#A1 INTEGERS 14 (2014)

UPPER AND LOWER BOUNDS ON B_k^+-SETS

Craig Timmons[1]
Dept. of Mathematics, University of California San Diego, La Jolla, California
ctimmons@ucsd.edu

Received: 11/11/12, Revised: 10/2/13, Accepted: 12/6/13, Published: 1/6/14

Abstract

Let G be an abelian group. A set $A \subset G$ is a B_k^+*-set* if whenever $a_1 + \cdots + a_k = b_1 + \cdots + b_k$ with $a_i, b_j \in A$, there is an i and a j such that $a_i = b_j$. If A is a B_k-set then it is also a B_k^+-set, but the converse is not true in general. Determining the largest size of a B_k-set in the interval $\{1, 2, \dots, N\} \subset \mathbb{Z}$ or in the cyclic group $\mathbb{Z}_N$ is a well-studied problem. In this paper we investigate the corresponding problem for B_k^+-sets. We prove nontrivial upper bounds on the maximum size of a B_k^+-set contained in the interval $\{1, 2, \dots, N\}$. For odd $k \geq 3$, we construct B_k^+-sets that have more elements than the B_k-sets constructed by Bose and Chowla. We prove that any B_3^+-set $A \subset \mathbb{Z}_N$ has at most $(1 + o(1))(8N)^{1/3}$ elements. A set A is a B_k^**-set* if whenever $a_1 + \cdots + a_k = a_{k+1} + \cdots + a_{2k}$ with $a_i \in A$, there is an $i \neq j$ such that $a_i = a_j$. We obtain new upper bounds on the maximum size of a B_k^*-set $A \subset \{1, 2, \dots, N\}$, a problem first investigated by Ruzsa.

1. Introduction

Let G be an abelian group. A set $A \subset G$ is a B_k^+*-set* if

$$a_1 + \cdots + a_k = b_1 + \cdots + b_k \quad \text{with} \quad a_1, \dots, a_k, b_1, \dots, b_k \in A \tag{1}$$

implies $a_i = b_j$ for some i and j. A set A is a B_k*-set* if (1) implies $(a_1, \dots, a_k)$ is a permutation of $(b_1, \dots, b_k)$. If A is a B_k-set then A is also a B_k^+-set, but in general the converse is not true. Often B_2-sets are called *Sidon sets* and have received much attention since they were first studied by Erdős and Turán [9] in 1941. Let $F_k(N)$ be the maximum size of a B_k-set $A \subset [N]$ and let $C_k(N)$ be the maximum size of a B_k-set $A \subset \mathbb{Z}_N$. If $A \subset \mathbb{Z}_N$ is a B_k-set, then A is also a B_k-set when viewed as a subset of $\mathbb{Z}$. Thus, for any $k \geq 2$, $C_k(N) \leq F_k(N)$.

Erdős and Turán proved $F_2(N) \leq N^{1/2} + O(N^{1/4})$. Their argument was used by Lindström [13] to show $F_2(N) \leq N^{1/2} + N^{1/4} + 1$. In 2010, Cilleruelo [5] obtained

[1] The author was partially supported by NSF Grant DMS-1101489 through Jacques Verstraëte.

$F_2(N) \leq N^{1/2}+N^{1/4}+\frac{1}{2}$ as a consequence of a more general result. This is the best known upper bound on $F_2(N)$. By counting differences $a-b$ with $a \neq b$, it is easy to prove $C_2(N) \leq \sqrt{N}+1$. There are several constructions of dense B_2-sets (see [17], [2], [16]) that show $C_2(N) \geq N^{1/2}$ for infinitely many N. These constructions imply $F_2(N) \sim \sqrt{N}$ and $\limsup \frac{C_2(N)}{\sqrt{N}} = 1$.

For $k \geq 3$, bounds on $F_k(N)$ and $C_k(N)$ are not as precise. For each $k \geq 2$ and prime power q, Bose and Chowla [2] constructed a B_k-set $A \subset \mathbb{Z}_{q^k-1}$ with $|A| = q$ so that

$$(1+o(1))N^{1/k} \leq F_k(N).$$

The current upper bounds on $F_k(N)$ and $C_k(N)$ do not match this lower bound for any $k \geq 3$. If $A \subset [N]$ is a B_k-set then each k-multiset in A gives rise to a unique sum in $\{1, \ldots, kN\}$. Therefore, $\binom{|A|+k-1}{k} \leq kN$ which implies $F_k(N) \leq (k! \cdot kN)^{1/k}$. Similar counting shows $C_k(N) \leq (k!N)^{1/k}$. By considering differences one can improve these bounds. We illustrate this idea with an example that is relevant to our results. Let $A \subset \mathbb{Z}_N$ be a B_3-set. There are $\binom{|A|}{2}(|A|-2)$ sums of the form $a_1+a_2-a_3$ where a_1, a_2, and a_3 are distinct elements of A. Let $A^{(2)} = \{\{x,y\} : x, y \in A, x \neq y\}$. It is not hard to check that each $n \in \mathbb{Z}_N$ has at most one representation as $n = a_1+a_2-a_3$ with $\{a_1,a_2\} \in A^{(2)}$ and $a_3 \in A\backslash\{a_1,a_2\}$. This implies $\binom{|A|}{2}(|A|-2) \leq N$ so $|A| \leq (2N)^{1/3}+2$. In general, for any $k \geq 2$

$$C_k(N) \leq \left(\left\lfloor \frac{k}{2} \right\rfloor ! \left\lceil \frac{k}{2} \right\rceil !N \right)^{1/k} + O_k(1), \tag{2}$$

and

$$F_k(N) \leq \left(\left\lfloor \frac{k}{2} \right\rfloor ! \left\lceil \frac{k}{2} \right\rceil ! \cdot \left\lceil \frac{k}{2} \right\rceil N \right)^{1/k} + O_k(N^{1/2k}). \tag{3}$$

These bounds were first obtained by Jia [12] in the even case, and Chen [3] in the odd case. The best upper bounds on $F_k(N)$ are to due to Green [10]. For every $k \geq 2$, (3) has been improved (see for example [10] or [4]), but there is no value of $k \geq 3$ for which (2) has been improved. This is interesting since all of the constructions take place in cyclic groups and provide lower bounds on $C_k(N)$. For other bounds on B_k-sets the interested reader is referred to Green [10], Cilleruelo [4], O'Bryant's survey [14], or the book of Halberstam and Roth [11].

Now we discuss B_k^+-sets. Write $F_k^+(N)$ for the maximum size of a B_k^+-set $A \subset [N]$, and $C_k^+(N)$ for the maximum size of a B_k^+-set $A \subset \mathbb{Z}_N$. Ruzsa [16] proved that a set $A \subset [N]$ with no solution to the equation $x_1+\cdots+x_k = y_1+\cdots+y_k$ in $2k$ distinct integers has at most $(1+o(1))k^{2-1/k}N^{1/k}$ elements. Call such a set a B_k^*-set and define $F_k^*(N)$ in the obvious way. Any B_k^+-set is also a B_k^*-set so that $F_k^+(N) \leq F_k^*(N)$. Using the constructions of Bose and Chowla [2] and Ruzsa's Theorem 5.1 of [16], we get for every $k \geq 3$,

$$(1+o(1))N^{1/k} \leq F_k(N) \leq F_k^+(N) \leq F_k^*(N) \leq (1+o(1))k^{2-1/k}N^{1/k}.$$

In this paper we improve this upper bound on $F_k^+(N)$ and $F_k^*(N)$. We also improve this lower bound on $F_k^+(N)$ for all odd $k \geq 3$, and we prove a nontrivial upper bound on $C_3^+(N)$. We do not consider the case when $k = 2$. The reason for this is that Ruzsa [16] proved $F_2^*(N) \leq N^{1/2} + 4N^{1/4} + 11$, and thus $F_2(N) \sim F_2^+(N) \sim F_2^*(N) \sim N^{1/2}$. In fact, a B_2-set is the same as a B_2^+-set.

Our first result is a construction which shows that for any odd $k \geq 3$, there is a B_k^+-set in $[N]$ that has more elements than any known B_k-set contained in $[N]$.

Theorem 1.1. *For any prime power q and odd integer $k \geq 3$, there is a B_k^+-set $A \subset \mathbb{Z}_{2(q^k-1)}$ with $|A| = 2q$.*

Using known results on densities of primes (see [1] for example), Theorem 1.1 implies

Corollary 1.2. *For any integer $N \geq 1$ and any odd integer $k \geq 3$,*

$$F_k^+(N) \geq (1 + o(1))2^{1-1/k}N^{1/k}.$$

Green proved $F_3(N) \leq (1+o(1))(3.5N)^{1/3}$. We will use a Bose-Chowla B_3-set to construct a B_3^+-set $A \subset [2q^3]$ with $|A| = 2q = (4 \cdot 2q^3)^{1/3}$. Putting the two results together we see that A is denser than any B_3-set in $[2q^3]$ for sufficiently large prime powers q. Our construction and Green's upper bound show that $F_3(N)$ and $F_3^*(N)$ are not asymptotically the same.

The proof of Theorem 1.1 is based on a simple lemma, Lemma 2.1, which implies

$$2C_k(N) \leq C_k^+(2N) \text{ for any odd } k \geq 3. \tag{4}$$

This inequality provides us with a method of estimating $C_k(N)$ by proving upper bounds on $C_k^+(N)$ for odd k. Our next theorem provides such an estimate when $k = 3$.

Theorem 1.3. *If $A \subset \mathbb{Z}_N$ is a B_3^+-set, then $|A| \leq (1 + o(1))(8N)^{1/3}$.*

Theorem 1.3 and (4) imply

Corollary 1.4. *If $A \subset \mathbb{Z}_N$ is a B_3-set, then $|A| \leq (1 + o(1))(2N)^{1/3}$.*

As shown above, there is a simpler argument that implies this bound. The novelty here is that our results imply (2) for $k = 3$. It is important to mention that the error term we obtain is larger than the error term in the bound $C_3(N) \leq (2N)^{1/3} + 2$. We feel that any improvement in the leading term of Theorem 1.3 or (2) would be significant.

In $\mathbb{Z}$ we obtain the following bounds for small k.

Theorem 1.5. *(i) If $A \subset [N]$ is a B_3^+-set, then $|A| \leq (1 + o(1))(18N)^{1/3}$.*

(ii) If $A \subset [N]$ is a B_4^+-set, then $|A| \leq (1 + o(1))(272N)^{1/4}$.

Recall that Ruzsa [16] proved $F_k^*(N) \leq (1+o(1))k^{2-1/k}N^{1/k}$ which implies $F_k^+(N) \leq (1+o(1))k^{2-1/k}N^{1/k}$. For $k \geq 5$, we were able to improve this upper bound on $F_k^+(N)$ by modifying arguments of Ruzsa. Our method also applies to B_k^*-sets. As a consequence, we improve the upper bound on $F_k^*(N)$ for all $k \geq 3$. We state our result only for $k = 3$ and for large k. For other small values of k the reader is referred to Table 1 in Section 6.

Theorem 1.6. *If $A \subset [N]$ is a B_3^*-set, then $|A| \leq (1+o(1))(162N)^{1/3}$. If $A \subset [N]$ is a B_k^*-set, then*

$$|A| \leq \left(\frac{1}{4} + \epsilon(k)\right) k^2 N^{1/k}$$

where $\epsilon(k) \to 0$ as $k \to \infty$.

We remark that Ruzsa's upper bound on $F_k^*(N)$ is asymptotic to $k^2N^{1/k}$. Our results do not rule out the possibility of $F_k^+(N)$ being asymptotic to $F_k^*(N)$.

