ISRAEL JOURNAL OF MATHEMATICS 154 (2006), 221–233

LARGE SUM-FREE SETS IN $\mathbb{Z}/p\mathbb{Z}$

BY

VSEVOLOD F. LEV

Department of Mathematics, University of Haifa at Oranim
Tivon 36006, Israel
e-mail: seva@math.haifa.ac.il

ABSTRACT

We show that if p is prime and A is a sum-free subset of $\mathbb{Z}/p\mathbb{Z}$ with $n := |A| > 0.33p$, then A is contained in a dilation of the interval $[n, p-n]$ (mod p).

1. Introduction

A subset A of an abelian group is said to be **sum-free** if $a_1 + a_2 = a_3$ with $a_1, a_2, a_3 \in A$ is impossible; that is, if the equation $x + y = z$ has no solutions in the elements of A. To our knowledge, sum-free sets were introduced by Schur whose celebrated result (considered now one of the origins of the Ramsey theory) is that the set of positive integers cannot be partitioned into finitely many sum-free sets. Further study of sum-free sets was motivated to a large extent by a famous conjecture of Cameron and Erdős, recently settled by Green [G04]. We refer the reader to [GR05, K98, L03, ŁLS01, WSW72] for an extended historical account, current state of the art, and the background motivating one's interest in sum-free sets.

How large can a sum-free subset of a finite abelian group be? For some groups the answer has been known for over 35 years, see [DY69, RS70, Y72, Y75]; however, for a number of particularly "tough" groups the problem remained open until the recent paper by Green and Ruzsa [GR05]. Much effort has also been made to determine the structure of sum-free subsets of the maximum possible size; for numerous results of this sort and further references see [WSW72]. On the other hand, there were almost no attempts to advance further and to

Received October 11, 2004

study sum-free subsets of size *close* to the maximum possible. We mention two exceptions. One is the remarkable paper by Davydov and Tombak [DT89], well-known to coding theorists and experts in finite geometries. As shown in [DT89], any sum-free subset A of the elementary abelian 2-group of rank $r \ge 4$, such that $|A| > 5 \cdot 2^{r-4}$, is contained in a proper coset. Another exception is [L05] where a result of this sort is established for elementary abelian 3-groups. Similar in its spirit is the problem of classifying large integer sum-free subsets of the interval $[1, n]$; see [F92, DFST99].

2. The main result

In the present paper we consider the problem for cyclic groups of prime order which, following the number-theoretic tradition, are understood as the quotient groups $\mathbb{Z}/p\mathbb{Z}$.

It is not difficult to prove that if $A \subseteq \mathbb{Z}/p\mathbb{Z}$ is sum-free, where $p \ge 2$ is a (not necessarily prime) integer, then $|A| \le \lfloor (p+1)/3 \rfloor$. This is best possible as one verifies easily considering appropriate intervals. More precisely, let $\varphi_p \colon \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ denote the canonical homomorphism and for a set $\mathcal{S} \subseteq \mathbb{Z}$ write $\mathcal{S}_p := \varphi_p(\mathcal{S})$, the image of $\mathcal{S}$ under φ_p. (Here $\mathcal{S}$ can be substituted by a letter or any notation, customarily used for integer sets.) Then for $a := \lfloor (p+1)/3 \rfloor$ the set $[a, 2a-1]_p$ is sum-free. Moreover, any subset of $[a, 2a-1]_p$ is sum-free, as well as any dilation of such a subset by a factor, co-prime with p. The aim of this paper is to establish the following result showing that if p is prime and a sum-free subset $A \subseteq \mathbb{Z}/p\mathbb{Z}$ is large, then A has the structure close to that just described.

THEOREM 1: *Let p be a prime and suppose that $A \subseteq \mathbb{Z}/p\mathbb{Z}$ is sum-free. If $n := |A| > 0.33p$, then there exists an integer d such that $A \subseteq \{dz \colon z \in [n, p-n]_p\}$.*

We notice that the interval $[n, p-n]_p$ contains $n + (p+1-3n)$ elements of $\mathbb{Z}/p\mathbb{Z}$, so that the set A of Theorem 1 is actually a *very dense* subset of a dilation of this interval.

What makes Theorem 1 non-trivial is that $0.33 < 1/3$. The constant 0.33 is merely an artifact of our method, and it would be interesting to replace it with a smaller value. It is not quite clear to us how far can one go in this direction, though we have an example showing that it cannot be reduced to below 0.2. In contrast, the interval $[n, p-n]_p$ is best possible, as we proceed to explain.

