

COUNTING INDEPENDENT SETS IN GRAPHS

WOJCIECH SAMOTIJ

ABSTRACT. In this short survey article, we present an elementary, yet quite powerful, method of enumerating independent sets in graphs. This method was first employed more than three decades ago by Kleitman and Winston and has subsequently been used numerous times by many researchers in various contexts. Our presentation of the method is illustrated with several applications of it to ‘real-life’ combinatorial problems. In particular, we derive bounds on the number of independent sets in regular graphs, sum-free subsets of $\{1, \dots, n\}$, and C_4 -free graphs and give a short proof of an analogue of Roth’s theorem on 3-term arithmetic progressions in sparse random sets of integers which was originally formulated and proved by Kohayakawa, Luczak, and Rödl.

1. INTRODUCTION

Many well-studied problems in combinatorics concern characterising discrete structures that satisfy certain ‘local’ constraints. For example, the celebrated theorem of Szemerédi [43] gives an upper bound on the maximum size of a subset of the first n integers which does not contain an arithmetic progression of a fixed length k . To give another example, the archetypal problem studied in extremal graph theory, dating back to the work of Mantel [33] and Turán [44], is that of characterising graphs which do not contain a fixed graph H as a subgraph.

Problems of this type fall into the following general framework. We are given a finite set V and a collection \mathcal{H} of subsets of V . What can be said about sets $I \subseteq V$ that do not contain any member of \mathcal{H} ? Such a collection \mathcal{H} is often called a *hypergraph* with vertex set V , members of \mathcal{H} are termed *edges*, and any set $I \subseteq V$ that contains no edge is called an *independent set*. In view of this, one might say that a large part of combinatorics is concerned with studying independent sets in various hypergraphs. For instance, in the first example from the previous paragraph, V is the set $\{1, \dots, n\}$ and \mathcal{H} is the collection of all k -term arithmetic progressions contained in V ; stated in this language, Szemerédi’s theorem says that for every positive constant δ , every independent set in \mathcal{H} has fewer than δn elements, provided that n is sufficiently large. In the second example, V is the edge set of a complete graph on a given set of n vertices and \mathcal{H} is the family of all $\binom{n}{|V(H)|}$ sets of $|E(H)|$ edges that form a copy of H in the complete graph; in this notation, if H is a clique with $k + 1$ vertices, then Turán’s theorem says that the largest independent sets in \mathcal{H} are precisely the edge sets of the complete balanced k -partite subgraphs of the complete graph with edge set V and the well-known theorem of Kolaitis, Prömel, and Rothschild [30] states that almost all independent sets of \mathcal{H} are k -partite, that is, the number $i^*(\mathcal{H})$ of independent sets in \mathcal{H} that are not the edge sets of k -partite subgraphs of the complete graph with edge set V satisfies $i^*(\mathcal{H})/i(\mathcal{H}) \rightarrow 0$ as $n \rightarrow \infty$.

For a hypergraph \mathcal{H} , let $\mathcal{I}(\mathcal{H})$ denote the family of all independent sets in \mathcal{H} , let $i(\mathcal{H}) = |\mathcal{I}(\mathcal{H})|$, and let $\alpha(\mathcal{H})$ be the largest cardinality of an element of $\mathcal{I}(\mathcal{H})$, usually called the *independence number* of \mathcal{H} . There are two natural problems that one usually poses about a specific hypergraph \mathcal{H} :

Date: February 27, 2015.

Research supported in part by a grant from the Israel Science Foundation.

- (i) Determine $\alpha(\mathcal{H})$ and describe all $I \in \mathcal{I}(\mathcal{H})$ with $\alpha(\mathcal{H})$ elements.
- (ii) Estimate $i(\mathcal{H})$ and describe a ‘typical’ member of $\mathcal{I}(\mathcal{H})$.

Let us remark here that providing a precise characterisation of a typical element of $\mathcal{I}(\mathcal{H})$ usually yields a precise estimate for $i(\mathcal{H})$.

An apparent connection between problems (i) and (ii) may be easily observed in the following two inequalities, which are trivial consequences of the above definitions and the fact that the family $\mathcal{I}(\mathcal{H})$ is closed under taking subsets:

$$2^{\alpha(\mathcal{H})} \leq i(\mathcal{H}) \leq \sum_{m=0}^{\alpha(\mathcal{H})} \binom{|V(\mathcal{H})|}{m}. \quad (1)$$

Note that, unless $\alpha(\mathcal{H})$ is very close to $|V(\mathcal{H})|$, the lower and upper bounds on $i(\mathcal{H})$ given in (1) are quite far apart. Since for many interesting hypergraphs \mathcal{H} this naive lower bound is actually fairly close to being best possible, the efforts of many researchers have been focused on improving the upper bound.

In this short survey article, we present an elementary, yet very powerful, method for proving stronger upper bounds in the case when all edges of \mathcal{H} have size two, that is, when \mathcal{H} is a graph. This method was first described more than three decades ago by Kleitman and Winston, who used it to obtain upper bounds on the number of lattices¹ [26] and graphs without cycles of length four [27]. Variations of this method were subsequently rediscovered by several researchers, most notably by Sapozhenko, in the context of enumerating independent sets in regular graphs [1, 37] and sum-free sets in abelian groups [1, 32, 38]. We shall illustrate our presentation of this method with several applications of it to ‘real-life’ combinatorial problems. We would like to stress here that none of the results or proof techniques presented here are new, but we hope that there is some value in seeing them next to one another.

