

THE NUMBER OF ADDITIVE TRIPLES IN SUBSETS OF ABELIAN GROUPS

WOJCIECH SAMOTIJ AND BENNY SUDAKOV

ABSTRACT. A set of elements of a finite abelian group is called sum-free if it contains no Schur triple, i.e., no triple of elements x, y, z with $x + y = z$. The study of how large the largest sum-free subset of a given abelian group is had started more than thirty years before it was finally resolved by Green and Ruzsa a decade ago. We address the following more general question. Suppose that a set A of elements of an abelian group G has cardinality a . How many Schur triples must A contain? Moreover, which sets of a elements of G have the smallest number of Schur triples? In this paper, we answer these questions for various groups G and ranges of a .

1. INTRODUCTION

A typical problem in extremal combinatorics has the following form: What is the largest size of a structure which does not contain any forbidden configurations? Once this extremal value is known, it is very natural to ask how many forbidden configurations one is guaranteed to find in every structure of a certain size that is larger than the extremal value. There are many results of this kind. Most notably, there is a very large body of work on the problem of determining the smallest number of k -vertex cliques in a graph with n vertices and m edges, attributed to Erdős and Rademacher; see [13, 15, 17, 26, 29, 31, 32]. In extremal set theory, there is an extension of the celebrated Sperner's theorem, where one asks for the minimum number of chains in a family of subsets of $\{1, \dots, n\}$ with more than $\binom{n}{\lfloor n/2 \rfloor}$ members; see [8, 11, 16, 22]. Another example is a recent work in [7], motivated by the classical theorem of Erdős, Ko, and Rado. It studies how many disjoint pairs must appear in a k -uniform set system of a certain size.

Analogous questions have been studied in the context of Ramsey theory. Once we know the maximum size of a structure which does not contain some unavoidable pattern, we may ask how many such patterns are bound to appear in every structure whose size exceeds this maximum. For example, a well-known problem posed by Erdős is to determine the minimum number of monochromatic k -vertex cliques in a 2-colouring of the edges of K_n ; see, e.g., [6, 19, 35]. This may be viewed as an extension of Ramsey's theorem. Another example is an extension of the famous theorem of Erdős and Szekeres [18], which states that any sequence of more than k^2 numbers contains a monotone (that is, monotonically increasing or monotonically decreasing) subsequence of length $k + 1$. Here, one may ask what the minimum number of monotone subsequences of length $k + 1$ contained in a sequence of n numbers is; see [2, 27, 34].

Date: November 3, 2015.

Research supported in part by: (WS) Institute for Mathematical Research (FIM), ETH Zürich and Israel Science Foundation grant 1147/14; (BS) SNSF grant 200021-149111.

In this paper, we consider a similar Erdős–Rademacher-type generalisation of a classical problem in additive combinatorics. Recall that a *Schur triple* in an abelian group G is a triple of elements x, y, z of G , not necessarily distinct, satisfying $x + y = z$. A set A of elements of G is called *sum-free* if it contains no Schur triples. The study of sum-free sets in abelian groups goes back to the work of Erdős [14]. In 1965, he proved that any set of n non-zero integers contains a sum-free subset of size at least $n/3$ and asked whether the fraction $1/3$ could be improved. Despite significant interest in this problem, the matching upper bound was proved only recently by Eberhard, Green, and Manners [12], who constructed a sequence of sets showing that Erdős’ result is asymptotically tight.

A related question, which is also more than forty years old, is to determine how large the largest sum-free subset of a given finite abelian group is. The following two simple observations provide strong lower bounds for this quantity. First, note that by considering the ‘middle’ interval of an appropriate length, one sees that the cyclic group \mathbb{Z}_m contains a sum-free subset with $\lfloor \frac{m+1}{3} \rfloor$ elements. Second, if G is an abelian group, H is a subgroup of G , $\pi: G \rightarrow G/H$ is the canonical homomorphism, and B is a sum-free subset of G/H , then the set $\pi^{-1}(B) \subseteq G$ is also sum-free. The appearance of the expression $\lfloor \frac{m+1}{3} \rfloor$ above explains why the following nomenclature is commonly used in this context.

Definition 1.1. Let G be an abelian group of order n . We say that G is of: (i) *type I* if n has a prime factor p satisfying $p \equiv 2 \pmod{3}$; (ii) *type II* if n has no such prime factor but 3 divides n ; (iii) *type III* otherwise, i.e., if each prime factor p of n satisfies $p \equiv 1 \pmod{3}$.

Using the above two observations, one can check that if G is an abelian group with n elements, then the largest sum-free set in G has size at least

- $(\frac{1}{3} + \frac{1}{3p})n$ if G is of type I and p is the smallest prime factor of n with $p \equiv 2 \pmod{3}$,
- $\frac{n}{3}$ if G is of type II,
- $(\frac{1}{3} - \frac{1}{3m})n$ if G is of type III and m is the largest order of an element in G .

It turns out that these simple lower bounds are actually tight, but the task of showing that this is indeed the case took more than thirty five years. This was first proved by Diananda and Yap [10] for groups of types I and II and in [33, 36, 37] for some groups of type III. Only many years later, Green and Ruzsa [20] established it for all groups.

Motivated by these results on the size of the largest sum-free sets, we consider the following more general questions.

Problem 1.2. *Let A be an a -element subset of a finite abelian group G . How many Schur triples must A contain? Which sets of a elements of G have the minimum number of Schur triples?*

In this paper, we answer these questions for various groups G and ranges of a . Some estimates for the number of Schur triples in large subsets of abelian groups appeared already in [20, 25], but to the best of our knowledge, we are the first to explicitly consider these questions and obtain exact results.

Given a subset A of an abelian group, we shall denote by $\text{ST}(A)$ the number of Schur triples contained in A . More precisely, we let

$$\text{ST}(A) = |\{(x, y, z) \in A^3: x + y = z\}|,$$

so that if $x + y = z$ and $x \neq y$, then we consider (x, y, z) and (y, x, z) as different triples.

Our first result concerns cyclic groups of prime order. In this case, we derive a complete answer to both parts of Problem 1.2 from a classical result of Pollard [30] and its stability counterpart due to Nazarewicz, O'Brien, O'Neill, and Staples [28].

Theorem 1.3. *Suppose that p is an odd prime and order the elements of the p -element cyclic group \mathbb{Z}_p as x_1, \dots, x_p , where*

$$x_{2i} = \frac{p-1}{2} + i \quad \text{and} \quad x_{2i+1} = \frac{p-1}{2} - i.$$

For every $A \subseteq \mathbb{Z}_p$ with a elements,

$$\text{ST}(A) \geq \text{ST}(\{x_1, \dots, x_a\}) = \max \left\{ 0, \left\lfloor \frac{3a-p}{2} \right\rfloor \left\lceil \frac{3a-p}{2} \right\rceil \right\}. \quad (1)$$

Moreover, if $\text{ST}(\{x_1, \dots, x_a\}) > 0$, then equality holds above only if $A = \varphi(\{x_1, \dots, x_a\})$ for some $\varphi \in \text{Aut}(\mathbb{Z}_p)$, that is, if $A = \xi \cdot \{x_1, \dots, x_a\}$ for some nonzero $\xi \in \mathbb{Z}_p$.

Our second result concerns groups of type I. We shall say that a group G is of type $I(p)$ if p is the smallest prime factor of $|G|$ among those satisfying $p \equiv 2 \pmod{3}$. Suppose that G is of type $I(p)$. It was proved by Diananda and Yap [10] that the largest sum-free set in G has $(\frac{1}{3} + \frac{1}{3p})|G|$ elements. We shall generalise this result by answering both questions in Problem 1.2 under the assumption that $|A| \leq (\frac{1}{3} + \frac{1+\delta}{3p})|G|$ for some absolute constant δ .

Theorem 1.4. *There exists a positive constant δ such that the following holds. Suppose that p is a prime satisfying $p \equiv 2 \pmod{3}$ and let G be a group of type $I(p)$. If $0 \leq t \leq \delta|G|/p$, then for every $A \subseteq G$ with $(\frac{1}{3} + \frac{1}{3p})|G| + t$ elements,*

$$\text{ST}(A) \geq \frac{3t|G|}{p} + \mathbb{1}[p \neq 2] \cdot t^2. \quad (2)$$

Our proof of Theorem 1.4 will also yield the following characterisation of all sets achieving equality in (2). Let p and G be as in the statement of the theorem and suppose that $p = 3k+2$. Let $\varphi: G \rightarrow \mathbb{Z}_p$ be an arbitrary surjective homomorphism, let $A_0 = \varphi^{-1}(\{k+1, \dots, 2k+1\})$, and note that A_0 is a sum-free set with $(\frac{1}{3} + \frac{1}{3p})|G|$ elements. Given a t with $0 \leq t \leq 2|G|/(7p)$, let A'_t be an arbitrary sum-free subset of $\varphi^{-1}(\{k\})$ with t elements¹ and let $A_t = A_0 \cup A'_t$. Then $\text{ST}(A_t) = \frac{3t|G|}{p} + \mathbb{1}[p \neq 2] \cdot t^2$. Moreover, every set $A \subseteq G$ that achieves equality in (2) is of this form.

Our third result is a complete solution to Problem 1.2 for the ‘hypercube’, i.e., the group \mathbb{Z}_2^n . Here, there is a very elegant way of describing a sequence of sets minimising the number of Schur triples among all subsets of \mathbb{Z}_2^n of the same cardinality.