Given a subset A of an abelian group we write

$$2A := \{a_1 + a_2 \colon a_1, a_2 \in A\}$$

(the **sumset** of A),

$$A - A := \{a_1 - a_2\colon a_1, a_2 \in A\}$$

(the **difference set** of A), and

$$d * A := \{da\colon a \in A\}$$

(the **dilation** of A by the factor $d \in \mathbb{Z}$).

Example 1: For a prime p and a positive integer $a \le (p+1)/4$ let

$$A := [a, 2a-1]_p \cup [p-2a+1, p-a]_p \tag{1}$$

so that the cardinality of A is $n := 2a$ and

$$2A = [2a, 4a-2]_p \cup [p-a+1, p+a-1]_p \cup [p-4a+2, p-2a]_p. \tag{2}$$

If $a \le (p+1)/6$ then the intervals in (1) are disjoint with those in (2), hence A is sum-free. Furthermore,

$$2 * A = \{2a, 2a+2, \dots, 4a-2\}_p \cup \{p-4a+2, p-4a+4, \dots, p-2a\}_p$$

whence $2 * A \subseteq [n, p-n]_p$ and, moreover, $2 * A$ is not contained in a proper subinterval of $[n, p-n]_p$. Finally, we show that if $a \ge (p+3)/8$ then $d * A \not\subseteq [n, p-n]_p$ for any $d \in [3, p-3]$. It suffices to prove that

$$(d * [a, 2a-1]_p) \cap [-2a, 2a]_p = \varnothing \tag{3}$$

does not hold for $3 \le d \le (p-1)/2$. For $d = 3$ this is immediate from $p - 2a \le 3(2a-1) \le p + 2a$. For $d \ge 4$ we have

$$d \le \frac{p+3}{2} - 2 \le 4a - 2 < (2a+1) - (-2a-1).$$

Thus if (3) were true then, taking into account that $d * [a, 2a-1]_p$ is the image under φ_p of an arithmetic progression with the difference d between consecutive elements, we would conclude that

$$(2a-1)d - ad \le (p-2a-1) - (2a+1) = p - 4a - 2.$$

Equivalently,

$$(a-1)d \le p - 6 - 4(a-1),$$
$$(a-1)(d+4) \le p - 6,$$

and it would follow that $a \le (p-6)/8 + 1 < (p+3)/8$, contrary to the assumptions.

We now turn to the proof of Theorem 1. Our argument involves two parts. First, character sums are used to show that there is a dilation of A with unproportionally many elements in an interval of the form $[u, u+p/2)_p$. The standard tool to derive a conclusion of this kind is a classical lemma of Freiman [F62, Lemma 1], but unfortunately the estimate it yields is too weak for our purposes. For this reason we use [L, Corollary 2] instead, gaining a vital improvement in the constants. Secondly (and this is where the major difficulty lies), a combinatorial argument is employed to show that if u is suitably chosen, then in fact the *whole* set A is contained in $[u, u+p/2)_p$ and, moreover, $A \subseteq [n, p-n]_p$. The proof is presented in Section 4; several auxiliary results are gathered in the next section.

3. The tools

We start with three lemmas dealing with the structure of the difference set $A-A$ for the case where A is a dense set of integers.

LEMMA 1: *Let n and l be positive integers satisfying $l \le 2n-2$ and suppose that $A \subseteq [0,l]$ is a set of integers such that $|A| = n$. Then*

$$[-(2n-2-l), 2n-2-l] \subseteq A-A.$$

Proof: If $g > 0$ is an integer with $g \notin A - A$ then $A \cap (g+A) = \varnothing$ and both A and $g+A$ are contained in $[0, l+g]$, whence $l+g+1 \ge 2n$ by the boxing principle and therefore $g \ge 2n-1-l$. By symmetry, if $g < 0$ is an integer with $g \notin A-A$, then in fact $g \le -(2n-1-l)$. ∎