Problem 1.7. Determine whether or not $F_k^+(N)$ is asymptotic to $F_k^*(N)$ for $k \geq 3$.

If $A \subset [N]$ is a B_k^*-set, then the number of solutions to $2x_1 + x_2 + \cdots + x_{k-1} = y_1 + \cdots + y_k$ with $x_i, y_j \in A$ is $o(|A|^k)$ (see [16]). A B_k^*-set allows solutions to this equation with $x_1, \ldots, x_{k-1}, y_1, \ldots, y_k$ all distinct, but such a solution cannot occur in a B_k^+-set. If it were true that $F_k^+(N)$ is asymptotic to $F_k^*(N)$, then this would confirm the belief that it is the sums of k distinct elements of A that control the size of A and the lower order sums should not matter. Jia [12] defines a *semi-B_k-set* to be a set A with the property that all sums consisting of k distinct elements of A are distinct. He states that Erdős conjectured [8] that a semi-B_k-set $A \subset [N]$ should satisfy $|A| \leq (1+o(1))N^{1/k}$. A positive answer to Problem 1.7 would be evidence in favor of this conjecture.

At this time we do not know how to construct B_{2k}^+-sets or B_{2k}^*-sets for any $k \geq 2$ that are bigger than the corresponding Bose-Chowla B_{2k}-sets. We were able to construct interesting B_4^+-sets in the non-abelian setting.

Let G be a non-abelian group. A set $A \subset G$ is a *non-abelian B_k-set* if

$$a_1 a_2 \cdots a_k = b_1 b_2 \cdots b_k \quad \text{with} \quad a_i, b_j \in A \tag{5}$$

implies $a_i = b_i$ for $1 \leq i \leq k$. If $A \subset G$ is a non-abelian B_k-set, then every k-letter word in $|A|$ is different so $|A|^k \leq |G|$. Odlyzko and Smith [15] proved that there exist infinitely many groups G such that G has a non-abelian B_4-set $A \subset G$ with $|A| = (1+o(1))\left(\frac{|G|}{1024}\right)^{1/4}$. They actually proved a more general result that gives constructions of non-abelian B_k-sets for all $k \geq 2$. The case when $k = 4$ is the only result that we will need. Define a *non-abelian B_k^+-set* to be a set $A \subset G$ such that (5) implies $a_i = b_i$ for some $i \in \{1, 2, \ldots, k\}$. As in the abelian setting, a non-abelian B_k-set is also a non-abelian B_k^+-set but the converse is not true in general. Using a construction of [15], we prove

Theorem 1.8. *For any prime p with $p-1$ divisible by 4, there is a non-abelian group G of order $48(p^4-1)$ that contains a non-abelian B_4^+-set $A \subset G$ with*

$$|A| = \frac{1}{2}(p-1).$$

Our result shows that there are infinitely many groups G such that G has a non-abelian B_4^+-set A with $|A| = \left(\frac{|G|}{768}\right)^{1/4} + o(|G|^{1/4})$. We conclude our introduction with the following conjecture concerning B_{2k}^+-sets.

Conjecture 1.9. If $k \geq 4$ is any even integer, then there exists a positive constant c_k such that for infinitely many N,

$$F_k^+(N) \geq (1 + c_k + o(1))N^{1/k}.$$

If Conjecture 1.9 is true with $c_k = 2^{1-1/k} - 1$ as in the odd case, then using Green's upper bound $F_4(N) \leq (1+o(1))(7N)^{1/4}$, we can conclude that $F_4(N)$ and $F_4^*(N)$ are not asymptotically the same just as in the case when $k=3$. Our hope is that a positive answer to Conjecture 1.9 will either provide an analogue of (4) for even $k \geq 4$, or a construction of a B_k^+-set that does not use Bose-Chowla B_k-sets.

2. Proof of Theorem 1.1

In this section we show how to construct B_k^+-sets for odd $k \geq 3$. Our idea is to take a dense B_k-set A and a translate of A.

Lemma 2.1. *If $A \subset \mathbb{Z}_N$ is a B_k-set where $k \geq 3$ is odd, then*

$$A^+ := \{a + bN : a \in A, b \in \{0,1\}\}$$

is a B_k^+-set in $\mathbb{Z}_{2N}$.

Proof. Let $k \geq 3$ be odd and suppose

$$\sum_{i=1}^{k} a_i + b_i N \equiv \sum_{i=1}^{k} c_i + d_i N \pmod{2N} \tag{6}$$

where $a_i, c_i \in A$, and $b_i, d_i \in \{0,1\}$. Taking (6) modulo N gives

$$\sum_{i=1}^{k} a_i \equiv \sum_{i=1}^{k} c_i \pmod{N}.$$

Since A is a B_k-set in $\mathbb{Z}_N$, $(a_1, \dots, a_k)$ must be a permutation of $(c_1, \dots, c_k)$. If we label the a_i's and c_i's so that $a_1 \leq a_2 \leq \cdots \leq a_k$ and $c_1 \leq c_2 \leq \cdots \leq c_k$, then $a_i = c_i$ for $1 \leq i \leq k$. Rewrite (6) as

$$\sum_{i=1}^{k} b_i N \equiv \sum_{i=1}^{k} d_i N \pmod{2N}.$$

The sums $\sum_{i=1}^{k} b_i$ and $\sum_{i=1}^{k} d_i$ have the same parity. Since k is odd and $b_i, d_i \in \{0,1\}$, there must be a j such that $b_j = d_j$, so $a_j + b_j N \equiv c_j + d_j N \pmod{2N}$. □

Let q be a prime power, $k \geq 3$ be an odd integer, and A_k be a Bose-Chowla B_k-set with $A_k \subset \mathbb{Z}_{q^k-1}$ (see [2] for a description of A_k). Let

$$A_k^+ = \{a + b(q^k - 1) : a \in A_k, b \in \{0,1\}\}.$$

By Lemma 2.1, A_k^+ is a B_k^+-set in $\mathbb{Z}_{2(q^k-1)}$ and $|A_k^+| = 2|A_k| = 2q$. This proves Theorem 1.1.

3. Proof of Theorem 1.3

Let $A \subset \mathbb{Z}_N$ be a B_3^+-set. If N is odd, then $2x \equiv 2y \pmod{N}$ implies $x \equiv y \pmod{N}$. If N is even, then $2x \equiv 2y \pmod{N}$ implies $x \equiv y \pmod{N}$ or $x \equiv y + N/2 \pmod{N}$. Because of this, the odd case is quite a bit easier to deal with and so we present the more difficult case. **In this section N is assumed to be even**. If N is odd, then the proof of Theorem 1.5(i) given in the next section works in $\mathbb{Z}_N$. The only modification needed is to divide by N instead of $3N$ when applying Cauchy-Schwarz. For simplicity of notation, we write $x = y$ rather than $x \equiv y \pmod{N}$.

For $n \in \mathbb{Z}_N$, define

$$f(n) = \#\left\{(\{a,c\}, b) \in A^{(2)} \times A : n = a - b + c, \{a,c\} \cap \{b\} = \emptyset\right\}.$$

Recall that $A^{(2)} = \{\{x,y\} : x, y \in A, x \neq y\}$. The sum $\sum f(n)(f(n)-1)$ counts the number of ordered pairs $((\{a,c\},b),(\{x,z\},y))$ such that the tuples $(\{a,c\},b)$ and $(\{x,z\},y)$ are distinct, and both are counted by $f(n)$. For each such pair we cannot have $\{a,c\} = \{x,z\}$. Otherwise, the tuples would be equal. If $((\{a,c\},b),(\{x,z\},y))$ is counted by $\sum f(n)(f(n)-1)$, then $a + y + c = x + b + z$. By the B_3^+ property, $\{a,y,c\} \cap \{x,b,z\} \neq \emptyset$ so that $\{a,c\} \cap \{x,z\} \neq \emptyset$ or $b = y$. The tuples are distinct, so both of these cases cannot occur at the same time.

`Case 1:` $\{a,c\} \cap \{x,z\} \neq \emptyset$ and $b \neq y$.

Without loss of generality, assume $a = x$. Cancel a from both sides of the equation $a - b + c = x - y + z$ and solve for c to get $c = b - y + z$. Here we are using the ordering of the tuples $((\{a,c\},b),(\{x,z\},y))$ to designate which element is solved for after the cancellation of the common term.

If $z=b$, then $c+y=2b$ and we have a 3-term arithmetic progression (a.p. for short). The number of trivial 3-term a.p.'s in A is at most $2|A|$ since for any $a \in A$,

$$a+a=2a=2(a+N/2).$$

Next we count the number of nontrivial 3-term a.p.'s. By nontrivial, we mean that all terms involved in the a.p. are distinct, and $a+a=2(a+N/2)$ is considered to be trivial.

If $p+q=2r$ is a 3-term a.p., then call p and q *outer terms*. Let p be an outer term of the 3-term a.p. $p+q=2r$ where $p,q,r \in A$. We will show that p is an outer term of at most one other nontrivial a.p. Let $p+q'=2r'$ be another a.p. with $q',r' \in A$ and $(q,r,) \neq (q',r')$.

If $r=r'$, then $p+q=2r=2r'=p+q'$ so $q=q'$. This is a contradiction and so we can assume that $r \neq r'$.

If $q=q'$, then $2r=p+q=p+q'=2r'$ so $r'=r$ or $r'=r+N/2$. Thus, $p+q=2r$ or $p+q=2(r+N/2)$.

Now suppose $r \neq r'$ and $q \neq q'$. Since $2r-q=p=2r'-q'$ we have by the B_3^+ property,

$$\{r,q'\} \cap \{r',q\} \neq \emptyset.$$

The only two possibilities are $r=q$ or $r'=q'$, but in either of these cases we get a trivial 3-term a.p. Putting everything together proves the following lemma.

Lemma 3.1. *If $A \subset \mathbb{Z}_N$ is a B_3^+-set, then the number of 3-term arithmetic progressions in A is at most $4|A|$.*

Given a fixed element $a \in A$ and a fixed 3-term a.p. $c+y=2b$ in A, there are at most $4!$ ways to form an ordered tuple of the form $((\{a,c\},b),(\{a,b\},y))$. The number of ordered tuples counted by $\sum f(n)(f(n)-1)$ when $\{a,c\} \cap \{x,z\} \neq \emptyset$ and $z=b$ is at most $4!|A| \cdot 4|A| = 96|A|^2$. The first factor of $|A|$ in the expression $4!|A| \cdot 3|A|$ comes from the number of ways to choose the element a.

Assume now that $z \neq b$. Recall that we have solved for c to get $c=b-y+z$. If $b=y$, then $c=z$ which implies $\{a,c\}=\{x,z\}$, a contradiction as the tuples are distinct. By definition $y \neq z$, so $c=b-y+z$ where $\{b,z\} \in A^{(2)}$ and $\{y\} \cap \{b,z\} = \emptyset$. The number of ways to write c in this form is $f(c)$. Given such a solution $\{b,z\},y$ counted by $f(c)$, there are two ways to order b and z, and $|A|$ ways to choose $a=x$. The number of ordered tuples we obtain when $\{a,c\} \cap \{x,z\} \neq \emptyset$ and $z \neq b$ is at most $|A| \cdot 2\sum_{c \in A} f(c)$. This completes the analysis in Case 1.

