A GENERALIZATION OF MESHULAM'S THEOREM ON SUBSETS OF FINITE ABELIAN GROUPS WITH NO 3-TERM ARITHMETIC PROGRESSION

YU-RU LIU AND CRAIG V. SPENCER

Abstract. Let $r_1, \ldots, r_s$ be non-zero integers satisfying $r_1 + \cdots + r_s = 0$. Let

$$G \simeq \mathbb{Z}/k_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/k_n\mathbb{Z}$$

be a finite abelian group with $k_i | k_{i-1}$ $(2 \leq i \leq n)$, and suppose that $(r_i, k_1) = 1$ $(1 \leq i \leq s)$. Let $D_{\mathbf{r}}(G)$ denote the maximal cardinality of a set $A \subseteq G$ which contains no non-trivial solution of $r_1x_1 + \cdots + r_sx_s = 0$ with $x_i \in A$ $(1 \leq i \leq s)$. We prove that $D_{\mathbf{r}}(G) \ll |G|/n^{s-2}$. We also apply this result to study problems in finite projective spaces.

1. Introduction

For $k \in \mathbb{N} = \{1, 2, \ldots\}$, let $D_3([1, k])$ denote the maximal cardinality of an integer set $A \subseteq \{1, \ldots, k\}$ containing no non-trivial 3-term arithmetic progression. In a fundamental paper [5], Roth proved that $D_3([1, k]) \ll k/\log\log k$ via an application of the circle method. His result was later improved by Heath-Brown [2] and Szemerédi [7] to $D_3([1, k]) \ll k/(\log k)^\alpha$ for some small positive constant $\alpha > 0$. Bourgain [1] proved that $D_3([1, k]) \ll k(\log\log k)^2/(\log k)^{2/3}$. In this paper, we prove a generalization of Roth's theorem in finite abelian groups.

For a natural number $s \geq 3$, let $\mathbf{r} = (r_1, \ldots, r_s)$ be a vector of non-zero integers satisfying $r_1 + \cdots + r_s = 0$. Given a finite abelian group G, we can write

$$G \simeq \mathbb{Z}/k_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/k_n\mathbb{Z},$$

where $\mathbb{Z}/k_i\mathbb{Z}$ is a cyclic group of order k_i $(1 \leq i \leq n)$ and $k_i | k_{i-1}$ $(2 \leq i \leq n)$. We denote by $c(G) = n$ the number of constituents of G. Moreover, we say that G is *coprime to* $\mathbf{r}$ provided that $(r_i, k_1) = 1$ for all $1 \leq i \leq s$.

A solution $\mathbf{x} = (x_1, \ldots, x_s) \in G^s$ of $r_1x_1 + \cdots + r_sx_s = 0$ is said to be *trivial* if $x_{j_1} = \cdots = x_{j_l}$ for some subset $\{j_1, \ldots, j_l\} \subseteq \{1, \ldots, s\}$ with $r_{j_1} + \cdots + r_{j_l} = 0$. Otherwise, we say that a solution $\mathbf{x}$ is *non-trivial*. For a finite abelian group G coprime to $\mathbf{r}$, let $D_{\mathbf{r}}(G)$ denote the maximal cardinality of a set $A \subseteq G$ which contains no non-trivial solution of $r_1x_1 + \cdots + r_sx_s = 0$ with $x_i \in A$ $(1 \leq i \leq s)$. Also, for $n \in \mathbb{N}$, we denote by $d_{\mathbf{r}}(n)$ the

Date: September 24, 2023.

2000 *Mathematics Subject Classification.* 11B25, 20D60, 11T24.

Key words and phrases. Roth's theorem, finite abelian groups, character sums.

The research of the first author is supported in part by an NSERC discovery grant.

The research of the second author is supported in part by NSF grants DMS-0601367 and DMS-0635607.

supremum of $D_{\mathbf{r}}(G)/|G|$ as G ranges over all finite abelian groups G with $c(G) \geq n$ and G coprime to $\mathbf{r}$. Here, $|G|$ denotes the cardinality of G. In this paper, we prove the following theorem.

