gamma\in\widehat{G}\\ \gamma\neq e}} \left|\sum_{x\in A} \gamma(x)\right| \leq d(n-1)|G| - |A|.$$

Proof. This proof is similar in spirit to the proof of Lemma 6. Recall $\delta : \widehat{G} \to \{0, 1\}$ was defined by

$$\delta(\gamma) = \begin{cases} 1, & \text{if } \gamma = e, \\ 0, & \text{otherwise,} \end{cases}$$

and that $\chi_A : G \to \{0,1\}$ was defined by

$$\chi_A(g) = \begin{cases} 1, & \text{if } g \in A, \\ 0, & \text{otherwise.} \end{cases}$$

We first show that

$$\sup_{\gamma \in \widehat{G}} ||G|d(N-1)\delta(\gamma) - \widehat{\chi_{-A}}(\gamma)| \leq d(N-1)|G| - |A|.$$

Let $\gamma \in \widehat{G}$ and let $W = \ker(\gamma)$. Since $\gamma(G)$ is a cyclic group and $\gamma(G) \cong G/W$, we have that $c(W) \geq c(G) - 1 \geq N - 1$. Note that

$$|W|\big||G|d(N-1)\delta(\gamma) - \widehat{\chi_{-A}}(\gamma)\big| = \left| \sum_{y \in W} \sum_{x \in G} d(N-1)\gamma(-x) - \sum_{y \in W} \sum_{x \in G} \chi_{-A}(x)\gamma(-x) \right|.$$

For any $y \in W = \ker(\gamma)$, we have $\gamma(-x) = \gamma(-x-y)$ and

$$\sum_{x \in G} \chi_{-A}(x)\gamma(-x) = \sum_{x \in G} \chi_{-A}(x)\gamma(-x-y) = \sum_{x \in G} \chi_{-A}(x-y)\gamma(-x).$$

Therefore

$$\begin{aligned} |W|\big||G|d(N-1)\delta(\gamma) - \widehat{\chi_{-A}}(\gamma)\big| &= \left| \sum_{x \in G} \left(\sum_{y \in W} d(N-1) - \sum_{y \in W} \chi_{-A}(x-y) \right) \gamma(-x) \right| \\ &\leq \sum_{x \in G} \left| \sum_{y \in W} d(N-1) - \sum_{y \in W} \chi_{-A}(x-y) \right|. \end{aligned}$$

Since

$$\chi_{-A}(x-y) = \begin{cases} 1, & \text{if } x - y \in -A, \\ 0, & \text{otherwise,} \end{cases}$$

we have that

$$\sum_{y \in W} \chi_{-A}(x-y) = |(x-W) \cap -A| = |W \cap (x+A)|.$$

Suppose that $\overline{w} = (w_1, \ldots, w_s) = (x+a_1, x+a_2, \ldots, x+a_s) \in (W \cap (x+A))^S$ with $Y\overline{w} = 0$. Let $\overline{x} = (x, x, \ldots, x) \in G^s$ and $\overline{a} = (a_1, \ldots, a_s) \in A^s$, so that $0 = Y\overline{w} = Y\overline{x} + Y\overline{a}$. Since the elements of each row of Y sum to 0, we have $Y\overline{x} = 0$ which implies $Y\overline{a} = 0$. We chose A so that if $Y\overline{a} = 0$ there is some $i, j \in \{1, \ldots, s\}$ with $i \neq j$ and $a_i = a_j$, so that $w_i = w_j$. Therefore there is no vector $\overline{w} = (w_1, \ldots, w_s) \in W \cap (x+A)$ of distinct elements satisfying $Y\overline{w} = 0$. As such,

$$d(N-1) \geq \frac{|W \cap (x+A)|}{|W|}$$

and

$$\begin{aligned} |W|\big||G|d(N-1)\delta(\gamma) - \widehat{\chi_{-A}}(\gamma)\big| &\leq \sum_{x\in G}\left|\sum_{y\in W} d(N-1) - \sum_{y\in W}\chi_{-A}(x-y)\right|. \\ &= \sum_{x\in G}||W|d(N-1) - |W\cap(x+A)|| \\ &= \sum_{x\in G}|W|d(N-1) - |W\cap(x+A)|. \end{aligned}$$

To compute $\sum_{x\in G}|W\cap(x+A)|$, we first arbitrarily choose $a\in A$. There are $|W|$ different $x\in G$ with $x+a\in W$, so that

$$\sum_{x\in G}|W\cap(x+A)| = |A||W|.$$

It holds that

$$\sum_{x\in G}|W|d(N-1) = |G||W|d(N-1),$$

which results in

$$|W|\big||G|d(N-1)\delta(\gamma) - \widehat{\chi_{-A}}(\gamma)\big| \leq |G||W|d(N-1) - |A||W|.$$

Therefore, for each $\gamma\in\widehat{G}$,

$$\big||G|d(N-1)\delta(\gamma) - \widehat{\chi_{-A}}(\gamma)\big| \leq |G|d(N-1) - |A|,$$

so that

$$\sup_{\gamma\in\widehat{G}}||G|d(N-1)\delta(\gamma) - \widehat{\chi_{-A}}(\gamma)| \leq d(N-1)|G| - |A|.$$

When $\gamma\neq e$, we have $\delta(\gamma)=0$, so that

$$\sup_{\substack{\gamma\in\widehat{G}\\ \gamma\neq e}}|\widehat{\chi_{-A}}(\gamma)| \leq |G|d(N-1) - |A|.$$

We have

$$\widehat{\chi_{-A}}(\gamma) = \sum_{x\in G}\chi_{-A}(x)\gamma(-x) = \sum_{a\in A}\gamma(a),$$

so that

$$\sup_{\substack{\gamma\in\widehat{G}\\ \gamma\neq e}}\left|\sum_{a\in A}\gamma(a)\right| = \sup_{\substack{\gamma\in\widehat{G}\\ \gamma\neq e}}|\widehat{\chi_{-A}}(\gamma)| \leq |G|d(N-1)-|A|.$$