Before addressing Case 2, the case when $b=y$ and $\{a,c\} \cap \{x,z\} = \emptyset$, some additional notation is needed. For $d \in A+A$, define

$$S(d) = \big\{\{a,b\} \in A^{(2)} : a+b=d \text{ and there is a pair } \{a',b'\} \in A^{(2)} \\ \text{with } \{a,b\} \cap \{a',b'\} = \emptyset \text{ and } a'+b'=d\big\}.$$

Let $d_1, d_2, \dots, d_M$ be the integers for which $S(d_i) \neq \emptyset$. Write S_i^2 for $S(d_i)$ and define

$$T_i^1 = \{a : a \in \{a,b\} \text{ for some } \{a,b\} \in S_i^2\}.$$

Let $s_i = |S_i^2|$ and $d_1, d_2, \dots, d_m$ be the integers for which $s_i = 2$. Let $d_{m+1}, \dots, d_M$ be the integers for which $s_i \geq 3$. For $1 \leq i \leq M$, we will use the notation $S_i^2 = \{\{a_1^i, b_1^i\}, \{a_2^i, b_2^i\}, \dots, \{a_{s_i}^i, b_{s_i}^i\}\}$. A simple, but important, observation is that for any fixed $i \in \{1, \dots, M\}$, any element of A appears in at most one pair in S_i^2.

If A was a B_3-set, then there would be no d_i's. This suggests that a B_3^+-set or a B_3^*-set that is denser than a B_3-set should have many d_i's. The B_3^+-set A_3^+ constructed in Theorem 1.1 has $m \approx \frac{1}{2}\binom{|A_3^+|}{2}$. However, if A_3^+ is viewed as a subset of $\mathbb{Z}$, then $m \approx \frac{1}{4}\binom{|A_3^+|}{2}$ (see Lemma 4.3 which also holds in $\mathbb{Z}_N$ if N is odd).

Case 2: $b = y$ and $\{a,c\} \cap \{x,z\} = \emptyset$.

If $b = y$, then $a + c = x + z$. There are $|A|$ choices for $b = y$ and

$$\sum_{i=1}^{M} |S_i^2|(|S_i^2| - 1)$$

ways to choose an ordered pair of different sets $\{a,c\}, \{x,z\} \in A^{(2)}$ with $a+c = x+z$, and $\{a,c\} \cap \{x,z\} = \emptyset$.

Putting Cases 1 and 2 together gives the estimate

$$\sum f(n)(f(n)-1) \leq |A| \left(2\sum_{c \in A} f(c) + \sum_{i=1}^{M} |S_i^2|(|S_i^2| - 1) \right) + 96|A|^2. \qquad (7)$$

Our goal is to find upper bounds on the sums $\sum_{c \in A} f(c)$ and $\sum_{i=1}^{M} |S_i^2|(|S_i^2| - 1)$.

Lemma 3.2. *If $x \in T_i^1 \cap T_j^1$ for some $i \neq j$, then (i) $\max\{s_i, s_j\} \leq 3$ and (ii) if $s_i = s_j = 3$, then for some $x_1, y, z \in A$ depending on i and j, we have $d_j = d_i + N/2$ and $S_i^2 = \{\{x, x_1\}, \{y, z\}, \{y + \frac{N}{2}, z + \frac{N}{2}\}\}$, $S_j^2 = \{\{x, x_1 + \frac{N}{2}\}, \{y + \frac{N}{2}, z\}, \{y, z + \frac{N}{2}\}\}$.*

Proof. If $s_i = 2$ and $s_j = 2$ then we are done. Assume $s_j > 2$. Let $S_i^2 = \{\{a_1^i, b_1^i\}, \dots, \{a_{s_i}^i, b_{s_i}^i\}\}$ and $S_j^2 = \{\{a_1^j, b_1^j\}, \dots, \{a_{s_j}^j, b_{s_j}^j\}\}$. Without loss of generality, suppose $x = a_i^1$ and $x = a_j^1$. By definition, $s_i \geq 2$ so we can write $d_i = x + b_1^i = a_2^i + b_2^i$ and $d_j = x + b_1^j = a_2^j + b_2^j = a_3^j + b_3^j$.

Solve for x to get $x = a_2^i + b_2^i - b_1^i = a_2^j + b_2^j - b_1^j$. This can be rewritten as

$$a_2^i + b_2^i + b_1^j = a_2^j + b_2^j + b_1^i. \qquad (8)$$

Since $d_i \neq d_j$, b_1^i cannot be b_1^j therefore b_1^j is not on the right hand side of (8), and b_1^i is not on the left hand side of (8). By the B_3^+ property, $\{a_2^i, b_2^i\} \cap \{a_2^j, b_2^j\} \neq \emptyset$.

The same argument can be repeated with a_3^j in place of a_2^j and b_3^j in place of b_2^j to get

$$\{a_2^i, b_2^i\} \cap \{a_3^j, b_3^j\} \neq \emptyset.$$

Recall any element of A can occur at most once in the list $a_1^j, b_1^j, a_2^j, b_2^j, \ldots a_{s_j}^j, b_{s_j}^j$ thus $s_j \leq 3$. By symmetry, $s_i \leq 3$.

Now suppose $s_i = s_j = 3$. Repeating the argument above, we have for each $2 \leq k \leq 3$ and $2 \leq l \leq 3$,

$$|\{a_l^i, b_l^i\} \cap \{a_k^j, b_k^j\}| = 1.$$

This intersection cannot have size 2 since $d_i \neq d_j$. Without loss of generality, let $y = a_2^i = a_2^j$, $z = b_2^i = a_3^j$, $u = a_3^i = b_2^j$, and $v = b_3^i = b_3^j$. We represent these equalities between T_i^1 and T_j^1 using a bipartite graph with parts T_i^1 and T_j^1 where $w \in T_i^1$ is adjacent to $w' \in T_j^1$ if and only if $w = w'$ (see Figure 1).

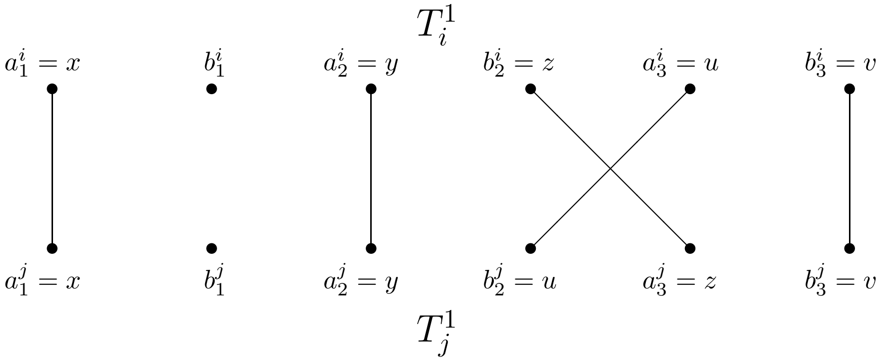

Figure 1 - Equality Graph for Lemma 3.2

The equalities $d_i = y+z = u+v$ and $d_j = y+u = z+v$ imply $d_i - d_j = z - u$ and $d_i - d_j = u - z$. Therefore $2z = 2u$. If $z = u$, then this is a contradiction since the elements in the list x, b_1^i, y, z, u, v are all distinct. It is in this step that the parity of N plays an important role. We conclude $u = z + N/2$ and

$$d_j = y + u = y + (z + N/2) = y + z + N/2 = d_i + N/2.$$

Let $b_1^i = x_1$ so $b_1^j = x_1 + N/2$. Since $d_i = y + z = u + v$ and $u = z + N/2$,

$$v = y + z - u = y + z - (z + N/2) = y - N/2 = y + N/2.$$

Substituting $u = z + N/2$ and $v = y + N/2$ gives the assertion about the pairs in S_i^2 and S_j^2 when $s_i = s_j = 3$. □

Corollary 3.3. *If $s_i \geq 4$, then for any $j \neq i$, $T_i^1 \cap T_j^1 = \emptyset$. Furthermore, any $x \in A$ is in at most two T_i^1's with $s_i = 3$.*

Proof. The first statement follows immediately from Lemma 3.2. For the second statement, suppose $x \in T_i^1 \cap T_j^1$ with $s_i = s_j = 3$ and $i \neq j$. By Lemma 3.2, $\{x, x_1\} \in S_i^2$ and $\{x, x_1 + N/2\} \in S_j^2$ for some $x_1 \in A$. If $x \in T_k^1$ with $k \neq i$, then $\{x, x_1 + N/2\} \in S_k^2$ so $d_j = x + (x_1 + N/2) = d_k$ and $j = k$. □

Lemma 3.4. *If $A \subset \mathbb{Z}_N$ is a B_3^+-set, then*

$$\sum_{c \in A} f(c) \leq |A|^2 + 7|A|.$$

Proof. For $c \in A$, let

$$g_1(c) = \# \left\{ (\{x, z\}, y) \in A^{(2)} \times A : c = x - y + z, c \neq y, \{x, z\} \cap \{y\} = \emptyset \right\}$$

and

$$g_2(c) = \# \left\{ (\{x, z\}, y) \in A^{(2)} \times A : c = x - y + z, c = y, \{x, z\} \cap \{y\} = \emptyset \right\}.$$

For each $c \in A$, $f(c) = g_1(c) + g_2(c)$. The sum $\sum_{c \in A} g_2(c)$ is exactly the number of nontrivial 3-term a.p.'s in A. By Lemma 3.1, $\sum_{c \in A} g_1(c) \leq 4|A|$. Estimating $\sum_{c \in A} g_1(c)$ takes more work. To compute $g_1(c)$ with $c \in A$, we first choose an i with $c \in T_i^1$, and then choose one of the pairs $\{x, z\} \in S_i^2 \backslash \{c, y\}$ to obtain a solution $c = x - y + z$ with $c \neq y$ and $\{x, z\} \cap \{y\} = \emptyset$.

If $c \notin T_1^1 \cup \cdots \cup T_M^1$, then the equation $c + y = x + z$ with c, y, x, and z all distinct has no solutions in A so $g_1(c) = 0$. Assume $c \in T_1^1 \cup \cdots \cup T_M^1$.

`Case 1:` $c \notin T_1^1 \cup \cdots \cup T_m^1$.

By Corollary 3.3, there are two possibilities. One is that there is a unique j with $c \in T_j^1$ and $s_j \geq 3$. In this case, $|S_j^2| \leq \frac{|A|}{2}$ so $g_1(c) \leq \frac{|A|}{2}$. The other possibility is that $c \in T_i^1 \cap T_j^1$ with $s_i = s_j = 3$ and $i \neq j$. In this case, $g_1(c) \leq 4$ because we can choose either i or j, and then one of the two pairs in S_i^2 or S_j^2 that does not contain c.

`Case 2:` $c \in T_1^1 \cup \cdots \cup T_m^1$.

By Lemma 3.2, c is not in any T_j^1 with $s_j \geq 4$ and c is in at most two T_j^1's with $s_j = 3$. There are at most $|A|$ T_i^1's with $c \in T_i^1$ since there are at most $|A|$ pairs $\{c, y\}$ that contain c so $g_1(c) \leq |A| + 4$.