¹Such a set exists as if $k > 0$, then the set $\varphi^{-1}(\{k\})$ itself is sum-free and has $|G|/p$ elements; if $k = 0$, then $\varphi^{-1}(\{k\})$ is a subgroup of G with index 2 and every nontrivial abelian group H contains a sum-free set with at least $2|H|/7$ elements.

Theorem 1.5. *Let n be a positive integer. For each $a \in \{1, \dots, 2^n - 1\}$, let A_a be the set of vectors in $\{0, 1\}^n$ that are binary representations of the numbers $2^n - 1, \dots, 2^n - a$. Let k be the unique integer satisfying $2^n - 2^k \leq a < 2^n - 2^{k-1}$. Then for every $A \subseteq \mathbb{Z}_2^n$ with a elements,*

$$\text{ST}(A) \geq \text{ST}(A_a) = (3a + 2^k - 2^{n+1})(2^n - 2^k). \quad (3)$$

Our proof of Theorem 1.5 will also yield the following characterisation of sets achieving equality in (3). Let a , k , and n be as in the statement of the theorem. For every a -element $A \subseteq \mathbb{Z}_2^n$ satisfying $\text{ST}(A) = \text{ST}(A_a)$, the following holds. There is a subgroup $K < \mathbb{Z}_2^n$ with 2^k elements such that $\mathbb{Z}_2^n \setminus K \subseteq A$ and $A \cap K$ is sum-free. One may check that each A of this form satisfies $\text{ST}(A) = \text{ST}(A_a)$. As clearly each such K is isomorphic to \mathbb{Z}_2^k , one may say a little more about the structure of $A \cap K$ for certain ranges of a . In particular, it was proved in [4, 5] that each sum-free subset of \mathbb{Z}_2^k with more than $5 \cdot 2^{k-4}$ elements is contained in some maximum-size sum-free subset of \mathbb{Z}_2^k , i.e., the odd coset of some subgroup of index two. (Smaller sum-free sets of \mathbb{Z}_2^k do not admit such an elegant structural description. For example, if $k \geq 4$, then the set $\{e_1, e_2, e_3, e_4, e_1 + e_2 + e_3 + e_4\} + \text{span}\{e_5, \dots, e_k\}$, where e_1, \dots, e_k is a basis of \mathbb{Z}_2^k as a vector space over \mathbb{Z}_2 , is sum-free, has $5 \cdot 2^{k-4}$ elements, and is not contained in any maximum-size sum-free subset of \mathbb{Z}_2^k .)

Finally, we consider Problem 1.2 for groups of type II, i.e., groups whose order is divisible by three. As it turns out, here the answer is much less ‘uniform’ among all groups in this class. To be more precise, given an abelian group G , let f_G be the function defined by

$$f_G(a) = \min\{\text{ST}(A) : A \subseteq G \text{ and } |A| = a\} \quad (4)$$

and let a_G be the largest cardinality of a sum-free set in G , i.e., $a_G = \max\{a : f_G(a) = 0\}$. On the one hand, if $G = \mathbb{Z}_3^n$, then f_G ‘behaves’ similarly as in the case when G is of type I(p) for some fixed prime p , namely, $f_G(a+1) - f_G(a)$ is of order $|G|$ for all a in an interval of length $\Omega(|G|/p)$ starting at a_G . On the other hand, if $G = \mathbb{Z}_3 \times \mathbb{Z}_p$, where p is a prime with $p \equiv 1 \pmod{3}$, then $f_G(a)$ is merely of order $(a - a_G)^2$ for all $a \geq a_G$. (As G is of type II, $a_G = p$.)

Theorem 1.6. *There exists a positive constant δ such that the following holds. Let n be a positive integer and suppose that $0 \leq t \leq \delta 3^{n-1}$. Then for every $A \subseteq \mathbb{Z}_3^n$ with $3^{n-1} + t$ elements,*

$$\text{ST}(A) \geq 3^{n-1}t + t^2. \quad (5)$$

Moreover, (5) holds with equality when A is the union of $\{x \in \mathbb{Z}_3^n : x_1 = 1\}$ and an arbitrary t -element sum-free subset of $\{x \in \mathbb{Z}_3^n : x_1 = 2\}$.

Proposition 1.7. *Let p be a prime. Then for every $a \in \{p+1, \dots, 3p\}$, there exists an a -element set $A \subseteq \mathbb{Z}_3 \times \mathbb{Z}_p$ with*

$$\text{ST}(A) \leq 21(a - p)^2.$$

Last but not least, the argument we use in our proof of Theorem 1.4 can be adapted to show that every sufficiently large set A of elements of an arbitrary finite abelian group that is nearly sum-free must necessarily contain a genuinely sum-free set B such that $|A \setminus B|$ is very small.

Proposition 1.8. *Suppose that $\varepsilon > 0$ and let G be a finite abelian group. If some $A \subseteq G$ has at least $(\frac{1}{3} + \varepsilon)|G|$ elements and $\text{ST}(A) \leq \varepsilon^2|G|^2/2$, then A contains a sum-free set B with $|A \setminus B| \leq \varepsilon|G|$.*

A slightly weaker version of this useful fact was first proved by Green and Ruzsa [20] (their statement has a stronger requirement on the number of Schur triples). Observe that our assumption on $\text{ST}(A)$ in the above proposition is optimal up to an absolute multiplicative constant. Indeed, Proposition 1.7 implies that for every $\varepsilon \in (0, \frac{2}{3})$, there are a group G with no sum-free set larger than $|G|/3$ and a set A with $\text{ST}(A) \leq 22\varepsilon^2|G|^2$ and more than $(\frac{1}{3} + \varepsilon)|G|$ elements (and hence no sum-free subset B with $|A \setminus B| \leq \varepsilon|G|$).

2. CYCLIC GROUPS OF PRIME ORDER

In this section, we prove Theorem 1.3. The first part of the theorem, a lower bound on the number of Schur triples in an arbitrary set of a elements of \mathbb{Z}_p is a fairly straightforward consequence of the following result of Pollard [30], which generalises the well-known theorem of Cauchy [3] and Davenport [9].

Theorem 2.1. *Let p be a prime and let $A, B \subseteq \mathbb{Z}_p$. For an integer r , denote by N_r the number of elements of \mathbb{Z}_p which are expressible in at least r ways as $x + y$ with $x \in A$ and $y \in B$. Then for every r with $1 \leq r \leq \min\{|A|, |B|\}$,*

$$N_1 + \dots + N_r \geq r \cdot \min\{p, |A| + |B| - r\}. \quad (6)$$

The second part of Theorem 1.3 will be derived from the following stability counterpart of Pollard's result due to Nazarewicz, O'Brien, O'Neill, and Staples [28].

Theorem 2.2. *Let p be a prime, let $A, B \subseteq \mathbb{Z}_p$, and let r be an integer with $1 \leq r \leq \min\{|A|, |B|\}$. Then equality holds in (6) of Theorem 2.1 if and only if at least one of the following conditions holds:*

- (1) $\min\{|A|, |B|\} = r$,
- (2) $|A| + |B| \geq p + r$,
- (3) $|A| = |B| = r + 1$ and $B = x - A$ for some $x \in \mathbb{Z}_p$, or
- (4) A and B are arithmetic progressions with the same common difference.

Proof of Theorem 1.3. Fix an arbitrary set A of a elements of \mathbb{Z}_p . Given an $r \geq 1$, let S_r denote the set of all elements in \mathbb{Z}_p that are expressible in at least r ways as $x + y$ with $x, y \in A$. Recall that $N_r = |S_r|$. Moreover, let $N'_r = |S_r \cap A|$. Clearly, $N'_r \geq N_r + a - p$ and hence by Theorem 2.1, for any $R \geq 0$,

$$\text{ST}(A) = \sum_{r \geq 1} N'_r \geq \sum_{r=1}^R N'_r \geq \sum_{r=1}^R N_r + R(a - p) \geq R \cdot (\min\{p, 2a - R\} + a - p). \quad (7)$$

Let $R = \max\{0, \lceil \frac{3a-p}{2} \rceil\}$. Note that $a \leq p$ implies that $2a \leq p + \frac{3a-p}{2}$ and consequently

$$2a \leq p + \left\lceil \frac{3a-p}{2} \right\rceil \leq p + R.$$

In particular, the minimum in the right-hand side of (7) is equal to $2a - R$ and therefore,

$$\text{ST}(A) \geq R(3a - R - p) = \max \left\{ 0, \left\lceil \frac{3a - p}{2} \right\rceil \left\lfloor \frac{3a - p}{2} \right\rfloor \right\}. \quad (8)$$

