COUNTING SUM-FREE SETS IN ABELIAN GROUPS

NOGA ALON, JÓZSEF BALOGH, ROBERT MORRIS, AND WOJCIECH SAMOTIJ

Abstract. In this paper we study sum-free sets of order m in finite Abelian groups. We prove a general theorem on 3-uniform hypergraphs, which allows us to deduce structural results in the sparse setting from stability results in the dense setting. As a consequence, we determine the typical structure and asymptotic number of sum-free sets of order m in Abelian groups G whose order is divisible by a prime q with $q \equiv 2 \pmod 3$, for every $m \geqslant C(q)\sqrt{n \log n}$, thus extending and refining a theorem of Green and Ruzsa. In particular, we prove that almost all sum-free subsets of size m are contained in a maximum-size sum-free subset of G. We also give a completely self-contained proof of this statement for Abelian groups of even order, which uses spectral methods and a new bound on the number of independent sets of size m in an (n, d, λ)-graph.

1. Introduction

An important trend in Combinatorics in recent years has been the formulation and proof of various 'sparse analogues' of classical extremal results in Graph Theory and Additive Combinatorics. Due to the recent breakthroughs of Conlon and Gowers [10] and Schacht [34], many such theorems, e.g., the theorems of Turán [37] and Erdős and Stone [14] in extremal graph theory, and the theorem of Szemerédi [36] on arithmetic progressions, are now known to extend to sparse random sets. For structural and enumerative results, such as the theorem of Kolaitis, Prömel and Rotshchild [25] which states that almost all K_{r+1}-free graphs are r-colorable, perhaps the most natural sparse analogue is a corresponding statement about subsets of a given fixed size m, whenever m is not too small. In this paper, we prove such a result in the context of sum-free subsets of Abelian groups and provide a general framework for solving problems of this type. To be precise, we obtain a sparse analogue of a result of Green and Ruzsa [18], which describes the structure of a typical sum-free subset of an Abelian group.

Sparse versions of classical extremal and Ramsey-type results were first proved for graphs by Babai, Simonovits and Spencer [5], and for additive structures by Kohayakawa, Łuczak and Rödl [24], and in recent years there has been a tremendous interest in such problems (see, e.g, [15, 30, 31]). Mostly, these results have been in the random setting; for example, Graham, Rödl and Ruciński [17] showed that if $p \gg 1/\sqrt{n}$, and $B \subseteq \mathbb{Z}_n$ is a p-random subset[1], then

Research supported in part by: (NA) ERC Advanced Grant DMMCA, a USA-Israeli BSF grant and the Israeli I-Core program; (JB) NSF CAREER Grant DMS-0745185, UIUC Campus Research Board Grant 11067, and OTKA Grant K76099; (RM) a CNPq bolsa de Produtividade em Pesquisa; (WS) ERC Advanced Grant DMMCA and a Trinity College JRF.

[1]A p-random subset of a set X is a random subset of X, where each element is included with probability p, independently of all other elements.

with high probability every 2-colouring of B contains a monochromatic solution of $x+y=z$. The extremal version of this question was open for fifteen years, until it was recently resolved by Conlon and Gowers [10] and Schacht [34].

For problems of the type we are considering, results are known only in a few special cases. Most notably, Osthus, Prömel and Taraz [27], confirming (and strengthening) a conjecture of Prömel and Steger [29], proved that if $m \geqslant \big(\frac{\sqrt{3}}{4} + \varepsilon\big) n^{3/2}\sqrt{\log n}$ then almost all triangle-free graphs with m edges are bipartite; moreover, the constant $\sqrt{3}/4$ is best possible. This result can be seen as a sparse version of the classical theorem of Erdős, Kleitman and Rothschild [12], which states that almost all triangle-free graphs are bipartite. A similarly sharp result was proved by Friedgut, Rödl, Ruciński and Tetali [15] for the existence of monochromatic triangles in two-colourings of $G_{n,p}$. It is an interesting open problem to prove such a sharp threshold in the setting of Theorem 1.1, below.

A set $A \subseteq G$, where G is an Abelian group, is said to be *sum-free* if $(A+A)\cap A = \emptyset$, or equivalently, if there is no solution to the equation $x+y=z$ with $x,y,z \in A$. Sum-free subsets of Abelian groups are central objects of interest in Additive Combinatorics, and have been studied intensively in recent years. The main questions are as follows: What are the largest sum-free subsets of G? How many sum-free sets are there? And what does a typical such set look like? Over forty years ago, Diananda and Yap [11] determined the maximum density $\mu(G)$ of a sum-free set in G whenever $|G|$ has a prime factor $q \not\equiv 1 \pmod 3$, but it was not until 2005 that Green and Ruzsa [18] completely solved this extremal question for all finite Abelian groups. On the second and third questions, Lev, Łuczak and Schoen [26] and Sapozhenko [33] determined the asymptotic number of sum-free subsets in an Abelian group of even order by showing that almost all such sets[2] lie in the complement of a subgroup of index 2. Green and Ruzsa [18] extended this result to Abelian groups which have a prime factor $q \equiv 2 \pmod 3$, and showed also that a general finite Abelian group G has $2^{(1+o(1))\mu(G)|G|}$ sum-free subsets.

We say that G is of Type I if $|G|$ has a prime divisor q with $q \equiv 2 \pmod 3$, and Type I(q) if q is the smallest such prime. Diananda and Yap [11] proved that if G is of Type I(q), then $\mu(G) = (q+1)/(3q)$; moreover, they described all sum-free subsets of G with $\mu(G)|G|$ elements. Green and Ruzsa [18] determined the asymptotic number of sum-free subsets of an Abelian group G of Type I, by showing that almost every sum-free set in G is contained in some sum-free set of maximum size. Balogh, Morris and Samotij [6] studied p-random subsets of such groups, and showed that if $p \geqslant C(q)\sqrt{\log n / n}$, G is an Abelian group of Type I(q) and order n, and G_p is a p-random subset of G, then with high probability every maximum-size sum-free subset of G_p is contained in some sum-free subset of G of maximum size. In the case $G = \mathbb{Z}_{2n}$, they showed that if $p \geqslant \big(\frac{1}{\sqrt{3}} + \varepsilon\big)\sqrt{n \log n}$ and $A \subseteq G$ is a p-random subset, then with high probability the unique largest sum-free subset of is $A \cap O_{2n}$, where $O_{2n} \subseteq \mathbb{Z}_{2n}$ denotes the set of odd residues modulo $2n$. Moreover, the constant $1/\sqrt{3}$ in this result is best possible.

[2]We say that almost all sets in a family $\mathcal{F}$ of subsets of G satisfy some property $\mathcal{P}$ if the ratio of the number of sets in $\mathcal{F}$ that have $\mathcal{P}$ to the number of all sets in $\mathcal{F}$ tends to 1 as $|G|$ tends to infinity.

Let us denote by $\mathrm{SF}(G,m)$ the collection of sum-free subsets of size m in a finite Abelian group G. The following theorem refines the result of Green and Ruzsa [18] to sum-free sets of fixed size m, provided that $m \geqslant C(q)\sqrt{n \log n}$.

Theorem 1.1. *For every prime $q \equiv 2 \pmod 3$, there exists a constant $C(q) > 0$ such that the following holds. Let G be an Abelian group of Type $I(q)$ and order n, and let $m \geqslant C(q)\sqrt{n \log n}$. Then almost every sum-free subset of G of size m is contained in a maximum-size sum-free subset of G, and hence*

$$|\mathrm{SF}(G,m)| \,=\, \lambda_q \cdot \big(\#\big\{\textit{elements of } G \textit{ of order } q\big\} + o(1)\big) \binom{\mu(G)n}{m}$$

as $n \to \infty$, where $\lambda_q = 1$ if $q = 2$ and $\lambda_q = 1/2$ otherwise.

Although the factor $\lambda_q \cdot \#\{$elements of $G$of order $q\}$ above may appear mysterious, it is a natural consequence of the characterization of maximum-size sum-free sets in groups of Type I, see Theorem 6.2. We remark that the lower bound $m \geqslant C(q)\sqrt{n \log n}$ is sharp up to a constant factor, since there are at least $(n/2)\big(\mu(G)n - 3m\big)^{m-1}/(m-1)!$ sum-free subsets of G which contain exactly one element outside a given maximum-size sum-free subset of G, and this is larger than $m^{1/5}\binom{\mu(G)n}{m}$ if $m \leqslant \frac{1}{5}\sqrt{n \log n}$. (Here, and throughout, log denotes the natural logarithm.) Hence, assuming $m^{1/5}$ is much larger than the number of elements of order q in G, almost no sum-free subset of G of this size is contained in a maximum-size sum-free subset of G.

We shall prove Theorem 1.1 using a new theorem (see Section 2) which describes the structure of a typical independent set in a 3-uniform hypergraph $\mathcal{H}$ that satisfies a certain natural 'stability' property, see Definition 2.1. The key ingredient in the proof of this theorem is a new method of enumerating independent sets in 3-uniform hypergraphs. We shall also use a simplified version of this method to prove a new bound on the number of independent sets in a certain class of expander graphs known as (n,d,λ)-graphs.

First, let us recall the definition of (n,d,λ)-graphs, which are an important class of expanders; for a detailed introduction to expander graphs, we refer the reader to [4] or [19]. Given a graph $\mathcal{G}$, let $\lambda_1 \geqslant \ldots \geqslant \lambda_n$ denote the eigenvalues of the adjacency matrix of $\mathcal{G}$. We call $\max\{|\lambda_2|, |\lambda_n|\}$ the *second eigenvalue* of $\mathcal{G}$.

Definition 1.2 ((n,d,λ)-graphs)**.** A graph $\mathcal{G}$ is an (n,d,λ)-graph if it is d-regular, has n vertices, and the absolute value of each of its nontrivial eigenvalues is at most λ.

Alon and Rödl [3] gave an upper bound on the number of independent sets in an (n,d,λ)-graph, and used their result to give sharp bounds on multicolour Ramsey numbers. When $\lambda = \Omega(d)$ (as $n \to \infty$), Theorem 1.3 below provides a significantly stronger bound than that of Alon and Rödl, for a wider range of m; it is moreover asymptotically sharp. In fact, we will not assume anything about the second eigenvalue of a graph $\mathcal{G}$ as our bound on the number of independent sets of $\mathcal{G}$ will depend only on the *smallest* eigenvalue of $\mathcal{G}$. Given a graph $\mathcal{G}$, let $\lambda(\mathcal{G})$ be the smallest eigenvalue of the adjacency matrix of $\mathcal{G}$ (denoted by λ_n above) and let $I(\mathcal{G},m)$ be the number of independent sets of size m in $\mathcal{G}$. Observe that $\lambda(\mathcal{G}) < 0$ for every non-empty $\mathcal{G}$ and that, by definition, every (n,d,λ)-graph satisfies $\lambda(\mathcal{G}) \geqslant -\lambda$.

Theorem 1.3. *For every $\varepsilon > 0$, there exists a constant $C = C(\varepsilon)$ such that the following holds. If $\mathcal{G}$ is an n-vertex d-regular graph with $\lambda(\mathcal{G}) \geqslant -\lambda$, then*

$$I(\mathcal{G}, m) \leqslant \binom{\left(\frac{\lambda}{d+\lambda} + \varepsilon\right) n}{m}$$

for every $m \geqslant Cn/d$.

We remark that the constant $\frac{\lambda}{d+\lambda}$ in Theorem 1.3 is best possible, since there exist n-vertex d-regular graphs with $\lambda(\mathcal{G}) \geqslant -\lambda$ and $\alpha(\mathcal{G}) = \frac{\lambda}{d+\lambda}n$ for many values of n, d and λ (here $\alpha(\mathcal{G})$ denotes the independence number of $\mathcal{G}$). For example, consider a blow-up of the complete graph K_{t+1}, where each vertex is replaced by a set of size $n/(t+1)$ and each edge is replaced by a random d/t-regular bipartite graph with colour classes of size $n/(t+1)$ each. This blown-up graph $\mathcal{G}$ is d-regular and, with high probability, it satisfies $\lambda(\mathcal{G}) = -d/t$ and $\alpha(\mathcal{G}) = n/(t+1)$.

In Section 7, we shall use Theorem 1.3, together with some basic facts about characters of finite Abelian groups, to give a completely self-contained proof of Theorem 1.1 in the case $q = 2$. For previous results relating the problem of estimating the number of sum-free subsets of groups, to that of estimating the number of independent sets in regular graphs, see for example [1, 26, 33]. For other results on counting independent sets in graphs and hypergraphs, see Balogh and Samotij [7, 8], Carroll, Galvin and Tetali [9], Galvin and Kahn [16], Kahn [21, 22], Peled and Samotij [28], Sapozhenko [32] and Zhao [38].

The rest of the paper is organised as follows. In Section 2, we state our structural theorem for 3-uniform hypergraphs, and in Section 3 we prove Theorem 1.3. In Sections 4 and 5, we prove the structural theorem, and in Sections 6 we shall apply it to prove Theorem 1.1. Finally, in Section 7, we shall prove Theorem 1.1 again in the case $q = 2$.