In all cases, $g_1(c) \leq |A| + 4$ and

$$\sum_{c \in A} f(c) = \sum_{c \in A} (g_1(c) + g_2(c)) \leq |A|(|A| + 4) + 4|A|$$

which proves the lemma. □

Lemma 3.5. *If $g_1(c)$ is the function of Lemma 3.4, then*

$$2 \sum_{i=1}^{M} |S_i^2|(|S_i^2| - 1) = \sum_{c \in A} g_1(c).$$

Proof. Define an edge-colored graph G with vertex set A, edge set $\cup_{i=1}^{M} S_i^2$, and such that the color of edge $\{a, b\}$ is $a + b$. The sum $\sum_{i=1}^{M} |S_i^2|(|S_i^2| - 1)$ counts ordered pairs $(\{c, y\}, \{x, z\})$ of distinct edges of G where $\{c, y\}$ and $\{x, z\}$ have the same color, i.e., $c + y = x + z$, and c, y, x, and z are all distinct elements of A. The sum $\sum_{c \in A} g_1(c)$ counts each such ordered pair $(\{c, y\}, \{x, z\})$ exactly two times, one contribution coming from $g_1(c)$ and the other from $g_1(y)$. □

By Lemma 3.5,

$$\sum_{i=1}^{M} |S_i^2|(|S_i^2| - 1) \le \frac{1}{2} \sum_{c \in A} f(c). \tag{9}$$

Next we use the following version of the Cauchy-Schwarz inequality.

Lemma 3.6. (Cauchy-Schwarz) *If $x_1, \ldots, x_n$ are real numbers, $t \in \{1, 2, \ldots, n-1\}$, and $\Delta = \frac{1}{t}\sum_{i=1}^{t} x_i - \frac{1}{n}\sum_{i=1}^{n} x_i$, then*

$$\sum_{i=1}^{n} x_i^2 \ge \frac{1}{n}\left(\sum_{i=1}^{n} x_i\right)^2 + \frac{tn\Delta^2}{n-t}.$$

A simple counting argument shows $\sum f(n) = \binom{|A|}{2}(|A| - 2)$. Let $\sum_{c \in A} f(c) = \delta |A|^2$. If

$$\Delta := \frac{1}{|A|}\sum_{c \in A} f(c) - \frac{1}{N}\sum_{n} f(n) = \delta|A| - \frac{1}{N}\sum_{n} f(n)$$

then, using Ruzsa's bound $|A| = O(N^{1/3})$ and $C_3^+(N) \le F_3^+(N)$, we get

$$\Delta = \delta|A| - \frac{\binom{|A|}{2}(|A| - 2)}{N} \ge \delta|A| - C$$

where C is some absolute constant. By Lemma 3.6,

$$\begin{aligned}
\sum f(n)^2 &\ge \frac{\binom{|A|}{2}^2(|A| - 2)^2}{N} + \frac{|A| \cdot N(\delta|A| - C)^2}{N - |A|} \\
&= \frac{\binom{|A|}{2}^2(|A| - 2)^2}{N} + \delta^2|A|^3 \frac{\left(1 - \frac{C}{\delta|A|}\right)^2}{1 - \frac{|A|}{N}}.
\end{aligned}$$

By (7) and (9),

$$\begin{aligned}
\sum f(n)^2 &\le \sum f(n) + |A|\left(2\sum_{c \in A} f(c) + \sum_{i=1}^{M} |S_i^2|(|S_i^2| - 1)\right) + 96|A|^2 \\
&\le \frac{|A|^3}{2} + \frac{5|A|}{2}\sum_{c \in A} f(c) + 96|A|^2 \\
&= |A|^3\left(\frac{1 + 5\delta}{2}\right) + 96|A|^2.
\end{aligned}$$

Combining the two estimates on $\sum f(n)^2$ gives the inequality

$$\frac{\binom{|A|}{2}^2(|A|-2)^2}{N}+\delta^2|A|^3\frac{\left(1-\frac{C}{\delta|A|}\right)^2}{1-\frac{|A|}{N}}\leq |A|^3\left(\frac{1+5\delta}{2}\right)+96|A|^2. \qquad (10)$$

If $\delta=0$, then (10) is not valid but we still get

$$\frac{\binom{|A|}{2}^2(|A|-2)^2}{N}\leq\frac{|A|^3}{2}+96|A|^2.$$

This inequality implies $|A|\leq(1+o(1))(2N)^{1/3}$. Assume that $\delta>0$. In this case, (10) simplifies to

$$|A|\leq(1+o(1))\left(2+10\delta-4\delta^2\right)^{1/3}N^{1/3}. \qquad (11)$$

At this point we find the maximum of the right hand side of (11) using the fact that $0\leq\delta\leq 1+\frac{7}{|A|}$, which follows from Lemma 3.4. For $|A|\geq 28$, the maximum occurs when $\delta=1+\frac{7}{|A|}$ therefore, after some simplifying, we find

$$|A|\leq(1+o(1))(8N)^{1/3}.$$

4. Proof of Theorem 1.5(i)

The proof of Theorem 1.5(i) follows along the same lines as the proof of Theorem 1.3. We will use the same notation as in the previous section. The derivation of (7) is very similar except in $\mathbb{Z}$, or in $\mathbb{Z}_N$ with N odd, there are fewer 3-term a.p.'s in A. Regardless, (7) still holds under the assumption that $A\subset[N]$ is a B_3^+-set, or $A\subset\mathbb{Z}_N$ is a B_3^+-set and N odd.

Next we prove a lemma that corresponds to Lemma 3.2.

Lemma 4.1. *If $x\in T_i^1\cap T_j^1$ for distinct i and j, then either $s_i=s_j=2$, or if $s_j>2$, then $s_i=2$, $s_j=3$, and $|T_i^1\cap T_j^1|\geq 3$.*

Proof. The proof of this lemma is exactly the same as the proof of Lemma 3.2 up until the point where we write the equation $2z=2u$. In $\mathbb{Z}$ (or $\mathbb{Z}_N$ with N odd), this implies $z=u$ which is a contradiction since the elements x,b_1^i,y,z,u,v are all distinct. This allows us to conclude that $T_i^1\cap T_j^1=\emptyset$ for any $i\neq j$ with $s_i\geq 3$ and $s_j\geq 3$.

The assertion $|T_i^1\cap T_j^1|\geq 3$ can be verified with some easy computations. Alternatively, one can just ignore $a_3^i=u$ and $b_3^i=v$ in Figure 1 to see $|T_i^1\cap T_j^1|\geq 3$. □

Corollary 4.2. *If $m+1\leq i<j\leq M$, then $T_i^1\cap T_j^1=\emptyset$.*

Proof. If $x \in T_i \cap T_j$ with $i \neq j$, then by Lemma 4.1, one of s_i or s_j must be equal to 2. □

The next lemma has no corresponding lemma from the previous section. It will be used to estimate $\sum_{c \in A} f(c)$.

Lemma 4.3. *If $A \subset [N]$ is a B_3^+-set or if $A \subset \mathbb{Z}_N$ is a B_3^+-set and N is odd, then for any $a \in A$, the number of distinct $i \in \{1, 2, \ldots, m\}$ such that $a \in T_i^1$ is at most $\frac{|A|}{2}$.*

Proof. To make the notation simpler, we suppose $a \in T_i^1$ for $1 \leq i \leq k$ and we will show $k \leq \frac{|A|}{2}$. The case when $a \in T_{i_1}^1 \cap \cdots \cap T_{i_k}^1$ for some sequence $1 \leq i_1 < \cdots < i_k \leq m$ is the same. For this lemma we deviate from the notation $S_i^2 = \{\{a_1^i, b_1^i\}, \ldots \{a_{s_i}^i, b_{s_i}^i\}\}$. Write $S_i^2 = \{\{a, a_i\}, \{b_i, c_i\}\}$ and $a + a_i = b_i + c_i$ where $1 \leq i \leq k$, and for fixed i, the elements a, a_i, b_i, and c_i are all distinct. Observe $a_1, \ldots, a_k$ are all distinct since the sums $a + a_i$ are all distinct. For $1 \leq i \leq k$, $a = b_i + c_i - a_i$. Therefore,

$$b_i + c_i + a_j = b_j + c_j + a_i$$

for any $1 \leq i, j \leq k$. These two sums must intersect and they cannot intersect at a_j or a_i, unless $i = j$, so for $2 \leq j \leq k$,

$$\{b_1, c_1\} \cap \{b_j, c_j\} \neq \emptyset.$$

Let $2 \leq j \leq l$ be the indices for which the sums intersect at b_1. Let $l + 1 \leq j \leq k$ be the indices for which the sums intersect at c_1. Let $b = b_1$ and $c = c_1$. We have the k equations

$$\begin{aligned}
a + a_1 &= b + c, \\
a + a_2 &= b + c_2, \\
&\vdots \\
a + a_l &= b + c_l, \\
a + a_{l+1} &= b_{l+1} + c, \\
&\vdots \\
a + a_k &= b_k + c.
\end{aligned}$$

We will show that $a_1, \ldots, a_k, c_1, \ldots, c_l, b_{l+1}, \ldots, b_k$ are all distinct which implies $2k \leq |A|$.

Suppose $a_i = b_j$ for some $2 \leq i \leq l$ and $l+1 \leq j \leq k$. Then $a+b_j = a+a_i = b+c_i$, but $a = b_j + c - a_j$. Therefore, $b + c_i = a + b_j = 2b_j + c - a_j$ which implies $2b_j + c = b + c_i + a_j$. The elements a_j, b_j, and c are all distinct so these sums cannot intersect at a_j. Similarly they cannot intersect at c. The only remaining possibility is $b_j = c_i$, but then $a_i = b_j = c_i$, which is a contradiction. We conclude that a_i and b_j are distinct for $2 \leq i \leq l$ and $l+1 \leq j \leq k$. A similar argument shows that a_j and c_i are distinct for $l+1 \leq j \leq k$ and $2 \leq i \leq l$.

Suppose now that $a_i = c_{i'}$ for some $2 \leq i \neq i' \leq l$. Then $b + c_i = a + a_i = a + c_{i'} = a + (a + a_{i'} - b)$, so that $2b + c_i = 2a + a_{i'}$. Since $2 \leq i' \leq l$, these sums cannot intersect at b and they cannot intersect at a. If $c_i = a_{i'}$, then $a = b$ which is impossible. The equation $2b + c_i = 2a + a_{i'}$ contradicts the B_3^+ property. Note that $2b = 2a$ need not imply $a = b$ if $A \subset \mathbb{Z}_N$ with N even. We conclude that $a_i \neq c_{i'}$ for each $2 \leq i \neq i' \leq l$. Similarly, $a_j \neq b_{j'}$ for $l+1 \leq j \neq j' \leq k$.

The previous two paragraphs imply

$$\{a_1, a_2, \ldots, a_k\} \cap \{c_2, c_3, \ldots, c_l, b_{l+1}, b_{l+2}, \ldots, b_k\} = \emptyset.$$

To finish the proof we show $\{c_2, c_3, \ldots, c_l\} \cap \{b_{l+1}, b_{l+2}, \ldots, b_k\} = \emptyset$. Suppose $c_i = b_j$ for some $2 \leq i \leq l$ and $l+1 \leq j \leq k$. Then

$$a + a_i = b + c_i = b + b_j = b + (a + a_j - c) = b + a + a_j - (a + a_1 - b) = a_j + 2b - a_1$$

which implies $a + a_i + a_1 = a_j + 2b$. Since $i < l + 1 \leq j$, these sums cannot intersect at a_j. They cannot intersect at b either since a, a_i, b, and c_i are all distinct whenever $1 \leq i \leq l$. This is a contradiction. Therefore, $c_i \neq b_j$ for all $2 \leq i \leq l$ and $l+1 \leq j \leq k$. □

Lemma 4.4. *If $A \subset [N]$ is a B_3^+-set, then*

$$\sum_{c \in A} f(c) \leq \frac{|A|^2}{2} + 4|A|.$$

Proof. Again we write f as a sum of the simpler functions g_1 and g_2. Recall that for $c \in A$,

$$g_1(c) = \# \left\{ (\{x, z\}, y) \in A^{(2)} \times A : c = x - y + z, c \neq y, \{x, z\} \cap \{y\} = \emptyset \right\},$$

and

$$g_2(c) = \# \left\{ (\{x, z\}, y) \in A^{(2)} \times A : c = x - y + z, c = y, \{x, z\} \cap \{y\} = \emptyset \right\}.$$

For each $c \in A$, $f(c) = g_1(c) + g_2(c)$. The sum $\sum_{c \in A} g_2(c)$ is exactly the number of nontrivial 3-term a.p.'s in A. By Lemma 3.1, this is at most $4|A|$.