In order to derive (1), it now suffices to prove that $\text{ST}(\{x_1, \dots, x_a\})$ is equal to the right-hand side of (8). Assume first that a is even. Then $\{x_1, \dots, x_a\} = \left\{ \frac{p+1-a}{2}, \dots, \frac{p+a-1}{2} \right\}$. A Schur triple (x, y, z) in $\{x_1, \dots, x_a\}$ may be of one of the following two types: either $x + y = z$ or $x + y = z + p$, where the equalities hold in \mathbb{Z} . Let $R' = \max \left\{ 0, \frac{3a-p-1}{2} \right\}$. It is easy to check that $\frac{p+1-a}{2}$ plays the role of x in exactly R' triples of the first type, as y ranges over the R' smallest elements of the interval $\left\{ \frac{p+1-a}{2}, \dots, \frac{p+a-1}{2} \right\}$. More generally, the element $\frac{p+1-a}{2} + i$ plays the role of x in exactly $R' - i$ triples of the first type. By symmetry, $\frac{p+a-1}{2}$ plays the role of x in exactly R' triples of the second type, as y ranges over the R' largest elements of the interval $\left\{ \frac{p+1-a}{2}, \dots, \frac{p+a-1}{2} \right\}$, and more generally, $\frac{p+a-1}{2} - i$ plays the role of x in exactly $R' - i$ triples of the second type. It follows that

$$\begin{aligned} \text{ST}(\{x_1, \dots, x_a\}) &= 2 \cdot \sum_{r=1}^{R'} r = 2 \cdot \binom{R'+1}{2} = (R'+1)R' \\ &= \max \left\{ 0, \frac{3a-p+1}{2} \cdot \frac{3a-p-1}{2} \right\} = \max \left\{ 0, \left\lceil \frac{3a-p}{2} \right\rceil \left\lfloor \frac{3a-p}{2} \right\rfloor \right\}. \end{aligned}$$

When a is odd, then $\{x_1, \dots, x_a\} = \left\{ \frac{p-a}{2}, \dots, \frac{p+a-2}{2} \right\}$ and, letting $R'' = \max \left\{ 0, \frac{3a-p}{2} \right\}$, analogous considerations yield

$$\text{ST}(\{x_1, \dots, x_a\}) = \binom{R''+1}{2} + \binom{R''}{2} = (R'')^2 = \max \left\{ 0, \left\lceil \frac{3a-p}{2} \right\rceil \left\lfloor \frac{3a-p}{2} \right\rfloor \right\}.$$

We now characterise all sets A with a elements that achieve the lower bound in (1) whenever the right-hand side of (1) is nonzero, that is, when $a > \lfloor \frac{p+1}{3} \rfloor$. To this end, let us analyse when all inequalities in (7) hold with equality. In particular, equality must hold in (6) of Theorem 2.1 invoked with $A \leftarrow A$, $B \leftarrow A$, and $r \leftarrow R$, where $R = \max \left\{ 0, \left\lceil \frac{3a-p}{2} \right\rceil \right\} \geq 1$ and the inequality follows from our assumption that $a > \lfloor \frac{p+1}{3} \rfloor$. Theorem 2.2 tells us that (7) can hold with equality only if one of the following conditions is satisfied:

- (1) $a = R$,
- (2) $2a \geq p + R$,
- (3) $a = R + 1$ and $A = x - A$ for some $x \in \mathbb{Z}_p$,
- (4) A is an arithmetic progression.

Now observe that

$$\begin{aligned} a = R = \left\lceil a - \frac{p-a}{2} \right\rceil &\iff \left\lfloor \frac{p-a}{2} \right\rfloor = 0 \iff a \geq p-1, \\ 2a \geq p + R &\iff a \geq \left\lceil \frac{a+p}{2} \right\rceil \iff a \geq p, \\ a = R + 1 &\iff \left\lfloor \frac{p-a}{2} \right\rfloor = 1 \iff a \in \{p-3, p-2\}, \end{aligned}$$

and every set $A \subseteq \mathbb{Z}_p$ that satisfies either $|A| \geq p - 2$ or $|A| = p - 3$ and $A = x - A$ for some $x \in \mathbb{Z}_p$ is an arithmetic progression (to see this, note that A^c is an arithmetic progression), we deduce that each of (i)–(iv) implies that A must be an arithmetic progression with common difference d . We may assume that $d = 1$ as otherwise we may replace A by its automorphic image $d^{-1} \cdot A$. Hence, $A = \{x, \dots, x + a - 1\}$ for some $x \in \mathbb{Z}_p$.

In order for (7) to hold with equality, it must also be that

$$|A \cap S_R| = N'_R = N_R + a - p = |S_R| - |A^c|,$$

that is, $A^c \subseteq S_R$. One easily checks that $S_R = \{2x + R - 1, \dots, 2x + 2a - R - 1\}$ and hence $|S_R| = 2(a - R) + 1 = 2\lfloor \frac{p-a}{2} \rfloor + 1$. If a is even, then $|A^c| = p - a = |S_R|$ and hence $x + a = 2x + R - 1$, which yields $x = \frac{p-a+1}{2}$, that is,

$$A = \left\{ \frac{p+1}{2} - \frac{a}{2}, \dots, \frac{p-1}{2} + \frac{a}{2} \right\} = \{x_1, \dots, x_a\}.$$

If a is odd, then $|A^c| = |S_R| - 1$ and hence either $x + a = 2x + R - 1$ or $x + a = 2x + R$, yielding $x = \frac{p-a}{2}$ or $x = \frac{p-a}{2} + 1$, that is,

$$A = \pm \left\{ \frac{p-a}{2} + 1, \dots, \frac{p+a}{2} \right\} = \pm \{x_1, \dots, x_a\}. \quad \square$$

3. GROUPS OF TYPE I

In this section, we prove Theorem 1.4. Our argument uses some ideas from [20, 25]. Actually, one may adapt the arguments of these two papers to establish Theorem 1.4 under the stronger assumption that $t \leq \delta n/p^4$ for some positive constant δ . Our main tool will be the following classical result of Kneser [23, 24]. The version stated below is [21, Theorem 3.1]. Recall that the *stabiliser* of a set A of elements of an abelian group G , denoted by $\text{Stab}(A)$, is defined by

$$\text{Stab}(A) = \{x \in G : A + x = A\}.$$

Theorem 3.1. *Let A and B be finite non-empty subsets of an Abelian group G satisfying $|A + B| \leq |A| + |B| - 1$. Then $H = \text{Stab}(A + B)$ satisfies*

$$|A + B| = |A + H| + |B + H| - |H|.$$

Proof of Theorem 1.4. Let $\delta = 1/82$ and let p , G , and t be as in the statement of the theorem. Denote the order of G by n and let A be an arbitrary set of $(\frac{1}{3} + \frac{1}{3p})n + t$ elements of G . Let $n' = n/(3p)$ and define

$$C_- = \{x \in A : |(x - A) \cap A| \geq n'\} \quad \text{and} \quad C_+ = \{x \in A : |(x + A) \cap A| \geq n'\}.$$

Using the inclusion-exclusion principle (Bonferroni's inequality) to count Schur triples $(x, y, z) \in A^3$ such that $x \in C_+$, $y \in C_+$, or $z \in C_-$ yields

$$ST(A) \geq (2|C_+| + |C_-|) \cdot n' - |C_+|^2 - 2|C_-||C_+|.$$

Therefore, if $|C_-| \geq 4t$ and $|C_+| \geq 4t$, then, passing to subsets of C_- and C_+ of size exactly $4t$, we have

$$ST(A) \geq 12tn' - 48t^2 = \frac{4tn}{p} - 48t^2 > \frac{3tn}{p} + t^2,$$

where the last inequality follows as $49t^2 \leq 49\delta tn/p < tn/p$. Hence, we may assume that either $|C_-| < 4t$ or $|C_+| < 4t$.

Given a $*$ $\in \{-, +\}$, let $B = A \setminus C_*$ and observe that $|(x * A) \cap A^c| \geq |A| - n'$ for each $x \in B$ and hence for every $x, y \in B$,

$$\begin{aligned} |(x * A) \cap (y * A)| &\geq |(x * A) \cap (y * A) \cap A^c| \geq 2(|A| - n') - (n - |A|) \\ &= 3|A| - n - 2n' = n/p + 3t - 2n' = n/(3p) + 3t \geq n/(3p). \end{aligned}$$

In other words, for every pair $x, y \in B$, there are at least $n/(3p)$ pairs $a, b \in A$ such that $x - y = a - b$.

Fix a $*$ $\in \{-, +\}$ such that $|C_*| < 4t$ and let $B = A \setminus C_*$. Using our observation above to count Schur triples $(x, y, z) \in A^3$ such that $x \in B - B$ yields

$$ST(A) \geq |(B - B) \cap A| \cdot n/(3p). \quad (9)$$

Hence, we may assume that $|(B - B) \cap A| \leq 9t + 3t^2p/n \leq 10t$, where the last inequality holds as $t \leq \delta n/p$. In particular,

$$|B - B| \leq n - |A| + 10t = 2|A| - n/p + 7t \leq 2|B| - n/p + 15t, \quad (10)$$

where the last inequality follows as $|B| = |A| - |C_*| \geq |A| - 4t$. Letting $H = \text{Stab}(B - B)$, Kneser's theorem (Theorem 3.1) implies that

$$|B - B| = 2|B + H| - |H| \geq 2|B| - |H|. \quad (11)$$

Putting (10) and (11) together yields

$$|H| \geq n/p - 15t \quad \text{and} \quad |B + H| - |B| \leq \frac{|H| - n/p + 15t}{2}. \quad (12)$$

Let $m = |G/H|$ and observe that (12) yields

$$m \leq \frac{n}{n/p - 15t} \leq \frac{p}{1 - 15\delta}. \quad (13)$$

Note also that by our assumption that $|C_*| < 4t$, we have

$$|B| > |A| - 4t = n/3 + n/(3p) - 3t \geq n/3 + (1/3 - 3\delta)n/p > n/3. \quad (14)$$

Now, let $B_H = (B + H)/H$. As $|B_H| > m/3$ by (14), we must have $|B_H| \geq \lceil \frac{m+1}{3} \rceil$. We shall now consider two cases.

CASE 1. $m \not\equiv 2 \pmod{3}$.