Theorem 1. *Let $\mathbf{r} = (r_1, \ldots, r_s)$ be a vector of non-zero integers satisfying $r_1 + \cdots + r_s = 0$. There exists an effectively computable constant $C(\mathbf{r}) > 0$ such that for $n \in \mathbb{N}$,*

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

We note that in the special case that $\mathbf{r} = (1, -2, 1)$ and G is a finite abelian group of odd order, the number $D_{\mathbf{r}}(G)$ denotes the maximal cardinality of a set $A \subseteq G$ which contains no non-trivial 3-term arithmetic progression. Moreover, the constant $C(\mathbf{r})$ can be taken to be 2 in this case (see Remark 6). Hence, we can deduce from Theorem 1 the result of Meshulam in [4, Theorem 1.2] which states that if G is a finite abelian group of odd order, then $D_{\mathbf{r}}(G) \leq 2|G|/c(G)$.

In the following corollary, we provide an application of Theorem 1.

Corollary 2. *Let p be an odd prime and $q = p^h$ for some $h \in \mathbb{N}$. For $n \in \mathbb{N}$, let $PG(n, q)$ denote the projective space of dimension n over the finite field $\mathbb{F}_q$ of q elements. For $v \in \mathbb{N}$ with $v > 1$, let $\mathcal{M}_v(n, q)$ denote the maximum cardinality of a set $A \subseteq PG(n, q)$ for which no $(v + 1)$ points in A are linearly dependent over $\mathbb{F}_q$. Then, there exists an effectively computable constant $\widetilde{C}(p, v) > 0$ such that*

$$\mathcal{M}_v(n, q) \leq \frac{\widetilde{C}(p, v)}{h^{v-1}} \cdot \sum_{j=1}^{n} \frac{q^j}{j^{v-1}} + 1.$$

An m-cap is a set of m points of $PG(n, q)$ for which no three points are collinear. In the special case that $v = 2$, the quantity $\mathcal{M}_2(n, q)$ denotes the maximal value of m for which there exists an m-cap in $PG(n, q)$. For an odd prime p, we can take $\widetilde{C}(p, 2) = 2$ (see Remark 6). Hence, Corollary 2 implies the result of Storme, Thas, and Vereecke in [6, Theorem 1.2] about the sizes of caps in finite projective spaces.

For $v \in \mathbb{N}$ with $v > 1$, let $\mathbf{M}_v(n, q)$ denote the maximum cardinality of a set $A \subseteq PG(n, q)$ for which no $(v+1)$ points in A are linearly dependent over $\mathbb{F}_q$, and some $(v+2)$ points in A are linearly dependent over $\mathbb{F}_q$. In [3], Hirschfeld and Storme provide a general discussion on $\mathbf{M}_v(n, q)$. We note that $\mathbf{M}_v(n, q) \leq \mathcal{M}_v(n, q)$. Hence, Corollary 2 gives a bound for $\mathbf{M}_v(n, q)$ which is useful when n is sufficiently large.

Before proving Theorem 1 and Corollary 2, we introduce the Fourier transform on a finite abelian group G. Let $\widehat{G}$ denote the character group of G. The *Fourier transform* of a function $g : G \to \mathbb{C}$ is the function $\widehat{g} : \widehat{G} \to \mathbb{C}$ defined by

$$\widehat{g}(\chi) = \sum_{x \in G} g(x)\, \chi(-x).$$

Then, we have *Parseval's identity*,

$$\sum_{\chi \in \widehat{G}} |\widehat{g}(\chi)|^2 = |G| \sum_{x \in G} |g(x)|^2.$$

Acknowledgement The authors are grateful to Prof. Trevor Wooley for many valuable discussions during the completion of this work. The authors would like to thank Prof. James Hirschfeld for providing a reference to [3] and Michael Lipnowski for correcting an argument in the original proof of Theorem 1. The authors also would like to thank the referees for providing valuable suggestions and corrections.