2. A structural theorem for 3-uniform hypergraphs

In this section we shall introduce our main tool: a theorem which allows us to deduce structural results for sparse sum-free sets from stability results in the dense setting. Since we wish to apply our result to sum-free sets in various Abelian groups, we shall use the language of general 3-uniform (sequences of) hypergraphs $\mathcal{H} = (\mathcal{H}_n)_{n\in\mathbb{N}}$, where $|V(\mathcal{H}_n)| = n$. Throughout the paper, the reader should think of $\mathcal{H}$ as encoding the Schur triples (that is, triples (x, y, z) with $x + y = z$) in an additive structure.

We now define the stability property with which we shall be able to work. Let $\alpha \in (0, 1)$ and let $\mathcal{B} = (\mathcal{B}_n)_{n\in\mathbb{N}}$, where $\mathcal{B}_n$ is a family of subsets of $V(\mathcal{H}_n)$. We shall write $|\mathcal{B}_n|$ for the number of sets in $\mathcal{B}_n$, and set $\|\mathcal{B}_n\| = \max\{|B| : B \in \mathcal{B}_n\}$.

Definition 2.1. A sequence of hypergraphs $\mathcal{H} = (\mathcal{H}_n)_{n\in\mathbb{N}}$ is said to be $(\alpha, \mathcal{B})$-stable if for every $\gamma > 0$ there exists $\beta > 0$ such that the following holds. If $A \subseteq V(\mathcal{H}_n)$ with $|A| \geqslant (\alpha - \beta)n$, then either $e(\mathcal{H}_n[A]) \geqslant \beta e(\mathcal{H}_n)$, or $|A \setminus B| \leqslant \gamma n$ for some $B \in \mathcal{B}_n$.

Roughly speaking, a sequence of hypergraphs $(\mathcal{H}_n)$ is $(\alpha, \mathcal{B})$-stable if for every $A \subseteq V(\mathcal{H}_n)$ such that $|A|$ is almost as large as the extremal number for $\mathcal{H}_n$ (i.e., the size of the largest independent set), the set A is either very close to an extremal set $B \in \mathcal{B}_n$, or it contains many (i.e., a positive fraction of all) edges of $\mathcal{H}_n$. Observe that classical stability results, such as that of Erdős and Simonovits [13, 35], are typically of this form.

We shall need two further technical conditions on $\mathcal{H}$. Let

$$\Delta_2(\mathcal{H}_n) \,=\, \max_{T \subseteq V(\mathcal{H}_n), |T|=2} \big|\big\{ e \in \mathcal{H}_n \colon T \subseteq e \big\}\big|,$$

and note that if $\mathcal{H}$ encodes Schur triples then $\Delta_2(\mathcal{H}_n) \leqslant 3$. Also define

$$\delta(\mathcal{H}_n, \mathcal{B}_n) \,:=\, \min_{B \in \mathcal{B}_n} \min_{v \in V(\mathcal{H}_n) \setminus B} \Big|\Big\{ e \in \mathcal{H}_n \,:\, |e \cap B| = 2 \text{ and } v \in e \Big\}\Big|,$$

and, as usual, write $\alpha(\mathcal{H}_n)$ for the size of the largest independent set in $\mathcal{H}_n$.

The following theorem is the key step in the proof of Theorem 1.1.

Theorem 2.2. *Let $\mathcal{H} = (\mathcal{H}_n)_{n \in \mathbb{N}}$ be a sequence of 3-uniform hypergraphs which is $(\alpha, \mathcal{B})$-stable, with $e(\mathcal{H}_n) = \Theta(n^2)$ and $\Delta_2(\mathcal{H}_n) = O(1)$. Suppose that $|\mathcal{B}_n| = n^{O(1)}$, that $\alpha(\mathcal{H}_n) \geqslant \|\mathcal{B}_n\| \geqslant \alpha n$, and that $\delta(\mathcal{H}_n, \mathcal{B}_n) = \Omega(n)$. Then there exists a constant $C = C(\mathcal{H}, \mathcal{B}) > 0$ such that if*

$$m \,\geqslant\, C\sqrt{n \log n},$$

then almost every independent set in $\mathcal{H}_n$ of size m is a subset of some $B \in \mathcal{B}_n$.

We shall prove Theorem 2.2 in Sections 4 and 5. In Section 6, we shall use it to prove Theorem 1.1.

3. Independent sets in regular graphs with no small eigenvalues

As a warm-up for the proof of Theorem 2.2, we shall prove a bound on the number of independent sets in regular graphs with no small eigenvalues, Theorem 1.3, which improves a theorem of Alon and Rödl [3]. This result will be a key tool in our self-contained proof of Theorem 1.1 in the case $q = 2$, see Section 7. Moreover, many of the ideas from the proof of Theorem 1.3 will be used again in the proof of Theorem 2.2. We remark that the technique of enumerating independent sets in graphs used in this section was pioneered by Kleitman and Winston [23] and our proof of Theorem 1.3, below, requires little more than their original method.

Given a graph $\mathcal{G}$ on n vertices, and an integer $m \in [n]$, let $I(\mathcal{G})$ denote the number of independent sets in $\mathcal{G}$, and recall that $I(\mathcal{G}, m)$ denotes the number of independent sets of size m in $\mathcal{G}$. Alon [1] proved that if $\mathcal{G}$ is a d-regular graph on n vertices, then $I(\mathcal{G}) \leqslant 2^{n/2 + o(n)}$ (as $d \to \infty$), resolving a conjecture of Granville (see [1]), and suggested that the unique $\mathcal{G}$ that maximizes $I(\mathcal{G})$ among all such (i.e., n-vertex d-regular) graphs might be a disjoint union of copies of $K_{d,d}$. This conjecture was proven (using the entropy method) by Kahn [21] for bipartite graphs, and recently in full generality by Zhao [38].

Theorem 3.1 (Kahn [21], Zhao [38])**.** *Let $\mathcal{G}$ be a d-regular graph on n vertices. Then*

$$I(\mathcal{G}) \,\leqslant\, \big(2^{d+1} - 1\big)^{n/2d},$$

where equality holds if and only if $\mathcal{G}$ is a disjoint union of copies of $K_{d,d}$.

Since $-d$ is an eigenvalue of $K_{d,d}$, any d-regular graph $\mathcal{G}$ containing a copy of $K_{d,d}$ satisfies $\lambda(\mathcal{G}) = -d$. One might hope that a stronger bound on $I(\mathcal{G})$ holds for d-regular graphs $\mathcal{G}$ with $\lambda(\mathcal{G}) > -d$. Alon and Rödl [3] proved such a bound on $I(\mathcal{G}, m)$ for the slightly narrower class of (n, d, λ)-graphs and used their result to give sharp bounds on Ramsey numbers.

Theorem 3.2 (Alon and Rödl [3]). *Let $\mathcal{G}$ be an (n, d, λ)-graph. Then*

$$I(\mathcal{G}, m) \leqslant \left(\frac{emd^2}{4\lambda n \log n}\right)^{2(n/d)\log n} \binom{2\lambda n/d}{m}$$

for every $m \geqslant 2(n/d) \log n$.

If $\lambda = \Omega(d)$ as $n \to \infty$, then Theorem 1.3 improves the above result in three ways: it provides a stronger bound for a wider range of values of m in a wider class of graphs. Theorem 1.3 is an immediate consequence of the following theorem, combined with the Alon-Chung lemma (Lemma 3.4, below).

Theorem 3.3. *For every $\varepsilon, \delta > 0$, there exists a constant $C = C(\varepsilon, \delta)$ such that the following holds. Let $\mathcal{G}$ be a d-regular graph on n vertices, and suppose that $2e(A) \geqslant \varepsilon|A|d$ for every $A \subseteq V(\mathcal{G})$ with $|A| \geqslant (\alpha + \delta)n$. Then*

$$I(\mathcal{G}, m) \leqslant \binom{(\alpha + 2\delta)n}{m}$$

for every $m \geqslant Cn/d$.

The assumption in Theorem 3.3 that $2e(A) \geqslant \varepsilon|A|d$ might seem somewhat strong; however, it follows from the Expander Mixing Lemma that it is satisfied by every (n, d, λ)-graph with $\lambda/(d+\lambda) \leqslant \alpha$. For two sets $S, T \subseteq V(\mathcal{G})$, let $e(S, T)$ denote the number of pairs $(x, y) \in S \times T$ such that $\{x, y\} \in E(\mathcal{G})$. In particular, we have $e(S, S) = 2e(S)$ for every $S \subseteq V(\mathcal{G})$. The following result is proved[3] in [2].

Lemma 3.4 (Alon-Chung [2]). *Let $\mathcal{G}$ be an n-vertex d-regular graph. Then for all $A \subseteq V(G)$,*

$$2e(A) \geqslant \frac{d}{n}|A|^2 + \frac{\lambda(\mathcal{G})}{n}|A|\big(n - |A|\big).$$

We first deduce Theorem 1.3 from Theorem 3.3 and Lemma 3.4.

Proof of Theorem 1.3. We claim that if $\mathcal{G}$ is an n-vertex d-regular graph with $\lambda(\mathcal{G}) \geqslant -\lambda$ and $\alpha = \lambda/(d + \lambda)$, then $2e(A) \geqslant \varepsilon|A|d$ for every $A \subseteq V(\mathcal{G})$ with $|A| \geqslant (\alpha + \varepsilon)n$. This implies that $\mathcal{G}$ satisfies the assumption of Theorem 3.3 (with $\delta = \varepsilon$), and so the theorem follows.

To prove the claim, suppose that $A \subseteq V(\mathcal{G})$ satisfies $|A| \geqslant (\alpha + \varepsilon)n$. By Lemma 3.4,

$$2e(A) \;\geqslant\; \frac{d}{n} \cdot |A|^2 \;-\; \frac{\lambda}{n} \cdot |A|\big(n - |A|\big) \;=\; \frac{|A|}{n}\Big[\big(d + \lambda\big)|A| - \lambda n\Big].$$

[3]Although the result is stated in [2] in a slightly different form, its proof there in fact implies Lemma 3.4.

Our lower bound on $|A|$ and the choice of $\alpha = \lambda/(d+\lambda)$ now give

$$2e(A) \;\geqslant\; |A|\Big[\big(d+\lambda\big)\big(\alpha+\varepsilon\big) - \lambda\Big] \;=\; \varepsilon|A|\big(d+\lambda\big) \;\geqslant\; \varepsilon|A|d,$$

as required. □

In the proof of Theorem 3.3, we shall use an algorithm which uniquely encodes every independent set I of size m in $\mathcal{G}$ as a pair $(S, I \setminus S)$, where $|S| \leqslant 2n/\varepsilon d \leqslant 2m/C\varepsilon$, and $I \setminus S$ is contained in some set A, with $|A| \leqslant (\alpha+\delta)n$, which depends only on S. At all times, it maintains a partition of $V(\mathcal{G})$ into sets S, X, and A (short for Selected, eXcluded, and Available), such that $S \subseteq I \subseteq A \cup S$.

At each stage of the algorithm, we will need to order the vertices of A with respect to their degrees. For the sake of brevity and clarity of the presentation, let us make the following definition.

Definition 3.5 (Max-degree order)**.** Given a graph $\mathcal{G}$ and a set $A \subseteq V(\mathcal{G})$, the *max-degree order* on A is the following linear order $(v_1, \ldots, v_{|A|})$ on the elements of A: For every $i \in \{1, \ldots, |A|\}$, v_i is the maximum-degree vertex in the graph $\mathcal{G}[A \setminus \{v_1, \ldots, v_{i-1}\}]$; we break ties by giving preference to vertices that come earlier in some predefined ordering of $V(\mathcal{G})$.

We are now ready to describe the Basic Algorithm.

The Basic Algorithm. Set $A = V(\mathcal{G})$ and $S = X = \emptyset$. Now, while $|A| > (\alpha+\delta)n$, we repeat the following:

(a) Let i be the minimal index (in the max-degree order on A) such that $v_i \in I$.
(b) Move v_i from A to S.
(c) Move $v_1, \ldots, v_{i-1}$ from A to X (since they are not in I by the choice of i).
(d) Move $N(v_i)$ from A to X (since I is independent and $v_i \in I$).

Finally, when $|A| \leqslant (\alpha+\delta)n$, we output S (which is a subset of $V(\mathcal{G})$) and $I \setminus S$ (which is a subset of A).

We remark that, as well as in [23], algorithms similar to the one above have been considered before to bound the number of independent sets in graphs [3, 32] and hypergraphs [7, 8].

Proof of Theorem 3.3. The theorem is an easy consequence of the following two statements:

$$I(\mathcal{G}, m) \;\leqslant\; \sum_{t=1}^{t_0} \binom{n}{t}\binom{(\alpha+\delta)n}{m-t}, \tag{1}$$

where $t_0 = \dfrac{n}{\varepsilon d} + 1$, and

$$\binom{n}{t}\binom{(\alpha+\delta)n}{m-t} \;\leqslant\; \frac{1}{m}\binom{(\alpha+2\delta)n}{m} \tag{2}$$

if $t \leqslant 2n/\varepsilon d$ and $m \geqslant Cn/d$. We shall prove (1) using the Basic Algorithm; (2) follows from a straightforward calculation.