In this case, $|B_H| \geq \frac{m+2}{3}$ and it follows from (11) that $|B - B|/|H| = 2|B_H| - 1 \geq \frac{2m+1}{3}$. This implies that

$$|(B - B) \cap A| \geq \left(\frac{2}{3} + \frac{1}{3m}\right)n + \left(\frac{1}{3} + \frac{1}{3p}\right)n - n > \frac{n}{3p} \geq 10t,$$

contradicting our assumption, cf. (9).

CASE 2. $m \equiv 2 \pmod{3}$.

Let q be the smallest prime factor of m satisfying $q \equiv 2 \pmod{3}$; m has such a prime factor as otherwise $m \not\equiv 2 \pmod{3}$. Since m divides n and p is the smallest prime factor of

n satisfying $p \equiv 2 \pmod{3}$, we must have $q \geq p$. But $m < 2p$ by (13), so necessarily $m = q$, that is, m is a prime satisfying $m \equiv 2 \pmod{3}$ and $m \geq p$. This means that G/H is the cyclic group \mathbb{Z}_m .

We now claim that $B_H \cap (B_H - B_H) = \emptyset$. Indeed, otherwise we would have $|(B + H) \cap (B - B)| \geq |H|$ (since $B - B$ is a union of cosets of H) and, since $B \subseteq A$, by (12),

$$|(B + H) \setminus A| \leq |B + H| - |B| \leq \frac{n/m - n/p + 15t}{2} \leq 7.5t, \quad (15)$$

which in turn would yield

$$|A \cap (B - B)| \geq |H| - 7.5t = n/m - 7.5t \geq (1 - 15\delta)n/p - 7.5t > 10t,$$

contradicting our assumption, cf. (9).

Therefore, it must be that $B_H \cap (B_H - B_H) = \emptyset$, that is, $B_H \subseteq \mathbb{Z}_m$ is a sum-free set. But $|B_H| > m/3$, which means that $|B_H| = \frac{m+1}{3}$ and it follows from the results of Diananda and Yap [10] that, up to isomorphism, $B_H = \{\ell + 1, \dots, 2\ell + 1\}$, where $m = 3\ell + 2$.

Let $A_0 = B + H$ and let $\varphi: G \rightarrow \mathbb{Z}_m$ be a homomorphism that maps A_0 to $\{\ell + 1, \dots, 2\ell + 1\}$; in particular $H = \varphi^{-1}(0)$ and $B_H = \{\ell + 1, \dots, 2\ell + 1\}$. As $-\varphi$ is also such a homomorphism and $-\ell = 2\ell + 2$ in \mathbb{Z}_m , we may assume that $|A \cap \varphi^{-1}(\ell)| \geq |A \cap \varphi^{-1}(2\ell + 2)|$. It follows from (15) that $|A_0 \setminus A| \leq 7.5t$. We shall now perform a stability analysis of A and prove that (2) holds and the inequality there is strict unless $A_0 \subseteq A$, $m = p$, and $A \setminus A_0$ is a sum-free subset of $\varphi^{-1}(\{\ell\})$.

We first claim that replacing an element from $A \setminus A_0$ with an element of $A_0 \setminus A$ only decreases the number of Schur triples in A . Indeed, as A_0 is sum-free, a given element of A_0 participates only in Schur triples that contain an element of $A \setminus A_0$; clearly, the number of such triples is at most $6|A \setminus A_0|$, which is at most $51t$ as

$$|A \setminus A_0| = |A| - |A \cap A_0| = (|A_0| + t) - (|A_0| - |A_0 \setminus A|) \leq 8.5t.$$

On the other hand, for every $j \notin \{\ell + 1, \dots, 2\ell + 1\}$, there are $h, i \in \{\ell + 1, \dots, 2\ell + 1\}$ such that $h + i = j$. Therefore if $x \in A \setminus A_0$, then, letting $j = \varphi(x) \notin \{\ell + 1, \dots, 2\ell + 1\}$, the number $\text{ST}_x(A)$ of Schur triples in A that contain x satisfies

$$\begin{aligned} \text{ST}_x(A) &\geq |(x - (\varphi^{-1}(i) \cap A)) \cap (\varphi^{-1}(h) \cap A)| \geq |\varphi^{-1}(i) \cap A| + |\varphi^{-1}(h) \cap A| - |H| \\ &\geq 2(|H| - 7.5t) - |H| \geq n/m - 15t > (1 - 15\delta)n/p - 15t > 51t. \end{aligned}$$

Therefore, it suffices to prove (2), and characterise all cases of equality there, under the assumption that $A_0 \subseteq A$.

Now, note that each of ℓ and $2\ell + 2$ participates in exactly three Schur triples with two elements of $\{\ell + 1, \dots, 2\ell + 1\}$, namely: $(\ell, \ell + 1, 2\ell + 1)$, $(\ell + 1, \ell, 2\ell + 1)$, and $(2\ell + 1, 2\ell + 1, \ell)$ and $(\ell + 1, \ell + 1, 2\ell + 2)$, $(2\ell + 1, 2\ell + 2, \ell + 1)$, and $(2\ell + 2, 2\ell + 1, \ell + 1)$. On the other hand, every element of $\mathbb{Z}_m \setminus \{\ell, \dots, 2\ell + 2\}$ participates in at least four such triples. It follows that:

- (1) Every element of $\varphi^{-1}(\{\ell, 2\ell + 2\})$ forms $3n/m$ Schur triples with two elements of A_0 and at most $6|A \setminus A_0|$ additional Schur triples with two elements of A (one of which is not in A_0).

- (2) Every element of $\varphi^{-1}(\mathbb{Z}_m \setminus \{\ell, \dots, 2\ell + 2\})$ forms at least $4n/m$ Schur triples with two elements of A_0 .

Since $|A_0| = (\frac{1}{3} + \frac{1}{3m})n$, our assumption that $A_0 \subseteq A$ and (13) imply that

$$|A \setminus A_0| = \frac{n}{3p} + t - \frac{n}{3m} \leq \left(\frac{1}{3} + \delta\right) \frac{n}{p} - \frac{n}{3m} \leq \left[\frac{1}{1-15\delta} \left(\frac{1}{3} + \delta\right) - \frac{1}{3}\right] \frac{n}{m} < \frac{n}{6m}.$$

It therefore follows from (i) and (ii) that moving elements from $A \cap \varphi^{-1}(\mathbb{Z}_m \setminus \{\ell, \dots, 2\ell + 2\})$ to $\varphi^{-1}(\{\ell, 2\ell + 2\})$ only decreases $\text{ST}(A)$. Therefore, we may restrict our attention to sets A satisfying

$$\varphi^{-1}(\{\ell + 1, \dots, 2\ell + 1\}) = A_0 \subseteq A \subseteq A_0 \cup \varphi^{-1}(\{\ell, 2\ell + 2\}) = \varphi^{-1}(\{\ell, \dots, 2\ell + 2\}).$$

Observe that if $\ell > 0$, then every ordered pair of elements $(x, y) \in \varphi^{-1}(\ell)^2 \cup \varphi^{-1}(2\ell + 2)^2$ satisfying $(x, y) \in A^2$ participates in a unique Schur triple (in A) in which x precedes y , the triple $(x, y, x + y)$. On the other hand, if $\ell > 0$, then every pair $(x, y) \in \varphi^{-1}(\ell) \times \varphi^{-1}(2\ell + 2)$ satisfying $(x, y) \in A^2$ participates in four Schur triples in A : the triples $(x, y - x, y)$, $(y - x, x, y)$, $(y, x - y, x)$, and $(x - y, y, x)$. Counting separately Schur triples in A that contain two (using (i)), one (using the above observation), and no elements of A_0 yields

$$\begin{aligned} \text{ST}(A) &\geq |A \setminus A_0| \cdot \frac{3n}{m} + \mathbb{1}[m > 2] \cdot |A \setminus A_0|^2 + \text{ST}(A \setminus A_0) \\ &= \left(\frac{n}{3p} + t - \frac{n}{3m}\right) \cdot \frac{3n}{m} + \mathbb{1}[m > 2] \cdot \left(\frac{n}{3p} + t - \frac{n}{3m}\right)^2 + \text{ST}(A \setminus A_0) \\ &\geq \frac{3nt}{p} + \mathbb{1}[p > 2] \cdot t^2 + \text{ST}(A \setminus A_0), \end{aligned}$$

where the first inequality is strict unless $\ell = 0$, $A \cap \varphi^{-1}(\ell) = \emptyset$, or $A \cap \varphi^{-1}(2\ell + 2) = \emptyset$ and the last inequality is strict unless $m = p$ (recall that $p \leq m \leq 2p$). This completes the proof. \square

4. THE HYPERCUBE \mathbb{Z}_2^n

In this section, we prove Theorem 1.5. One way of obtaining lower bounds on $\text{ST}(A)$ in our proof will be using eigenvalue analysis of the *Cayley graph* of G generated by A . Recall that given an abelian group G and an $A \subseteq G \setminus \{0\}$ satisfying $A = -A$, we define \mathcal{G}_A to be the graph with vertex set G whose edges are all pairs $\{x, y\}$ such that $x - y \in A$. It follows from this definition that for every $A \subseteq G \setminus \{0\}$ with $A = -A$,

$$\text{ST}(A) = 2e(\mathcal{G}_A[A]), \tag{16}$$

where $\mathcal{G}_A[A]$ denotes the subgraph of \mathcal{G}_A induced by A . We shall derive lower bounds on $e(\mathcal{G}_A[A])$ using the following well-known result of Alon and Chung [1].