Notation For $k \in \mathbb{N}$, let $f(k)$ and $g(k)$ be functions of k. If $g(k)$ is positive and there exists a constant $C = C(\mathbf{r}) > 0$ such that $|f(k)| \leq Cg(k)$, we write $f(k) \ll g(k)$. In this paper, all the implicit constants depend only on $\mathbf{r}$.

2. Proof of Theorem 1

Let $r_1, \dots, r_s$ be non-zero integers with $r_1 + \cdots + r_s = 0$. For $n \in \mathbb{N}$, let G be a finite abelian group coprime to $\mathbf{r}$ with $c(G) \geq n$. For convenience, in what follows, we write $D(G)$ in place of $D_{\mathbf{r}}(G)$ and $d(n)$ in place of $d_{\mathbf{r}}(n)$. For a set $A \subseteq G$, we denote by $T(A) = T_{\mathbf{r}}(A)$ the number of solutions of

$$r_1x_1 + \cdots + r_sx_s = 0$$

with $x_i \in A$ $(1 \leq i \leq s)$. For $1 \leq i \leq s$, let $r_iA = \{r_ix\colon x \in A\}$, and let 1_{r_iA} be the characteristic function of r_iA, i.e., $1_{r_iA}(x) = 1$ if $x \in r_iA$ and $1_{r_iA}(x) = 0$ otherwise. Let $f_i = \widehat{1_{r_iA}}$. We note that since G is coprime to $\mathbf{r}$, the map from G to G defined by $x \mapsto r_ix$ is a bijection. Thus, for $\chi \in \widehat{G}$, we have

$$f_i(\chi) = \sum_{x\in G} 1_{r_iA}(x)\chi(-x) = \sum_{x\in A} \chi(-r_ix) \qquad (1 \leq i \leq s).$$

It follows that

$$\begin{aligned}\sum_{\chi\in\widehat{G}} f_1(\chi)f_2(\chi)\cdots f_s(\chi) &= \sum_{x_1\in A}\cdots\sum_{x_s\in A}\sum_{\chi\in\widehat{G}} \chi\big(-(r_1x_1 + \cdots + r_sx_s)\big) \\ &= |G|\,T(A).\end{aligned} \tag{1}$$

Moreover, we define

$$h(\chi) = \sum_{x\in G} d(n-1)\chi(-x).$$

Hence, $h(\chi) = d(n-1)|G|$ if $\chi = \chi_0$ and $h(\chi) = 0$ otherwise. The function $h(\chi)$ is a good approximation for $f_i(\chi)$. More precisely, we have the following lemma.

Lemma 3. *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 solution of $r_1x_1 + \cdots + r_sx_s = 0$ with $x_i \in A$ $(1 \leq i \leq s)$. Then we have*

$$\sup_{\chi\in\widehat{G}} |h(\chi) - f_i(\chi)| = d(n-1)|G| - |A|.$$

In particular, since $h(\chi) = 0$ for $\chi \neq \chi_0$, it follows that

$$\sup_{\chi\neq\chi_0} \big|f_i(\chi)\big| \leq d(n-1)|G| - |A|.$$

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

$$|W||h(\chi) - f_i(\chi)| = \left| \sum_{y \in W} \sum_{x \in G} d(n-1)\chi(-x) - \sum_{y \in W} \sum_{x \in G} 1_{r_i A}(x)\chi(-x) \right|.$$

Since $y \in \ker(\chi)$, by a change of variables, we have

$$\sum_{x \in G} 1_{r_i A}(x)\chi(-x) = \sum_{x \in G} 1_{r_i A}(x)\chi(-(x+y)) = \sum_{x \in G} 1_{r_i A}(x-y)\chi(-x).$$