If $c \notin T_1^1 \cup \cdots \cup T_M^1$, then the equation $c + y = x + z$ with c, y, x, and z all distinct has no solutions in A so $g_1(c) = 0$. Assume $c \in T_1^1 \cup \cdots \cup T_M^1$.

`Case 1:` $c \notin T_1^1 \cup \cdots \cup T_m^1$.

By Corollary 4.2, there is a unique j with $c \in T_j^1$ and $m+1 \leq j \leq M$. For such a j we have $|S_j^2| \leq \frac{|A|}{2}$ by Corollary 4.2. There is a unique pair in S_j^2 that contains c so y is determined. There are at most $\frac{|A|}{2}$ choices for the pair $\{x,z\} \in S_j^2 \backslash \{c,y\}$ so $g_1(c) \leq \frac{|A|}{2}$.

Case 2: $c \in T_1^1 \cup \cdots \cup T_m^1$.

First assume $c \notin T_{m+1}^1 \cup \cdots \cup T_M^1$. A solution to $c+y=x+z$ with c,y,x, and z all distinct corresponds to a choice of an S_i^2 with $1 \leq i \leq m$ and $c \in T_i^1$. By Lemma 4.3, c is in at most $\frac{|A|}{2}$ T_i^1's and so $g_1(c) \leq \frac{|A|}{2}$.

Lastly suppose $c \in T_{m+1}^1 \cup \cdots \cup T_M^1$. There is a unique j with $c \in T_j^1$ and $m+1 \leq j \leq M$. Furthermore, for this j we have $|T_j^1| = 6$ by Lemma 4.1. If $c \in T_i^1$ with $1 \leq i \leq m$ then, again by Lemma 4.1, $|T_i^1 \cap T_j^1| \geq 3$. There are $\binom{6}{3}$ 3-subsets of T_j^1 and given such a 3-subset, there are $\binom{3}{1}$ ways to pair up an element in the 3-subset with c in S_i^2. This implies c is in at most $3\binom{6}{3}$ S_i^2's with $1 \leq i \leq m$, so $g_1(c) \leq 2 + 3\binom{6}{3} \leq \frac{|A|}{2}$. The 2 comes from choosing one of the two pairs in $S_j^2 \backslash \{c,y\}$. □

The rest of the proof of Theorem 1.5(i) is almost identical to that of Theorem 1.3. If $\sum_{c \in A} f(c) = \delta |A|^2$, then by (7) and (9),

$$\sum f(n)^2 \leq |A|^3 \left(\frac{1+5\delta}{2} \right) + O(|A|^2).$$

We use the same version of the Cauchy-Schwarz inequality to get

$$\frac{\binom{|A|}{2}^2 (|A|-2)^2}{3N} + \delta^2 |A|^3 \frac{\left(1 - \frac{C}{\delta |A|}\right)}{1 - \frac{|A|}{3N}} \leq |A|^3 \left(\frac{1+5\delta}{2} \right) + O(|A|^2). \tag{12}$$

If $\delta = 0$, then

$$\frac{\binom{|A|}{2}^2 (|A|-2)^2}{3N} \leq \frac{|A|^3}{2} + O(|A|^2)$$

which implies $|A| \leq (1+o(1))(6N)^{1/3}$. Assume $\delta > 0$. Then (12) simplifies to

$$|A| \leq (1+o(1))(6 + 30\delta - 12\delta^2)^{1/3} N^{1/3}.$$

By Lemma 4.4, $0 \leq \delta \leq \frac{1}{2} + \frac{3}{|A|}$. The maximum occurs when $\delta = \frac{1}{2} + \frac{3}{|A|}$ and we get

$$|A| \leq (1+o(1))(18N)^{1/3}.$$

If we were working in $\mathbb{Z}_N$ with N odd, then in (12) the $3N$ can be replaced by N. Some simple calculations show that we get Theorem 1.3 in the odd case. We actually obtain the upper bound $|A| \leq (1+o(1))(6N)^{1/3}$ when $A \subset \mathbb{Z}_N$ is a B_3^+-set and N is odd.

5. Proof of Theorem 1.5(ii)

Let $A \subset [N]$ be a B_4^+-set. For $n \in [-2N, 2N]$, define

$$\begin{aligned} f(n) = \#\{(\{a_1, a_2\}, \{b_1, b_2\}) \quad &\in \quad A^{(2)} \times A^{(2)} : a_1 + a_2 - b_1 - b_2 = n, \\ &\qquad \{a_1, a_2\} \cap \{b_1, b_2\} = \emptyset\}. \end{aligned}$$

Recall that $A^{(2)} = \{\{x, y\} : x, y \in A, x \neq y\}$.

Lemma 5.1. *If $A \subset [N]$ is a B_4^+-set, then A is a B_2-set.*

Proof. Suppose $a + b = c + d$ with $a, b, c, d \in A$. If $\{a, b\} \cap \{c, d\} = \emptyset$, then the equation $2(a + b) = 2(c + d)$ contradicts the B_4^+ property so $\{a, b\} \cap \{c, d\} \neq \emptyset$. Since $a + b = c + d$ and $\{a, b\} \cap \{c, d\} \neq \emptyset$, we have $\{a, b\} = \{c, d\}$. □

Lemma 5.2. *If $A \subset [N]$ is a B_4^+-set, then for any integer n, $f(n) \leq 2|A|$.*

Proof. Suppose $f(n) \geq 1$. Fix a tuple $(\{a_1, a_2\}, \{b_1, b_2\})$ counted by $f(n)$. Let $(\{c_1, c_2\}, \{d_1, d_2\})$ be another tuple counted by $f(n)$, not necessarily different from $(\{a_1, a_2\}, \{b_1, b_2\})$. Then $a_1 + a_2 - b_1 - b_2 = c_1 + c_2 - d_1 - d_2$ so

$$a_1 + a_2 + d_1 + d_2 = c_1 + c_2 + b_1 + b_2. \tag{13}$$

By the B_4^+ property, $\{a_1, a_2, d_1, d_2\} \cap \{c_1, c_2, b_1, b_2\} \neq \emptyset$. In order for this intersection to be non-empty, it must be the case that $\{a_1, a_2\} \cap \{c_1, c_2\} \neq \emptyset$ or $\{b_1, b_2\} \cap \{d_1, d_2\} \neq \emptyset$.

`Case 1:` $\{a_1, a_2\} \cap \{c_1, c_2\} \neq \emptyset$.

Assume $a_1 = c_1$. There are at most $|A|$ choices for c_2 so we fix one. The equality $a_1 = c_1$ and (13) imply

$$d_1 + d_2 = b_1 + b_2 + c_2 - a_2. \tag{14}$$

The right hand side of (14) is determined. By Lemma 5.1, there is at most one pair $\{d_1, d_2\}$ such that (14) holds.

`Case 2:` $\{a_1, a_2\} \cap \{c_1, c_2\} = \emptyset$ and $\{b_1, b_2\} \cap \{d_1, d_2\} \neq \emptyset$.

Again there is no loss in assuming $b_1 = d_1$. There are at most $|A|$ choices for d_2 so fix one. The equality $b_1 = d_1$ and (13) imply

$$c_1 + c_2 = a_1 + a_2 - b_2 + d_2. \tag{15}$$

The right hand side of (15) is determined and there is at most one pair $\{c_1, c_2\}$ satisfying (15) as before.

Putting the two possibilities together we get at most $2|A|$ solutions $(\{c_1, c_2\}, \{d_1, d_2\})$. We have also accounted for the solution $(\{a_1, a_2\}, \{b_1, b_2\})$ in our count so $f(n) \leq 2|A|$. □

Lemma 5.3. *If $A \subset [N]$ is a B_4^+-set, then*

$$\sum f(n)(f(n)-1) \leq 2|A| \sum_{n \in A-A} f(n). \tag{16}$$

Proof. The left hand side of (16) counts the number of ordered tuples

$$((\{a_1,a_2\},\{b_1,b_2\}),(\{c_1,c_2\},\{d_1,d_2\}))$$

such that $(\{a_1,a_2\},\{b_1,b_2\}) \neq (\{c_1,c_2\},\{d_1,d_2\})$, and both tuples are counted by $f(n)$. Equation (13) holds for these tuples. As before we consider two cases.

`Case 1:` $\{a_1,a_2\} \cap \{c_1,c_2\} \neq \emptyset$.

Assume $a_1 = c_1$ so that $a_2 - c_2 = b_1 + b_2 - d_1 - d_2$.

If $\{b_1,b_2\} \cap \{d_1,d_2\} \neq \emptyset$, say $b_1 = d_1$, then $a_2 - c_2 = b_2 - d_2$. We can rewrite this equation as $a_2 + d_2 = b_2 + c_2$ so that $\{a_2,d_2\} = \{b_2,c_2\}$. Since $\{a_1,a_2\} \cap \{b_1,b_2\} = \emptyset$, it must be the case that $a_2 = c_2$ and $d_2 = b_2$. This contradicts the fact that the tuples are distinct. We conclude $\{b_1,b_2\} \cap \{d_1,d_2\} = \emptyset$.

There are $|A|$ choices for the element $a_1 = c_1$ and we fix one. Since $a_2 - c_2 = b_1 + b_2 - d_1 - d_2$ and $\{b_1,b_2\} \cap \{d_1,d_2\} = \emptyset$, there are $f(a_2 - c_2)$ ways to choose $\{b_1,b_2\}$ and $\{d_1,d_2\}$. Also observe that each $n \in A - A$ with $n \neq 0$ has a unique representation as $n = a_2 - c_2$ with $a_2, c_2 \in A$. This follows from the fact that A is a B_2-set.

`Case 2:` $\{a_1,a_2\} \cap \{c_1,c_2\} = \emptyset$ and $\{b_1,b_2\} \cap \{d_1,d_2\} \neq \emptyset$.

The argument in this case is essentially the same as that of Case 1.

Putting the two cases together proves the lemma.