Theorem 4.1. *Let \mathcal{G} be an N -vertex D -regular graph and let λ be the smallest eigenvalue of its adjacency matrix. Then for every $U \subseteq V(\mathcal{G})$,*

$$2e(\mathcal{G}[U]) \geq \frac{D}{N}|U|^2 + \frac{\lambda}{N}|U|(N - |U|).$$

Precise eigenvalue analysis of \mathcal{G}_A will be possible in our setting due to the fact that the *characters* of any abelian group G form a basis of eigenvectors of \mathcal{G}_A for every A . Moreover, in the case $G = \mathbb{Z}_2^n$, there is a one-to-one correspondence between nontrivial characters of G and subgroups of G with index two. More precisely, for each nontrivial character $\chi \in \hat{G}$ there is a subgroup $H < G$ of index 2 such that

$$\chi(x) = \begin{cases} 1, & \text{if } x \in H, \\ -1, & \text{if } x \notin H. \end{cases}$$

In particular, the smallest eigenvalue λ of \mathcal{G}_A satisfies

$$\lambda = \min \{ |A \cap H| - |A \cap H^c| : H < G \text{ with } [G : H] = 2 \}.$$

Proof of Theorem 1.5. Let n be a positive integer, let $G = \mathbb{Z}_2^n$, and let a and k be as in the statement of the theorem. We may assume that $k \leq n - 1$ as otherwise both (3) and the characterisation of sets achieving equality are vacuous. We shall first count Schur triples in the set A_a and establish the equality in (3). Given an $x \in G$, let us denote by \bar{x} the integer with binary representation x (viewed as a $\{0, 1\}$ -vector), so that

$$\{\bar{x} : x \in A_a\} = \{2^n - 1, \dots, 2^n - a\}.$$

Fix some $x \in A_a$ and let j be the unique integer such that $2^j \leq \bar{x} < 2^{j+1}$. We claim that the number $\text{ST}_x(A_a)$ of (ordered) Schur triples containing x such that \bar{x} is the smallest element is $3(2^n - 2^{j+1})$. (As $0 \notin A_a$, each Schur triple in A_a contains three distinct nonzero elements.) It is enough to show that the number of pairs $\{y, z\} \subseteq A_a$ satisfying $x + y + z = 0$ and $\bar{x} < \bar{y} < \bar{z}$ is $2^{n-1} - 2^j$. To this end, note first that for every such pair, $\bar{z} \geq 2^{j+1}$ since otherwise $2^j \leq \bar{x}, \bar{y}, \bar{z} < 2^{j+1}$ and then $\overline{x + y + z} \geq 2^j$; consequently, also $\bar{y} \geq 2^{j+1}$ as otherwise $\overline{x + y + z} \geq 2^{j+1}$. Conversely, given an arbitrary element z such that $\bar{z} \geq 2^{j+1}$, we have $\overline{z + x} \geq 2^{j+1} > \bar{x}$ and hence $\{z, z + x\} \subseteq A_a$ is such a pair. Thus the number of these pairs is $\frac{1}{2}(2^n - 2^{j+1})$, as claimed.

Now, recall that k satisfies $2^n - 2^k \leq a < 2^n - 2^{k-1}$. We may assume that $k \leq n - 1$ as otherwise $A_a \subseteq A_{2^{n-1}}$ is sum-free. Let $t = a - 2^n + 2^k$. Then $0 \leq t < 2^{k-1}$ and

$$\begin{aligned} \text{ST}(A_a) &= \sum_{x \in A_a} \text{ST}_x(A_a) = 3 \cdot \left[\sum_{j=k}^{n-1} 2^j (2^n - 2^{j+1}) + t(2^n - 2^k) \right] \\ &= 3(2^n - 2^k)2^n - 2(4^n - 4^k) + 3(a - 2^n + 2^k)(2^n - 2^k) \\ &= (3a - 2^{n+1} + 2^k)(2^n - 2^k). \end{aligned}$$

Let us now fix an arbitrary a -element set $A \subseteq G$. We shall prove that $\text{ST}(A) \geq \text{ST}(A_a)$ by induction on n . We may assume that $0 \notin A$ as one may easily check that replacing 0 with an arbitrary element of $G \setminus A$ decreases the number of Schur triples by at least one (as $x + x \neq x$ unless $x = 0$). The case $n = 1$ is trivial, including the characterisation of sets achieving equality in (3), so let us assume that $n \geq 2$. Let $H < G$ be the subgroup of index 2 that minimises $|A \cap H|$, let $A_e = A \cap H$ (the set of ‘even’ elements of A), and let $A_o = A \cap H^c$ (the set of ‘odd’ elements of A). Moreover, let $a_e = |A_e|$ and $a_o = |A_o|$.

Observe that each Schur triple in A contains an even number of ‘odd’ elements (elements of A_o). As $H \cong \mathbb{Z}_2^{n-1}$, the number of Schur triples that contain only elements of A_e satisfies

$$\text{ST}(A_e) \geq \text{ST}^{(n-1)}(A_{a_e}^{(n-1)}), \quad (17)$$

where the superscript ‘ $(n-1)$ ’ signifies the fact that we are referring to elements and Schur triples in \mathbb{Z}_2^{n-1} . The number of Schur triples that contain one element of A_e and two elements of A_o may be estimated as follows. Fix some $x \in A_e$. The number of Schur triples in A that contain x and two elements of A_o is precisely $3|(x + A_o) \cap A_o|$, as the elements of $(x + A_o) \cap A_o$ are in one-to-one correspondence with ordered pairs $(y, z) \in A_o^2$ such that $x + y + z = 0$. Since $x + A_o, A_o \subseteq H^c$, then

$$|(x + A_o) \cap A_o| \geq |x + A_o| + |A_o| - |H^c| = 2|A_o| - |H| = 2a_o - 2^{n-1} \quad (18)$$

and consequently, recalling (17),

$$\text{ST}(A) \geq \text{ST}(A_e) + 3a_e(2a_o - 2^{n-1}) \geq \text{ST}^{(n-1)}(A_{a_e}^{(n-1)}) + 3a_e(2(a - a_e) - 2^{n-1}). \quad (19)$$

We claim that the right-hand side of (19) is greater than or equal to $\text{ST}(A_a)$ as long as

$$a_e < \max \{2^{n-1} - 2^{k-1}, a - 2^{n-1} + 2^{k-2}\}, \quad (20)$$

and equality holds only when $a_e = a - 2^{n-1}$ or when $a_e = 2^{n-1} - 2^{k-1}$ and $a > 2^n - 2^{k-1} - 2^{k-2}$.

To see this, note first that $a_e \geq a - |H^c| = a - 2^{n-1} \geq 2^{n-1} - 2^k$. If moreover $a_e < 2^{n-1} - 2^{k-1}$, then by our inductive assumption,

$$\text{ST}^{(n-1)}(A_{a_e}^{(n-1)}) = (3a_e + 2^k - 2^n)(2^{n-1} - 2^k). \quad (21)$$

Substituting the right-hand side of (21) into (19), we verify that if $a - 2^{n-1} \leq a_e < 2^{n-1} - 2^{k-1}$, then the right-hand side of (19) is at least as large as $\text{ST}(A_a)$, with equality holding only if $a_e = a - 2^{n-1}$. To see this, observe that the difference of these functions is

$$6(a_e - 2^{n-1} + 2^{k-1})(a - a_e - 2^{n-1}),$$

which is quadratic in a_e , with the coefficient of a_e^2 negative, and equal to zero if $a_e = a - 2^{n-1}$ or $a_e = 2^{n-1} - 2^{k-1}$.

Assume now that $2^{n-1} - 2^{k-1} \leq a_e < a - 2^{n-1} + 2^{k-2}$. In particular, $a_e < 2^{n-1} - 2^{k-2}$ and hence by the inductive assumption,

$$\text{ST}^{(n-1)}(A_{a_e}^{(n-1)}) = (3a_e + 2^{k-1} - 2^n)(2^{n-1} - 2^{k-1}). \quad (22)$$

Substituting the right-hand side of (22) into (19), we verify that if $2^{n-1} - 2^{k-1} \leq a_e < a - 2^{n-1} + 2^{k-2}$, then the right hand side of (19) is at least as large as $\text{ST}(A_a)$, with equality holding only if $a_e = 2^{n-1} - 2^{k-1}$. To see this, observe that the difference of these functions is

$$6(a_e - 2^{n-1} + 2^{k-1})(a - a_e - 2^{n-1} + 2^{k-2}),$$

which is quadratic in a_e , with the coefficient of a_e^2 negative, and equal to zero if $a_e = 2^{n-1} - 2^{k-1}$ or $a_e = a - 2^{n-1} + 2^{k-2}$.