LEMMA 2: *Let n and l be positive integers satisfying $l \le 2n-2$ and suppose that $A \subseteq [0,l]$ is a set of integers such that $|A| = n$. Then for any integer $k \ge 1$ we have*

$$\left(\frac{l-n+1}{k}, \frac{n}{k}\right) \subseteq A-A.$$

Proof: Fix an integer $g > 0$ and for $j \in [0, g-1]$ consider the arithmetic progression $P_j := \{j, j+g, \dots, j+(2k-1)g\}$. If $g \notin A-A$ then of any two consecutive elements of each P_j at most one belongs to A so that $|P_j \cap A| \le k$, implying $|A \cap [0, 2kg-1]| \le kg$. If $l \le 2kg-1$ this gives $n \le kg$ whence $g \ge n/k$; if $l \ge 2kg$ then one derives easily that $n \le kg + (l+1-2kg)$ whence $g \le (l+1-n)/k$. In any case, g does not fall into the "forbidden" interval $((l-n+1)/k, n/k)$. ∎

LEMMA 3: *Let n and l be positive integers and suppose that $A \subseteq [0, l]$ is a set of integers such that $|A| = n$. If $l < \frac{2k-1}{k}n - 1$ with an integer $k \geq 2$, then*

$$\Big(-\frac{n}{k-1}, \frac{n}{k-1}\Big) \subseteq A - A.$$

Proof: This follows from Lemma 2 and the observation that if $\varkappa \geq k$ then $l < \frac{2\varkappa-1}{\varkappa}n - 1$ which is equivalent to $\frac{n}{\varkappa} > \frac{l-n+1}{\varkappa-1}$. ∎

It can be shown that Lemmas 1–3 are best possible in the sense that the intervals of these lemmas cannot be extended.

Our next lemma is the "difference version" of a well-known result of Freiman; it follows readily, for instance, from [LS95, Theorem 2].

LEMMA 4: *Let l and n be positive integers and suppose that $A \subseteq [0, l]$ is a set of integers such that $|A| = n$, $0 \in A$, $l \in A$, and $\gcd(A) = 1$. Then*

$$|A - A| \geq \min\{l + n, 3n - 3\}.$$

We notice that Lemmas 1–3 remain valid if A is a subset of $\mathbb{Z}/p\mathbb{Z}$ (rather than $\mathbb{Z}$), the condition $A \subseteq [0, l]$ is replaced by $A \subseteq [u, u+l]_p$ with integer u and $l < p$, and the intervals in the conclusions of the lemmas are replaced with their images under φ_p. Similarly, the estimate of Lemma 4 remains valid if $A \subseteq [u, u + l]_p$ with integer u and $l < p/2$ and given that the set $\varphi_p^{-1}(A) \cap [u, u + l]$ is not contained in an arithmetic progression of length smaller than l.

We finish this section with a reformulation of [L, Corollary 2]. We use the standard notation $\mathrm{e}_p(z) = \exp(2\pi i z/p)$ where p is a positive integer and z is either an integer or an element of $\mathbb{Z}/p\mathbb{Z}$.

LEMMA 5: *Let p be a positive integer and suppose that $A \subseteq \mathbb{Z}/p\mathbb{Z}$. Write $n := |A|$ and $S := \sum_{a\in A} \mathrm{e}_p(a)$. Then there exists an integer u such that*

$$|A \cap [u, u + p/2)_p| \geq \frac{n}{2} + \frac{p}{2\pi} \arcsin\Big(|S| \sin\frac{\pi}{p}\Big).$$

4. Proof of Theorem 1

We break the proof into a number of steps.

1) If $p < 100$ then $n > 0.33p > (p - 1)/3$ whence in view of $2A \cap A = \varnothing$ we have $|2A| \leq p - n < 2n$. Thus $|2A| \leq 2n - 1$ and by a well-known theorem of Vosper, A is an arithmetic progression; replacing it with a suitable dilation we can write $A = [u, u + n - 1]_p$, with an integer $0 < u \leq p - n$. One now verifies easily that the fact that A is sum-free implies $u \geq n$ and $u + n - 1 \leq p - n$,

concluding the proof in this special case. For the rest of the proof we assume that $p > 100$.