□

Lemma 11. *Define*

$$Q_Y(G;L) = \big\{B \subseteq l_Y(G;L) : |B| = L-R+1\big\}.$$

Given $B \in Q_Y(G;L)$, define

$$\Gamma_{B,Y}(G;L) = \big\{(\gamma_1,\gamma_2,\ldots,\gamma_R) \in \widehat{G}^R : \gamma_1^{y_{1,j}}\gamma_2^{y_{2,j}}\cdots\gamma_R^{y_{R,j}} \neq e \text{ for all } j \in B\big\}.$$

Then

$$\widehat{G}^R \setminus \{e\} = \Gamma(G) \subseteq \bigcup_{B\in Q_Y(G;L)} \Gamma_{B,Y}(G;L).$$

Proof. Fix $(\gamma_1,\gamma_2,\ldots,\gamma_R) \in \Gamma(G)$. It holds that amongst any R columns chosen from the L columns satisfying G's L-coprimality to Y, there exists some column indexed by k so that

$$\gamma_1^{y_{1,k}}\gamma_2^{y_{2,k}}\cdots\gamma_R^{y_{R,k}} \neq e.$$

To verify this we assume otherwise: Choose R columns from the L columns satisfying the L-coprimality of G, and let these R columns be indexed by $\{l_1,l_2,\ldots,l_R\} \subseteq l_Y(G;L)$. Let $Z \in \mathbb{Z}^R$ be the matrix formed by these R columns, and note that since G is L-coprime to Y, we have $Z = (y_{i,l_j})_{1\leq i,l_j\leq R}$ satisfies $\gcd(\det(Z),|G|) = 1$. Assume that

$$\gamma_1^{y_{1,l_j}}\gamma_2^{y_{2,l_j}}\cdots\gamma_R^{y_{R,l_j}} = e$$

for each $j \in \{1,\ldots,R\}$. We saw in Chapter 1 that $G \cong \widehat{G}$. Let $\rho : \widehat{G} \to G$ be an isomorphism, so that for each $j \in \{1,\ldots,R\}$,

$$0 = \rho(e) = \rho(\gamma_1^{y_{1,l_j}}\gamma_2^{y_{2,l_j}}\cdots\gamma_R^{y_{R,l_j}}) = y_{1,l_j}\rho(\gamma_1) + y_{2,l_j}\rho(\gamma_2) + \cdots + y_{R,l_j}\rho(\gamma_R).$$

As such,

$$\begin{aligned}
\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} &= \begin{pmatrix} y_{1,l_1}\rho(\gamma_1) + y_{2,l_1}\rho(\gamma_2) + \cdots + y_{R,l_1}\rho(\gamma_R) \\ y_{1,l_2}\rho(\gamma_1) + y_{2,l_2}\rho(\gamma_2) + \cdots + y_{R,l_2}\rho(\gamma_R) \\ \vdots \\ y_{1,l_R}\rho(\gamma_1) + y_{2,l_R}\rho(\gamma_2) + \cdots + y_{R,l_R}\rho(\gamma_R) \end{pmatrix} \\
&= \big(\rho(\gamma_1), \rho(\gamma_2), \ldots, \rho(\gamma_R)\big) \begin{pmatrix} y_{1,l_1} & y_{1,l_2} & \cdots & y_{1,l_R} \\ y_{2,l_1} & y_{2,l_2} & \cdots & y_{2,l_R} \\ \vdots & \vdots & \ddots & \vdots \\ y_{R,l_1} & y_{R,l_2} & \cdots & y_{R,l_R} \end{pmatrix} \\
&= \big(\rho(\gamma_1), \rho(\gamma_2), \ldots, \rho(\gamma_R)\big) Z.
\end{aligned}$$

By Lemma 8, we have $\rho(\gamma_1) = \rho(\gamma_2) = \cdots = \rho(\gamma_R) = 0$. Since ρ is an isomorphism from $\widehat{G}$ to G, we have that $(\gamma_1, \gamma_2, \ldots, \gamma_R) = e \in \widehat{G}^R$. This contradicts the fact that $(\gamma_1, \gamma_2, \ldots, \gamma_R) \in \Gamma(G)$. Therefore, there exists some $k \in \{l_1, \ldots, l_R\}$ with

$$\gamma_1^{y_{1,k}} \gamma_2^{y_{2,k}} \cdots \gamma_R^{y_{R,k}} \neq e.$$

Iteratively, choose R columns, indexed by $\{l_1, \ldots, l_R\} \subseteq l_Y(G; L)$. There is some $k_1 \in \{l_1, \ldots, l_R\}$ with

$$\gamma_1^{y_{1,k_1}} \gamma_2^{y_{2,k_1}} \cdots \gamma_R^{y_{R,k_1}} \neq e.$$

If possible, choose R columns indexed by $\{l_1, \ldots, l_R\} \subseteq l_Y(G; L) \setminus \{k_1\}$. There is some $k_2 \in \{l_1, \ldots, l_R\}$ with

$$\gamma_1^{y_{1,k_2}} \gamma_2^{y_{2,k_2}} \cdots \gamma_R^{y_{R,k_2}} \neq e.$$

At the i^{th} step, choose R columns indexed by $\{l_1, \ldots, l_R\} \subseteq l_Y(G; L) \setminus \{k_1, \ldots, k_{i-1}\}$ if possible, and choose $k_i \in \{l_1, \ldots, l_R\}$ with

$$\gamma_1^{y_{1,k_i}} \gamma_2^{y_{2,k_i}} \cdots \gamma_R^{y_{R,k_i}} \neq e.$$

After $L - R + 1$ steps, it is no longer possible to choose R columns since

$$\big|l_Y(G; L) \setminus \{k_1, \ldots, k_{L-R+1}\}\big| = R - 1.$$

Let $B = \{k_1, \ldots, k_{L-R+1}\}$. Then for all $j \in B$,

$$\gamma_1^{y_{1,j}} \gamma_2^{y_{2,j}} \cdots \gamma_R^{y_{R,j}} \neq e$$

so that $(\gamma_1, \gamma_2, \ldots, \gamma_R) \in \Gamma_{B,Y}(G; L)$. Since $(\gamma_1, \ldots, \gamma_R) \in \Gamma(G)$ was chosen arbitrarily,

$$\Gamma(G) \subseteq \bigcup_{B \in Q_Y(G;L)} \Gamma_{B,Y}(G; L)$$

as desired.