For the remainder of the proof, we may and shall assume that the reverse of (20) holds, i.e., that $a_e \geq 2^{n-1} - 2^{k-1}$ and $a_e \geq a - 2^{n-1} + 2^{k-2}$. By our choice of H , this means that the smallest eigenvalue λ of \mathcal{G}_A satisfies

$$\lambda = |A \cap H| - |A \cap H^c| = a_e - a_o = 2a_e - a \geq 2 \max \{2^{n-1} - 2^{k-1}, a - 2^{n-1} + 2^{k-2}\} - a,$$

that is,

$$\lambda \geq \begin{cases} -2^{k-2} & \text{if } a \leq 2^n - 2^{k-1} - 2^{k-2}, \\ a - 2^n + 2^{k-1} & \text{if } a \geq 2^n - 2^{k-1} - 2^{k-2}. \end{cases}$$

As every element of G has order 2, then trivially $A = -A$ and thus it follows from (16) and Theorem 4.1 that (recall that $0 \notin A$)

$$\text{ST}(A) \geq 2^{-n}a^3 + \begin{cases} -2^{k-2-n}a(2^n - a) & \text{if } a \leq 2^n - 2^{k-1} - 2^{k-2}, \\ 2^{-n}(a - 2^n + 2^{k-1})a(2^n - a) & \text{if } a \geq 2^n - 2^{k-1} - 2^{k-2}. \end{cases} \quad (23)$$

In order to finish the proof, we shall now show that the right-hand side of (23) is greater than $\text{ST}(A_a)$ for every a with $2^n - 2^k \leq a < 2^n - 2^{k-1}$.

First, denote by $f_1(a)$ the difference between the right-hand side of (23) and $\text{ST}(A_a)$ when $2^n - 2^k \leq a \leq 2^n - 2^{k-1} - 2^{k-2}$. That is, let

$$f_1(a) = 2^{-n}a^3 + 2^{k-2-n}a^2 - 2^{k-2}a - (3a + 2^k - 2^{n+1})(2^n - 2^k).$$

Let $a_\ell = 2^n - 2^k$ and $a_r = 2^n - 2^{k-1} - 2^{k-2}$. We need to show that $f_1(a) > 0$ for each a satisfying $a_\ell \leq a \leq a_r$. This follows because f_1 is cubic in a , with the coefficient of a^3 positive, and

- $f_1(a_r) = 2^{2k-2} - 9 \cdot 2^{3k-n-5} \geq 2^{2k-2} - 9 \cdot 2^{2k-6} = 7 \cdot 2^{2k-6} > 0$, since $k \leq n - 1$.
- $f'_1(a_\ell) = 2^{k-2}(5 \cdot 2^{k-n+1} - 11) \leq -6 \cdot 2^{k-2} < 0$, since $k \leq n - 1$.
- $f'_1(a_r) = 2^{k-4}(21 \cdot 2^{k-n} - 20) \leq -19 \cdot 2^{k-5} < 0$, since $k \leq n - 1$.

Indeed, since f'_1 is quadratic in a , with the coefficient of a^2 positive, it has only one continuous interval where it takes negative values. Therefore $f'_1(a)$ is negative for all $a \in [a_\ell, a_r]$ and thus f_1 is decreasing in this interval, attaining its minimum at $a = a_r$.

Similarly, denote by $f_2(a)$ the difference between the right-hand side of (23) and $\text{ST}(A_a)$ when $2^n - 2^{k-1} - 2^{k-2} \leq a < 2^n - 2^{k-1}$. That is, let

$$\begin{aligned} f_2(a) &= 2^{-n}a^3 + 2^{-n}(a - 2^n + 2^{k-1})a(2^n - a) - (3a + 2^k - 2^{n+1})(2^n - 2^k) \\ &= (2 - 2^{k-n-1})a^2 + (7 \cdot 2^{k-1} - 2^{n+2})a + 2^{2n+1} + 2^{2k} - 3 \cdot 2^{k+n}. \end{aligned}$$

Let $a_\ell = 2^n - 2^{k-1} - 2^{k-2}$ and $a_r = 2^n - 2^{k-1}$. We need to show that $f_2(a) > 0$ for each a satisfying $a_\ell \leq a \leq a_r$. This follows because f_2 is quadratic in a , with the coefficient of a^2 positive, and

- $f'_2(a_m) = 0$, where $a_m = \frac{2^{n+3} - 7 \cdot 2^k}{8 - 2^{k+1} - n}$.
- $f_2(a_m) = \frac{7 \cdot 2^{n+2k-3} - 2^{3k}}{2^{n+2} - 2^k} > 0$, since $k \leq n - 1$.

Finally, we characterise sets achieving equality in (3). To this end, suppose that $\text{ST}(A) = \text{ST}(A_a)$. This means, in particular, that (20) holds (as otherwise $\text{ST}(A) > \text{ST}(A_a)$), the two

inequalities in (19) hold with equality, and the right-hand side of (19) is equal to $\text{ST}(A_a)$. As noted above, this may happen only in the following two cases.

CASE 1. $a_e = a - 2^{n-1}$.

In this case, $a_o = a - a_e = 2^{n-1}$ and thus $A \supseteq H^c$. Moreover, $\text{ST}(A_e) = \text{ST}^{(n-1)}\left(A_{a_e}^{(n-1)}\right)$ and hence we may appeal to our inductive assumption. Since

$$2^{n-1} - 2^k \leq a_e = a - 2^{n-1} < 2^{n-1} - 2^{k-1},$$

then there is a $K < H$ with 2^k elements such that $H \setminus K \subseteq A_e$ and $A_e \cap K$ is sum-free. But then the set $A \cap K = A_e \cap K$ is sum-free, and $\mathbb{Z}_2^n \setminus K = H^c \cup (H \setminus K) \subseteq A$.

CASE 2. $a_e = 2^{n-1} - 2^{k-1}$ and $a > 2^n - 2^{k-1} - 2^{k-2}$.

Since $\text{ST}(A_e) = \text{ST}^{(n-1)}\left(A_{a_e}^{(n-1)}\right)$, we may appeal to the inductive assumption and deduce that $A_e = H \setminus K$ for some $K < H$ with 2^{k-1} elements. Let L be an arbitrary subgroup satisfying $K < L < H$ and $[H : L] = 2$. Such a subgroup exists as $H/K \cong \mathbb{Z}_2^{n-k}$ and we have assumed that $n \geq k - 1$.

Note that $\mathbb{Z}_2^n/L \cong \mathbb{Z}_2^2$ and hence there are two subgroups $H_1, H_2 < \mathbb{Z}_2^n$ such that $[\mathbb{Z}_2^n : H_i] = 2$ and $H \cap H_i = L$ for each $i \in \{1, 2\}$ and $H^c \cap H_1 = H^c \setminus H_2$. Define $A_o^1 = A_o \cap H_1 = A_o \setminus H_2$ and $A_o^2 = A_o \cap H_2 = A_o \setminus H_1$. We claim that $A_o^{3-i} = H^c \cap H_i^c$ for some $i \in \{1, 2\}$. Before we prove the claim, let us show that its statement contradicts the assumption that $a < 2^n - 2^{k-1}$, which in turn implies that $\text{ST}(A) = \text{ST}(A_a)$ cannot hold in Case 2. As $H \setminus L \subseteq H \setminus K = A_e \subseteq A$, the claim implies that $H_i^c = (H_i^c \cap H^c) \cup (H \setminus L) \subseteq A$. But H_i is a subgroup of \mathbb{Z}_2^n of index 2 and therefore by our choice of H , we have

$$2^{n-1} - 2^{k-1} = a_e = |A \cap H| \leq |A \cap H_i| = |A| - |A \cap H_i^c| = |A| - |H_i^c| = a - 2^{n-1},$$

a contradiction. Therefore, in order to complete the proof, it suffices to prove the claim. To this end, suppose that it is not true, i.e., there are $y_1 \in (H^c \cap H_2^c) \setminus A_o$ and $y_2 \in (H^c \cap H_1^c) \setminus A_o$. Let $x \in H \setminus L$ be such that $x + y_1 = y_2$; such an x exists as $(H^c \cap H_1^c) - (H^c \cap H_2^c) = H \setminus L$. It is easy to see that this x satisfies

$$|(x + A_o) \cap A_o| = |(x + A_o) \cap A_o \cap (H^c \setminus \{y_2\})| \geq 2|A_o| - |H^c \setminus \{y_2\}| > 2|A_o| - |H^c|.$$

Since $x \in H \setminus L \subseteq H \setminus K = A_e$, then the first inequality in (19) is strict, see (18), contradicting our assumption that $\text{ST}(A) = \text{ST}(A_a)$. \square

5. GROUPS OF TYPE II

In this section, we prove Theorem 1.6 and Proposition 1.7. Our proof of Theorem 1.6 will again employ simple eigenvalue analysis. Given an abelian group G and an $A \subseteq G$, we define $\vec{\mathcal{G}}_A$ to be the directed graph with vertex set G whose arcs are all ordered pairs (x, y) such that $y - x \in A$. It follows from this definition that for each $A \subseteq G$,

$$\text{ST}(A) = e(\vec{\mathcal{G}}_A[A]).$$

A straightforward adaptation of the proof of Theorem 4.1 yields the following proposition. Here, the adjacency matrix of a directed graph $\vec{\mathcal{G}}$ with vertex set V is the $\{0, 1\}$ -valued V -by- V matrix $(\mathbb{1}[(x, y) \in \vec{\mathcal{G}}])_{x, y \in V}$.