2) Define $\alpha > 0.33$ by $n = \alpha p$ and for integer z write $\widehat{A}(z) := \sum_{a\in A} \mathrm{e}_p(az)$; thus $\widehat{A}(z)$ are the Fourier coefficients of the indicator function of A. Since A is sum-free we have $\sum_{z=0}^{p-1} \widehat{A}(z)|\widehat{A}(z)|^2 = 0$ whence using the Parseval identity we obtain

$$n^3 \le \sum_{z=1}^{p-1} |\widehat{A}(z)|^3 \le \max_{1\le z\le p-1} |\widehat{A}(z)| \cdot \sum_{z=1}^{p-1} |\widehat{A}(z)|^2 = n(p-n) \max_{1\le z\le p-1} |\widehat{A}(z)|.$$

Dilating A as necessary, we can assume that

$$|\widehat{A}(1)| \ge \frac{n^2}{p-n} = \frac{\alpha^2}{1-\alpha} p$$

and then by Lemma 5 there is an integer u such that the interval $[u, u+p/2)_p$ contains at least

$$(4) \qquad \frac{n}{2} + \frac{p}{2\pi} \arcsin\left(|\widehat{A}(1)| \sin\frac{\pi}{p}\right) \ge \left(\frac{\alpha}{2} + \frac{1}{2\pi} \arcsin\left(\frac{\alpha^2}{1-\alpha} p \sin\frac{\pi}{p}\right)\right)p$$

elements of A.

Set $A_0 := A \cap [u, u+p/2)_p$ and $n_0 := |A_0|$ and write the right-hand side of (4) as $g(\alpha, p)p$. Since $p > 100$ (see Step 1) and $\alpha > 0.33$ and since $g(\alpha, p)$ is an increasing function of both α and p, we have

$$n_0 > g(0.33, 100)p > 0.25p.$$

3) We have shown that there are integer u and $0 < l_0 < p/2$ such that, letting $A_0 := A \cap [u, u+l_0]_p$, we have $n_0 := |A_0| > 0.25p$. Without loss of generality we can assume that, moreover,

(i) $n_0 \ge |A \cap [u', u'+p/2)_p|$ for any integer u';

(ii) $u, u+l_0 \in A_0$ (to simplify the notation we occasionally identify integers with their images under φ_p);

(iii) $0 < u < p$;

(iv) $\varphi_p^{-1}(A_0) \cap [u, u+l_0]$ is not contained in an arithmetic progression of length smaller than l_0.

We notice that (iv) follows from the observation that A can be replaced with its dilations, and that (i) implies

$$(5) \qquad A \cap (u+l_0-p/2, u)_p = A \cap (u+l_0, u+p/2)_p = \varnothing.$$

4) Set $\delta := |A \setminus (-A)|$. Since A is sum-free we have

$$A \cap (A - A) = (-A) \cap (A - A) = \varnothing$$

and hence

$$n + \delta = |A \cup (-A)| \le p - |A - A| \le p - |A_0 - A_0|. \tag{6}$$

To estimate $|A_0 - A_0|$ we apply Lemma 4 (see also the remark following the lemma); this gives

$$p - n - \delta \ge |A_0 - A_0| \ge \min\{l_0 + n_0, 3n_0 - 3\}.$$

Assuming $l_0 \ge 2n_0 - 3$ we then obtain

$$p \ge n + \delta + 3n_0 - 3 > (0.33 + 3 \cdot 0.25)p - 3 = 1.08p - 3,$$

contradicting the assumption $p > 100$. Thus

$$l_0 \le 2n_0 - 4, \tag{7}$$

$$|A_0 - A_0| \ge l_0 + n_0, \tag{8}$$

and $p - n - \delta \ge l_0 + n_0$ whence

$$l_0 \le p - n - n_0 - \delta. \tag{9}$$

Notice that this gives

$$\begin{aligned} l_0 \le p - n - n_0 &= \frac{7}{4}n_0 - \left(n + \frac{11}{4}n_0 - p\right) \\ &< \frac{7}{4}n_0 - (0.33 + 11 \cdot 0.25^2 - 1)p = \frac{7}{4}n_0 - 0.0175p < \frac{7}{4}n_0 - 1 \end{aligned}$$

and hence

$$\left(-\frac{n_0}{3}, \frac{n_0}{3}\right)_p \subseteq A_0 - A_0 \tag{10}$$

by Lemma 3 as applied with $k = 4$.

5) We observe that to complete the proof it suffices to show that

$$l_0 < \frac{3}{2}n_0 - 1. \tag{11}$$

Indeed, if this holds then $(-n_0, n_0)_p \subseteq A_0 - A_0$ by Lemma 3 whence

$$A \subseteq [n_0, p - n_0]_p \subseteq (p/4, 3p/4)_p$$

(as A is disjoint with $A_0 - A_0$) and therefore $A_0 = A$ by assumption (i) of Step 2. This gives $n_0 = n$ and $A \subseteq [n, p-n]_p$, as required.