To prove (1), let $t \in \mathbb{N}$ be the number of elements of S at the end of the algorithm, and note that we have at most $\binom{n}{t}$ choices for S. Now, crucially, we observe that A is uniquely determined by S (given the original ordering of $V(\mathcal{G})$); indeed, step (a) of the Basic Algorithm requires no knowledge of I, only of S and $\mathcal{G}$. Since $|A| \leqslant (\alpha+\delta)n$, it follows that we have at most $\binom{(\alpha+\delta)n}{m-t}$ choices for $I \setminus S$.

It will thus suffice to show that, given our assumptions on $\mathcal{G}$, the algorithm terminates in at most $t_0 = \frac{n}{\varepsilon d} + 1 \leqslant \frac{2n}{\varepsilon d}$ steps. We shall show that A loses at least εd elements at each step of the algorithm (except perhaps the last), from which this bound follows immediately. Indeed, consider a step of the algorithm (not the last), in which a vertex v_i is moved to S, and set $A' = A \setminus \{v_1, \ldots, v_{i-1}\}$. Since this is not the last step, we have $|A'| \geqslant (\alpha+\delta)n$, and so $2e(A') \geqslant \varepsilon |A'| d$, by our assumption on $\mathcal{G}$. Thus $|N(v_i) \cap A'| \geqslant \varepsilon d$, since v_i is the vertex of maximum degree in $\mathcal{G}[A']$, and hence A loses at least εd elements in this step, as claimed.

To prove (2), we use the fact that, if t is replaced by $t+1$, then the left-hand side is multiplied by

$$\frac{n-t}{t+1} \cdot \frac{m-t}{(\alpha+\delta)n - m + t + 1}. \tag{3}$$

We claim that (3) is at most $\frac{2}{\delta} \cdot \left(\frac{m}{t}\right)^2$. To prove this, we consider two cases: if $m \leqslant (\alpha+\delta/2)n$, then (3) is at most

$$\frac{n}{t} \cdot \frac{2m}{\delta n} = \frac{2m}{\delta t}$$

while if $m > (\alpha+\delta/2)n$ then it is at most

$$\frac{n}{t} \cdot \frac{m}{t} \leqslant \frac{2}{\delta} \cdot \left(\frac{m}{t}\right)^2,$$

since $n \leqslant 2m/\delta$, and our assumptions imply that $\alpha(\mathcal{G}) < (\alpha+\delta)n$, so we may assume that $m < (\alpha+\delta)n$. Thus, for each t with $t \leqslant t_0 \leqslant \frac{2n}{\varepsilon d}$,

$$\binom{n}{t}\binom{(\alpha+\delta)n}{m-t} \leqslant \binom{(\alpha+\delta)n}{m} \prod_{r=1}^{t} \frac{2}{\delta} \cdot \left(\frac{m}{r}\right)^2 \leqslant \left(\frac{1}{t_0!}\right)^2 \left(\frac{2m}{\delta}\right)^{2t_0} \binom{(\alpha+\delta)n}{m}.$$

Since $\binom{b}{c} \leqslant \left(\frac{b}{a}\right)^c \binom{a}{c}$ for every $a > b > c \geqslant 0$, $k! > (k/e)^k$ for every $k \in \mathbb{N}$, the function $t_0 \mapsto \left(\frac{em}{\delta t_0}\right)^{t_0}$ is increasing on the interval $(0, m)$, and $t_0 \leqslant \frac{2n}{\varepsilon d} \leqslant \frac{2m}{C\varepsilon}$, this is at most

$$\left(\frac{2em}{\delta t_0}\right)^{2t_0} \binom{(\alpha+\delta)n}{m} \leqslant \left(\frac{C\varepsilon e}{\delta}\right)^{\frac{4}{C\varepsilon}m} \left(\frac{\alpha+\delta}{\alpha+2\delta}\right)^m \binom{(\alpha+2\delta)n}{m} \leqslant \frac{1}{m} \cdot \binom{(\alpha+2\delta)n}{m}$$

as required. In the final inequality we used the fact that C is sufficiently large as a function of δ and ε, and that m is sufficiently large (as a function of δ), since $m \geqslant Cn/d$. □

4. Algorithm argument

In this section, we shall introduce a more powerful algorithm than that used in Section 3. We shall use this algorithm in the proof of Theorem 2.2 to bound the number of independent sets which contain at least δm elements of $V(\mathcal{H}_n) \setminus B$ for every $B \in \mathcal{B}_n$. We shall show that when $m \gg \sqrt{n}$, then the number of such independent sets is exponentially small. The model example that the reader should keep in mind when reading this section is when $\mathcal{H}_n$ is the hypergraph of Schur triples in an n-element Abelian group of Type I(q), where q is some prime satisfying $q \equiv 2 \pmod 3$.

Given a hypergraph $\mathcal{H}_n$, a family of sets $\mathcal{B}_n$, and $\delta > 0$, we define

$$\mathrm{SF}^{(\delta)}_{\geqslant}(\mathcal{H}_n, \mathcal{B}_n, m) \,:=\, \Big\{ I \in \mathrm{SF}(\mathcal{H}_n, m) \,:\, |I \setminus B| \geqslant \delta m \text{ for every } B \in \mathcal{B}_n \Big\},$$

where $\mathrm{SF}(\mathcal{H}_n, m)$ denotes the collection of independent sets in $\mathcal{H}_n$ of size m. The following theorem shows that there are few independent sets in $\mathcal{H}_n$ (i.e., sum-free sets) of size m which are far from every set $B \in \mathcal{B}_n$.

Theorem 4.1. *Let $\alpha > 0$ and let $\mathcal{H} = (\mathcal{H}_n)_{n\in\mathbb{N}}$ be a sequence of 3-uniform hypergraphs which is $(\alpha, \mathcal{B})$-stable, has $e(\mathcal{H}_n) = \Theta(n^2)$ and $\Delta_2(\mathcal{H}_n) = O(1)$. If $\|\mathcal{B}_n\| \geqslant \alpha n$, then for every $\delta > 0$, there exists a $C > 0$ such that the following holds. If $m \geqslant C\sqrt{n}$ and n is sufficiently large, then*

$$\big|\mathrm{SF}^{(\delta)}_{\geqslant}(\mathcal{H}_n, \mathcal{B}_n, m)\big| \,\leqslant\, \Big(2^{-\varepsilon m} + \delta^m |\mathcal{B}_n| \Big) \binom{\|\mathcal{B}_n\|}{m}$$

for some $\varepsilon = \varepsilon(\mathcal{H}, \delta) > 0$.

We shall describe an algorithm which encodes every independent set I in $\mathcal{H}_n$ and produces short output for every $I \in \mathrm{SF}^{(\delta)}_{\geqslant}(\mathcal{H}_n, \mathcal{B}_n, m)$. As before, our algorithm will maintain a partition of $V(\mathcal{H}_n)$ into sets S, X, and A (short for Selected, eXcluded, and Available), such that $S \subseteq I \subseteq A \cup S$. We shall also maintain a set $T \subseteq S$ (for Temporary), and the corresponding graph $\mathcal{G}_T$, i.e., the graph with vertex set $V(\mathcal{H}_n)$, and edge set

$$E(\mathcal{G}_T) \,=\, \Big\{ \{u, v\} \subseteq V(\mathcal{G}_T) \,:\, \{u, v, w\} \in \mathcal{H}_n \text{ for some } w \in T \Big\}.$$

We shall frequently consider the max-degree order (defined in Section 3) on the vertices of the graph $\mathcal{G}_T[A]$.

4.1. **The Algorithm.** The idea of the algorithm is quite simple: we apply the Basic Algorithm of Section 3 to the graph $\mathcal{G}_T[A]$ as long as it is reasonably dense. If $\mathcal{G}_T[A]$ becomes too sparse, then there are four possibilities: either we have arrived at a set A which has at most $(\alpha - \beta)n$ elements, or a set A which is almost contained in some $B \in \mathcal{B}_n$; or if not, then we can use the $(\alpha, \mathcal{B})$-stability of $\mathcal{H}$ to find either a new set T for which $\mathcal{G}_T$ is dense (see Case 2 below), or a set of linear size that contains very few elements of I. Therefore, after moving relatively few vertices of $\mathcal{H}_n$ to S, our choice for $I \setminus S$ is limited to a set $A \subseteq V(\mathcal{G})$ that is either small or almost contained in some $B \in \mathcal{B}_n$. It follows that if I was far from every $B \in \mathcal{B}_n$, then (in both cases) the number of ways to choose $I \setminus S$ from A is very small.

We begin by choosing some constants. Let $\gamma > 0$ and note that since $\mathcal{H}$ is $(\alpha, \mathcal{B})$-stable, there exists $\beta > 0$ so that if $|A| \geqslant (\alpha - \beta)|V(\mathcal{H}_n)|$ and $|A \setminus B| > \gamma |V(\mathcal{H}_n)|$ for every $B \in \mathcal{B}_n$, then $e(\mathcal{H}_n[A]) \geqslant \beta e(\mathcal{H}_n)$. Let us choose $\beta > 0$ sufficiently small so that $e(\mathcal{H}_n) \geqslant \beta n^2$ and $\Delta_2(\mathcal{H}_n) \leqslant 1/\beta$ for all sufficiently large n. Let $C = C(\beta) > 0$ be sufficiently large, and set

$$d \,=\, \frac{Cn}{m} \,\leqslant\, \frac{m}{C} \,\leqslant\, \frac{n}{C}.$$

We are ready to describe the Main Algorithm; this is the key step in our proof of Theorem 2.2.

The Main Algorithm. We initiate the algorithm with $T = S \subseteq I$, a deterministically chosen subset of I of size d (the first d elements of I in our ordering of $V(\mathcal{H}_n)$, say), and with $A = V(\mathcal{H}_n) \setminus S$ and $X = \emptyset$. Now, while $|A| > (\alpha - \beta)n$ and $|A \setminus B| > \gamma n$ for every $B \in \mathcal{B}_n$, we repeat the following steps:

Case 1: If the average degree in $\mathcal{G}_T[A]$ is at least $\beta^4 d$, then:

(a) Let i be the minimal index in the max-degree order on $V(\mathcal{G}_T[A])$ such that $v_i \in I$.
(b) Move v_i from A to S.
(c) Move $v_1, \ldots, v_{i-1}$ from A to X (since they are not in I by the choice of i).
(d) Move $N(v_i)$ from A to X (since I is independent and $v_i \in I$).

Case 2: If the average degree of $\mathcal{G}_T[A]$ is less than $\beta^4 d$, then we find a new set T as follows. Since $\mathcal{H}$ is $(\alpha, \mathcal{B})$-stable, $|A| > (\alpha - \beta)n$, and $|A \setminus B| > \gamma n$ for every $B \in \mathcal{B}_n$, then A contains at least $\beta e(\mathcal{H}_n)$ edges of $\mathcal{H}_n$. Set

$$Z \,=\, \Big\{ z \in A :\, e\big(\mathcal{G}_z[A]\big) \geqslant \beta^2 n \Big\},$$

where $\mathcal{G}_z[A]$ is the graph with vertex set A and edge set $\big\{\{x,y\} : \{x,y,z\} \in E(\mathcal{H}_n)\big\}$. We call the elements of Z *useful*. Since $e(\mathcal{H}_n) \geqslant \beta n^2$, we have $e\big(\mathcal{H}_n[A]\big) \geqslant \beta^2 n^2$, and so

$$\sum_{z \in A} e\big(\mathcal{G}_z[A]\big) = 3e(\mathcal{H}_n[A]) \geqslant 3\beta^2 n^2.$$

Moreover, we have $e\big(\mathcal{G}_z[A]\big) \leqslant \Delta(\mathcal{H}_n) \leqslant \Delta_2(\mathcal{H}_n) n \leqslant n/\beta$ for every $z \in V(\mathcal{G})$. Thus, by the pigeonhole principle, it follows that $|Z| \geqslant 2\beta^3 n$.

Now we have two subcases:

(a) If I contains fewer than d useful elements, then move these elements from A to S and move the other useful elements from A to X.
(b) If I contains more than d useful elements, choose d of them $u_1, \ldots, u_d$ (the first d in our ordering, say) and move them from A to S. Moreover, set $T = \{u_1, \ldots, u_d\}$.

Finally, when $|A| \leqslant (\alpha - \beta)n$, or $|A \setminus B| \leqslant \gamma n$ for some $B \in \mathcal{B}_n$, then we output S (which is a subset of $V(\mathcal{G})$) and $I \setminus S$ (which is a subset of A) and stop.

We shall show that the Main Algorithm encodes at most $\beta^2 m$ elements of I in S, and that S determines A. Theorem 4.1 then follows from some simple counting.

4.2. **Proof of Theorem 4.1.** We begin by proving three straightforward claims about the Main Algorithm; these, together with some simple counting, will be enough to prove the theorem. The following statements all hold under the assumptions of Theorem 4.1.