Proposition 5.1. *Let $\vec{\mathcal{G}}$ be an N -vertex directed graph whose each vertex has both the in- and the outdegree equal to D . If the adjacency matrix of $\vec{\mathcal{G}}$ has an orthogonal basis of eigenvectors with eigenvalues satisfying $\operatorname{Re}(\lambda) \geq r$, then for every $U \subseteq V(\vec{\mathcal{G}})$,*

$$e(\vec{\mathcal{G}}[U]) \geq \frac{D}{N}|U|^2 + \frac{r}{N}|U|(N - |U|).$$

As it was the case with undirected Cayley graphs, the characters of G form a basis of eigenvectors of $\vec{\mathcal{G}}_A$ for every $A \subseteq G$. Moreover, the eigenvalues of $\vec{\mathcal{G}}_A$ are $\sum_{a \in A} \chi(a)$, where χ ranges over all $|G|$ characters of G . In the case $G = \mathbb{Z}_3^n$, as each element of G has order 3, all characters of G take values in the set $\{1, e^{\frac{2\pi i}{3}}, e^{-\frac{2\pi i}{3}}\} \subseteq \mathbb{C}$ of third roots of unity. Therefore, letting r_A be the smallest real part of an eigenvalue of the adjacency matrix of $\vec{\mathcal{G}}_A$, we have

$$r_A = \min \{ |A \cap H| - |A \setminus H|/2 : H < G \text{ with } [G : H] = 3 \}, \quad (24)$$

where we used the fact that $\operatorname{Re}(e^{\pm \frac{2\pi i}{3}}) = \cos \frac{2\pi}{3} = -\frac{1}{2}$. Proposition 5.1 now implies that for every $A \subseteq G$,

$$\operatorname{ST}(A) \geq 3^{-n}|A|^3 + r_A|A|(1 - 3^{-n}|A|), \quad (25)$$

where r_A is the quantity defined in (24).

Proof of Theorem 1.6. Let $\delta = 1/1000$, let n and t be as in the statement of the theorem, and denote \mathbb{Z}_3^n by G . Finally, fix some $A \subseteq G$ with $a = 3^{n-1} + t$ elements. Let us first consider the case when $|A \cap H| \geq t$ for every subgroup $H < G$ of index 3. In this case, the quantity r_A defined in (24) satisfies

$$r_A \geq -\frac{a-t}{2} + t = -\frac{3^{n-1}}{2} + t$$

and consequently (25) yields

$$\begin{aligned} \operatorname{ST}(A) &\geq 3^{-n}a^3 + \left(t - \frac{3^{n-1}}{2}\right)a(1 - 3^{-n}a) = a \left(t + 3^{-n}a(a-t) + \frac{a}{6} - \frac{3^{n-1}}{2} \right) \\ &= a \left(t + \frac{a}{3} + \frac{a}{6} - \frac{a-t}{2} \right) = \frac{3at}{2} \geq at = 3^{n-1}t + t^2. \end{aligned}$$

Hence, for the remainder of the proof we may assume that $|A \cap H| < t$ for some $H < G$ of index 3.

Fix an arbitrary H with this property and let $\varphi: G \rightarrow \mathbb{Z}_3$ be a homomorphism with $\varphi^{-1}(0) = H$. For each $i \in \{0, 1, 2\}$, let $A_i = A \cap \varphi^{-1}(i)$ and let $a_i = |A_i|$. As $-\varphi$ is also a homomorphism, we may assume that $a_2 \geq a_1$. Considering only the Schur triples $(x, y, z) \in A^3$ that φ maps to $(0, 2, 2)$, $(2, 0, 2)$, $(2, 2, 1)$, and $(1, 1, 2)$, we obtain

$$\begin{aligned} \operatorname{ST}(A) &\geq 2 \sum_{x \in A_0} |(x + A_2) \cap A_2| + \sum_{x \in A_1} |(x - A_2) \cap A_2| + \sum_{x \in A_1} |(x + A_1) \cap A_2| \\ &\geq 2a_0(2a_2 - 3^{n-1}) + a_1(2a_2 - 3^{n-1}) + a_1(a_1 + a_2 - 3^{n-1}) \\ &= (a - a_2)(2a_2 - 3^{n-1} + t) + a_0(3a_2 + a_0 - 2a). \end{aligned} \quad (26)$$

where we used the identity $3^{n-1} + t = a = a_0 + a_1 + a_2$. Treating a_0 as fixed, denote the right-hand side of (26) by $f_{a_0}(a_2)$. Observe that the function f_{a_0} is quadratic in a_2 , with the coefficient of a_2^2 negative. Thus, if $2 \cdot 3^{n-2} \leq a_2 \leq 3^{n-1}$, then

$$\text{ST}(A) \geq \min\{f_{a_0}(2 \cdot 3^{n-2}), f_{a_0}(3^{n-1})\}.$$

Note that

$$f_{a_0}(3^{n-1}) = t(3^{n-1} + t) + a_0(3^{n-1} + a_0 - 2t) \geq t(3^{n-1} + t),$$

as $t \leq \delta 3^{n-1} \leq 3^{n-1}/2$. Moreover,

$$f_{a_0}(2 \cdot 3^{n-2}) = (3^{n-2} + t)^2 + a_0(a_0 - 2t) \geq (3^{n-2} + t)^2 - t^2 \geq t(3^{n-1} + t),$$

as $t \leq \delta 3^{n-1}$ and $(\frac{1}{3} + \tau)^2 - \tau^2 \geq \tau(1 + \tau)$ for each $\tau \in [0, \delta]$. Therefore, it remains to consider the case $a_1 \leq a_2 < 2 \cdot 3^{n-2}$ and $a_0 < t$.

We let $\varepsilon = 1/30$ and define

$$C = \{x \in A_2 : |(x + A_2) \cap A_1| \geq \varepsilon 3^{n-1}\}.$$

Since clearly $\text{ST}(A) \geq |C| \cdot \varepsilon 3^{n-1}$, we may further assume that

$$|C| \leq \frac{at}{\varepsilon 3^{n-1}} \leq \frac{(1 + \delta)}{\varepsilon} \cdot t \leq \frac{(1 + \delta)\delta}{\varepsilon} \cdot 3^{n-1} \leq \varepsilon 3^{n-1}.$$

In the remainder of the proof, we show that this is impossible.

Let $B = A_2 \setminus C$. By definition, for every $x \in B$, we have $x + B \subseteq A_2 + A_2 \subseteq \varphi^{-1}(1)$ and $|(x + B) \setminus A_1| \geq |B| - \varepsilon 3^{n-1}$. Hence, for any two $x, y \in B$, we have

$$\begin{aligned} |(x + B) \cap (y + B)| &\geq |(x + B) \cap (y + B) \cap (\varphi^{-1}(1) \setminus A_1)| \\ &\geq 2(|B| - \varepsilon 3^{n-1}) - (3^{n-1} - a_1) \geq |B| - 3\varepsilon 3^{n-1}, \end{aligned}$$

as $|B| + a_1 = a_1 + a_2 - |C| \geq a - a_0 - \varepsilon 3^{n-1} > (1 - \varepsilon)3^{n-1}$ since $a_0 < t$. This means that every element of $B - B$ has at least $|B| - 3\varepsilon 3^{n-1}$ representations as a difference of two elements of B and hence

$$|B - B| \leq \frac{|B|^2}{|B| - 3\varepsilon 3^{n-1}} < 3^{n-1}, \quad (27)$$

where the last inequality follows as $|B|$ satisfies

$$\left(\frac{1}{2} - \varepsilon\right) \cdot 3^{n-1} < \frac{a - a_0}{2} - \varepsilon 3^{n-1} \leq a_2 - |C| = |B| \leq a_2 < \frac{2}{3} \cdot 3^{n-1}$$

and $\frac{\beta^2}{\beta - 3\varepsilon} < 1$ for all $\beta \in (\frac{1}{2} - \varepsilon, \frac{2}{3})$. As $|\text{Stab}(B - B)| \leq |B - B| < 3^{n-1}$, then necessarily $|\text{Stab}(B - B)| \leq 3^{n-2}$. It now follows from Kneser's theorem that

$$|B - B| \geq 2|B| - |\text{Stab}(B - B)| \geq 2|B| - 3^{n-2}. \quad (28)$$

But now (27) and (28) yield

$$2|B| - 3^{n-2} \leq \frac{|B|^2}{|B| - 3\varepsilon 3^{n-1}},$$

which is impossible as $|B| \geq (\frac{1}{2} - \varepsilon)3^{n-1}$ and $2\beta - \frac{1}{3} > \frac{\beta^2}{\beta - 3\varepsilon}$ if $\beta > \frac{1}{2} - \varepsilon$. \square

Proof of Proposition 1.7. Fix an $a \in \{p+1, \dots, 3p\}$, let $b = 3\lceil \frac{a}{3} \rceil$, and note that $b \geq a$ and $b-p \leq 3(a-p)$. It suffices to show that there is a set $B \subseteq \mathbb{Z}_3 \times \mathbb{Z}_p$ with b elements satisfying $\text{ST}(B) \leq \frac{21}{9}(b-p)^2$. One such set is $B = \mathbb{Z}_3 \times \{x_1, \dots, x_{b/3}\}$, where $x_1, \dots, x_p \in \mathbb{Z}_p$ are as in the statement of Theorem 1.3. Clearly,

$$\text{ST}(B) = \text{ST}(\mathbb{Z}_3) \cdot \text{ST}(\{x_1, \dots, x_{b/3}\}) = 9 \cdot \left\lfloor \frac{b-p}{2} \right\rfloor \left\lceil \frac{b-p}{2} \right\rceil \leq \frac{9}{4}(b-p)^2. \quad \square$$