□

Observe $\sum f(n) = \binom{|A|}{2}\binom{|A|-2}{2}$. Using Cauchy-Schwarz, and Lemmas 5.3 and 5.2,

$$\begin{aligned}
\frac{\left(\binom{|A|}{2}\binom{|A|-2}{2}\right)^2}{4N} &\leq \sum f(n)^2 \leq \binom{|A|}{2}\binom{|A|-2}{2} + 2|A| \sum_{n \in A-A} f(n) \\
&\leq \frac{|A|^4}{4} + 2|A||A-A| \cdot 2|A| \\
&\leq \frac{|A|^4}{4} + 4|A|^4 = \frac{17|A|^4}{4}.
\end{aligned}$$

After rearranging we get

$$|A| \leq (1+o(1))(16 \cdot 17N)^{1/4} = (1+o(1))(272N)^{1/4}.$$

6. Proof of Theorem 1.6

Lemma 6.1. *Let A be a B_k^+-set with $k \geq 4$. If $k = 2l$, then there is a subset $A' \subset A$ such that A' is a B_l^+-set and $|A'| \geq |A| - 2l$. If $k = 2l+1$, then there is a subset $A' \subset A$ such that $|A'| \geq |A| - 2k$ and A' is either a B_l^+-set or a B_{l+1}^+-set.*

Proof. Suppose $k = 2l$ with $l \geq 2$. If A is not a B_l^+-set, then there is a set of $2l$ (not necessarily distinct) elements $a_1, \dots, a_{2l} \in A$, such that

$$a_1 + \cdots + a_l = a_{l+1} + \cdots + a_{2l}$$

and $\{a_1, \dots, a_l\} \cap \{a_{l+1}, \dots, a_{2l}\} = \emptyset$. Let $A' = A \backslash \{a_1, a_2, \dots, a_{2l}\}$. If A' is not a B_l^+-set, then there is another set of $2l$ elements of A', say $b_1, \dots, b_{2l}$, such that

$$b_1 + \cdots + b_l = b_{l+1} + \cdots + b_{2l}$$

and $\{b_1, \dots, b_l\} \cap \{b_{l+1}, \dots, b_{2l}\} = \emptyset$. Adding these two equations together gives

$$a_1 + \cdots + a_l + b_1 + \cdots + b_l = a_{l+1} + \cdots + a_{2l} + b_{l+1} + \cdots + b_{2l}$$

with $\{a_1, \dots, a_l, b_1, \dots, b_l\} \cap \{a_{l+1}, \dots, a_{2l}, b_{l+1}, \dots, b_{2l}\} = \emptyset$. This is a contradiction.

The case when $k = 2l + 1 \geq 5$ can be handled in a similar way.

□

It is easy to modify the proof of Lemma 6.1 to obtain a version for B_k^*-sets.

Lemma 6.2. *Let A be a B_k^*-set with $k \geq 4$. If $k = 2l$, then there is a subset $A' \subset A$ such that A' is a B_l^*-set and $|A'| \geq |A| - 2l$. If $k = 2l+1$, then there is a subset $A' \subset A$ such that $|A'| \geq |A| - 2k$ and A' is either a B_l^*-set or a B_{l+1}^*-set.*

For $A \subset [N]$ and $j \geq 2$, let

$$\sigma_j(n) = \# \left\{ (a_1, \dots, a_j) \in A^j : a_1 + \cdots + a_j = n \right\}.$$

Let $e(x) = e^{2\pi i x}$ and $f(t) = \displaystyle\sum_{a \in A} e(at)$. For any $j \geq 1$, $f(t)^j = \sum \sigma_j(n) e(nt)$ so by Parseval's Identity, $\sum \sigma_j(n)^2 = \int_0^1 |f(t)|^{2j} dt$. The next lemma is (5.9) of [16].

Lemma 6.3. *If $A \subset [N]$ is a B_k^*-set, then*

$$\sum \sigma_k(n)^2 \leq (1 + o(1)) k^2 |A| \sum \sigma_{k-1}(n)^2. \tag{17}$$

In [16], Ruzsa estimates the right hand side of (17) using Hölder's Inequality and shows

$$\sum \sigma_{k-1}(n)^2 \leq \left(\sum \sigma_k(n) \right)^{\frac{k-2}{k-1}} |A|^{\frac{1}{k-1}}.$$

Our next lemma uses Hölder's Inequality in a different way.

Lemma 6.4. *Let $A \subset [N]$ be a B_k^*-set. If $k \geq 4$ is even, then*

$$\sum \sigma_k(n)^2 \leq (1+o(1))k^k|A|^{k/2} \sum \sigma_{k/2}(n)^2.$$

If $k = 2l+1 \geq 5$, then

$$\sum \sigma_k(n)^2 \leq (1+o(1)) \max \left\{ k^{k+1}|A|^{l+1} \sum \sigma_l(n)^2, k^{k-1}|A|^l \sum \sigma_{l+1}(n)^2 \right\}.$$

Proof. First assume that $k = 2l \geq 4$. By Lemma 6.2, we may assume that A is a B_l^*-set. Otherwise, we pass to a subset of A that is a B_l^* set and has at least $|A| - 2k$ elements. Applying Hölder's Inequality with $p = \frac{k}{k-2}$ and $q = \frac{k}{2}$, we get

$$\begin{aligned} \sum \sigma_{k-1}(n)^2 &= \int_0^1 |f(t)|^{2(k-1)} dt = \int_0^1 |f(t)|^{\frac{2k}{p}} |f(t)|^{\frac{2l}{q}} dt \\ &\leq \left(\int_0^1 |f(t)|^{2k} dt \right)^{1/p} \left(\int_0^1 |f(t)|^{2l} dt \right)^{1/q} \\ &= \left(\sum \sigma_k(n)^2 \right)^{(k-2)/k} \left(\sum \sigma_l(n)^2 \right)^{2/k}. \end{aligned}$$

Substituting this estimate into (17) and solving for $\sum \sigma_k(n)^2$ gives the first part of the lemma.

Now assume $k = 2l+1 \geq 5$. Again by Lemma 6.2, we can assume that A is either a B_l^*-set or a B_{l+1}^*-set.

Suppose A is a B_l^*-set. Applying Hölder's Inequality with $p = \frac{k+1}{k-1}$ and $q = \frac{k+1}{2}$, we get

$$\sum \sigma_{k-1}(n)^2 \leq \left(\sum \sigma_k(n)^2 \right)^{\frac{k-1}{k+1}} \left(\sum \sigma_l(n)^2 \right)^{\frac{2}{k+1}}.$$

This inequality and (17) imply

$$\sum \sigma_k(n)^2 \leq (1+o(1))k^{k+1}|A|^{\frac{k+1}{2}} \sum \sigma_l(n)^2.$$

If A is a B_{l+1}^*-set instead, then apply Hölder's Inequality with $p = \frac{l}{l-1}$ and $q = \frac{1}{l}$ and proceed as above. It is in this step that we must assume $k = 2l+1 \geq 5$ otherwise if $k = 3$, then $l = 1$ and p is not defined. □

For $k \geq 2$ let c_k^+ be the smallest constant such that for any B_k^+-set A,

$$\sum \sigma_k(n)^2 \leq (1+o(1))c_k^+|A|^k.$$

Define c_k^* similarly. The techniques of [16] can be used to show that $c_k^* \leq k^{2k}$ so c_k^+ and c_k^* are well defined. Observe that for any $k \geq 2$, $c_k^+ \leq c_k^*$. Using Lemma 6.4, it is not difficult to show that for even $k \geq 4$,

$$c_k^+ \leq k^k c_{k/2}^+ \text{ and } c_k^* \leq k^k c_{k/2}^*, \tag{18}$$

Similarly, one can show that for odd $k = 2l + 1 \geq 5$,

$$c_k^+ \leq \max\left\{k^{k+1}c_l^+, k^{k-1}c_{l+1}^+\right\} \text{ and } c_k^* \leq \max\left\{k^{k+1}c_l^*, k^{k-1}c_{l+1}^*\right\}. \tag{19}$$

Lemma 6.5. *Let $A \subset [N]$ be a B_k^+-set. If $k \geq 4$ is even, then*

$$|A| \leq (1 + o(1))\left(k^{k+1}c_{k/2}^+ N\right)^{1/k}. \tag{20}$$

If $k = 2l + 1 \geq 5$, then

$$|A| \leq (1 + o(1))\left(k^k \cdot \max\{k^2 c_l^+, c_{l+1}^+\}N\right)^{1/k}. \tag{21}$$

The same inequalities hold under the assumption that $A \subset [N]$ is a B_k^*-set provided that the c_k^+'s are replaced with c_k^*'s.

Proof. By Cauchy-Schwarz,

$$\frac{|A|^{2k}}{kN} \leq \sum \sigma_k(n)^2 \tag{22}$$

for any $k \geq 2$.

First suppose $k \geq 4$ is even. By (22) and Lemma 6.4,

$$\frac{|A|^{2k}}{kN} \leq \sum \sigma_k(n)^2 \leq (1 + o(1))k^k|A|^{k/2}\sum \sigma_{k/2}(n)^2 \leq (1 + o(1))k^k c_{k/2}^+|A|^k.$$

Solving this inequality for $|A|$ proves (20).

Now suppose $k = 2l + 1 \geq 5$. By (22) and Lemma 6.4,

$$\begin{aligned}\frac{|A|^{2k}}{kN} &\leq \sum \sigma_k(n)^2 \leq (1 + o(1))\max\left\{k^{k+1}c_l^+|A|^k, k^{k-1}c_{l+1}^+|A|^k\right\}\\ &= (1 + o(1))|A|^k k^{k-1}\max\{k^2 c_l^+, c_{l+1}^+\}.\end{aligned}$$

□

Lemma 6.5 shows that we can obtain upper bounds on B_k^+-sets and B_k^*-sets recursively. To start the recursion we need estimates on c_2^+, c_2^*, c_3^+, and c_3^*.

Lemma 6.6. *If A is a B_2^*-set, then*

$$\sum \sigma_2(n)^2 \leq 2|A|^2 + 32|A|$$

and therefore $c_2^* \leq 2$.

Proof. Let $\delta(n) = \#\{(a_1, a_2) \in A^2 : a_1 - a_2 = n\}$. Observe $\sum \sigma_2(n)^2 = \sum \delta(n)^2$. In [16] (see Theorem 4.7) it is shown that $\delta(n) \leq 1$ for any $n \neq 0$, and $\delta(n) = 2$ for at most $8|A|$ integers n. We conclude

$$\sum \delta(n)^2 \leq \delta(0)^2 + 8|A| \cdot 4 + |A - A| \leq 2|A|^2 + 32|A|.$$

□

Lemma 6.7. *If $A \subset [N]$ is a B_3^+-set, then*

$$\sum \sigma_3(n)^2 \leq (1+o(1))18|A|^3$$

and therefore $c_3^+ \leq 18$.

Proof. Let $A \subset [N]$ be a B_3^+-set and let

$$r_2(n) = \#\left\{\{a,b\} \in A^{(2)} : a+b=n\right\}.$$

Define $2 \cdot A := \{2a : a \in A\}$. For $n \in 2 \cdot A$, $\sigma_2(n) = 2r_2(n)+1$ and $\sigma_2(n) = 2r_2(n)$ otherwise. The sum $\sum_{n \in 2 \cdot A} r_2(n)$ counts the number of 3-term a.p.'s in A so by Lemma 3.1,

$$\begin{aligned}\sum \sigma_2(n)^2 &= 4\sum r_2(n)^2 + 4\sum_{n\in 2\cdot A} r_2(n) + |2\cdot A| \\ &\leq 4\sum r_2(n)^2 + 4\cdot 4|A| + |A| = 4\sum r_2(n)^2 + 17|A|.\end{aligned}$$

Using the notation and results of Section 3, and the inequality $x^2 \leq 2x(x-1)$ for $x \geq 2$, we have

$$\sum r_2(n)^2 = \sum_{i=1}^{M} |S_i^2|^2 \leq 2\sum_{i=1}^{M} |S_i^2|(|S_i^2|-1) \leq \sum_{c\in A} f(c) \leq \frac{|A|^2}{2} + 3|A|.$$

Combining this inequality with (17) gives

$$\begin{aligned}\sum \sigma_3(n)^2 &\leq (1+o(1))3^2|A|\sum \sigma_2(n)^2 \leq (1+o(1))9|A|(4\sum r_2(n)^2 + 17|A|) \\ &\leq (1+o(1))9|A|(2|A|^2 + 29|A|) \leq (1+o(1))(18|A|^3 + 261|A|^2).\end{aligned}$$

□

Lemma 6.8. *If $A \subset [N]$ is a B_3^*-set, then*

$$\sum \sigma_3(n)^2 \leq (1+o(1))54|A|^3$$

and therefore $c_3^* \leq 54$.