Claim 1. *The Main Algorithm passes through Case* 1 *at most* $2n/(\beta^4 d)$ *times, and through Case* 2 *at most* $1/\beta^5$ *times.*

Proof. We prove the second statement first. To do so, simply observe that each time we pass through Case 2(a), we move at least $2\beta^3 n - d \geqslant \beta^3 n$ vertices from A to X, and each time we pass through Case 2(b), we obtain a graph $\mathcal{G}_T[A]$ with at least $\beta^2 nd/\Delta_2(\mathcal{H}_n) - O(d^2) \geqslant 2\beta^4 nd$

edges. In the latter case, we must remove at least $\beta^4 nd$ edges from $\mathcal{G}_T[A]$ before we can return to Case 2. Since $\Delta_2(\mathcal{H}_n) \leqslant 1/\beta$, it follows that $\Delta(\mathcal{G}_T) \leqslant |T|/\beta = d/\beta$, since if $xy \in E(\mathcal{G}_T)$ then there exists $z \in T$ such that $\{x, y, z\} \in E(\mathcal{H}_n)$, and for each pair $\{x, z\}$ there are at most $\Delta_2(\mathcal{H}_n)$ such y. Thus we must remove at least $\beta^5 n$ vertices from A before returning to Case 2, and hence the algorithm can pass through Case 2 at most $1/\beta^5$ times before the set A shrinks to size αn, as claimed.

To prove the first statement, note that each time we pass through Case 1 on two successive steps of the algorithm, we remove at least $\beta^4 d$ vertices of A in the first of these. Indeed, since $\mathcal{G}_T[A]$ (for the second step) has average degree at least $\beta^4 d$, then by the definition of the max-degree order, the vertex we removed in the first step must have had forward degree at least $\beta^4 d$. By the argument above, there are at most $1/\beta^5$ steps at which this fails to hold, and therefore the algorithm passes through Case 1 at most

$$\frac{n}{\beta^4 d} + \frac{1}{\beta^5} \leqslant \frac{2n}{\beta^4 d}$$

times, as claimed. □

The next claim is a simple consequence of Claim 1 and our choice of d.

Claim 2. *If $C \geqslant 3/\beta^7$, then $|S| \leqslant \beta^2 m$ at the end of the Main Algorithm.*

Proof. Each time the Main Algorithm passes through Case 1, $|S|$ increases by one; each time it passes through Case 2, $|S|$ increases by at most d. Thus, by Claim 1 and our choice of d,

$$|S| \leqslant d + \frac{2n}{\beta^4 d} + \frac{d}{\beta^5} \leqslant \frac{m}{C} + \frac{2m}{\beta^4 C} + \frac{2m}{C\beta^5} \leqslant \beta^2 m$$

if $C \geqslant 3/\beta^7$, as claimed. □

We next make the key observation that the set S contains all the information we need to recover the final set A produced by the algorithm.

Claim 3. *The set A is uniquely determined by the set S of selected elements.*

Proof. This follows because all steps of the Main Algorithm are deterministic, and every element of I which we need to observe is placed in S. Indeed, in Case 1 we observe only that $v_i \in I$, and that the elements $v_1, \dots, v_{i-1} \notin I$. Since $v_i \in S$ and $v_1 \dots, v_{i-1} \notin S$, this can be deduced from S. In Case 2, the set Z does not depend on I. If at most $d-1$ elements of Z are in S, then we are in Case 2(a) and the remaining elements of Z are in X; otherwise, we are in Case 2(b) and the first d elements of $S \cap Z$ (in the order on $V(\mathcal{H}_n)$) form the set T. Thus, inductively, we see that at each stage of the algorithm, the set A is determined by the set S. □

After all this preparation, we are ready to prove Theorem 4.1.

Proof of Theorem 4.1. Let $\mathcal{H} = (\mathcal{H}_n)_{n \in \mathbb{N}}$ be an $(\alpha, \mathcal{B})$-stable sequence of 3-uniform hypergraphs as in the statement of the theorem, let $\delta > 0$ be arbitrary, and choose $\gamma = \gamma(\alpha, \delta) > 0$ to be sufficiently small. Since $\mathcal{H}$ is $(\alpha, \mathcal{B})$-stable, there exists $\beta > 0$ such that if $|I| \geqslant (\alpha - 2\beta)n$, then either $|I \setminus B| < \gamma n$ for some $B \in \mathcal{B}_n$, or I is not an independent set in $\mathcal{H}_n$.

In particular, note that if $\gamma < \delta/(\alpha - 2\beta)$, then either $m \leqslant (\alpha - 2\beta)\, n$ or $\mathrm{SF}_{\geqslant}^{(\delta)}(\mathcal{H}_n, \mathcal{B}_n, m)$ is empty. We choose such a β sufficiently small, set $C = 3/\beta^7$, and choose $\varepsilon = \varepsilon(\beta) > 0$ to be sufficiently small. Finally, let n be sufficiently large.

Applying the Main Algorithm to each independent set $I \in \mathrm{SF}_{\geqslant}^{(\delta)}(\mathcal{H}_n, \mathcal{B}_n, m)$, that is, to every independent set in $\mathcal{H}_n$ such that $|I| = m$ and $|I \setminus B| \geqslant \delta m$ for every $B \in \mathcal{B}_n$, we obtain (for each such I) a pair (A, S) such that $S \subseteq I \subseteq A \cup S$. There are two cases to deal with, corresponding to the two possibilities that can occur at the end of the Main Algorithm. We first show that if $|A \setminus B| \leqslant \gamma n$ for some $B \in \mathcal{B}_n$ then a much stronger bound holds.

Claim 4. *There are at most $\delta^m |\mathcal{B}_n| \binom{\|\mathcal{B}_n\|}{m}$ sets $I \in \mathrm{SF}_{\geqslant}^{(\delta)}(\mathcal{H}_n, \mathcal{B}_n, m)$ such that the Main Algorithm ends because $|A \setminus B| \leqslant \gamma n$ for some $B \in \mathcal{B}_n$.*

Proof. We claim first that the number of such sets I is at most

$$\sum_{B \in \mathcal{B}_n} \sum_{t=0}^{\beta^2 m} \sum_{r \geqslant \delta m} \binom{n}{t} \binom{\gamma n}{r - t} \binom{\|\mathcal{B}_n\|}{m - r}. \tag{4}$$

Indeed, let S and A be the selected and available sets at the end of the algorithm, set $t = |S|$, and recall that $t \leqslant \beta^2 m$ by Claim 2. We have at most $\binom{n}{t}$ choices for S and, by Claim 3, the set S determines the set A. Let $B \in \mathcal{B}_n$ be such that $|A \setminus B| \leqslant \gamma n$ and recall that $|I \setminus B| \geqslant \delta m$ by our assumption on I. Thus we must choose the set $B \in \mathcal{B}_n$, at least $\delta m - t$ elements of $A \setminus B$, and the remaining elements from B.

Note that $t \leqslant \delta m/2$ by our choice of β and so either $m \leqslant (2\gamma/\delta) n$ or the number of choices for I is zero. Since $\|B_n\| \geqslant \alpha n$ and γ is small, it follows that the summand in (4) is maximized exactly when $r = \delta m$. Now, using the inequalities $\binom{n}{k} \leqslant \left(\frac{en}{k}\right)^k$ and

$$\binom{a}{b - c} \leqslant \left(\frac{b}{a - b}\right)^c \binom{a}{b}, \tag{5}$$

which holds for every $a > b > c \geqslant 0$, and since $t \leqslant \delta m/2$, $m \leqslant (2\gamma/\delta) n \leqslant (\alpha/2) n$ and $\|\mathcal{B}_n\| \geqslant \alpha n$, we can bound each summand in (4) from above by

$$\left(\frac{en}{t}\right)^t \left(\frac{2e\gamma n}{\delta m}\right)^{\delta m - t} \left(\frac{m}{\alpha n - m}\right)^{\delta m} \binom{\|\mathcal{B}_n\|}{m}.$$

Since $t \leqslant \delta m/2$ and $t \mapsto (c/t)^t$ is increasing on $(0, c/e)$, this is at most

$$\left(\frac{\delta m}{2\gamma t}\right)^t \left(\frac{2e\gamma n}{\delta m} \cdot \frac{2m}{\alpha n}\right)^{\delta m} \binom{\|\mathcal{B}_n\|}{m} \leqslant \left(\frac{1}{\gamma}\right)^{\delta m/2} \left(\frac{4e\gamma}{\alpha\delta}\right)^{\delta m} \binom{\|\mathcal{B}_n\|}{m} \leqslant \delta^{2m} \binom{\|\mathcal{B}_n\|}{m}$$

if $\gamma \leqslant (\alpha\delta/4e)^2 \cdot \delta^{4/\delta}$. Since $m^2 \cdot \delta^{2m} \leqslant \delta^m$, the claim follows. □

Finally, we deal with the case in which $|A| \leqslant (\alpha - \beta)n$ for some $B \in \mathcal{B}_n$.

Claim 5. *There are at most $2^{-\varepsilon m} \binom{\|\mathcal{B}_n\|}{m}$ sets $I \in \mathrm{SF}_{\geqslant}^{(\delta)}(\mathcal{H}_n, \mathcal{B}_n, m)$ such that the Main Algorithm ends because $|A| \leqslant (\alpha - \beta)n$.*

Proof. As in the previous claim, we have $t = |S| \leqslant \beta^2 m$, by Claim 2, and the set S determines the set A, by Claim 3. Thus, the number of choices for I is at most

$$\sum_{t=0}^{\beta^2 m} \binom{n}{t}\binom{(\alpha-\beta)n}{m-t}. \tag{6}$$

Now, recall that either $m \leqslant (\alpha - 2\beta)\, n$ or $\mathrm{SF}^{(\delta)}_{\geqslant}(\mathcal{H}_n, \mathcal{B}_n, m)$ is empty. Thus, estimating each summand in (6) as in the proof of Claim 4, we obtain

$$\binom{n}{t}\binom{(\alpha-\beta)n}{m-t} \leqslant \left(\frac{en}{t}\right)^t \left(\frac{m}{(\alpha-\beta)n - m}\right)^t \binom{(\alpha-\beta)n}{m} \leqslant \left(\frac{em}{\beta t}\right)^t \binom{(\alpha-\beta)n}{m}.$$

Now, using the inequality $\binom{b}{c} \leqslant \left(\frac{b}{a}\right)^c \binom{a}{c}$, which is valid for all $a > b > c \geqslant 0$, and recalling that $t \leqslant \beta^2 m$ and that $t \mapsto (c/t)^t$ is increasing on $(0, c/e)$, we get

$$\left(\frac{em}{\beta t}\right)^t \binom{(\alpha-\beta)n}{m} \leqslant \left(\frac{e}{\beta^3}\right)^{\beta^2 m} \left(\frac{\alpha-\beta}{\alpha}\right)^m \binom{\alpha n}{m} \leqslant \left(\frac{e}{\beta^3}\right)^{\beta^2 m} e^{-\beta m/\alpha} \binom{\alpha n}{m}.$$

Since $\|B_n\| \geqslant \alpha n$, the right-hand side is at most $\frac{1}{m} \cdot 2^{-\varepsilon m} \binom{\|\mathcal{B}_n\|}{m}$ if $\beta > 0$ and $\varepsilon = \varepsilon(\beta) > 0$ are sufficiently small, as required. $\square$

Combining Claims 4 and 5, we obtain Theorem 4.1. $\square$

5. Janson argument

In this section, we shall complete the proof of Theorem 2.2 by showing that, under certain conditions, almost all independent (i.e., sum-free) sets I of size m in $\mathcal{H}_n$ either satisfy $I \subseteq B$ for some $B \in \mathcal{B}_n$, or $|I \setminus B| \geqslant \delta m$ for every $B \in \mathcal{B}_n$. The key properties of $\mathcal{H}$ which we will use are that $\Delta_2(\mathcal{H}_n) = O(1)$, and that $\delta(\mathcal{H}_n, \mathcal{B}_n) = \Omega(n)$; our key tool will be Janson's inequality. An argument similar to that presented in this section was used in [6] to study sum-free sets in random subsets of Abelian groups.

Given a hypergraph $\mathcal{H}_n$, a family of sets $\mathcal{B}_n$ and $\delta > 0$, we define

$$\mathrm{SF}^{(\delta)}_{\leqslant}(\mathcal{H}_n, \mathcal{B}_n, m) := \Big\{ I \in \mathrm{SF}(\mathcal{H}_n, m) : \, |I \setminus B| \leqslant \delta m \text{ for some } B \in \mathcal{B}_n \Big\}.$$

The following proposition shows that, if $\delta > 0$ is sufficiently small, then almost all independent sets in $\mathrm{SF}^{(\delta)}_{\leqslant}(\mathcal{H}_n, \mathcal{B}_n, m)$ are contained in some $B \in \mathcal{B}_n$. We write 2^B to denote the power set of B, i.e., the family of all subsets of B.

Proposition 5.1. *Let $\alpha > 0$, let $\mathcal{H} = (\mathcal{H}_n)_{n\in\mathbb{N}}$ be a sequence of 3-uniform hypergraphs with $\Delta_2(\mathcal{H}_n) = O(1)$, and let $\mathcal{B} = (\mathcal{B}_n)_{n\in\mathbb{N}}$ be a family of sets with $\|\mathcal{B}_n\| \geqslant \alpha n$. For every $\beta > 0$, there exists constants $\delta > 0$ and $C_0 > 0$ such that the following holds. If $\delta(\mathcal{H}_n, \mathcal{B}_n) \geqslant \beta n$ and $C \geqslant C_0$, then*

$$\Big| \mathrm{SF}^{(\delta)}_{\leqslant}(\mathcal{H}_n, \mathcal{B}_n, m) \setminus \bigcup_{B \in \mathcal{B}_n} 2^B \Big| \leqslant n^{-C} |\mathcal{B}_n| \binom{\|\mathcal{B}_n\|}{m}$$

for every $m \geqslant C\sqrt{n \log n}$.