6) We claim that

$$0 \notin [u, u + l_0]_p; \tag{12}$$

for otherwise A_0 and $A_0 - A_0$ are disjoint subsets of $[-l_0, l_0]_p$ so that

$$2l_0 + 1 \geq |A_0| + |A_0 - A_0| \geq l_0 + 2n_0$$

by (8), contradicting (7). On the other hand, modifying slightly (6) and using the Cauchy–Davenport inequality we can write

$$|A_0 \cup (-A_0)| \leq p - |A - A| \leq p - (2n-1) < 2n_0 = |A_0| + |-A_0|$$

(notice that $2n + 2n_0 > 2(0.33 + 0.25)p = 1.16p > p + 1$), hence $A_0 \cap (-A_0) \neq \varnothing$. Along with (12) and assumption (iii) of Step 3 this shows that

$$0 < u < p/2 < u + l_0 < p \tag{13}$$

and our next claim is that

$$p/4 < u < p/2. \tag{14}$$

For a contradiction, suppose that $0 < u < p/4$. As

$$\begin{aligned} l_0 + 1 - n_0 &\leq p/4 - (n + 2n_0 - 3p/4) + 1 \\ &< p/4 - (0.33 + 2 \cdot 0.25 - 0.75)p + 1 = p/4 - 0.08p + 1 < p/4 \end{aligned}$$

by (9) and the assumption $p > 100$ and since

$$(l_0 + 1 - n_0, p/4)_p \subseteq (l_0 + 1 - n_0, n_0)_p \subseteq A_0 - A_0$$

by Lemma 2, we have then $u \leq l_0 + 1 - n_0$ in view of $u \in A_0$. Furthermore, writing

$$[u, p/4)_p = [u, l_0 + 1 - n_0]_p \cup (l_0 + 1 - n_0, p/4)_p$$

and

$$(3p/4, p - u]_p = (3p/4, p - (l_0 + 1 - n_0)]_p \cup (p - (l_0 + 1 - n_0), p - u]_p$$

we obtain

$$|A \cap [u, p/4)_p| \leq l_0 + 2 - n_0 - u, \tag{15}$$

$$|A \cap (3p/4, p - u]_p| \leq l_0 + 2 - n_0 - u. \tag{16}$$

We also have

$$|A \cap (p/4, 3p/4)_p| \le n_0, \tag{17}$$

by Step 3, assumption (i). Adding together (15), (16), and (17) we obtain

$$|A_0 \cup (-A_0)| \le |A \cap [u, p-u]_p| + \delta \le n_0 + 2(l_0 + 2 - n_0 - u) + \delta. \tag{18}$$

On the other hand, since $A_0 \cap (-A_0) \subseteq [p - u - l_0, u + l_0]_p$ (as follows from (13)), we have

$$|A_0 \cap (-A_0)| \le (u + l_0) + 1 - (p - u - l_0) \tag{19}$$

in a trivial way. Summing up (18) and (19) we get

$$2n_0 \le (2l_0 + 4 - n_0 - 2u + \delta) + (2u + 2l_0 + 1 - p),$$

that is $3n_0 + p \le 4l_0 + 5 + \delta$. Taking into account (9) we derive that

$$3p + 5 \ge 7n_0 + 4n > (7 \cdot 0.25 + 4 \cdot 0.33)p = 3.07p$$

which contradicts the assumption $p > 100$.

Thus (14) is established and by symmetry (more precisely, since A can be replaced by $-A$ and u by $p - u - l_0$ in the above argument) we also have $u + l_0 < 3p/4$. Comparing with (13) we obtain

$$p/4 < u < p/2 < u + l_0 < 3p/4. \tag{20}$$

7) If $l_0 < p/3$ then $l_0/n_0 < 4/3$ whence

$$l_0 < \frac{3}{2}n_0 - \frac{1}{6}n_0 < \frac{3}{2}n_0 - 1$$

so that (11) holds true and the proof is over. Suppose now that

$$l_0 > p/3. \tag{21}$$

By (5) we have $A \setminus A_0 \subseteq (u - p/2, u + l_0 - p/2)_p$ and we represent $A \setminus A_0$ as a disjoint union $A_1 \cup A_2 \cup A_3$ where

$$\begin{aligned} A_1 &:= A \cap (u - p/2, p - 2l_0 - u)_p, \\ A_2 &:= A \cap [p - 2l_0 - u, l_0 - u]_p, \\ A_3 &:= A \cap (l_0 - u, u + l_0 - p/2)_p. \end{aligned} \tag{22}$$