Proof. Let $A \subset [N]$ be a B_3^*-set. The idea of the proof is motivated by the same arguments that we used for B_3^+-sets. For $d \in A+A$, let

$$P^2(d) = \{\{a,b\} \in A^{(2)} : a+b=d\}.$$

Define $m_0 = 0$ and for $1 \leq j \leq 4$, let $d_{m_{j-1}+1}, d_{m_{j-1}+2}, \ldots, d_{m_j}$ be the integers for which $|P^2(d_i)| = j$. Let $d_{m_4+1}, d_{m_4+2}, \ldots, d_M$ be the integers for which $|P^2(d_i)| \geq 5$. Write P_i^2 for $P^2(d_i)$, p_i for $|P_i^2|$, and for $1 \leq i \leq M$, let

$$Q_i^1 = \{a : a \in \{a,b\} \text{ for some } \{a,b\} \in P_i^2\}.$$

We will use the notation $P_i^2 = \{\{a_1^i, b_1^i\}, \dots, \{a_{p_i}^i, b_{p_i}^i\}\}$. A difference between the P_i^2's of this section and the S_i^2's of earlier sections is that we allow for a P_i^2 to contain only one pair.

Lemma 6.9. *If $x \in Q_i^1 \cap Q_j^1$ for some $i \neq j$ where $p_i \geq 3$ and $p_j \geq 3$, then $p_i + p_j \leq 7$.*

Proof. Without loss of generality, assume $x = a_1^i$ and $x = a_1^j$ where

$P_i^2 = \{\{a_1^i, b_1^i\}, \{a_2^i, b_2^i\}, \dots, \{a_{p_i}^i, b_{p_i}^i\}\}$ and $P_j^2 = \{\{a_1^j, b_1^j\}, \{a_2^j, b_2^j\}, \dots, \{a_{p_j}^j, b_{p_j}^j\}\}$.

For $2 \leq l \leq p_i$ we have $d_i = x + b_1^i = a_l^i + b_l^i$. Similarly, for $2 \leq k \leq p_j$ we have $d_j = x + b_1^j = a_k^j + b_k^j$. Then $a_l^i + b_l^i - b_1^i = x = a_k^j + b_k^j - b_1^j$, so

$$a_l^i + b_l^i + b_1^j = a_k^j + b_k^j + b_1^i \text{ for any } 2 \leq l \leq p_i \text{ and } 2 \leq k \leq p_j. \tag{23}$$

If $b_1^j \in T_i^1$, then there is no loss in assuming $b_1^j \in \{a_2^i, b_2^i\}$. The same assumption may be made with i and j interchanged. This means that for $l \geq 3$, b_1^j is not a term in the sum $a_l^i + b_l^i$ and for $k \geq 3$, b_1^i is not a term in the sum $a_k^j + b_k^j$. The B_3^* property and (23) imply

$$|\{a_l^i, b_l^i\} \cap \{a_k^j, b_k^j\}| = 1 \text{ for any } 3 \leq l \leq p_i \text{ and } 3 \leq k \leq p_j. \tag{24}$$

In particular, $\{a_3^i, b_3^i\} \cap \{a_3^j, b_3^j\} \neq \emptyset$ and $\{a_3^i, b_3^i\} \cap \{a_4^j, b_4^j\} \neq \emptyset$ so that $p_j \leq 4$. Here we are using the fact that any element of A can occur at most once in the list $a_1^i, b_1^i, \dots, a_{p_i}^i, b_{p_i}^i$. By symmetry, $p_i \leq 4$.

If $p_i = p_j = 4$, then by (24), $\{a_3^i, b_3^i, a_4^i, b_4^i\} = \{a_3^j, b_3^j, a_4^j, b_4^j\}$ but then $2d_i = a_3^i + b_3^i + a_4^i + b_4^i = 2d_j$ implying $d_i = d_j$, a contradiction. □

Corollary 6.10. *If $p_i \geq 4$ and $p_j \geq 4$ with $i \neq j$, then $Q_i^1 \cap Q_j^1 = \emptyset$.*

Using the definition of the P_i^2's, we can write

$$\sum r_2(n)^2 = \sum_{i=1}^{M} |P_i^2|^2 = m_1 + 4(m_2 - m_1) + 9(m_3 - m_2) + 16(m_4 - m_3) + \sum_{i=m_4+1}^{M} |P_i^2|^2.$$

If $p_i = p_j = 4$ for some $i \neq j$, then $Q_i^1 \cap Q_j^1 = \emptyset$ by Corollary 6.10 so $m_4 - m_3 \leq \frac{|A|}{8}$. For $1 \leq i \leq 3$, let $\delta_i |A|^2 = m_i - m_{i-1}$. Then

$$\sum r_2(n)^2 \leq |A|^2(\delta_1 + 4\delta_2 + 9\delta_3) + \sum_{i=m_4+1}^{M} |P_i^2|^2 + 2|A|. \tag{25}$$

Define a graph H with vertex set $Q_{m_2+1}^1 \cup \cdots \cup Q_{m_3}^1$ and edge set $P_{m_2+1}^2 \cup \cdots \cup P_{m_3}^2$. Let $n = |V(H)|$. The graph H has $3(m_3 - m_2) = 3\delta_3 |A|^2$ edges so $3\delta_3 |A|^2 \leq \frac{n}{2}$ which can be rewritten as

$$\sqrt{6\delta_3}|A| \leq |Q_{m_2+1}^1 \cup \cdots \cup Q_{m_3}^1|. \tag{26}$$

For any i and j with $m_2+1 \le i \le m_3$ and $m_4+1 \le j \le M$, $Q_i^1 \cap Q_j^1 = \emptyset$ by Lemma 6.9. Thus (26) implies

$$\sum_{i=m_4+1}^{M} |P_i^2| = \frac{1}{2}\sum_{i=m_4+1}^{M} |Q_i^1| = \frac{1}{2}|Q_{m_4+1}^1 \cup \cdots \cup Q_M^1| \le \frac{1}{2}(1-\sqrt{6\delta_3})|A|.$$

We conclude $\sum_{i=m_4+1}^{M} |P_i^2|^2 \le \left(\frac{1-\sqrt{6\delta_3}}{2}\right)^2 |A|^2$. This estimate and (25) give

$$\sum r_2(n)^2 \le |A|^2\left(\delta_1+4\delta_2+9\delta_3+\frac{1}{4}(1-\sqrt{6\delta_3})^2\right)+2|A|. \tag{27}$$

Each pair $\{a,b\} \in A^{(2)}$ is in at most one P_i^2 so

$$|A|^2(\delta_1+2\delta_2+3\delta_3) = m_1+2(m_2-m_1)+3(m_3-m_2) \le \binom{|A|}{2} \le \frac{|A|^2}{2}.$$

The maximum of $\delta_1+4\delta_2+9\delta_3+\frac{1}{4}(1-\sqrt{6\delta_3})^2$ subject to the conditions $\delta_1+2\delta_2+3\delta_3 \le \frac{1}{2}$, $\delta_1 \ge 0$, $\delta_2 \ge 0$, and $\delta_3 \ge 0$ is $\frac{3}{2}$, achieved when $\delta_1=\delta_2=0$ and $\delta_3=\frac{1}{6}$. By (27),

$$\sum r_2(n)^2 \le \frac{3|A|^2}{2}+2|A|. \tag{28}$$

An immediate consequence is that

$$\sum_{n\in 2\cdot A} r_2(n) = \sum \mathbb{1}_{2\cdot A}(n) r_2(n) \le |A|^{1/2}\left(\sum r_2(n)^2\right)^{1/2} \le 2|A|^{3/2}. \tag{29}$$

Next we proceed as in Lemma 6.7. Using (29) and (28),

$$\begin{aligned}\sum \sigma_2(n)^2 &= 4\sum r_2(n)^2 + 4\sum_{n\in 2\cdot A} r_2(n) + |2\cdot A|\\ &\le 6|A|^2+8|A|^{3/2}+9|A|.\end{aligned}$$

By Lemma 6.3,

$$\sum \sigma_3(n)^2 \le (1+o(1))3^2|A|\sum \sigma_2(n)^2.$$

The previous two estimates show that $\sum \sigma_3(n)^2 \le (1+o(1))54|A|^3$. This completes the proof of Lemma 6.8. □

Corollary 6.11. *If $A \subset [N]$ is a B_3^*-set, then*

$$|A| \le (1+o(1))(162N)^{1/3}.$$

Proof. Let $A \subset [N]$ be a B_3^*-set. By Cauchy-Schwarz and Lemma 6.8,

$$\frac{|A|^6}{3N} \le \sum \sigma_3(n)^2 \le (1+o(1))54|A|^3.$$

□

So far we have shown $c_2^+ \le c_2^* \le 2$, $c_3^+ \le 18$, and $c_3^* \le 54$. Now we describe our method for obtaining upper bounds on $F_k^+(N)$ and $F_k^*(N)$. Assume we have upper bounds on $c_2^+, c_3^+, \dots, c_{k-1}^+$. Lemma 6.5 gives an upper bound on $|A|$ in terms of $c_{k/2}^+$ when k is even, and in terms of c_l^+ and c_{l+1}^+ when $k = 2l+1 \ge 5$. An upper bound on c_k^+ is obtained from (18) and (19). We can also apply this method to B_k^*-sets. The upper bounds we obtain are given in Table 1 below. They have been rounded up to the nearest tenth. They hold for large enough N without error terms.

k	U.b. of [16] on F_k^*	Our U.b. on F_k^*	Our U.b. on F_k^+
3	$6.3N^{1/3}$	$5.5N^{1/3}$	$2.7N^{1/3}$
4	$11.4N^{1/4}$	$6.8N^{1/4}$	$4.1N^{1/4}$
5	$18.2N^{1/5}$	$11.2N^{1/5}$	$11N^{1/5}$
6	$26.8N^{1/6}$	$15.8N^{1/6}$	$13.1N^{1/6}$
7	$37.2N^{1/7}$	$21.6N^{1/7}$	$18.5N^{1/7}$
8	$49.4N^{1/8}$	$22.7N^{1/8}$	$22.7N^{1/8}$

Table 1: Upper bounds on B_k^+-sets and B_k^*-sets.