Note that δ and C_0 in the statement of Proposition 5.1 may depend on $\mathcal{H}$, $\mathcal{B}$, α and β. We begin by recalling the Janson inequalities, and some basic facts about the hypergeometric distribution.

5.1. **The hypergeometric distribution.** The following well-known inequality (see [20, page 35], for example) allows us to deduce bounds in the hypergeometric distribution from results on product measure. For completeness we give a proof.

Lemma 5.2 (Pittel's inequality). *Let $m, n \in \mathbb{N}$, and set $p = m/n$. For any property $\mathcal{Q}$ on $[n]$ we have*

$$\mathbb{P}\big(\mathcal{Q} \textit{ holds for a random } m\textit{-set}\big) \leqslant 3\sqrt{m} \cdot \mathbb{P}\big(\mathcal{Q} \textit{ holds for a random } p\textit{-subset of } [n]\big).$$

Moreover, if $\mathcal{Q}$ is monotone decreasing and $m \leqslant n-1$, then

$$\mathbb{P}\big(\mathcal{Q} \textit{ holds for a random } m\textit{-set}\big) \leqslant C \cdot \mathbb{P}\big(\mathcal{Q} \textit{ holds for a random } p\textit{-subset of } [n]\big)$$

for some absolute constant $C > 0$.

Proof. For the first part, simply note that a random p-subset of $[n]$ has size $m = pn$ with probability at least $1/(3\sqrt{m})$. If $\mathcal{Q}$ is monotone decreasing, say, then we apply the 'Local LYM inequality' to $\mathcal{Q}_m$, the set of m-sets in $\mathcal{Q}$, and deduce that

$$\mathbb{P}\big(\mathcal{Q} \text{ holds for a random } k\text{-set}\big) \geqslant \mathbb{P}\big(\mathcal{Q} \text{ holds for a random } m\text{-set}\big)$$

for every $k \leqslant m$. It is well-known that the median of the binomial distribution lies between $\lfloor pn \rfloor$ and $\lceil pn \rceil$, and if $m \leqslant n-1$ then it is easy to see that $\mathrm{Bin}(n,p) = \lceil pn \rceil$ has probability at most $(1-1/n)^{n-1} \to 1/e$ as $n \to \infty$. Thus, if $m \leqslant n-1$ and n is sufficiently large, then a random p-subset of $[n]$ has size at most $m = pn$ with probability at least $1/2 - 1/e + o(1)$ as $n \to \infty$, and the result follows. $\square$

The following result is an easy corollary of Janson's inequality (see [4, 20]), combined with Pittel's inequality.

Lemma 5.3 (Hypergeometric Janson Inequality). *Suppose that $\{U_i\}_{i \in I}$ is a family of subsets of an n-element set X and let $m \in \{0, \ldots, n\}$. Let*

$$\mu = \sum_{i \in I} (m/n)^{|U_i|} \quad \textit{and} \quad \Delta = \sum_{i \sim j} (m/n)^{|U_i \cup U_j|},$$

where the second sum is over ordered pairs (i,j) such that $i \neq j$ and $U_i \cap U_j \neq \emptyset$. Let R be a uniformly chosen random m-subset of X. Then

$$\mathbb{P}\big(U_i \nsubseteq R \textit{ for all } i \in I\big) \leqslant C \cdot \max\left\{ e^{-\mu/2}, e^{-\mu^2/(2\Delta)} \right\},$$

where $C > 0$ is the constant in Pittel's inequality.

We now return to the proof of Proposition 5.1.

5.2. **Proof of Proposition 5.1.** We begin by partitioning $\mathrm{SF}^{(\delta)}_{\leqslant}(\mathcal{H}_n, \mathcal{B}_n, m)$ according to the set $B \in \mathcal{B}_n$ such that $|I \setminus B| \leqslant \delta m$, and also according to the set $S = I \setminus B$. (Technically there could be more than one such set B, so in fact this might be a cover, rather than a partition.) Set

$$I(B,S) \,:=\, \Big| \Big\{ I \in \mathrm{SF}(\mathcal{H}_n, m) : \; I \setminus B = S \Big\} \Big|.$$

We shall prove the following lemma.

Lemma 5.4. *Let $\mathcal{H} = (\mathcal{H}_n)_{n \in \mathbb{N}}$ be a sequence of 3-uniform hypergraphs with $\Delta_2(\mathcal{H}_n) = O(1)$. For every sufficiently small $\beta > 0$, there exists a $C_0 > 0$ such that the following holds. Let $C \geqslant C_0$, let $B \subseteq [n]$ with $\delta(\mathcal{H}_n, B) \geqslant \beta n$, and let $S \subseteq [n] \setminus B$. Then, writing $k = |S|$,*

$$I(B,S) \,\leqslant\, \Big(|B|^{-5Ck} + e^{-\beta^3 m} \Big) \binom{|B|}{m-k}$$

for every $m \geqslant C\sqrt{n \log n}$.

In order to prove Lemma 5.4, we shall apply the following lemma to the Cayley graph of S, restricted to B. The lemma is a straightforward consequence of the Hypergeometric Janson's inequality.

Lemma 5.5. *For every $\beta > 0$, there exists a constant $C_0 > 0$ such that the following holds. Let $\mathcal{G}$ be a graph on n vertices with maximum degree at most d. If*

$$e(\mathcal{G}) \,\geqslant\, 4\beta d n,$$

then for every $C \geqslant C_0$,

$$I(\mathcal{G}, m) \,\leqslant\, \Big(n^{-Cd} + e^{-\beta m} \Big) \binom{n}{m}$$

for every $m \geqslant C\sqrt{n \log n}$.

Proof. Let $\{U_i\}_{i \in I}$ be the collection of pairs of vertices which span an edge of $\mathcal{G}$, so $U_i \not\subseteq R$ for all $i \in I$ if and only if R is an independent set in $\mathcal{G}$. It is easy to see that, letting μ and Δ to be the quantities defined in the statement of Lemma 5.3,

$$\mu \,=\, e(\mathcal{G}) \frac{m^2}{n^2} \quad \text{and} \quad \Delta \,\leqslant\, \binom{d}{2} \left(\frac{2e(\mathcal{G})}{d} \right) \left(\frac{m}{n} \right)^3 \,\leqslant\, e(\mathcal{G}) \frac{dm^3}{n^3}.$$

Thus, by our bounds on $e(\mathcal{G})$ and m, and assuming $C \geqslant 4/\beta$,

$$\mu \,\geqslant\, 4Cd \log n \quad \text{and} \quad \frac{\mu^2}{\Delta} \,\geqslant\, e(\mathcal{G}) \frac{m}{dn} \,\geqslant\, 4\beta m.$$

By the Hypergeometric Janson Inequality,

$$\begin{aligned} I(\mathcal{G}, m) \Big/ \binom{n}{m} \;&\leqslant\; C \cdot \max\Big\{ e^{-\mu/2}, e^{-\mu^2/(2\Delta)} \Big\} \\ &\leqslant\; C \cdot \max\Big\{ n^{-2Cd}, e^{-2\beta m} \Big\} \,\leqslant\, \max\Big\{ n^{-Cd}, e^{-\beta m} \Big\}, \end{aligned}$$

as required. $\square$

Recall that, given $\mathcal{H}_n$, the Cayley graph $\mathcal{G}_S$ of S is defined to be the graph with vertex set $V(\mathcal{H}_n)$ and edge set

$$E(\mathcal{G}_S) \, = \, \Big\{ \{u,v\} \subseteq V(\mathcal{H}_n) : \, \{u,v,w\} \in \mathcal{H}_n \text{ for some } w \in S \Big\}.$$

In order to apply Lemma 5.5, we shall need the following easy property of the Cayley graph.

Observation 5.6. $\Delta(\mathcal{G}_S) \leqslant |S| \Delta_2(\mathcal{H}_n)$.

We can now easily deduce Lemma 5.4 from Lemma 5.5 and Observation 5.6.

Proof of Lemma 5.4. If I is an independent set in $\mathcal{H}_n$ containing S, then $I \setminus S$ is an independent set in $\mathcal{G}_S$, so

$$I\big(B, S\big) \, \leqslant \, I\big(\mathcal{G}_S[B], m-k\big),$$

where $k = |S|$. Choose $\beta > 0$ sufficiently small so that $\Delta_2(\mathcal{H}_n) \leqslant 1/(2\beta)$, recall that $\delta(\mathcal{H}_n, B) \geqslant \beta n$, note that $d = \Delta(\mathcal{G}_S) \leqslant |S|\Delta_2(\mathcal{H}_n) \leqslant |S|/(2\beta)$, and observe that therefore

$$e\big(\mathcal{G}_S[B]\big) \, \geqslant \, \frac{\beta|S|n}{\Delta_2(\mathcal{H}_n)} \, \geqslant \, 2\beta^2|S| \cdot |B| \geqslant 4\beta^3 d|B|.$$

Thus, by Lemma 5.5, if $\beta < 1/10$ then $d \geqslant 5|S| = 5k$ and

$$I\big(\mathcal{G}_S[B], m-k\big) \, \leqslant \, \Big(|B|^{-5Ck} + e^{-\beta^3 m} \Big) \binom{|B|}{m-k},$$

for every $m \geqslant C\sqrt{n \log n}$, as required. $\square$

Finally, let us deduce Proposition 5.1 from Lemma 5.4.

Proof of Proposition 5.1. Summing over all sets $B \in \mathcal{B}_n$ and subsets $S \subseteq [n] \setminus B$, and applying Lemma 5.4, we have

$$\begin{aligned} \bigg| \mathrm{SF}^{(\delta)}_{\leqslant}(\mathcal{H}_n, \mathcal{B}_n, m) \setminus \bigcup_{B \in \mathcal{B}_n} 2^B \bigg| \; & \leqslant \; \sum_{B \in \mathcal{B}_n} \sum_{k=1}^{\delta m} \sum_{S \subseteq [n] \setminus B \, : \, |S| = k} I(B,S) \\ & \leqslant \; |\mathcal{B}_n| \sum_{k=1}^{\delta m} \binom{n}{k} \Big(n^{-4(C+k)} + e^{-\beta^3 m} \Big) \binom{\|\mathcal{B}_n\|}{m-k}, \end{aligned}$$

for every $m \geqslant C\sqrt{n \log n}$, since $\delta(\mathcal{H}_n, \mathcal{B}_n) \geqslant \beta n$ and $\Delta_2(\mathcal{H}_n) = O(1)$ together imply that $|B| = \Theta(n)$ for every $B \in \mathcal{B}_n$. We consider three cases.

Case 1: If $n^{-4(C+k)} \geqslant e^{-\beta^3 m}$, then

$$\binom{n}{k} \Big(n^{-4(C+k)} + e^{-\beta^3 m} \Big) \binom{\|\mathcal{B}_n\|}{m-k} \, \leqslant \, n^{-2C} \binom{\|\mathcal{B}_n\|}{m},$$

since $\binom{\|\mathcal{B}_n\|}{m-k} \leqslant \binom{n}{k} \binom{\|\mathcal{B}_n\|}{m}$.

Case 2: If $n^{-4(C+k)} \leqslant e^{-\beta^3 m}$ and $m \leqslant \alpha n/2$, then by (5) we have

$$\binom{\|\mathcal{B}_n\|}{m-k} \, \leqslant \, \left(\frac{m}{\alpha n - m} \right)^k \binom{\|\mathcal{B}_n\|}{m} \, \leqslant \, \left(\frac{2m}{\alpha n} \right)^k \binom{\|\mathcal{B}_n\|}{m},$$

since $\|\mathcal{B}_n\| \geqslant \alpha n$. Thus, using the bound $\binom{n}{k} \leqslant \left(\frac{en}{k}\right)^k$, we have

$$\binom{n}{k}\Big(n^{-4(C+k)} + e^{-\beta^3 m}\Big)\binom{\|\mathcal{B}_n\|}{m-k} \leqslant 2 \cdot e^{-\beta^3 m}\left(\frac{2em}{\alpha k}\right)^k \binom{\|\mathcal{B}_n\|}{m} \leqslant e^{-\beta^3 m/2}\binom{\|\mathcal{B}_n\|}{m},$$

if $\delta = \delta(\alpha, \beta) > 0$ is sufficiently small, since $k \leqslant \delta m$.

Case 3: If $\|\mathcal{B}_n\|^{-4(C+k)} \leqslant e^{-\beta^3 m}$ and $m \geqslant \alpha n/2$, then we again use the (trivial) bound $\binom{\|\mathcal{B}_n\|}{m-k} \leqslant \binom{n}{k}\binom{\|\mathcal{B}_n\|}{m}$, to obtain

$$\binom{n}{k}\Big(n^{-4(C+k)} + e^{-\beta^3 m}\Big)\binom{\|\mathcal{B}_n\|}{m-k} \leqslant 2e^{-\beta^3 m}\binom{n}{k}^2 \binom{\|\mathcal{B}_n\|}{m} \leqslant e^{-\beta^3 m/2}\binom{\|\mathcal{B}_n\|}{m},$$

if $\delta = \delta(\alpha, \beta) > 0$ is sufficiently small, since $\binom{n}{k} \leqslant \binom{2m/\alpha}{k} \leqslant \left(\frac{2e}{\alpha\delta}\right)^{\delta m} \leqslant e^{-\beta^3 m/6}$ for $k \leqslant \delta m$.