(Observe that A_1 and A_3 are well-defined as $u-p/2<p-2l_0-u$ and $l_0-u<u+l_0-p/2$ by (20), and A_2 is well-defined as $p-2l_0-u<l_0-u$ by (21).) We have

$$u+A_3\subseteq(l_0,2u+l_0-p/2)_p,\quad (u+l_0)+A_1\subseteq(2u+l_0-p/2,p-l_0)_p$$

so that the four sets $A_0-A_0\subseteq[-l_0,l_0]_p, u+A_3, (u+l_0)+A_1$, and A are pairwise disjoint and therefore

$$p\geq|A_1|+|A_3|+|A_0-A_0|+|A|\geq|A_1|+|A_3|+(l_0+n_0)+n=l_0+2n-|A_2|$$

by (8). Consequently,

$$|A_2|\geq l_0+2n-p. \tag{23}$$

8) We now claim that

$$l_0<\frac{5}{3}n_0-1. \tag{24}$$

Assuming this is wrong, let

$$I:=\left[\frac{n_0}{3},\frac{l_0-n_0+1}{2}\right]_p \quad\text{and}\quad J:=\left[\frac{n_0}{2},l_0-n_0+1\right]_p; \tag{25}$$

these intervals are well-defined as

$$\frac{l_0-n_0+1}{2}-\frac{n_0}{3}=\frac{1}{2}\Big(l_0-\frac{5}{3}n_0+1\Big)\geq 0$$

and

$$(l_0-n_0+1)-\frac{n_0}{2}=l_0-\frac{3}{2}n_0+1\geq 0. \tag{26}$$

Since $((l_0-n_0+1)/2,n_0/2)_p$, $(l_0-n_0+1,n_0)_p\subseteq A_0-A_0$ by Lemma 2 and taking into account (10) we get

$$A_2\subseteq A\cap(-p/4,p/4)_p\subseteq(-J)\cup(-I)\cup I\cup J,$$

with A_2 defined by (22).

We distinguish two cases. First, suppose that both intervals $-J$ and J contain elements of A_2. Since A_2 contains no elements in the "gaps" between $-J,-I,I$, and J, and is itself contained in an interval of length $(l_0-u)-(p-2l_0-u)$, we have in this case

$$\begin{aligned}|A_2|&<(l_0-u)+1-(p-2l_0-u)-2\Big(\frac{n_0}{2}-\frac{l_0-n_0+1}{2}-1\Big)-\Big(2\cdot\frac{n_0}{3}-1\Big)\\&=4l_0-\frac{8}{3}n_0-p+5.\end{aligned}$$

Comparing with (23) we get

$$\begin{aligned} l_0 + 2n - p &< 4l_0 - \frac{8}{3}n_0 - p + 5, \\ 2n + \frac{8}{3}n_0 &< 3l_0 + 5 \end{aligned}$$

whence by (9)

$$3p + 5 > 5n + \frac{17}{3}n_0 > (5 \cdot 0.33 + (17/3) \cdot 0.25)p > 3.06p,$$

contradicting the assumption $p > 100$.

Now suppose that at least one of the intervals $-J$ and J contains no elements of A_2; say, $A_2 \cap (-J) = \varnothing$. Since for any $a \in A_2 \cap I$ we have $2a \in J \setminus A_2$, it follows that

$$|A_2 \cap I| + |A_2 \cap J| \le |J| \le l_0 - \frac{3}{2}n_0 + 2$$

and hence

$$\begin{aligned} |A_2| &= |A_2 \cap (-I)| + |A_2 \cap I| + |A_2 \cap J| \\ &\le \Big(\frac{l_0 - n_0 + 1}{2} - \frac{n_0}{3} + 1\Big) + \Big(l_0 - \frac{3}{2}n_0 + 2\Big) \\ &= \frac{3}{2}l_0 - \frac{7}{3}n_0 + \frac{7}{2}. \end{aligned}$$

Combining this with (23) and (9) we get

$$\begin{aligned} l_0 + 2n - p &\le \frac{3}{2}l_0 - \frac{7}{3}n_0 + \frac{7}{2}, \\ 4n + \frac{14}{3}n_0 &\le l_0 + 2p + 7, \\ 3p + 7 &\ge 5n + \frac{17}{3}n_0. \end{aligned}$$

Since $n_0 \ge (p+1)/4$ we derive that

$$3p + 7 \ge (5 \cdot 0.33 + (17/3) \cdot 0.25)p + (17/12) > 3.06p + 1,$$

a contradiction again. This proves (24).