6. A REMOVAL-TYPE LEMMA OF GREEN AND RUZSA

In this section, we prove Proposition 1.8

Proof of Proposition 1.8. Suppose that $\varepsilon > 0$ and G is an abelian group of order n and let A be an arbitrary set of at least $(1/3 + \varepsilon)n$ elements of G with $\text{ST}(A) \leq \varepsilon^2 n^2/2$. Similarly as in the proof of Theorem 1.4, define

$$C = \{x \in A : |(x-A) \cap A| \geq \varepsilon n\}.$$

As clearly $\text{ST}(A) \geq |C| \cdot \varepsilon n$, we have $|C| \leq \varepsilon n/2$. Let $A' = A \setminus C$. We claim that for every $x, y \in A'$, there are at least εn representations of $x-y$ as $a-b$ with $a, b \in A$. Indeed, for each $x, y \in A'$,

$$\begin{aligned} |(x-A) \cap (y-A)| &\geq |(x-A) \cap (y-A) \cap A^c| \\ &\geq 2(|A| - \varepsilon n) - |A^c| = 3|A| - (1 + 2\varepsilon)n \geq \varepsilon n. \end{aligned}$$

In particular, $\text{ST}(A) \geq |(A' - A') \cap A| \cdot \varepsilon n$ and therefore

$$|(A' - A') \cap A'| \leq |(A' - A') \cap A| \leq \varepsilon n/2.$$

The set $B = A' \setminus (A' - A')$ is sum-free and

$$|A \setminus B| = |C| + |(A' - A') \cap A'| \leq \varepsilon n. \quad \square$$

7. CONCLUDING REMARKS

In this paper, we have determined the minimum number of Schur triples in a set of a elements of a finite abelian group G for various a and G . We have been able to resolve this problem completely in the cases when G is a cyclic group of prime order and when $G = \mathbb{Z}_2^n$. We have also obtained some partial results for groups of type I, that is, groups whose order is divisible by a prime p satisfying $p \equiv 2 \pmod{3}$. In this case, we have determined the minimum number of Schur triples for all a in a short interval starting from $(\frac{1}{3} + \frac{1}{3p})|G|$, which is the largest size of a sum-free set in G .

We believe that solving Problem 1.2 completely would be rather difficult. There are several reasons for it. First, determining merely the largest size of a sum-free set in a general group of type III requires considerable effort, see [20]. Second, the ‘behaviour’ of the function f_G defined in (4) already becomes highly ‘non-uniform’ when G ranges over groups of type II. Third, even the seemingly modest task of determining f_G for groups of even order, say, would most likely entail understanding f_G for general G ; simply consider the group $\mathbb{Z}_2 \times G$ for some ‘difficult’ G .

In view of this, it could be interesting to resolve Problem 1.2 for particular families of G . One natural candidate would be the cyclic groups \mathbb{Z}_{2^n} . Here, we are tempted to guess that, similarly to the cases $G = \mathbb{Z}_p$ and $G = \mathbb{Z}_2^n$, there exists an ordering of the elements of \mathbb{Z}_{2^n} as $x_1^n, \dots, x_{2^n}^n$ such that for every a , the set $\{x_1^n, \dots, x_a^n\}$ minimises $\text{ST}(A)$ among all a -element $A \subseteq \mathbb{Z}_{2^n}$. It is likely that one such family of sequences (x_i^n) is the one defined as follows: $x_1^0 = 0$ and $x_i^{n+1} = 2x_i^n + 1$ and $x_{2^n+i}^{n+1} = 2x_i^n$ for all $n \geq 0$ and $i \in [2^n]$.

Acknowledgement. Parts of this work were carried out when the first author visited the Institute for Mathematical Research (FIM) of ETH Zürich, and also when the second author visited the School of Mathematical Sciences of Tel Aviv University. We would like to thank both institutions for their hospitality and for creating a stimulating research environment.

REFERENCES

1. N. Alon and F. R. K. Chung, *Explicit construction of linear sized tolerant networks*, Proceedings of the First Japan Conference on Graph Theory and Applications (Hakone, 1986), vol. 72, 1988, pp. 15–19.
2. J. Balogh, P. Hu, B. Lidický, O. Pikhurko, B. Udvari, and J. Volec, *Minimum number of monotone subsequences of length 4 in permutations*, *Combin. Probab. Comput.* **24** (2015), 658–679.
3. A. Cauchy, *Recherches sur les nombres*, *J. École Polytech.* **9** (1813), 99–116.
4. W. E. Clark, L. A. Dunning, and D. G. Rogers, *Binary set functions and parity check matrices*, *Discrete Math.* **80** (1990), 249–265.
5. W. E. Clark and J. Pedersen, *Sum-free sets in vector spaces over GF(2)*, *J. Combin. Theory Ser. A* **61** (1992), 222–229.
6. D. Conlon, *On the Ramsey multiplicity of complete graphs*, *Combinatorica* **32** (2012), 171–186.
7. S. Das, W. Gan, and B. Sudakov, *The minimum number of disjoint pairs in set systems and related problems*, *Combinatorica*, to appear.
8. ———, *Sperner’s theorem and a problem of Erdős, Katona and Kleitman*, *Combin. Probab. Comput.* **24** (2015), 585–608.
9. H. Davenport, *On the addition of residue classes*, *J. London Math. Soc.* **10** (1935), 30–32.
10. P. H. Diananda and H. P. Yap, *Maximal sum-free sets of elements of finite groups*, *Proc. Japan Acad.* **45** (1969), 1–5.
11. A. P. Dove, J. R. Griggs, R. J. Kang, and J.-S. Sereni, *Supersaturation in the Boolean lattice*, *Integers* **14A** (2014), Paper No. A4, 7.
12. S. Eberhard, B. Green, and F. Manners, *Sets of integers with no large sum-free subset*, *Ann. of Math. (2)* **180** (2014), 621–652.
13. P. Erdős, *On a theorem of Rademacher-Turán*, *Illinois J. Math.* **6** (1962), 122–127.
14. ———, *Extremal problems in number theory*, *Proc. Sympos. Pure Math.*, Vol. VIII, Amer. Math. Soc., Providence, R.I., 1965, pp. 181–189.
15. ———, *On the number of complete subgraphs and circuits contained in graphs.*, *Časopis Pěst. Mat.* **94** (1969), 290–296.
16. P. Erdős and D. J. Kleitman, *Extremal problems among subsets of a set*, *Discrete Math.* **8** (1974), 281–294.
17. P. Erdős and M. Simonovits, *Supersaturated graphs and hypergraphs*, *Combinatorica* **3** (1983), 181–192.
18. P. Erdős and G. Szekeres, *A combinatorial problem in geometry*, *Compositio Math.* **2** (1935), 463–470.
19. F. Franek and V. Rödl, *2-colorings of complete graphs with a small number of monochromatic K_4 subgraphs*, *Discrete Math.* **114** (1993), 199–203, *Combinatorics and algorithms* (Jerusalem, 1988).
20. B. Green and I. Z. Ruzsa, *Sum-free sets in abelian groups*, *Israel J. Math.* **147** (2005), 157–188.
21. J. H. B. Kemperman, *On small sumsets in an abelian group*, *Acta Math.* **103** (1960), 63–88.
22. D. J. Kleitman, *A conjecture of Erdős-Katona on commensurable pairs among subsets of an n -set*, *Theory of Graphs* (Proc. Colloq., Tihany, 1966), Academic Press, New York, 1968, pp. 215–218.

23. M. Kneser, *Abschätzung der asymptotischen Dichte von Summenmengen*, Math. Z. **58** (1953), 459–484.
24. ———, *Ein Satz über abelsche Gruppen mit Anwendungen auf die Geometrie der Zahlen*, Math. Z. **61** (1955), 429–434.
25. V. F. Lev, T. Łuczak, and T. Schoen, *Sum-free sets in abelian groups*, Israel J. Math. **125** (2001), 347–367.
26. L. Lovász and M. Simonovits, *On the number of complete subgraphs of a graph. II*, Studies in pure mathematics, Birkhäuser, Basel, 1983, pp. 459–495.
27. J. S. Myers, *The minimum number of monotone subsequences*, Electron. J. Combin. **9** (2002/03), no. 2, Research paper 4, 17 pp. (electronic), Permutation patterns (Otago, 2003).
28. E. Nazarewicz, M. O’Brien, M. O’Neill, and C. Staples, *Equality in Pollard’s theorem on set addition of congruence classes*, Acta Arith. **127** (2007), 1–15.
29. V. Nikiforov, *The number of cliques in graphs of given order and size*, Trans. Amer. Math. Soc. **363** (2011), 1599–1618.
30. J. M. Pollard, *A generalisation of the theorem of Cauchy and Davenport*, J. London Math. Soc. (2) **8** (1974), 460–462.
31. A. A. Razborov, *On the minimal density of triangles in graphs*, Combin. Probab. Comput. **17** (2008), 603–618.
32. C. Reiher, *The clique density theorem*, arXiv:1212.2454v1 [math.CO].
33. 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.
34. W. Samotij and B. Sudakov, *On the number of monotone sequences*, J. Combin. Theory Ser. B **115** (2015), 132–163.
35. A. Thomason, *A disproof of a conjecture of Erdős in Ramsey theory*, J. London Math. Soc. (2) **39** (1989), 246–255.
36. H. P. Yap, *Maximal sum-free sets in finite abelian groups iv*, Nanta Mathematica **5** (1972), 70–75.
37. ———, *Maximal sum-free sets in finite abelian groups v*, Bulletin of the Australian Mathematical Society **13** (1975), 337–342.

SCHOOL OF MATHEMATICAL SCIENCES, TEL AVIV UNIVERSITY, TEL AVIV 6997801, ISRAEL
E-mail address: samotij@post.tau.ac.il

DEPARTMENT OF MATHEMATICS, ETH, 8092 ZÜRICH, SWITZERLAND
E-mail address: benjamin.sudakov@math.ethz.ch