Hence, it follows that

$$\begin{aligned} |W||h(\chi) - f_i(\chi)| &= \left| \sum_{x \in G} \left(\sum_{y \in W} d(n-1) - \sum_{y \in W} 1_{r_i A}(x-y) \right) \chi(-x) \right| \\ &\leq \sum_{x \in G} \left| \sum_{y \in W} d(n-1) - \sum_{y \in W} 1_{r_i A}(x-y) \right| \\ &= \sum_{x \in G} \Big| d(n-1)|W| - \big| W \cap (x - r_i A) \big| \Big|. \end{aligned}$$

We note that since A contains no non-trivial solution of $r_1 x_1 + \cdots + r_s x_s = 0$ with $x_i \in A$ $(1 \leq i \leq s)$, the set $W \cap (x - r_i A)$ also contains no non-trivial solution of the same equation. Furthermore, the fact that G is coprime to $\mathbf{r}$ implies that W is coprime to $\mathbf{r}$. Since $c(W) \geq (n-1)$, we have $\big| W \cap (x - r_i A) \big| \leq d(n-1)|W|$. We may conclude that

$$\begin{aligned} |W||h(\chi) - f_i(\chi)| &\leq \sum_{x \in G} \Big(d(n-1)|W| - \big| W \cap (x - r_i A) \big| \Big) \\ &= d(n-1)|W||G| - |W||A|. \end{aligned}$$

Hence, we have

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

We note that for $\chi = \chi_0$, one has

$$|h(\chi_0) - f_i(\chi_0)| = d(n-1)|G| - |A|.$$

This completes the proof of the lemma. □

Now, we are ready to prove Theorem 1.

Proof. (of Theorem 1) 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 solution of $r_1 x_1 + \cdots + r_s x_s = 0$ with $x_i \in A$ $(1 \leq i \leq s)$. Furthermore, suppose that $D(G) = |A|$, and let $d^*(G) = |A|/|G|$.

By (1), we have

$$\begin{aligned} |G|\, T(A) &= \sum_{\chi \in \widehat{G}} f_1(\chi) f_2(\chi) \cdots f_s(\chi) \\ &= f_1(\chi_0) f_2(\chi_0) \cdots f_s(\chi_0) + \sum_{\chi \neq \chi_0} f_1(\chi) f_2(\chi) \cdots f_s(\chi). \end{aligned} \tag{2}$$

We note that

$$f_1(\chi_0)f_2(\chi_0)\cdots f_s(\chi_0) = |A|^s = d^*(G)^s|G|^s. \tag{3}$$

Also, by Cauchy's inequality and Lemma 3, we have

$$\begin{aligned}
&\left|\sum_{\chi\neq\chi_0} f_1(\chi)f_2(\chi)\cdots f_s(\chi)\right| \\
&\leq \sup_{\chi\neq\chi_0} \left|f_3(\chi)\cdots f_s(\chi)\right| \left(\sum_{\chi\neq\chi_0}|f_1(\chi)|^2\right)^{1/2}\left(\sum_{\chi\neq\chi_0}|f_2(\chi)|^2\right)^{1/2} \\
&\leq \left(d(n-1)-d^*(G)\right)^{s-2}|G|^{s-2}\left(\sum_{\chi\in\widehat{G}}|f_1(\chi)|^2\right)^{1/2}\left(\sum_{\chi\in\widehat{G}}|f_2(\chi)|^2\right)^{1/2}.
\end{aligned}$$

By Parseval's identity,

$$\sum_{\chi\in\widehat{G}}|f_1(\chi)|^2 = |G|\sum_{x\in G}|1_{r_1A}(x)|^2 = |G||A|.$$

The same equality also holds if we replace f_1 by f_2. Thus, from the above estimates, we have

$$\left|\sum_{\chi\neq\chi_0} f_1(\chi)f_2(\chi)\cdots f_s(\chi)\right| \leq d^*(G)\left(d(n-1)-d^*(G)\right)^{s-2}|G|^s. \tag{4}$$