9) We are now in a position to establish (11), completing the proof of Theorem 1. Suppose that (11) does not hold and define then J as in (25); computation (26) shows that this definition is correct. By (24) and Lemma 3, we have

$$\Big(-\frac{n_0}{2}, \frac{n_0}{2}\Big)_p \subseteq A_0 - A_0$$

and by Lemma 2,

$$(l_0 - n_0 + 1, n_0)_p \subseteq A_0 - A_0.$$

These two inclusions along with the definition of J show that

$$A_2 \subseteq A \cap (-p/4, p/4)_p \subseteq (-J) \cup J.$$

On the other hand, A_2 is contained in an interval of length

$$(l_0 - u) - (p - 2l_0 - u) = 3l_0 - p < (l_0 - n_0 + 1) - (-n_0/2)$$

(an easy verification based on (9) is left to the reader), hence

$$|A_2| \le |J| \le l_0 - \frac{3}{2}n_0 + 2$$

which by (23) and (9) implies

$$l_0 + 2n - p \le l_0 - \frac{3}{2}n_0 + 2,$$
$$p + 2 \ge 2n + \frac{3}{2}n_0 > (2 \cdot 0.33 + (3/2) \cdot 0.25)p = 1.035p,$$

a contradiction proving (11).

ACKNOWLEDGEMENT: The author is grateful to Gregory Freiman for fruitful discussions.

References

[DT89] A. Davydov and L. Tombak, *Quasi-perfect linear binary codes with distance 4 and complete caps in projective geometry,* Problemy Peredachi Informatzii **25**(4) (1989), 11–23.

[DFST99] J.-M. Deshouillers, G. Freiman, V. Sós and M. Temkin, *On the structure of sum-free sets. II,* Astérisque **258** (1999), xii, 149–161.

[DY69] P. H. Diananda and H. P. Yap, *Maximal sum-free sets of elements in finite groups,* Proceedings of the Japan Academy **45** (1969), 1–5.

[F62] G. A. Freiman, *Inverse problems of additive number theory, VII. On addition of finite sets, IV,* Izvestiya Vysshikh Uchebnykh Zavedeniy Matematika **6**(31) (1962), 131–144.

[F92] G. A. Freiman, *On the structure and the number of sum-free sets,* Astérisque **209** (1992), 13, 195–201.

[G04] B. Green, *The Cameron–Erdős Conjecture,* The Bulletin of the London Mathematical Society **36** (2004), 769–778.

[GR05] B. Green and I. Z. Ruzsa, *Sum-free sets in abelian groups,* Israel Journal of Mathematics **147** (2005), 157–188.

[K98] K. S. Kedlaya, *Product-free subsets of groups,* The American Mathematical Monthly **105** (1998), 900–906.

[L03] V. F. Lev, *Sharp estimates for the number of sum-free sets,* Journal für die reine und angewandte Mathematik (Crelle's Journal) **555** (2003), 1–25.

[L05] V. F. Lev, *Large sum-free sets in ternary spaces,* Journal of Combinatorial Theory, Series A **111**(2) (2005), 337–346.

[L] V. F. Lev, *Distribution of points on arcs,* INTEGERS, to appear.

[LS95] V. F. Lev and P. Y. Smeliansky, *On addition of two distinct sets of integers,* Acta Arithmetica **70** (1995), 85–91.

[LLS01] T. Łuczak, V. F. Lev and T. Schoen, *Sum-free sets in abelian groups,* Israel Journal of Mathematics **125** (2001), 347–367.

[RS70] A. H. Rhemtulla and A. P. Street, *Maximal sum-free sets in finite abelian groups,* Bulletin of the Australian Mathematical Society **2** (1970), 289–297.

[WSW72] J. S. Wallis, A. P. Street and W. D. Wallis, *Combinatorics: Room squares, sum-free sets, Hadamard matrices,* Lecture Notes in Mathematics **292**, Springer-Verlag, Berlin, 1972.

[Y72] H. P. Yap, *Maximal sum-free sets in finite abelian groups. IV,* Nanta Mathematica **5**(3) (1972), 70–75.

[Y75] H. P. Yap, *Maximal sum-free sets in finite abelian groups. V,* Bulletin of the Australian Mathematical Society **13** (1975), 337–342.