□

Definition 5.3.1. Let G be a finite abelian group and let $A \subseteq G$. For $\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_R) \in \widehat{G}^R$, define

$$F_j(\gamma; A) = \sum_{x \in A} \gamma_1(y_{1,j}x)\gamma_2(y_{2,j}x) \cdots \gamma_R(y_{R,j}x).$$

When it is clear from context, we write $F_j(\gamma) = F_j(\gamma; A)$. By properties of the dual group, we can equivalently characterize $F_j(\gamma)$ in the following ways:

$$\begin{aligned} F_j(\gamma) &= \sum_{x \in A} \gamma_1(y_{1,j}x)\gamma_2(y_{2,j}x) \cdots \gamma_R(y_{R,j}x) \\ &= \sum_{x \in A} \gamma_1^{y_{1,j}}(x)\gamma_2^{y_{2,j}}(x) \cdots \gamma_R^{y_{R,j}}(x) \\ &= \sum_{x \in A} \gamma_1^{y_{1,j}}\gamma_2^{y_{2,j}} \cdots \gamma_R^{y_{R,j}}(x). \end{aligned}$$

Lemma 12. *It holds that*

$$\frac{1}{|G|^R} \sum_{\gamma \in \Gamma(G)} \big|F_1F_2 \cdots F_S(\gamma)\big| \leq \binom{L}{L-R+1} \big(d(N-1)|G| - |A|\big)^{L-R+1} |A|^{S-L-1}.$$

Proof. As defined in Lemma 11, let

$$Q_Y(G; L) = \big\{B \subseteq l_Y(G; L) : |B| = L - R + 1\big\},$$

and for $B \in Q_Y(G; L)$, let

$$\Gamma_{B,Y}(G; L) = \big\{(\gamma_1, \gamma_2, \ldots, \gamma_R) \in \widehat{G}^R : \gamma_1^{y_{1,j}}\gamma_2^{y_{2,j}} \cdots \gamma_R^{y_{R,j}} \neq e \text{ for all } j \in B\big\}.$$

Given $B \in Q$, we have

$$\begin{aligned}
\frac{1}{|G|^R}\sum_{\gamma\in\Gamma_B}\left|F_1F_2\cdots F_S(\gamma)\right| &= \frac{1}{|G|^R}\sum_{\gamma\in\Gamma_B}\left(\prod_{j\in B}|F_j(\gamma)|\right)\left(\prod_{j\notin B}|F_j(\gamma)|\right)\\
&\leq \frac{1}{|G|^R}\left(\sup_{\gamma\in\Gamma_B}\prod_{j\in B}|F_j(\gamma)|\right)\sum_{\gamma\in\Gamma_B}\prod_{j\notin B}|F_j(\gamma)|\\
&\leq \frac{1}{|G|^R}\left(\prod_{j\in B}\left(\sup_{\gamma\in\Gamma_B}|F_j(\gamma)|\right)\right)\sum_{\gamma\in\Gamma_B}\prod_{j\notin B}|F_j(\gamma)|.
\end{aligned}$$

Recalling the definition of Γ_B, we notice that for $j \in B$ and $\gamma \in \Gamma_B$,

$$\gamma_1^{y_{1,j}}\gamma_2^{y_{2,j}}\cdots\gamma_R^{y_{R,j}} \neq e$$

so that

$$\gamma_1^{y_{1,j}}\gamma_2^{y_{2,j}}\cdots\gamma_R^{y_{R,j}} \in \Gamma(G).$$

Therefore, by Lemma 10

$$\begin{aligned}
\sup_{\gamma\in\Gamma_B}|F_j(\gamma)| &= \sup_{\gamma\in\Gamma_B}\left|\sum_{x\in A}\gamma_1^{y_{1,j}}\gamma_2^{y_{2,j}}\cdots\gamma_R^{y_{R,j}}(x)\right|\\
&\leq \sup_{\gamma\in\Gamma(G)}\left|\sum_{x\in A}\gamma(x)\right|\\
&\leq d(N-1)|G|-|A|.
\end{aligned}$$

This implies that

$$\begin{aligned}
\frac{1}{|G|^R}\sum_{\gamma\in\Gamma_B}\left|F_1F_2\cdots F_S(\gamma)\right| &\leq \frac{1}{|G|^R}\left(\prod_{j\in B}d(N-1)|G|-|A|\right)\sum_{\gamma\in\Gamma_B}\prod_{j\notin B}|F_j(\gamma)|\\
&= \frac{1}{|G|^R}\left(d(N-1)|G|-|A|\right)^{|B|}\sum_{\gamma\in\Gamma_B}\prod_{j\notin B}|F_j(\gamma)|\\
&= \left(d(N-1)|G|-|A|\right)^{L-R+1}\frac{1}{|G|^R}\sum_{\gamma\in\Gamma_B}\prod_{j\notin B}|F_j(\gamma)|.
\end{aligned}$$

We have that $B \subseteq l_Y(G;L)$ with $|B| = L-R+1$, so that we can apply the second condition of G being L-coprime to Y: After removing the columns indexed by B we can find two disjoint subsets $U, V \subseteq \{1,\ldots,S\}\setminus B$ so that

1. $|U| = |V| = R$,
2. the matrix formed by the columns indexed by U has determinant coprime to $|G|$,
3. the matrix formed by the columns indexed by V has determinant coprime to $|G|$.

Let $U = \{j_1, j_2, \ldots, j_R\}$, and let $Z \in \mathbb{Z}^{R\times R}$ be the matrix formed by the columns indexed by U, i.e.

$$Z = \begin{pmatrix} y_{1,j_1} & y_{1,j_2} & \cdots & y_{1,j_R} \\ y_{2,j_1} & y_{2,j_2} & \cdots & y_{2,j_R} \\ \vdots & \vdots & \ddots & \vdots \\ y_{R,j_1} & y_{R,j_2} & \cdots & y_{R,j_R} \end{pmatrix},$$