We conclude this section with our proof of the second statement of Theorem 1.6. Recall that (18) states $c_k^* \le k^k c_{k/2}^*$ for any even $k \ge 4$. For $k = 2l+1 \ge 5$, (19) gives $c_k^* \le k^{k+1} \max\{c_l^*, c_{l+1}^*\}$. For $x \ge 0$, let $\lceil x \rceil$ be the smallest integer greater than or equal to x. Let $\lfloor x \rfloor$ be the greatest integer less than or equal to x. For $k \ge 0$, define $\phi_1(k) = \lceil \frac{k}{2} \rceil$ and $\phi_i(k) := \phi_1(\phi_{i-1}(k))$ for $i \ge 2$. A simple induction argument can be used to show that for all $i \ge 1$, $\phi_i(k) \le k2^{-i} + \sum_{t=0}^{i-1} 2^{-t}$. The conclusion is that for every $i \ge 1$, $\phi_i(k) \le k2^{-i} + 2$. For any $k \ge 5$,

$$c_k^* \le k^{k+1} \prod_{i=1}^{\lfloor \log_2 k \rfloor} \phi_i(k)^{\phi_i(k)+1} \le k^{k+1} \prod_{i=1}^{\lfloor \log_2 k \rfloor} \left(k2^{-i}+2\right)^{k2^{-i}+3}.$$

Taking k-th roots,

$$\begin{aligned}
(c_k^*)^{1/k} &\le k^{1+1/k} \prod_{i=1}^{\lfloor \log_2 k \rfloor} (k2^{-i}+2)^{2^{-i}+3/k} \\
&\le k^{1+1/k} \left(\frac{k}{2}+2\right)^{\frac{3\log_2 k}{k}} \prod_{i=1}^{\lfloor \log_2 k \rfloor} (k2^{-i}+2)^{2^{-i}} \\
&\le k^{1+1/k} k^{\frac{3\log_2 k}{k}} k^{\sum_{i=1}^{\lfloor \log_2 k \rfloor} 2^{-i}} \prod_{i=1}^{\lfloor \log_2 k \rfloor} \left(2^{-i}+\frac{2}{k}\right)^{2^{-i}} \\
&\le k^2 k^{\frac{4\log_2 k}{k}} \prod_{i=1}^{\lfloor \log_2 k \rfloor} \left(2^{-i}+\frac{2}{k}\right)^{2^{-i}}.
\end{aligned}$$

We claim the sequence $(c_k^*)^{1/k}$ is bounded above by a function $F(k)$ that tends to $\frac{k^2}{4}$ as $k \to \infty$. With this in mind, we rewrite the previous inequality as

$$\frac{4(c_k^*)^{1/k}}{k^2} \leq 4k^{\frac{4\log_2 k}{k}} \prod_{i=1}^{\lfloor \log_2 k \rfloor} \left(2^{-i} + \frac{2}{k}\right)^{2^{-i}}. \tag{30}$$

It is easy to check $k^{\frac{4\log_2 k}{k}} \to 1$ as $k \to \infty$. Using $\sum_{n=0}^{\infty} nx^{n-1} = \frac{1}{(1-x)^2}$ from elementary calculus, we obtain

$$\prod_{i=1}^{\lfloor \log_2 k \rfloor} (2^{-i})^{2^{-i}} = \left(\frac{1}{2}\right)^{\sum_{i=1}^{\lfloor \log_2 k \rfloor} i2^{-i}} \to \frac{1}{4}$$

as $k \to \infty$. Using the inequality $1 + x \leq e^x$ for $x \geq 0$, we have

$$\begin{aligned} 1 \quad &\leq \quad \frac{\prod_{i=1}^{\lfloor \log_2 k \rfloor} (2^{-i} + 2/k)^{2^{-i}}}{\prod_{i=1}^{\lfloor \log_2 k \rfloor} (2^{-i})^{2^{-i}}} = \prod_{i=1}^{\lfloor \log_2 k \rfloor} \left(1 + \frac{2^{i+1}}{k}\right)^{2^{-i}} \\ &\leq \quad \prod_{i=1}^{\lfloor \log_2 k \rfloor} e^{2^{i+1}/k} \leq e^{\frac{1}{k}\sum_{i=2}^{\lfloor \log_2 k \rfloor} 2^i} \leq e^{1/k}. \end{aligned}$$

As $k \to \infty$, $e^{1/k} \to 1$ so

$$\prod_{i=1}^{\lfloor \log_2 k \rfloor} \left(2^{-i} + \frac{2}{k}\right)^{2^{-i}} \to \frac{1}{4}.$$

This shows that the right hand side of (30) tends to 1 as $k \to \infty$ which proves the claim.

Given $\epsilon > 0$, we can choose k large enough so that $k^{1/k}(c_k^*)^{1/k} \leq (1+\epsilon)\frac{k^2}{4}$. The theorem now follows from the definition of c_k^* and the estimate $\frac{|A|^{2k}}{kN} \leq \sum \sigma_k(n)^2$.

7. Proof of Theorem 1.8

Lemma 7.1. *If $A \subset G$ is a non-abelian B_k-set and $B \subset H$ is a non-abelian B_k^+-set, then $A \times B$ is a non-abelian B_k^+-set in $G \times H$.*

Proof. Suppose $a_1, \ldots, a_k, a_1', \ldots, a_k' \in A$, $b_1, \ldots, b_k, b_1', \ldots, b_k' \in B$ and

$$(a_1, b_1) \cdots (a_k, b_k) = (a_1', b_1') \cdots (a_k', b_k').$$

Then $a_1 \cdots a_k = a_1' \cdots a_k'$ and $b_1 \cdots b_k = b_1' \cdots b_k'$ so that $a_i = a_i'$ for every i and $b_j = b_j'$ for some j. Thus, $(a_j, b_j) = (a_j', b_j')$. □

Let $\mathbb{F}_4 = \{0, 1, a, b\}$ be the finite field with four elements. Let

$$H = \left\{ \begin{pmatrix} x & y \\ 0 & x^{-1} \end{pmatrix} : x \in \mathbb{F}_4^*, y \in \mathbb{F}_4 \right\}.$$

Then H is a group under matrix multiplication and $|H| = 12$. Let

$$\alpha = \begin{pmatrix} a & 1 \\ 0 & b \end{pmatrix} \quad \text{and} \quad \beta = \begin{pmatrix} a & a \\ 0 & b \end{pmatrix}.$$

Simple computations show that α and β satisfy $\alpha^3 = \beta^3 = \text{id}$ and $\alpha^2\beta = \beta^2\alpha$.

Lemma 7.2. *The set $\{\alpha, \beta\}$ is a B_4^+-set in H.*

Proof. Suppose there is a solution to the equation $x_1x_2x_3x_4 = y_1y_2y_3y_4$ with $x_i \neq y_i$ for $1 \leq i \leq 4$, and $x_i, y_j \in \{\alpha, \beta\}$ for all i, j. Without loss of generality, assume $x_1 = \alpha$ and $y_1 = \beta$. There are eight cases which we can deal with using the relations $\alpha^3 = \beta^3 = \text{id}$ and $\alpha^2\beta = \beta^2\alpha$. Instead of considering each individually, we handle several cases at the same time.

`Case 1:` $\alpha^4 = \beta^4$ or $\alpha^3\beta = \beta^3\alpha$ or $\alpha\beta^3 = \beta\alpha^3$.

If any of these equations hold, then the relation $\alpha^3 = \beta^3 = \text{id}$ implies $\alpha = \beta$, a contradiction.

`Case 2:` $\alpha^2\beta\alpha = \beta^2\alpha\beta$ or $\alpha^2\beta^2 = \beta^2\alpha^2$.

If either of these equations hold, then the relation $\alpha^2\beta = \beta^2\alpha$ implies $\alpha = \beta$.

`Case 3:` $\alpha\beta\alpha^2 = \beta\alpha\beta^2$.

Multiplying the equation on the right by β and using $\beta^3 = \text{id}$, we get $\alpha\beta\alpha^2\beta = \beta\alpha$. On the other hand, $\alpha\beta\alpha^2\beta = \alpha\beta^3\alpha = \alpha^2$ so combining the two equations we get $\beta\alpha = \alpha^2$. This implies $\alpha = \beta$, a contradiction.

`Case 4:` $\alpha\beta\alpha\beta = \beta\alpha\beta\alpha$.

Multiply the equation on the left by β^2 to get $\beta^2\alpha\beta\alpha\beta = \alpha\beta\alpha$. This can be rewritten as $\alpha^2\beta^2\alpha\beta = \alpha\beta\alpha$ using $\beta^2\alpha = \alpha^2\beta$. Replace $\beta^2\alpha$ with $\alpha^2\beta$ on the left hand side of $\alpha^2\beta^2\alpha\beta = \alpha\beta\alpha$ and cancel α to get $\beta^2 = \beta\alpha$. This implies $\beta = \alpha$.

`Case 5:` $\alpha\beta^2\alpha = \beta\alpha^2\beta$.

Using the relation $\beta^2\alpha = \alpha^2\beta$, we can rewrite this equation as $\alpha^3\beta = \beta^3\alpha$ which implies $\alpha = \beta$ since $\alpha^3 = \beta^3 = \text{id}$. □

The set $\{\alpha, \beta\}$ is not a non-abelian B_4-set since $\alpha^2\beta\beta = \beta^2\alpha\beta$. The next theorem is a special case of a result of Odlyzko and Smith. We will use it in our construction.

Theorem 7.3. (Odlyzko, Smith, [15]) *For each prime p with $p-1$ divisible by 4, there is a non-abelian group G of order $4(p^4-1)$ and a non-abelian B_4-set $A \subset G$ with*

$$|A| = \frac{1}{4}(p-1).$$

Armed with Lemma 7.1, Lemma 7.2, and Theorem 7.3, we now prove Theorem 1.8.

Let p be any prime with $p-1$ divisible by 4. By Theorem 7.3, there is a group G_1 of order $4(p^4-1)$ and a non-abelian B_4-set $A_1 \subset G_1$ with $|A_1| = \frac{1}{4}(p-1)$. Define the group G to be the product group $G = G_1 \times H$. Let $A = A_1 \times \{\alpha, \beta\}$. Clearly $|G| = 12 \cdot 4(p^4-1)$, $|A| = \frac{1}{2}(p-1)$, and by Lemma 7.1, A is a non-abelian B_4^+-set in G.

Acknowledgement The author would like to thank Jacques Verstraëte and the anonymous referee for helpful comments.

References

[1] R. C. Baker, G. Harman, J. Pintz, *The difference between consecutive primes II*, Proc. London Math. Soc. **83** (3) (2001), 532-562.

[2] R. C. Bose, S. Chowla, *Theorems in the additive theory of numbers*, Comment. Math. Helv. **37** (1962/1963), 141-147.

[3] S. Chen, *On the size of finite Sidon sequences*, Proc. Amer. Math. Soc. Vol. 121 **2** (1994), 353-356.

[4] J. Cilleruelo, *New upper bound for finite B_h Sequences*, Adv. Math. **159** (2001), 1-17.

[5] J. Cilleruelo, *Sidon sets in $\mathbb{N}^d$*, J. Combin. Theory Ser. A **117** (2010), 857-871.

[6] P. Erdős, *Some problems in additive number theory*, Amer. Math. Monthly **77** (1970), 619-621.

[7] P. Erdős, *A survey of problems in combinatorial number theory*, Annals of Discrete Mathematics **6** (1980), 89-115.

[8] P. Erdős, *Some problems and results on combinatorial number theory*, Graph theory and its applications, Ann. New York Acad. Sci. 576 (1989), 132-145.

[9] P. Erdős, P. Turán, *On a problem of Sidon in additive number theory, and on some related results*, J. London Math. Soc. 16 (1941).

[10] B. Green, *The number of squares and $B_h[g]$ sets*, Acta Arith. **100** (2001), 365-390.

[11] H. Halberstam, K. F. Roth, *Sequences*, Vol. I, Clarendon Press, Oxford, 1966.

[12] X. Jia, *On finite Sidon sequences*, J. Number Theory **44** (1993), 84-92.

[13] B. Lindström, *An inequality for B_2-sequences*, J. Combin. Theory **6** (1969), 211-212.

[14] K. O'Bryant, *A complete annotated bibliography of work related to Sidon sequences*, Electron. J. Combin. **DS 11** (2004).

[15] A.M. Odlyzko, W.D. Smith, *Nonabelian sets with distinct k-sums*, Discrete Math. 146 (1995), 169-177.

[16] I. Ruzsa, *Solving a linear equation in a set of integers I*, Acta Arith. **65** 3 (1993), 259-282.

[17] J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. 43 (1938), 377-385.