Since $e^{-\beta^3 m/2} \ll n^{-2C}$ for $m \geqslant C\sqrt{n \log n}$, the claimed bound follows. □

We finish this section by observing that Theorem 4.1 and Proposition 5.1 together imply Theorem 2.2.

Proof of Theorem 2.2. Let $\mathcal{H} = (\mathcal{H}_n)_{n\in\mathbb{N}}$ be a sequence of 3-uniform hypergraphs which is $(\alpha, \mathcal{B})$-stable, where $\mathcal{B} = (\mathcal{B}_n)_{n\in\mathbb{N}}$ is a family of sets, and $\alpha > 0$. Suppose that $\alpha(\mathcal{H}_n) \geqslant \|\mathcal{B}_n\| \geqslant \alpha n$, and that there exists $\beta > 0$ such that $e(\mathcal{H}_n) \geqslant \beta n^2$, $\Delta_2(\mathcal{H}_n) \leqslant 1/\beta$, $|\mathcal{B}_n| \leqslant n^{1/\beta}$ and $\delta(\mathcal{H}_n, \mathcal{B}_n) \geqslant \beta n$ for every $n \in \mathbb{N}$. Let $\delta = \delta(\beta) > 0$ be sufficiently small, and let $C = C(\beta, \delta) > 0$ be sufficiently large. We claim that if

$$m \geqslant C\sqrt{n \log n},$$

then almost every independent set in $\mathcal{H}_n$ of size m is a subset of some $B \in \mathcal{B}_n$.

Indeed, by Theorem 4.1, the number of independent sets I in $\mathcal{H}_n$ of size m for which $|I \setminus B| \geqslant \delta m$ for every $B \in \mathcal{B}_n$ is at most

$$\Big(2^{-\varepsilon m} + \delta^m |\mathcal{B}_n|\Big)\binom{\|\mathcal{B}_n\|}{m}$$

for some $\varepsilon > 0$ and by Proposition 5.1, the number of such sets for which $1 \leqslant |I \setminus B| \leqslant \delta m$ for some $B \in \mathcal{B}_n$ is at most

$$n^{-C}|\mathcal{B}_n|\binom{\|\mathcal{B}_n\|}{m}.$$

Since $|\mathcal{B}_n| \leqslant n^{1/\beta}$, $C > 1/\beta$, and $\alpha(\mathcal{H}_n) \geqslant \|\mathcal{B}_n\|$, the result follows. □

6. Abelian groups of Type I

In this section, we shall use Theorem 2.2 to prove Theorem 1.1 for all $q > 2$. We remark that the proof below can also be adapted to cover the case $q = 2$; however, since we shall give a different proof of the case $q = 2$ in Section 7, we leave the details to the reader. (If $\mathcal{H}_n$ denotes the hypergraph that encodes Schur triples in a group G of even order n and $\mathcal{B}_n$ denotes the collection of maximum-size sum-free subsets of G, then it is not always true that

$\Omega(\mathcal{H}_n, \mathcal{B}_n) = \Omega(n)$. This problem can be easily overcome by considering triples of the form $(x, x, 2x)$, cf. the proof of the 1-statement in [6, Theorem 1.2].)

In order to prove that our hypergraph is $(\alpha, \mathcal{B})$-stable, we shall use the following result (see [6, Corollary 2.8]), which follows immediately by combining results of Green and Ruzsa [18] and Lev, Łuczak, and Schoen [26]. Let $\mathrm{SF}_0(G)$ denote the collection of maximal-size sum-free subsets of G and recall that each $B \in \mathrm{SF}_0(G)$ has size $\mu(G)|G|$.

Proposition 6.1. *Let G be a finite Abelian group of Type $I(q)$, where $q \equiv 2 \pmod 3$ and let $0 < \gamma < \gamma(q)$ and $0 < \beta < \beta_0(\gamma, q)$ be sufficiently small. Let $A \subseteq G$, and suppose that*

$$|A| \geqslant \big(\mu(G) - \beta\big)|G|.$$

Then one of the following holds:

(*a*) *$|A \setminus B| \leqslant \gamma|G|$ for some $B \in \mathrm{SF}_0(G)$.*

(*b*) *A contains at least $\beta|G|^2$ Schur triples.*

We shall also use the following classification of extremal sum-free sets for Type I groups.

Theorem 6.2 (Diananda and Yap [11])**.** *Let G be a finite Abelian group of Type $I(q)$, where $q \equiv 2 \pmod 3$. Then every $B \in \mathrm{SF}_0(G)$ is a union of cosets of some subgroup H of G of index q, B/H is an arithmetic progression in G/H, and $B \cup (B + B) = G$.*

In other words, for every $B \in \mathrm{SF}_0(G)$, there exists a homomorphism $\varphi \colon G \to \mathbb{Z}_q$ such that $B = \varphi^{-1}(\{k+1, \ldots, 2k+1\})$, where $q = 3k + 2$.

Combining Theorem 6.2 with Kronecker's Decomposition Theorem, we easily obtain the following well-known corollary.

Corollary 6.3. *Let G be an arbitrary group of Type I. Then $|\mathrm{SF}_0(G)| \leqslant |G|$.*

It is now straightforward to deduce Theorem 1.1 from Theorem 2.2, Proposition 6.1, and Corollary 6.3.

Proof of Theorem 1.1 for $q \neq 2$. Let $q \equiv 2 \pmod 3$ be an odd prime, let $C = C(q)$ be sufficiently large, and let G_n be an Abelian group of Type I(q), with $|G_n| = n$. We shall show that if $m \geqslant C(q)\sqrt{n \log n}$, then almost every sum-free set of size m in G_n is contained in a member of $\mathrm{SF}_0(G)$.

We begin by choosing an infinite set $X \subseteq \mathbb{N}$ such that, for every $n \in X$, q is the smallest prime divisor of n with $q \equiv 2 \pmod 3$. For each $n \in X$, let G_n be an Abelian group of Type I(q), with $|G_n| = n$, and define $\mathcal{H} = (\mathcal{H}_n)_{n \in X}$ to be the sequence of hypergraphs on vertex set $V(\mathcal{H}_n) = G_n$ which encodes Schur triples. To be precise, let $V(\mathcal{H}_n) = G_n$, let $\{x, y, z\} \in \binom{G_n}{3}$ be an edge of $\mathcal{H}_n$ whenever $x + y = z$, and observe that every sum-free subset of G_n is an independent set in $\mathcal{H}_n$.[4] Let $\mathcal{B}_n = \mathrm{SF}_0(G_n)$, the collection of maximum size sum-free subsets of G_n, and recall that $|\mathcal{B}_n| \leqslant n$, by Corollary 6.3.

We claim that $\mathcal{H}$ and $\mathcal{B}$ satisfy the conditions of Theorem 2.2. Indeed, $\mathcal{H}_n$ is 3-uniform, has $\Theta(n^2)$ edges, and satisfies $\Delta_2(\mathcal{H}_n) = 3$. Setting $\alpha = \mu(G)$, we have $\alpha(\mathcal{H}_n) = \|\mathcal{B}_n\| = \alpha n$

[4]But not vice-versa, since $\mathcal{H}_n$ does not contain the Schur triples in G_n of the form $(x, x, 2x)$. Thus, by bounding $I(\mathcal{H}_n, m)$ we are in fact proving a statement which is slightly stronger than Theorem 1.1.

and $|\mathcal{B}_n| \leqslant n$, as observed above. Moreover, the statement that $\mathcal{H}$ is $(\alpha, \mathcal{B})$-stable is exactly Proposition 6.1. Thus it will suffice to show that $\delta(\mathcal{H}_n, \mathcal{B}_n) = \Omega(n)$.

Claim. *For each $B \in \mathrm{SF}_0(G)$ and every $x \in G \setminus B$,*

$$\left| \left\{ \{y, z\} \in \binom{B}{2} : x = y + z \right\} \right| \geqslant \frac{n}{2q} - \frac{1}{2}.$$

Proof of claim. Let $B \in \mathrm{SF}_0(G)$ and let $x \in G \setminus B$. By Theorem 6.2, there exists a subgroup H of G of index q such that B is a union of cosets of H and $B \cup (B + B) = G$. It follows that $x = y + z$ for some $y, z \in B$, and that $y + h, z - h \in B$ for every $h \in H$. Thus,

$$\{y + h, z - h\} \in C(x) := \left\{ \{y, z\} \in \binom{B}{2} : x = y + z \right\}$$

whenever $h \in H$ and $y + h \neq z - h$. Moreover, since $|G|$ is odd, there is at most one $h \in H$ such that $2h = z - y$, so $|C(x)| \geqslant (|H| - 1)/2 = n/2q - 1/2$, as required. □

Thus the pair $(\mathcal{H}, \mathcal{B})$ satisfies the conditions of Theorem 2.2 and hence if $C(q)$ is sufficiently large and $m \geqslant C(q)\sqrt{n \log n}$, then almost every sum-free set of size m in G_n is contained in some $B \in \mathcal{B}_n$, as required.

Finally, let us deduce that if G is an Abelian group of Type I(q), and $m \geqslant C(q)\sqrt{n \log n}$, then

$$|\mathrm{SF}(G, m)| \;=\; \frac{1}{2} \cdot \big(\#\{\text{elements of } G \text{ of order } q\} + o(1) \big) \binom{\mu(G)n}{m}.$$

Indeed, it suffices to observe that $|\mathrm{SF}_0(G)| = \#\{\text{elements of } G \text{ of order } q\}/2$, by Theorem 6.2, and that each pair $B, B' \in \mathrm{SF}_0(G)$ intersect in at most $(1 - 1/q)\mu(G)|G|$ elements. The result now follows from some easy counting. □

7. Abelian groups of even order

In this section, we shall prove the following theorem, which implies Theorem 1.1 in the case $q = 2$. We shall use Theorem 1.3 and some ideas from Section 5, but otherwise this section is self-contained. In particular, we shall not use Proposition 6.1 and thus we give a new proof of the main theorem of [26] and [33].

Theorem 7.1. *If G is an Abelian group of order n, then*

$$|\mathrm{SF}(G, m)| \;=\; \big(\#\{\text{elements of } G \text{ of order } 2\} + o(1) \big) \binom{n/2}{m}$$

for every $m \geqslant 4\sqrt{n \log n}$.

We remark that we shall prove the theorem for *all* finite Abelian groups, not just those of even order. We begin by partitioning the collection of sum-free sets into two pieces. Given an Abelian group G, let

$$\mathrm{SF}^{(\delta)}_{\leqslant}(G, m) \;:=\; \Big\{ I \in \mathrm{SF}(G, m) : \; |I \cap H| \leqslant \delta m \text{ for some } H \leqslant G \text{ with } [G : H] = 2 \Big\},$$

and

$$\mathrm{SF}^{(\delta)}_{\geqslant}(G,m) \,:=\, \Big\{ I \in \mathrm{SF}(G,m) :\, |I \cap H| \geqslant \delta m \text{ for every } H \leqslant G \text{ with } [G:H] = 2 \Big\}.$$

Note that if $|G|$ is odd then $\mathrm{SF}^{(\delta)}_{\leqslant}(G,m)$ is empty. We shall prove the following proposition using the method of Section 5.

Proposition 7.2. *Let G be an Abelian group of order n, and let $\delta > 0$ be sufficiently small. Then*

$$|\mathrm{SF}^{(\delta)}_{\leqslant}(G,m)| \,\leqslant\, \big(\#\big\{ \textit{elements of } G \textit{ of order } 2 \big\} + o(1) \big) \cdot \binom{n/2}{m}$$

for every $m \geqslant 4\sqrt{n \log n}$.

For sets in $\mathrm{SF}^{(\delta)}_{\geqslant}(G,m)$, i.e., far from any $H \leqslant G$ of index 2, we shall prove the following stronger bound using Theorem 1.3.

Proposition 7.3. *Let G be an Abelian group of order n, and let $\delta > 0$. If $\varepsilon = \varepsilon(\delta) > 0$ is sufficiently small and $C = C(\delta)$ is sufficiently large, then*

$$|\mathrm{SF}^{(\delta)}_{\geqslant}(G,m)| \,\leqslant\, 2^{-\varepsilon m} \binom{n/2}{m}$$

for every $m \geqslant C\sqrt{n}$ and every sufficiently large $n \in \mathbb{N}$.

We begin by proving Proposition 7.2. In this section, we shall use a slightly different notion of Cayley graph than that used earlier. Given $S \subseteq G$, define $\mathcal{G}^*_S$ to be the graph with vertex set $G \setminus S$ and edge set $\big\{ xy \colon x - y \in S \big\}$, and note that if I is a sum-free set in G with $S \subseteq I$, then $I \setminus S$ is an independent set in $\mathcal{G}^*_S$.

Proof of Proposition 7.2. Let G be an Abelian group of even order n, let H be a subgroup of G of index 2, and let $S \subseteq H$ satisfy $|S| = k \leqslant \delta m$. Set $\gamma = 1/65$. We claim that for every $m \geqslant 4\sqrt{n \log n}$, there are at most

$$\Big(n^{-4k} + e^{-\gamma m} \Big) \binom{n/2}{m-k} \tag{7}$$

sum-free subsets I of G of order m with $I \cap H = S$.