By combining (2), (3), and (4), it follows that

$$\begin{aligned}
T(A) &\geq \frac{1}{|G|}f_1(\chi_0)f_2(\chi_0)\cdots f_s(\chi_0) - \frac{1}{|G|}\left|\sum_{\chi\neq\chi_0} f_1(\chi)f_2(\chi)\cdots f_s(\chi)\right| \\
&\geq \left(d^*(G)^s - d^*(G)\left(d(n-1)-d^*(G)\right)^{s-2}\right)|G|^{s-1}.
\end{aligned}$$

Since A contains no non-trivial solution of $r_1x_1+\cdots+r_sx_s=0$ with $x_i\in A$ $(1\leq i\leq s)$, there exists a constant $B=B(\mathbf{r})$ such that

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

Combining the above two estimates, we have

$$d^*(G)^s - Bd^*(G)^{s-2}|G|^{-1} - d^*(G)\big(d(n-1)-d^*(G)\big)^{s-2}\leq 0. \tag{5}$$

We now claim that there exists a constant $C=C(\mathbf{r})\geq 1$ such that for all $n\in\mathbb{N}$,

$$d(n)\leq \frac{C^{s-2}}{n^{s-2}}. \tag{6}$$

This statement follows by induction on n. Since $d(n)\leq 1$, the cases where $n\leq C$ hold trivially. Let $n>C$, and suppose that $d(n-1)\leq C^{s-2}(n-1)^{2-s}$. We now verify that $d^*(G)\leq C^{s-2}n^{2-s}$, and since this inequality holds for any finite abelian group G coprime to $\mathbf{r}$ with $c(G)\geq n$, we may conclude that $d(n)\leq C^{s-2}n^{2-s}$. Let F be any real number with $F>1$. We split the proof into two cases:

(1) Suppose that $d^*(G)^2\leq FB|G|^{-1}$. Since $|G|\geq 2^n$, we have $d^*(G)\leq (FB2^{-n})^{1/2}$. Hence, if $(FB2^{-m})^{1/2}m^{s-2}\leq C^{s-2}$ for all $m>C$, one has that $d^*(G)\leq C^{s-2}n^{2-s}$. For

$m > 0$, the function $2^{-m/2}m^{s-2}$ obtains its global maximum of $(2s-4)^{s-2}(e\log 2)^{2-s}$ when $m = (2s-4)/\log 2$. Therefore, this case follows provided that

$$C \geq (FB)^{1/(2s-4)}\left(\frac{2s-4}{e\log 2}\right).$$

(2) Suppose that $d^*(G)^2 > FB|G|^{-1}$. Since $F^{-1}d^*(G)^s > Bd^*(G)^{s-2}|G|^{-1}$, by (5), we have

$$(1-F^{-1})d^*(G)^s < d^*(G)(d(n-1)-d^*(G))^{s-2}.$$

Let $E = E(F)$ be the unique positive number satisfying $E^{s-2} = (1-F^{-1})$. By the induction hypothesis for $d(n-1)$, the above inequality implies that

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

Since $Ex^{\frac{s-1}{s-2}} + x$ is an increasing function of x, to prove that $d^*(G) \leq C^{s-2}n^{s-2}$, it suffices to show that

$$\frac{C^{s-2}}{(n-1)^{s-2}} \leq E\left(\frac{C^{s-2}}{n^{s-2}}\right)^{\frac{s-1}{s-2}} + \frac{C^{s-2}}{n^{s-2}}.$$

We note that the above inequality is equivalent to

$$\frac{n^{s-1}}{(n-1)^{s-2}} - n \leq CE. \tag{7}$$

For $m > 1$,

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

is a decreasing function of m. Since $n > C$, to prove (7), it is enough to show that

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

The above inequality is satisfied whenever

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

Hence, provided that C is large enough in terms of $\mathbf{r}$, it follows by induction that (6) holds for all $n \in \mathbb{N}$. This completes the proof of Theorem 1. □