$\gcd(\det(Z), |G|) = 1$, and Z is invertible over G by Lemma 8. Notice that

$$\begin{aligned} \frac{1}{|G|^R} \sum_{\gamma\in\widehat{G}^R} \left| \prod_{j\in U} F_j(\gamma) \right|^2 &= \frac{1}{|G|^R} \sum_{\gamma\in\widehat{G}^R} \prod_{j\in U} |F_j(\gamma)|^2 \\ &= \frac{1}{|G|^R} \sum_{\gamma\in\widehat{G}^R} \prod_{j\in U} \langle F_j(\gamma), F_j(\gamma)\rangle \\ &= \frac{1}{|G|^R} \sum_{\gamma\in\widehat{G}^R} \prod_{j\in U} \left\langle \sum_{a\in A} \gamma_1^{y_{1,j}} \gamma_2^{y_{2,j}} \cdots \gamma_R^{y_{R,j}}(a), \sum_{b\in A} \gamma_1^{y_{1,j}} \gamma_2^{y_{2,j}} \cdots \gamma_R^{y_{R,j}}(b) \right\rangle. \end{aligned}$$

Utilizing properties of the dual group and by indexing $U = \{j_1, j_2, \ldots, j_R\}$, we have

$$\begin{aligned} \frac{1}{|G|^R} \sum_{\gamma\in\widehat{G}^R} \left| \prod_{j\in U} F_j(\gamma) \right|^2 &= \frac{1}{|G|^R} \sum_{\gamma\in\widehat{G}^R} \prod_{i=1}^{R} \sum_{a,b\in A} \left\langle \gamma_1^{y_{1,j_i}} \gamma_2^{y_{2,j_i}} \cdots \gamma_R^{y_{R,j_i}}(a), \gamma_1^{y_{1,j_i}} \gamma_2^{y_{2,j_i}} \cdots \gamma_R^{y_{R,j_i}}(b) \right\rangle \\ &= \frac{1}{|G|^R} \sum_{\gamma\in\widehat{G}^R} \prod_{i=1}^{R} \left(\sum_{a,b\in A} \gamma_1^{y_{1,j_i}} \gamma_2^{y_{2,j_i}} \cdots \gamma_R^{y_{R,j_i}}(a-b) \right) \\ &= \frac{1}{|G|^R} \sum_{\gamma\in\widehat{G}^R} \prod_{i=1}^{R} \left(\sum_{a,b\in A} \gamma_1(y_{1,j_i}a - y_{1,j_i}b) \cdots \gamma_R(y_{R,j_i}a - y_{R,j_i}b) \right). \end{aligned}$$

For $\overline{a} = (a_1, \ldots, a_R), \overline{b} = (b_1, \ldots, b_R) \in A^R$, we may instead write

$$\overline{a} = \begin{pmatrix} a_{j_1} \\ a_{j_2} \\ \vdots \\ a_{j_R} \end{pmatrix} \quad \text{and} \quad \overline{b} = \begin{pmatrix} b_{j_1} \\ b_{j_2} \\ \vdots \\ b_{j_R} \end{pmatrix}.$$

It holds that

$$\begin{aligned} &\prod_{i=1}^{R} \left(\sum_{a,b \in A} \gamma_1(y_{1,j_i} a - y_{1,j_i} b) \cdots \gamma_R(y_{R,j_i} a - y_{R,j_i} b) \right) \\ &= \sum_{\overline{a},\overline{b} \in A^R} \gamma_1 \left(\sum_{i=1}^{R} y_{1,j_i}(a_{j_i} - b_{j_i}) \right) \cdots \gamma_R \left(\sum_{i=1}^{R} y_{R,j_i}(a_{j_i} - b_{j_i}) \right). \end{aligned}$$

Therefore

$$\begin{aligned} &\frac{1}{|G|^R} \sum_{\gamma \in \widehat{G}^R} \left| \prod_{j \in U} F_j(\gamma) \right|^2 \\ &= \frac{1}{|G|^R} \sum_{\gamma \in \widehat{G}^R} \sum_{a,b \in A^R} \gamma_1 \left(\sum_{i=1}^{R} y_{1,j_i}(a_{j_i} - b_{j_i}) \right) \cdots \gamma_R \left(\sum_{i=1}^{R} y_{R,j_i}(a_{j_i} - b_{j_i}) \right) \\ &= \sum_{a,b \in A^R} \frac{1}{|G|^R} \sum_{\gamma \in \widehat{G}^R} \gamma_1 \left(\sum_{i=1}^{R} y_{1,j_i}(a_{j_i} - b_{j_i}) \right) \cdots \gamma_R \left(\sum_{i=1}^{R} y_{R,j_i}(a_{j_i} - b_{j_i}) \right). \end{aligned}$$

By Proposition 5.2.2, the inner sum is only non-zero when

$$\sum_{i=1}^{R} y_{1,j_i}(a_{j_i} - b_{j_i}) = \cdots = \sum_{i=1}^{R} y_{R,j_i}(a_{j_i} - b_{j_i}) = 0.$$

In this case, the inner sum is equal to $|G|^R$. We therefore have

$$\frac{1}{|G|^R} \sum_{\gamma \in \widehat{G}^R} \gamma_1 \left(\sum_{i=1}^{R} y_{1,j_i}(a_{j_i} - b_{j_i}) \right) \cdots \gamma_R \left(\sum_{i=1}^{R} y_{R,j_i}(a_{j_i} - b_{j_i}) \right) = 1$$

if and only if

$$\begin{pmatrix} y_{1,j_1}a_{j_1} + y_{1,j_2}a_{j_2} + \cdots y_{1,j_R}a_{j_R} \\ y_{2,j_1}a_{j_1} + y_{2,j_2}a_{j_2} + \cdots y_{2,j_R}a_{j_R} \\ \vdots \\ y_{R,j_1}a_{j_1} + y_{R,j_2}a_{j_2} + \cdots y_{R,j_R}a_{j_R} \end{pmatrix} = \begin{pmatrix} y_{1,j_1}b_{j_1} + y_{1,j_2}b_{j_2} + \cdots y_{1,j_R}b_{j_R} \\ y_{2,j_1}b_{j_1} + y_{2,j_2}b_{j_2} + \cdots y_{2,j_R}b_{j_R} \\ \vdots \\ y_{R,j_1}b_{j_1} + y_{R,j_2}b_{j_2} + \cdots y_{R,j_R}b_{j_R} \end{pmatrix},$$

which is equivalent to

$$\begin{pmatrix} y_{1,j_1} & y_{1,j_2} & \cdots & y_{1,j_R} \\ y_{2,j_1} & y_{2,j_2} & \cdots & y_{2,j_R} \\ \vdots & \vdots & \ddots & \vdots \\ y_{R,j_1} & y_{R,j_2} & \cdots & y_{R,j_R} \end{pmatrix} \begin{pmatrix} a_{j_1} \\ a_{j_2} \\ \vdots \\ a_{j_R} \end{pmatrix} = \begin{pmatrix} y_{1,j_1} & y_{1,j_2} & \cdots & y_{1,j_R} \\ y_{2,j_1} & y_{2,j_2} & \cdots & y_{2,j_R} \\ \vdots & \vdots & \ddots & \vdots \\ y_{R,j_1} & y_{R,j_2} & \cdots & y_{R,j_R} \end{pmatrix} \begin{pmatrix} b_{j_1} \\ b_{j_2} \\ \vdots \\ b_{j_R} \end{pmatrix}.$$