Observe first that the graph $\mathcal{G}^*_S[G \setminus H]$ is d-regular, where $d = |S \cup (-S)| \in [k, 2k]$. Indeed, for each $x \in G \setminus H$, let

$$N(x) \,=\, \big\{ y \in G \setminus H :\, x - y \in S \text{ or } y - x \in S \big\}.$$

Since $S \subseteq H$, it follows that $x - S$ and $x + S$ are in $G \setminus H$, and hence $|N(x)| = |S \cup (-S)|$, as claimed. Since $|S| = k$, we have $k \leqslant d \leqslant 2k$.

Now, by the Hypergeometric Janson Inequality, Lemma 5.3, there are at most

$$C \cdot \max\Big\{ e^{-km^2/4n}, e^{-m/64} \Big\} \binom{n/2}{m-k} \,\leqslant\, \Big(n^{-4k} + e^{-\gamma m} \Big) \binom{n/2}{m-k},$$

independent sets of size $m-k$ in $\mathcal{G}_S^*[G\setminus H]$. This follows because $k \leqslant \delta m$, so

$$\mu \,\geqslant\, \binom{kn}{4}\binom{(m-k)^2}{(n/2)^2} \,\geqslant\, \frac{km^2}{2n} \quad\text{and}\quad \Delta \,\leqslant\, \binom{2k}{2}\frac{n}{2}\binom{(m-k)^3}{(n/2)^3} \,\leqslant\, \frac{8k^2m^3}{n^2},$$

and $m \geqslant 4\sqrt{n\log n}$. Since each sum-free subset $I \subseteq G$ induces an independent set in $\mathcal{G}_S^*[G\setminus H]$, then (7) follows.

Finally, summing (7) over subgroups H and sets S, we obtain

$$\begin{aligned} |\mathrm{SF}_{\leqslant}^{(\delta)}(G,m)| \;&\leqslant\; \#\big\{H \leqslant G\colon [G:H]=2\big\} \sum_{k=0}^{\delta m} \binom{n}{k}\Big(n^{-4k}+e^{-\gamma m}\Big)\binom{n/2}{m-k} \\ &\leqslant\; \bigg(\#\big\{\text{elements of } G \text{ of order } 2\big\} + O\bigg(\frac{1}{n^2}\bigg)\bigg)\binom{n/2}{m} \end{aligned} \tag{8}$$

for every $m \geqslant 4\sqrt{n\log n}$. To see the last inequality, observe that the number of subgroups H of index 2 in G is exactly the number of elements of G of order 2 and consider three cases as in the proof of Proposition 5.1. Indeed, if $n^{-4k} \geqslant e^{-\gamma m}$ or $m \geqslant n/4$, then each summand in (8) is at most $\big(n^{-2k}+e^{-\gamma m/2}\big)\binom{n/2}{m}$ by the trivial bound $\binom{n/2}{m-k} \leqslant \binom{n}{k}\binom{n/2}{m}$. But if $n^{-4k} \leqslant e^{-\gamma m}$ and $m \leqslant n/4$, then by (5),

$$\binom{n}{k}\binom{n/2}{m-k} \,\leqslant\, \bigg(\frac{en}{k}\bigg)^k\bigg(\frac{2m}{n-2m}\bigg)^k\binom{n/2}{m} \,\leqslant\, \bigg(\frac{4em}{k}\bigg)^k\binom{n/2}{m} \,\leqslant\, e^{O(\sqrt{\delta}m)}\binom{n/2}{m}$$

since $k \leqslant \delta m$. Thus, if $\delta > 0$ is chosen small enough, then each summand in (8) is at most $e^{-\gamma m/2}\binom{n/2}{m}$, as required. $\square$

We next turn to the proof of Proposition 7.3. We shall divide into two cases: either the smallest eigenvalue $\lambda(I)$ of I (see below) is at most $(\delta-1)|I|$, in which case we shall use some basic facts about characters of finite Abelian groups to show that there are few such sets; or $\lambda(I)$ is larger, in which case we shall find a small subset $S \subseteq I$ such that $\mathcal{G}_S^*$ is a d-regular graph with smallest eigenvalue satisfying $\lambda > (\delta/4-1)d$, and apply Theorem 1.3. We begin with the following key definition.

Definition 7.4 (The smallest eigenvalue of S)**.** Given a finite Abelian group G, and a subset $0 \notin S \subseteq G$, let

$$\lambda(S) \,:=\, \min\big\{\mathrm{Re}(\lambda) :\; A(S)v = \lambda v \text{ for some } v \neq \mathbf{0}\big\},$$

where $\mathrm{Re}(\lambda)$ is the real part of the complex number λ, $A(S)$ is the adjacency matrix of the directed Cayley graph on G, i.e., the $(0,1)$-matrix with $A(x,y)=1$ iff $y-x \in S$, and $\mathbf{0}$ is the zero vector.

Next, we recall some simple properties of characters of finite Abelian groups.

7.1. **Characters of finite Abelian groups.**

Definition 7.5. A *character* of a group G is a homomorphism from G into the multiplicative group of non-zero complex numbers, i.e., a function $\chi\colon G \to \mathbb{C}^*$ such that $\chi(a+b) = \chi(a)\chi(b)$ for all $a,b \in G$.

A character χ is called trivial if $\chi(x) = 1$ for all $x \in G$; we will denote the trivial character by χ_T. The set of all characters of G is denoted by $\hat{G}$. The following statement establishes a relation between the smallest eigenvalue of the matrix $A(S)$ and the characters of G.

Lemma 7.6. *For every $0 \notin S \subseteq G$,*

$$\lambda(S) \;=\; \min\left\{ \mathrm{Re}\left(\sum_{s \in S} \chi(s) \right) \,:\, \chi \in \hat{G} \right\} \;\geqslant\; -|S|.$$

We shall use the following facts about finite Abelian groups in the proof of Lemma 7.6.

Fact 1. *If G is a finite Abelian group of order n, then all its characters take values in the set*

$$U_n \;:=\; \big\{ (\xi_n)^k \colon k \in \{0, \ldots, n-1\} \big\}, \quad \textit{where} \quad \xi_n = e^{2\pi i/n},$$

of nth roots of unity. Moreover, if $\chi \in \hat{G}$ then $\mathrm{range}(\chi) = U_k$ *for some $k = k(\chi)$.*

Fact 2. *$\hat{G}$ is an orthogonal basis of the vector space $\mathbb{C}^G$.*

Proof of Lemma 7.6. Let us start by breaking up the adjacency matrix $A(S)$ into $|S|$ pieces as follows:

$$A(S) = \sum_{s \in S} A_s, \quad \text{where} \quad A_s(x,y) = \begin{cases} 1 & \text{if } \; y - x = s \\ 0 & \text{otherwise.} \end{cases}$$

Thus, for every $s, x \in G$ and $\chi \in \hat{G}$,

$$(A_s \chi)(x) \;=\; \chi(x+s) \;=\; \chi(x)\chi(s) \;=\; (\chi(s)\chi)(x),$$

and so every $\chi \in \hat{G}$ is an eigenvector of each A_s with $\chi(s)$ being the corresponding eigenvalue. Hence, every $\chi \in \hat{G}$ is an eigenvector of $A(S)$, with eigenvalue $\sum_{s \in S} \chi(s)$. Since the characters of G form an orthogonal basis of $\mathbb{C}^G$, it follows that the set of eigenvalues of $A(S)$ is exactly

$$\left\{ \sum_{s \in S} \chi(s) \,:\, \chi \in \hat{G} \right\}.$$

The inequality $\lambda(S) \geqslant -|S|$ follows since $|\chi(s)| = 1$ for every $s \in S$ and $\chi \in \hat{G}$. ∎

Let us note for future reference the following fact from the proof above.

Lemma 7.7. *For every $0 \notin S \subseteq G$, the characters of G form a basis of eigenvectors of the matrix $A(S)$.*

7.2. **Sum-free sets with small smallest eigenvalue.** Using the properties described above, we shall prove the following lemma.

Lemma 7.8. *Let $\delta > 0$ be sufficiently small and let $n \in \mathbb{N}$ be sufficiently large. Then, there exist constants $\varepsilon = \varepsilon(\delta) > 0$ and $C = C(\delta)$ such that, for every $m \geqslant C\sqrt{n}$,*

$$\left| \left\{ I \in \mathrm{SF}^{(\delta)}_{\geqslant}(G, m) \,:\, \lambda(I) \leqslant (\delta - 1)|I| \right\} \right| \;\leqslant\; 2^{-\varepsilon m} \binom{n/2}{m}.$$

Proof. For each character χ of G and each $A \subseteq G$, define $\lambda(A,\chi) = \mathrm{Re}\big(\sum_{x \in A} \chi(x)\big)$. We shall bound the number of $I \in \mathrm{SF}^{(\delta)}_{\geqslant}(G,m)$ such that $\lambda(I,\chi) \leqslant (\delta-1)|I|$ by

$$\frac{2^{-\varepsilon m}}{n}\binom{n/2}{m}.$$

The desired bound will follow since $\lambda(I) = \min_{\chi \in \hat{G}} \lambda(I,\chi)$ and there are at most $|G|$ characters of G. We split into two cases, depending on the number of different values taken by χ.

Case 1. $|\mathrm{range}(\chi)| = 2$.

Since χ is a group homomorphism, it corresponds to a subgroup H of G of index 2, namely, $H = \chi^{-1}(1)$. Since $|I \cap H| \geqslant \delta n$ for every such H, we have

$$\lambda(I,\chi) \,=\, \mathrm{Re}\left(\sum_{x \in I} \chi(x)\right) \,=\, |I \cap H| - |I \setminus H| \,\geqslant\, \big(2\delta - 1\big)|I|$$

and hence in this case, there are no $I \in \mathrm{SF}^{(\delta)}_{\geqslant}(G,m)$ such that $\lambda(I,\chi) \leqslant (\delta-1)|I|$.

Case 2. $|\mathrm{range}(\chi)| \geqslant 3$.

Let $k = |\mathrm{range}(\chi)|$ and recall (from Fact 1) that $\mathrm{range}(\chi) = U_k$, where U_k is the multiplicative group of kth roots of unity. Observe that $|\chi^{-1}(\xi)| = n/k$ for every $\xi \in U_k$, and consider, for each ζ on the complex unit circle S^1, the open arc C_ζ of length $\pi/3$ centred at ζ on S^1. Set $K_\zeta := \chi^{-1}(C_\zeta)$, and note that $|C_\zeta \cap U_k| \leqslant k/3$ for every $\zeta \in S^1$, and hence $|K_\zeta| \leqslant n/3$. Note also that, even though there are infinitely many C_ζ, there are at most $2k$ different sets K_ζ.

Let $c > 0$ and suppose first that there exists $\zeta \in S^1$ such that $|K_\zeta \cap I| \geqslant (1-c)|I|$. The number of such sets I is at most

$$2k \cdot \sum_{\ell=0}^{cm} \binom{n - |K_\zeta|}{\ell}\binom{|K_\zeta|}{m-\ell} \,\leqslant\, n^2 \binom{n/3}{(1-c)m}\binom{2n/3}{cm} \,\leqslant\, \left(\frac{2}{3} + c'\right)^m \binom{n/2}{m},$$

where $c'(c) \to 0$ as $c \to 0$.

So suppose that $|K_\zeta \cap I| \leqslant (1-c)|I|$ for every $\zeta \in S^1$. We claim that, if $\delta > 0$ is sufficiently small, then

$$|\lambda(I,\chi)| \,=\, \Big|\sum_{x \in I} \chi(x)\Big| \,\leqslant\, \Big(1 - c + c \cdot \cos\big(\pi/6\big)\Big) \cdot |I| \,<\, \big(1 - \delta\big)|I|. \tag{9}$$

To see this let $v = \sum_{x \in I} \chi(x)$, note that if $v = 0$ then we are done, and otherwise observe that, by our assumption, $\chi(x)$ can lie within the open arc of length $\pi/3$ centred in direction v for at most $(1-c)|I|$ elements $x \in I$. Since each of the others contribute at most $\cos(\pi/6)$ in the direction of v, (9) follows. This is a contradiction, so the proof is now complete. □

7.3. **Sum-free sets with large smallest eigenvalue.** We shall prove the following statement using Theorem 1.3. Together with Lemma 7.8 it will easily imply Proposition 7.3, and hence Theorem 7.1.

Lemma 7.9. *For every finite Abelian group G and every $\delta > 0$, there exist $\varepsilon = \varepsilon(\delta) > 0$ and $C = C(\delta) > 0$ such that*

$$\left|\left\{ I \in \mathrm{SF}^{(\delta)}_{\geqslant}(G,m) : \lambda(I) \geqslant (\delta - 1)|I| \right\}\right| \leqslant 2^{-\varepsilon m}\binom{n/2}{m}$$

for every $m \geqslant C\sqrt{n}$.