Remark 4. *We see from the above proof that our constant $C = C(\mathbf{r})$ can be computed explicitly. For any value of E such that $0 < E < 1$, we may choose C to be*

$$\max\left\{\left(\frac{B}{1-E^{s-2}}\right)^{1/(2s-4)}\left(\frac{2s-4}{e\log 2}\right), \frac{(E+1)^{1/(s-2)}}{(E+1)^{1/(s-2)}-1}\right\},$$

where $B = B(\mathbf{r})$ is chosen as in the proof of Theorem 1. For any choice of $\mathbf{r} = (r_1, \ldots, r_s)$, one can numerically choose E to minimize the above expression. We note that

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

Thus, for fixed B, the constant C can be chosen in such a way that it grows like a linear function in s.

Remark 5. *If the vector $\mathbf{r} = (r_1, \dots, r_s) \in \mathbb{Z}^s$ satisfies the condition that there is no proper subset $\{j_1, \dots, j_l\} \subsetneq \{1, \dots, s\}$ with $r_{j_1} + \cdots + r_{j_l} = 0$, then a solution $\mathbf{x} = (x_1, \dots, x_s) \in A^s$ is trivial if and only if $x_1 = \cdots = x_s$. Hence, $T(A) = |A|$, and in place of (5), we obtain the inequality*

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

By an argument similar to the proof of Theorem 1, for any value of E such that $0 < E < 1$, we may choose C to be

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

We note that in this case, the constant C depends only on s. Moreover, we can change the constant E as n varies in our proof, i.e., $E = E(n)$ can be chosen to be a function of n. Table 1 lists valid choices of $C(s)$ for small values of s.

Table 1. Values of the Constant $C(s)$ in Remark 5

s	3	4	5	6	7	8	9	10	11
$C(s)$	2.050	3.138	4.766	6	7.598	9	10.436	12	13.277

Remark 6. *One can also optimize the choice of $C = C(\mathbf{r})$ by utilizing the inequality in* (5) *directly. Consider the special case that $\mathbf{r} = (1, -2, 1)$ and G is a finite abelian group of odd order with $c(G) \geq n$. Since a solution $\mathbf{x} = (x_1, x_2, x_3)$ is trivial if and only if $x_1 = x_2 = x_3$, we can take $B(\mathbf{r}) = 1$ in this case. Since $|G| \geq 3^n$, by* (5)*, we have*

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

We note that for $n \geq 3$,

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

Since $x^2 + x - 3^{-n}$ is an increasing function of x, by induction, we can show that $d(n) \leq 2/n$ for all $n \in \mathbb{N}$. In other words, when $\mathbf{r} = (1, -2, 1)$, we can take $C(\mathbf{r}) = 2$.

3. Proof of Corollary 2

Let p be an odd prime and $q = p^h$ for some $h \in \mathbb{N}$. For $n \in \mathbb{N}$, let $PG(n, q)$ denote the projective space of dimension n over $\mathbb{F}_q$. For $v \in \mathbb{N}$ with $v > 1$, define $\mathcal{M}_v(n, q)$ to be the maximum cardinality of a set $A \subseteq PG(n, q)$ for which no $(v+1)$ points in A are linearly dependent over $\mathbb{F}_q$. We can similarly define $\widetilde{\mathcal{M}}_v(n, q)$ as the maximum cardinality of a set $B \subseteq \mathbb{F}_q^n \oplus \{1\} \subseteq PG(n, q)$ for which no $(v+1)$ points in B are linearly dependent over $\mathbb{F}_q$.