The preceding equality can be expressed as $Z\overline{a} = Z\overline{b}$. Since Z is invertible over G, this equality holds if and only if $\overline{a} = \overline{b}$, so that having chosen $\overline{a} \in A^R$, it determines $\overline{b} = \overline{a}$. As such, we can write

$$\frac{1}{|G|^R} \sum_{\gamma \in \widehat{G}^R} \left| \prod_{j \in U} F_j(\gamma) \right|^2 = \sum_{\overline{a} \in A^R} 1 = |A|^R.$$

Similarly,

$$\frac{1}{|G|^R} \sum_{\gamma \in \widehat{G}^R} \left| \prod_{j \in V} F_j(\gamma) \right|^2 = \sum_{\overline{a} \in A^R} 1 = |A|^R.$$

Notice that for $\gamma \in \widehat{G}^R$ and $j \in \{1, \ldots, S\}$,

$$|F_j(\gamma)| = \left| \sum_{x \in A} \gamma_1^{y_{1,j}} \gamma_2^{y_{2,j}} \cdots \gamma_R^{y_{R,j}}(x) \right| \leq \sum_{x \in A} \left| \gamma_1^{y_{1,j}} \gamma_2^{y_{2,j}} \cdots \gamma_R^{y_{R,j}}(x) \right| = \sum_{x \in A} 1 = |A|.$$

Therefore

$$\begin{aligned} \frac{1}{|G|^R} \sum_{\gamma \in \widehat{G}^R} \prod_{j \notin B} |F_j(\gamma)| &= \frac{1}{|G|^R} \sum_{\gamma \in \widehat{G}^R} \prod_{j \in U} |F_j(\gamma)| \prod_{j \in V} |F_j(\gamma)| \prod_{\substack{j \notin B \\ j \notin U \cup V}} |F_j(\gamma)| \\ &\leq \frac{1}{|G|^R} \sum_{\gamma \in \widehat{G}^R} \left| \prod_{j \in U} F_j(\gamma) \right| \left| \prod_{j \in V} F_j(\gamma) \right| |A|^{|\{1,\ldots,S\} \setminus (B \cup U \cup V)|} \\ &= |A|^{S-L-1-R} \frac{1}{|G|^R} \sum_{\gamma \in \widehat{G}^R} \left| \prod_{j \in U} F_j(\gamma) \right| \left| \prod_{j \in V} F_j(\gamma) \right|. \end{aligned}$$

Remark that B, U, V are all disjoint, with $|B| = L - R + 1$ and $|U| = |V| = R$, so that $|\{1, \dots, S\} \setminus (B \cup U \cup V)| = S - L - 1 - R$. By Cauchy's inequality and previous calculations, it follow that

$$\begin{aligned}
\frac{1}{|G|^R} \sum_{\gamma \in \widehat{G}^R} \prod_{j \notin B} |F_j(\gamma)| &\leq |A|^{S-L-1-R} \left(\frac{1}{|G|^R} \sum_{\gamma \in \widehat{G}^R} \left| \prod_{j \in U} F_j(\gamma) \right|^2 \right)^{\frac{1}{2}} \left(\frac{1}{|G|^R} \sum_{\gamma \in \widehat{G}^R} \left| \prod_{j \in V} F_j(\gamma) \right|^2 \right)^{\frac{1}{2}} \\
&= |A|^{S-L-1-R} |A|^{\frac{R}{2}} |A|^{\frac{R}{2}} \\
&= |A|^{S-L-1}.
\end{aligned}$$

Continuing with previous estimates, we see that

$$\begin{aligned}
\frac{1}{|G|^R} \sum_{\gamma \in \Gamma_B} \left| F_1 F_2 \cdots F_S(\gamma) \right| &\leq (d(N-1)|G| - |A|)^{L-R+1} \frac{1}{|G|^R} \sum_{\gamma \in \Gamma_B} \prod_{j \notin B} |F_j(\gamma)| \\
&\leq (d(N-1)|G| - |A|)^{L-R+1} \frac{1}{|G|^R} \sum_{\gamma \in \widehat{G}^R} \prod_{j \notin B} |F_j(\gamma)| \\
&\leq (d(N-1)|G| - |A|)^{L-R+1} |A|^{S-L-1}.
\end{aligned}$$

We also have that

$$\sum_{\gamma \in \Gamma_B} \left| F_1 F_2 \cdots F_S(\gamma) \right| \leq |G|^R (d(N-1)|G| - |A|)^{L-R+1} |A|^{S-L-1}.$$

By Lemma 11, it holds that

$$\Gamma(G) \subseteq \bigcup_{B \in Q_Y(G;L)} \Gamma_{B,Y}(G; L),$$

so that

$$\begin{aligned}
\sum_{\gamma \in \Gamma(G)} \left| F_1 F_2 \cdots F_S(\gamma) \right| &\leq \sum_{B \in Q_Y(G;L)} \sum_{\gamma \in \Gamma_B} \left| F_1 F_2 \cdots F_S(\gamma) \right| \\
&\leq |Q_Y(G; L)| |G|^R (d(N-1)|G| - |A|)^{L-R+1} |A|^{S-L-1}.
\end{aligned}$$

Since

$$Q_Y(G; L) = \big\{ B \subseteq l_Y(G; L) : |B| = L - R + 1 \big\},$$

we have that

$$|Q_Y(G; L)| = \binom{L}{L - R + 1}$$

and

$$\frac{1}{|G|^R}\sum_{\gamma\in\Gamma(G)} \leq \binom{L}{L-R+1}\left(d(N-1)|G|-|A|\right)^{L-R+1}|A|^{S-L-1},$$

as desired.