The idea of the proof is as follows: we choose a set $S \subseteq I$ of size εm and observe that, since I is sum-free, $I \setminus S$ is an independent set in $\mathcal{G}^*_S$, the Cayley graph of S. The key point is that, for some such S, our bound on $\lambda(I)$ implies the existence of a non-trivial bound on $\lambda(\mathcal{G}^*_S)$, the smallest eigenvalue of the adjacency matrix of the Cayley graph of S. Combined with Theorem 1.3, this implies that there are only very few choices for $I \setminus S$, and hence for I itself.

The first step is the following lemma, which shows that our bound on $\lambda(I)$ allows us to find a small set S such that $\lambda(S)/|S|$ is also bounded away from minus one.

Lemma 7.10. *If $I \in \mathrm{SF}^{(\delta)}_{\geqslant}(G,m)$ satisfies $\lambda(I) \geqslant (\delta - 1)|I|$, then there exists a set $S \subseteq I$ of size εm such that*

$$\lambda(S) \geqslant \left(\frac{\delta}{2} - 1\right)|S|. \tag{10}$$

Proof. Recall the definition of $\lambda(A,\chi)$ from the proof of Lemma 7.8. Since $\lambda(I) \geqslant (\delta-1)|I|$, it follows from Lemma 7.6 that $\lambda(I,\chi) \geqslant (\delta - 1)|I|$ for every $\chi \in \hat{G}$. Choose a subset $S \subseteq I$ of size εm uniformly at random; we claim that $\lambda(S,\chi)$ is tightly concentrated around the mean, i.e., around $\varepsilon\lambda(I,\chi)$. Indeed, by Chernoff's inequality, we have

$$\mathbb{P}\Big(\lambda(S,\chi) \leqslant (\delta/2 - 1)\varepsilon|I|\Big) \leqslant e^{-\Omega(m)},$$

where the implicit constant depends on ε and δ. There are exactly n characters in $\hat{G}$, and so, by the union bound, the probability that S does not satisfy (10) is at most $1/2$. Thus there exists a set S as claimed. $\square$

Next, we show that this bound on $\lambda(S)$ implies a similar bound on $\lambda(\mathcal{G}^*_S)$, the smallest eigenvalue of the adjacency matrix of the Cayley graph of S. Recall that the adjacency matrix of $\mathcal{G}^*_S$ is $A\big(S \cup (-S)\big)$, and hence

$$\lambda\big(\mathcal{G}^*_S\big) = \lambda\big(S \cup (-S)\big).$$

We shall use the following lemma, which bounds $\lambda(\mathcal{G}^*_S)$ in terms of $\lambda(S)$.

Lemma 7.11. *Let $0 \notin S \subseteq G$ and $\delta > 0$. If $\lambda(S) \geqslant (\delta - 1)|S|$, then*

$$\lambda\big(\mathcal{G}^*_S\big) \geqslant \left(\frac{\delta}{2} - 1\right)|S \cup (-S)|.$$

Proof of Lemma 7.11. By Lemma 7.7, the characters of G are a basis of eigenvectors of both $A(S)$ and $A((-S) \setminus S)$. Thus, by Lemma 7.6,

$$\begin{aligned} \lambda\big(\mathcal{G}_S^*\big) &= \lambda\big(S \cup (-S)\big) = \lambda(S) + \lambda\big((-S) \setminus S\big) \\ &\geqslant (\delta - 1)|S| - |(-S) \setminus S| \geqslant \left(\frac{\delta}{2} - 1\right) |S \cup (-S)|, \end{aligned}$$

as required. The last inequality follows from the fact that $|(-S) \setminus S| \leqslant |(-S)| = |S|$. $\square$

We can now complete the proof of Lemma 7.9.

Proof of Lemma 7.9. Let $I \in \mathrm{SF}_{\geqslant}^{(\delta)}(G, m)$ and suppose that $\lambda(I) \geqslant (\delta - 1)|I|$. By Lemmas 7.10 and 7.11, there exists a set $S \subseteq I$ with $|S| = \varepsilon m$, such that

$$\lambda(\mathcal{G}_S^*) \geqslant \left(\frac{\delta}{4} - 1\right) |S \cup (-S)|.$$

Since I is sum-free, $I \setminus S$ is an independent set in $\mathcal{G}_S^*$. We claim that $\mathcal{G}_S^*$ satisfies the conditions of Theorem 1.3. Indeed, $\mathcal{G}_S^*$ is a d_S-regular graph on n vertices, where $d_S = |S \cup (-S)|$, and

$$|I \setminus S| = \big(1 - \varepsilon\big)m \geqslant \frac{C(\varepsilon)n}{\varepsilon m} \geqslant \frac{C(\varepsilon)n}{|S \cup (-S)|},$$

since $m \geqslant C\sqrt{n}$. Note also that

$$\frac{|\lambda(\mathcal{G}_S^*)|}{d_S + |\lambda(\mathcal{G}_S^*)|} \leqslant \frac{1 - (\delta/4)}{2 - (\delta/4)} \leqslant \frac{1}{2} - \frac{\delta}{16}.$$

Hence, by Theorem 1.3,

$$I(\mathcal{G}_S^*, (1 - \varepsilon)m) \leqslant \binom{(1/2 - \delta/20)n}{(1 - \varepsilon)m},$$

and so

$$\left|\Big\{I \in \mathrm{SF}_{\geqslant}^{(\delta)}(G, m) : \, \lambda(I) \leqslant (1 - \delta)|I|\Big\}\right| \leqslant \binom{n}{\varepsilon m}\binom{(1/2 - \delta/20)n}{(1 - \varepsilon)m} \leqslant 2^{-\varepsilon m}\binom{n/2}{m}$$

if $\varepsilon = \varepsilon(\delta) > 0$ is sufficiently small. This proves the lemma. $\square$

Finally, note that Lemmas 7.8 and 7.9 imply Proposition 7.3.

7.4. **Proof of Theorem 7.1.** First, observe that if $|G|$ is even, then the claimed lower bound on $|\mathrm{SF}(G, m)|$ is a straightforward consequence of the fact that, by Theorem 6.2, $|\mathrm{SF}_0(G)| = \#\big\{\text{elements of } G \text{ of order } 2\big\}$ and that each pair of distinct $B, B' \in \mathrm{SF}_0(G)$ intersects in $|G|/4$ elements. If $|G|$ is odd, then Theorem 7.1 only gives an upper bound on $|\mathrm{SF}(G, m)|$.

For the upper bound, observe that by Propositions 7.2 and 7.3, we have

$$\begin{aligned} |\mathrm{SF}(G, m)| &\leqslant |\mathrm{SF}_{\leqslant}^{(\delta)}(G, m)| + |\mathrm{SF}_{\geqslant}^{(\delta)}(G, m)| \\ &\leqslant \big(\#\big\{\text{elements of } G \text{ of order } 2\big\} + o(1)\big)\binom{n/2}{m} + 2^{-\varepsilon m}\binom{n/2}{m}, \end{aligned}$$

for every $m \geqslant 4\sqrt{n \log n}$, as required.

References

[1] N. Alon, Independent sets in regular graphs and sum-free subsets of abelian groups, *Israel J. Math.*, **78** (1991), 247–256.

[2] N. Alon and F.R.K. Chung. Explicit construction of linear sized tolerant networks, *Discrete Math.*, **72** (1989), 15–19.

[3] N. Alon and V. Rödl, Sharp bounds for some multicolor Ramsey numbers, *Combinatorica*, **25** (2005), 125–141.

[4] N. Alon and J. Spencer, The Probabilistic Method (3rd edition), Wiley Interscience, 2008.

[5] L. Babai, M. Simonovits and J. Spencer, Extremal subgraphs of random graphs, *J. Graph Theory*, **14** (1990), 599–622.

[6] J. Balogh, R. Morris and W. Samotij, Random sum-free subsets of Abelian groups, submitted.

[7] J. Balogh and W. Samotij, The number of $K_{m,m}$-free graphs, *Combinatorica*, **31** (2011), 131–150.

[8] J. Balogh and W. Samotij, The number of $K_{s,t}$-free graphs, *J. London Math. Soc.*, **83** (2011), 368–388.

[9] T. Carroll, D. Galvin and P. Tetali, Matchings and independent sets of a fixed size in regular graphs, *J. Combin. Theory, Ser. A*, **116** (2009), 1219–1227.

[10] D. Conlon and W.T. Gowers, Combinatorial Theorems in sparse random sets, submitted.

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

[12] P. Erdős, D.J. Kleitman and B.L. Rothschild, Asymptotic enumeration of K_n-free graphs, in *Colloquio Internazionale sulle Teorie Combinatorie* (Rome, 1973), Vol. II, pp. 19–27. *Atti dei Convegni Lincei*, **17**, Accad. Naz. Lincei, Rome, 1976.

[13] P. Erdős, Some recent results on extremal problems in graph theory. In *Theory of Graphs* (*Internat. Sympos.*, Rome, 1966), pages 117–123 (English); pp. 124–130 (French); Gordon and Breach, New York, 1967.

[14] P. Erdős and A. Stone, On the structure of linear graphs, *Bull. Amer. Math. Soc.*, **52** (1946), 1087–1091.

[15] E. Friedgut, V. Rödl, A. Ruciński and P. Tetali, A sharp threshold for random graphs with a monochromatic triangle in every edge coloring, *Mem. Amer. Math. Soc.*, **179** (2006), 66pp.

[16] D. Galvin and J. Kahn, On phase transition in the hard-core model on $\mathbb{Z}^d$, *Combin., Probab. Computing*, **13** (2004), 137–164.

[17] R. Graham, V. Rödl and A. Ruciński, On Schur properties of random subsets of integers, *J. Number Theory*, **61** (1996), 388–408.

[18] B.J. Green and I.Z. Ruzsa, Sum-free sets in abelian groups, *Israel J. Math.*, **147** (2005), 157–188.

[19] S. Hoory, N. Linial and A. Wigderson, Expander graphs and their applications, *Bull. Amer. Math. Soc.*, **43** (2006), 439–561.

[20] S. Janson, T. Łuczak and A. Ruciński, Random Graphs, Wiley, 2000

[21] J. Kahn, An entropy approach to the hard-core model on bipartite graphs, *Combin. Probab. Computing*, **10** (2001), 219–237.

[22] J. Kahn, Entropy, independent sets and antichains: A new approach to Dedekinds problem, *Proc. Amer. Math. Soc.*, **130** (2002), 371–378 (electronic).

[23] D.J. Kleitman and K.J. Winston: On the number of graphs without 4-cycles, *Discrete Math.*, **41** (1982), 167–172.

[24] Y. Kohayakawa, T. Łuczak and V. Rödl, Arithmetic progressions of length three in subsets of a random set, *Acta Arith.*, **75** (1996), 133–163.

[25] Ph.G. Kolaitis, H.J. Prömel, and B.L. Rothschild, $K_{\ell+1}$-free graphs: asymptotic structure and a 0-1 law, *Trans. Amer. Math. Soc.*, **303** (1987), 637–671.

[26] V. F. Lev, T. Łuczak and T. Schoen, Sum-free sets in abelian groups, *Israel J. Math.*, **125** (2001), 347–367.

[27] D. Osthus, H.J. Prömel and A. Taraz, For which densities are random triangle-free graphs almost surely bipartite?, *Combinatorica*, **23** (2003),ˇ 201–250.
[28] R. Peled and W. Samotij, Odd cutsets and the hard-core model on $\mathbb{Z}^d$, submitted.
[29] H.J. Prömel and A. Steger, On the asymptotic structure of sparse triangle free graphs, *J. Graph Theory*, **21** (1996), 137–151.
[30] V. Rödl and A. Ruciński, Threshold functions for Ramsey properties, *J. Amer. Math. Soc.*, **8** (1995), 917–942.
[31] V. Rödl and A. Ruciński, Rado partition theorem for random subsets of integers, *Proc. London Math. Soc.*, **74** (1997), 481–502.
[32] A.A. Sapozhenko, On the number of independent sets in expanders, *Diskretn. Mat. Moscow* **13** (2001) 56–62.
[33] A.A. Sapozhenko, Asymptotics of the number of sum-free sets in abelian groups of even order, (Russian) *Dokl. Akad. Nauk*, **383** (2002), no. 4, 454–457.
[34] M. Schacht, Extremal results for random discrete structures, submitted.
[35] M. Simonovits, A method for solving extremal problems in graph theory, stability problems, In *Theory of Graphs* (*Proc. Colloq., Tihany*, 1966), 279–319, Academic Press, 1968.
[36] E. Szemerédi, On sets of integers containing no k elements in arithmetic progression, *Acta Arith.*, **27** (1975), 199–245.
[37] P. Turán, Eine Extremalaufgabe aus der Graphentheorie, Mat. Fiz. Lapok 48 (1941) 436452 (in Hungarian; German summary).
[38] Yufei Zhao, The number of independent sets in a regular graph, *Combin. Prob. Computing*, 19 (2010), 315–320.

School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel
E-mail address: `nogaa@post.tau.ac.il`

Department of Mathematics, University of Illinois, 1409 W. Green Street, Urbana, IL 61801
E-mail address: `jobal@math.uiuc.edu`

IMPA, Estrada Dona Castorina 110, Jardim Botânico, Rio de Janeiro, RJ, Brasil
E-mail address: `rob@impa.br`

School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel; and Trinity College, Cambridge CB2 1TQ, UK
E-mail address: `ws299@cam.ac.uk`