Corollary 7. *Let p be an odd prime and $q = p^h$ for some $h \in \mathbb{N}$. There exists an effectively computable constant $\widetilde{C}(p,v) > 0$ such that*

$$\widetilde{\mathcal{M}}_v(n,q) \leq \frac{\widetilde{C}(p,v)q^n}{(nh)^{v-1}}.$$

Proof. Let $r_1, \dots, r_{v-1}$ be integers that are not divisible by p. Since $p \geq 3$, there exists an $r_v \in \mathbb{Z}$ such that $p \nmid r_v$ and $r_1 + \cdots + r_v \not\equiv 0 \pmod p$. By taking $r_{v+1} = -(r_1 + \cdots + r_v)$, we have shown that there exists a vector $\mathbf{r} = (r_1, \dots, r_{v+1})$ of integers not divisible by p that satisfies $r_1 + \cdots + r_{v+1} = 0$.

Suppose that $B \subseteq \mathbb{F}_q^n \oplus \{1\}$ and no $(v+1)$ points in B are linearly dependent over $\mathbb{F}_q$. Let $\mathbf{r} = (r_1, \dots, r_{v+1})$ be a vector of integers not divisible by p that satisfies $r_1 + \cdots + r_{v+1} = 0$. If B contains a non-trivial solution of $r_1x_1 + \cdots + r_{v+1}x_{v+1} = 0$ with $x_i \in B$ $(1 \leq i \leq v+1)$, then there are $(v+1)$ points in B that are linearly dependent over $\mathbb{F}_q$. Hence, by viewing $\mathbb{F}_q^n$ as a finite abelian group with nh constituents, we can derive from Theorem 1 that

$$\widetilde{\mathcal{M}}_v(n,q) \leq \frac{C(\mathbf{r})^{v-1}\, q^n}{(nh)^{v-1}}. \tag{8}$$

Define

$$\widetilde{C}(p,v) = \inf_{\mathbf{r}} \left\{ C(\mathbf{r})^{v-1} \right\},$$

where $\mathbf{r}$ runs through all vectors $(r_1, \dots, r_{v+1})$ of integers not divisible by p with $r_1 + \cdots + r_{v+1} = 0$. Then, by (8), the corollary follows. □

We are now ready to prove Corollary 2, which states that

$$\mathcal{M}_v(n,q) \leq \frac{\widetilde{C}(p,v)}{h^{v-1}} \cdot \sum_{j=1}^{n} \frac{q^j}{j^{v-1}} + 1.$$

Proof. (of Corollary 2) We note that an element of $PG(n,q)$ can be written either as $(y,1)$ with $y \in \mathbb{F}_q^n$ or as $(z,0)$ with $z \in PG(n-1,q)$. Thus, for $n \geq 1$, we have

$$\mathcal{M}_v(n,q) \leq \widetilde{\mathcal{M}}_v(n,q) + \mathcal{M}_v(n-1,q). \tag{9}$$

We note that

$$\mathcal{M}_v(1,q) \leq \widetilde{\mathcal{M}}_v(1,q) + 1. \tag{10}$$

By (9), (10), and Corollary 7, we have

$$\mathcal{M}_v(n,q) \leq \sum_{j=1}^{n} \widetilde{\mathcal{M}}_v(j,q) + 1 \leq \frac{\widetilde{C}(p,v)}{h^{v-1}} \cdot \sum_{j=1}^{n} \frac{q^j}{j^{v-1}} + 1.$$

The corollary now follows. □

References

[1] J. Bourgain, *Roth's theorem on progressions revisited*, J. Anal. Math. **104** (2008), 155-192.

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

[3] J. Hirschfeld and L. Storme, The packing problem in statistics, coding theory and finite projective spaces: update 2001. *Finite geometries*, Dev. Math. 3, Kluwer Acad. Publ., Dordrecht (2001), 201-246.

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

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

[6] L. Storme, J. Thas, and S. Vereecke, *New upper bounds for the sizes of caps in finite projective spaces*, J. Geom. 73 (2002), 176-193.

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

Y.-R. Liu, Department of Pure Mathematics, Faculty of Mathematics, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1

E-mail address: `yrliu@math.uwaterloo.ca`

C. V. Spencer, School of Mathematics, Institute for Advanced Study, 1 Einstein Drive, Princeton, NJ 08540

E-mail address: `craigvspencer@gmail.com`