□

Lemma 13. *It holds that*

$$\frac{|A|^S}{|G|^R}-\binom{L}{L-R+1}\left(d(N-1)|G|-|A|\right)^{L-R+1}|A|^{S-L-1} \leq \binom{S}{2}|A|^{S-R-1}.$$

Proof. Recall that $T(A)=|\{\overline{x}\in A^S : Y\overline{x}=0\}|$, and notice that

$$\begin{aligned}
\sum_{\gamma\in\widehat{G}^R} F_1F_2\cdots F_S(\gamma) &= \sum_{\gamma\in\widehat{G}^R}\left(\prod_{i=1}^{S}F_i(\gamma)\right)\\
&= \sum_{\gamma\in\widehat{G}^R}\left(\prod_{i=1}^{S}\left(\sum_{x\in A}\gamma_1(y_{1,i}x)\gamma_2(y_{2,i}x)\cdots\gamma_R(y_{R,i}x)\right)\right)\\
&= \sum_{\gamma\in\widehat{G}^R}\left(\sum_{x_1\in A}\gamma_1(y_{1,1}x_1)\cdots\gamma_R(y_{R,1}x_1)\right)\cdots\left(\sum_{x_R\in A}\gamma_1(y_{1,S}x_S)\cdots\gamma_R(y_{R,S}x_S)\right)\\
&= \sum_{\gamma\in\widehat{G}^R}\sum_{(x_1,\ldots,x_S)\in A^S}\left(\prod_{i=1}^{S}\gamma_1(y_{1,i}x_i)\right)\cdots\left(\prod_{i=1}^{S}\gamma_R(y_{1,i}x_i)\right)\\
&= \sum_{(x_1,\ldots,x_S)\in A^S}\sum_{\gamma\in\widehat{G}^R}\gamma_1\left(\sum_{i=1}^{S}y_{1,i}x_i\right)\cdots\gamma_R\left(\sum_{i=1}^{S}y_{R,i}x_i\right).
\end{aligned}$$

By Proposition 5.2.2, we have

$$\sum_{\gamma\in\widehat{G}^R}\gamma_1\left(\sum_{i=1}^{S}y_{1,i}x_i\right)\cdots\gamma_R\left(\sum_{i=1}^{S}y_{R,i}x_i\right)=\begin{cases}|G|^R, & \text{if } \left(\sum_{i=1}^{S}y_{1,i}x_i\right)=\cdots=\left(\sum_{i=1}^{S}y_{R,i}x_i\right)=0,\\ 0, & \text{otherwise.}\end{cases}$$

Therefore

$$\begin{aligned}
\sum_{\gamma\in\widehat{G}^R}F_1F_2\cdots F_S(\gamma) &= |G|^R\left|\left\{(x_1,\ldots,x_S)\in A^S : \sum_{i=1}^{S}y_{j,i}x_i=0 \text{ for each } j\in\{1,\ldots,R\}\right\}\right|\\
&= |G|^R\left|\left\{\overline{x}\in A^S : Y\overline{x}=0\right\}\right|\\
&= |G|^RT(A).
\end{aligned}$$

Note that for each $i \in \{1, \ldots, S\}$,

$$F_i(e) = \sum_{x \in A} e(y_{1,i}x)e(y_{2,i}x)\cdots e(y_{R,i}x) = \sum_{x \in A} 1 = |A|.$$

We can therefore deduce that

$$\begin{aligned} T(A) &= \frac{1}{|G|^R}F_1(e)F_2(e)\cdots F_S(e) + \frac{1}{|G|^R}\sum_{\gamma \in \Gamma(G)} F_1F_2\cdots F_S(\gamma) \\ &= \frac{|A|^S}{|G|^R} + \frac{1}{|G|^R}\sum_{\gamma \in \Gamma(G)} F_1F_2\cdots F_S(\gamma). \end{aligned}$$

By Lemma 12 we can conclude that

$$\begin{aligned} T(A) &\geq \frac{|A|^S}{|G|^R} - \frac{1}{|G|^R}\sum_{\gamma \in \Gamma(G)} |F_1F_2\cdots F_S(\gamma)| \\ &\geq \frac{|A|^S}{|G|^R} - \binom{L}{L-R+1}\big(d(N-1)|G| - |A|\big)^{L-R+1}|A|^{S-L-1}. \end{aligned}$$

By Lemma 9,

$$\frac{|A|^S}{|G|^R} - \binom{L}{L-R+1}\big(d(N-1)|G| - |A|\big)^{L-R+1}|A|^{S-L-1} \leq \binom{S}{2}|A|^{S-R-1}$$

therefore proving the lemma.

□

5.4 Proof of Theorem 5.1.1

Let $R, S \in \mathbb{N}$ with $S \geq 2R+1$. Let $Y = (y_{i,j}) \in \mathbb{Z}^{R\times S}$ be a matrix satisfying $y_{i,1} + y_{i,2} + \cdots + y_{i,S} = 0$ for each $i \in \{1, \ldots, R\}$. Let $L \in \mathbb{N}$ with $R \leq L \leq S-R-1$. Let $N \in \mathbb{N}$. Let G be a finite abelian group so that $c(G) \geq N$ and G is L-coprime to Y. Let $A \subseteq G$ contain only trivial solutions to Y. Let $d^*(G) = |A|/|G|$.To ease our calculations, we introduce the

following notation:

1) $C_1 = \binom{S}{2}$,

2) $C_2 = \binom{L}{L-R+1}$,

3) $C_3 = (2C_2)^{\frac{-1}{L-R+1}} = \left(2\binom{L}{L-R+1}\right)^{\frac{-1}{L-R+1}}$,

4) $C_4 = (C_3+1)^{\frac{R}{L-R+1}} = \left(\left(2\binom{L}{L-R+1}\right)^{\frac{-1}{L-R+1}}+1\right)^{\frac{R}{L-R+1}}$.

Let

$$C = \max\left\{\frac{(R+1)(L-R+1)}{eR\ln(2)}(2C_1)^{\frac{R}{(R+1)(L-R+1)}}, \quad \frac{C_4}{C_4-1}\right\}.$$

We will show by induction that

$$d^*(G) \leq \left(\frac{C}{N}\right)^{\frac{L-R+1}{R}},$$

and since G and A were chosen arbitrarily, we can conclude that

$$d_Y(N;L) = \sup\left\{d^*(G) | G \text{ is } L\text{-coprime to } Y, c(G) \geq N\right\} \leq \left(\frac{C}{N}\right)^{\frac{L-R+1}{R}},$$

thus proving Theorem 5.1.1.

Notice that when $N \leq C$, we always have that

$$d^*(G) = \frac{|A|}{|G|} \leq 1 \leq \left(\frac{C}{N}\right)^{\frac{L-R+1}{R}}$$

so the theorem holds trivially. Notice also that $C \geq \frac{C_4}{C_4-1} > 1$, so this addresses the base case. We now assume that $N > C$ and consider two cases:

Case I: Suppose that

$$d^*(G) - \frac{C_1 d^*(G)^{S-R-1}}{|G|} \leq \frac{d^*(G)^S}{2}$$

so that

$$\frac{d^*(G)^S}{2} \leq \frac{C_1 d^*(G)^{S-R-1}}{|G|}.$$

This simplifies to

$$d^*(G)^{R+1} \leq \frac{2C_1}{|G|}$$

so that

$$d^*(G) \leq \left(\frac{2C_1}{|G|}\right)^{\frac{1}{R+1}}.$$

Since $c(G) \geq N$, it holds that $|G| \geq 2^N$, so that

$$d^*(G) \leq \left(\frac{2C_1}{|G|}\right)^{\frac{1}{R+1}} \leq \left(\frac{2C_1}{2^N}\right)^{\frac{1}{R+1}} = (2C_1)^{\frac{1}{R+1}} 2^{\frac{-N}{R+1}}.$$

To obtain the result of Theorem 5.1.1, we will verify that

$$\left(\frac{2C_1}{2^N}\right)^{\frac{1}{R+1}} \leq \left(\frac{C}{N}\right)^{\frac{L-R+1}{R}}.$$

Define a function $f : [0, \infty) \to \mathbb{R}$ with

$$f(x) = 2^{\frac{-x}{R+1}} x^{\frac{L-R+1}{R}}.$$

Notice that f is continuous, f is non-negative on $[0, \infty)$, $f(0) = 0$, and that the limit of f as x approaches infinity is 0. Therefore, f attains its maximum on $[0, \infty)$. We have that

$$f'(x) = 2^{\frac{-x}{R+1}} \left(\frac{L-R+1}{R}\right) x^{\frac{L-2R+1}{R}} - \frac{\ln(2)}{R+1} 2^{\frac{-x}{R+1}} x^{\frac{L-R+1}{R}}.$$

Setting $f'(x) = 0$ gives us the unique critical point of f at

$$x = \frac{(L-R+1)(R+1)}{R\ln(2)},$$

so that for $x \in [0, \infty)$,

$$f(x) \leq f\left(\frac{(L-R+1)(R+1)}{R\ln(2)}\right) = \left(\frac{(L-R+1)(R+1)}{eR\ln(2)}\right)^{\frac{L-R+1}{R}}.$$

Therefore

$$\begin{aligned}\left(\frac{2C_1}{2^N}\right)^{\frac{1}{R+1}} N^{\frac{L-R+1}{R}} &= (2C_1)^{\frac{1}{R+1}} f(N) \\ &\leq (2C_1)^{\frac{1}{R+1}} \left(\frac{(L-R+1)(R+1)}{eR\ln(2)}\right)^{\frac{L-R+1}{R}} \\ &\leq C^{\frac{L-R+1}{R}}.\end{aligned}$$

As such, we have

$$d^*(G) \leq \left(\frac{2C_1}{2^N}\right)^{\frac{1}{R+1}} \leq \left(\frac{C}{N}\right)^{\frac{L-R+1}{R}}$$

as desired.

Case II: Suppose that

$$d^*(G)^S - \frac{C_1 d^*(G)^{S-R-1}}{|G|} > \frac{d^*(G)^S}{2}.$$

Noticing that $|A| = d^*(G)|G|$ and incorporating the definitions of $C_1$and C_2, the conclusion of Lemma 13 can be expressed as

$$d^*(G)^S|G|^{S-R} - C_1 d^*(G)^{S-R-1}|G|^{S-R-1} - C_2\big(d(N-1)|G| - d^*(G)|G|\big)^{L-R+1} d^*(G)^{S-L-1}|G|^{S-L-1} \leq 0,$$

which reduces to

$$d^*(G)^S - \frac{C_1 d^*(G)^{S-R-1}}{|G|} - C_2\big(d(N-1) - d^*(G)\big)^{L-R+1} d^*(G)^{S-L-1} \leq 0.$$

Our assumption for the second case means that

$$\frac{d^*(G)^S}{2} \leq C_2\big(d(N-1) - d^*(G)\big)^{L-R+1} d^*(G)^{S-L-1},$$

which simplifies to

$$d^*(G)^{L+1} \leq 2C_2\big(d(N-1) - d^*(G)\big)^{L-R+1}.$$

We get that

$$d^*(G)^{\frac{L+1}{L-R+1}} \leq (2C_2)^{\frac{1}{L-R+1}}\big(d(N-1) - d^*(G)\big)$$

so that

$$C_3 d^*(G)^{\frac{L+1}{L-R+1}} + d^*(G) \leq d(N-1).$$

For $x \in (1, \infty)$, define

$$g(x) = \frac{x^{\frac{L+1}{R}}}{(x-1)^{\frac{L-R+1}{R}}} - x.$$

We will see that $g(x)$ is a decreasing function, and to ease our computations we let $s = \frac{L+1}{R}$. As such, $s > 1$ because $L \geq R$. Write

$$g(x) = x^s(x-1)^{s-1} - x.$$

Therefore

$$g'(x) = sx^{s-1}(x-1)^{1-s} + x^s(1-s)(x-1)^{-s} - 1.$$

We have

$$\begin{aligned} g''(x) &= s(s-1)x^{s-2}(x-1)^{1-s} + sx^{s-1}(1-s)(x-1)^{-s} \\ &\quad +(1-s)sx^{s-1}(x-1)^{-s} + (1-s)x^s(-s)(x-1)^{-s-1} \\ &= s(s-1)\frac{x^{s-2}}{(x-1)^{s-1}}\left(1 - 2\left(\frac{x}{x-1}\right) + \left(\frac{x}{x-1}\right)^2\right) \\ &= s(s-1)\frac{x^{s-2}}{(x-1)^{s-1}}\left(1 - \frac{x}{x-1}\right)^2. \end{aligned}$$

Since $x > 1$ and $s > 1$ we conclude that g is concave up. By L'Hopital's rule, we see that

$$\begin{aligned} \lim_{x\to\infty} g(x) &= \lim_{x\to\infty} x\left(\left(\frac{x}{x-1}\right)^{s-1} - 1\right) \\ &= \lim_{x\to\infty} \frac{\left(\frac{x}{x-1}\right)^{s-1} - 1}{\frac{1}{x}} \\ &= \frac{(s-1)\left(\frac{x}{x-1}\right)^{s-2}\frac{-1}{(x-1)^2}}{\frac{-1}{x^2}} \\ &= \lim_{x\to\infty}(s-1)\left(\frac{x}{x-1}\right)^s \\ &= s-1. \end{aligned}$$

We have shown that $g(x)$ is a concave up function with a finite limit point, so we may conclude that $g(x)$ is decreasing on $(1, \infty)$.

Since we are only addressing the cases when $N > C$, it holds that

$$\frac{N^{\frac{L+1}{R}}}{(N-1)^{\frac{L-R+1}{R}}} - N \leq \frac{C^{\frac{L+1}{R}}}{(C-1)^{\frac{L-R+1}{R}}} - C.$$

Notice that

$$\begin{aligned}
& \frac{C_4}{C_4 - 1} && \leq && C \\
\iff & \frac{C}{C-1} && \leq && C_4 = (C_3+1)^{\frac{R}{L-R+1}} \\
\iff & \left(\frac{C}{C-1}\right)^{\frac{L-R+1}{R}} - 1 && \leq && C_3 \\
\iff & C\left(\frac{C}{C-1}\right)^{\frac{L-R+1}{R}} - C && \leq && CC_3 \\
\iff & \frac{C^{\frac{L+1}{R}}}{(C-1)^{\frac{L-R+1}{R}}} - C && \leq && CC_3.
\end{aligned}$$

We therefore have

$$\begin{aligned}
& \frac{N^{\frac{L+1}{R}}}{(N-1)^{\frac{L-R+1}{R}}} - N && \leq && C_3 C \\
\iff & \frac{N^{\frac{L+1}{R}}}{(N-1)^{\frac{L-R+1}{R}}} C^{\frac{L-R+1}{R}} - NC^{\frac{L-R+1}{R}} && \leq && C_3 C^{\frac{L+1}{R}} \\
\iff & \frac{N^{\frac{L+1}{R}}}{(N-1)^{\frac{L-R+1}{R}}} C^{\frac{L-R+1}{R}} && \leq && C_3 C^{\frac{L+1}{R}} + NC^{\frac{L-R+1}{R}} \\
\iff & \left(\frac{C}{N-1}\right)^{\frac{L-R+1}{R}} && \leq && C_3 \left(\tfrac{C}{N}\right)^{\frac{L+1}{R}} + \left(\tfrac{C}{N}\right)^{\frac{L-R+1}{R}}.
\end{aligned}$$

By the induction hypothesis, we see that

$$\begin{aligned} C_3 d^*(G)^{\frac{L+1}{L-R+1}} + d^*(G) &< d(N-1) \\ &\leq \left(\frac{C}{N-1}\right)^{\frac{L-R+1}{R}} \\ &\leq C_3 \left(\frac{C}{N}\right)^{\frac{L+1}{R}} + \left(\frac{C}{N}\right)^{\frac{L-R+1}{R}} \\ &= C_3 \left(\left(\frac{C}{N}\right)^{\frac{L-R+1}{R}}\right)^{\frac{L+1}{L-R+1}} + \left(\frac{C}{N}\right)^{\frac{L-R+1}{R}}. \end{aligned}$$

If we let $f(x) = C_3 x^{\frac{L+1}{L-R+1}} + x$, it is clear that $f(x)$ is increasing on $[0, \infty)$. Therefore we can conclude that

$$d^*(G) \leq \left(\frac{C}{N}\right)^{\frac{L-R+1}{R}}$$

which finishes Case II and therefore the proof of Theorem 5.1.1.

References

[1] T.C. Brown and J.C. Buhler, A density version of a geometric Ramsey theorem, *J. Combin. Theory, Ser. A* **32** (1982), 20-34.

[2] P. Frankl, R.Graham, and V. Rodl, On subsets of abelian groups with no 3-term arithmetic progression, *J. Combin. Theory. Ser. A* **45** (1987)157-161.

[3] R. Heath-Brown, Integer sets containing no arithmetic progressions, *J. London Math. Soc.* **35** (1987), 385-394.

[4] Jacobson, N. (**1985**), *Basic Algebra I, 2nd ed.*, W.H. Freeman and Company (New York). p. 192.

[5] V. F. Lev, Progression-free sets in finite abelian groups, *Journal of Number Theory* **104** (2004) 162-169.

[6] Y.R. Liu and C. Spencer, A generalization of Meshulam's theorem, *J. Lond. Math. Soc.* **52** (2009) 83-91.

[7] Y.R. Liu, C. Spencer, and X. Zhao, A generalization of Meshulam's theorem on subsets of finite abelian groups with no 3-term arithmetic progressions (II), *European Journal of Combinatorics* **32** (2011) 258-264.

[8] R. Meshulam, On subsets of finite abelian groups with no 3-term arithmetic progressions, *J. Combin. Theory, Ser. A* **71** (1995) 168-172.

[9] K. F. Roth, On certain sets of integers, *J. London Math. Soc.* **28** (1953), 104-109.

[10] T. Sanders, On Roth's theorem on progressions, *Ann. of Math* **174** (2011) 619-636.

[11] Szemeredi, E., Integer sets containing no arithmetic progressions, *Acta Math. Hungar.* **56**(1990), 155-158.