2. THE KLEITMAN–WINSTON ALGORITHM

Suppose that we are given an arbitrary graph G with n vertices. Our goal is to give an upper bound on $i(G)$, the number of independent sets in G . The idea of Kleitman and Winston was to devise an algorithm that, given a particular independent set $I \in \mathcal{I}(G)$, would encode I in an invertible way. Crucially, the encoding should be performed in a way which makes it easy to estimate the total number of outputs of the algorithm. Since for every invertible encoding, the total number of outputs is precisely $i(G)$, in this way one could derive an upper bound on this quantity.

The crucial idea of Kleitman and Winston was to consider the vertices of G ordered according to their degrees and encode each independent set I as a sequence of positions of the elements of I in that ordering. We make this precise below.

Definition. Let G be a graph and fix an arbitrary total order on $V(G)$. For every $A \subseteq V(G)$, the *max-degree ordering* of A is the ordering $(v_1, \dots, v_{|A|})$ of all elements of A , where for each $j \in \{1, \dots, |A|\}$, v_j is the maximum-degree vertex in the subgraph of G induced by $A \setminus \{v_1, \dots, v_{j-1}\}$; ties are broken by giving preference to vertices that come earlier in the fixed total order on $V(G)$.

The Algorithm. Suppose that a graph G , an $I \in \mathcal{I}(G)$, and an integer $q \leq |I|$ are given. Set $A = V(G)$ and $S = \emptyset$. For $s = 1, \dots, q$, do the following:

¹A lattice is a partially ordered set in which every two elements have a supremum and an infimum.

- (a) Let $(v_1, \dots, v_{|A|})$ be the max-degree ordering of A .
 - (b) Let j_s be the minimal index j such that $v_j \in I$.
 - (c) Move v_{j_s} from A to S .
 - (d) Delete v_1, \dots, v_{j_s-1} from A .
 - (e) Delete $N_G(v_{j_s}) \cap A$ from A .
- Output (j_1, \dots, j_q) and $A \cap I$.

For each output sequence (j_1, \dots, j_q) and every $s \in \{1, \dots, q\}$, denote by $A(j_1, \dots, j_s)$ and $S(j_1, \dots, j_s)$ the sets A and S at the end of the s th iteration of the algorithm (run on some input I that produces this particular sequence (j_1, \dots, j_q)), respectively. Observe that these definitions do not depend on the choice of I as the sequence (j_1, \dots, j_q) uniquely determines how the sets S and A evolve throughout the algorithm. More precisely, if running the algorithm on two inputs $I, I' \in \mathcal{I}(G)$ produces the same sequence (j_1, \dots, j_q) , then both these executions will also yield the same sets S and A . Indeed, all the modifications of the sets S and A in the s th iteration of the algorithm depend solely on j_s .

Note crucially that $S(j_1, \dots, j_s) \subseteq I$ and $I \setminus S(j_1, \dots, j_s) \subseteq A(j_1, \dots, j_s)$ for every s . Indeed, by the minimality of j_s and the assumption that I is independent, the only vertices of I that are deleted from A are moved to S . It follows that one may recover the set I from the output of the algorithm, as $I = S(j_1, \dots, j_q) \cup (A(j_1, \dots, j_q) \cap I)$. We also note for future reference that the sequence (j_1, \dots, j_q) can be recovered from the set $S(j_1, \dots, j_q)$. Indeed, if running the algorithm on some input $I \in \mathcal{I}(G)$ produces a sequence (j_1, \dots, j_q) and $S = S(j_1, \dots, j_q)$, then the same sequence will be produced by running the algorithm with I replaced by S . Finally, let us observe that $j_1 + \dots + j_q \leq |V(G)| - |A(j_1, \dots, j_q)|$, as in steps (c) and (d) of the s th iteration of the main loop, we removed from A some j_s vertices.

Let $i(G, m)$ be the number of independent sets in G that have precisely m elements. The above observations readily imply that for every m and q with $m \geq q$,

$$i(G, m) \leq \sum_{(j_s)} i(G[A(j_1, \dots, j_q)], m - q) \leq \sum_{(j_s)} \binom{|A(j_1, \dots, j_q)|}{m - q}, \quad (2)$$

where the above sums range over all output sequences (j_1, \dots, j_q) . In particular, letting $n = |V(G)|$,

$$i(G) \leq \sum_{m=0}^{q-1} \binom{n}{m} + \sum_{(j_s)} i(G[A(j_1, \dots, j_q)]) \leq \sum_{m=0}^{q-1} \binom{n}{m} + \sum_{(j_s)} 2^{|A(j_1, \dots, j_q)|}. \quad (3)$$

In view of (2) and (3), it is in our interest to make the set $A(j_1, \dots, j_q)$ as small as possible, uniformly for all values of (j_1, \dots, j_q) . This is why we consider the vertices of A listed according to the max-degree ordering. (An attentive reader might have already noticed that this particular ordering maximises $\deg_G(v_{j_s}, A)$ in each iteration of the algorithm.) Suppose that we are at the s th iteration of the main loop of the algorithm and let $A' = A \setminus \{v_1, \dots, v_{j_s-1}\}$, where A is as at the start of this iteration, that is, $A = A(j_1, \dots, j_{s-1})$. By the definition of the max-degree ordering,

$$|N_G(v_{j_s}) \cap A'| = \max_{v \in A'} \deg_G(v, A') \geq \frac{2e_G(A')}{|A'|}.$$

In particular, if $e_G(A') = \beta \binom{|A'|}{2}$, then the right-hand side of the above inequality is $\beta(|A'| - 1)$. Consequently, the number of vertices that are removed from A during the s th iteration of the main loop of the algorithm is at least $j_s + \beta(|A'| - 1)$, which is at least $\beta|A|$, as $|A'| - 1 = |A| - j_s$

and $\beta \leq 1$. In other words, as long as the density of the subgraph induced by the set A exceeds some β , each iteration of the main loop of the algorithm shrinks A by a factor of at most $1 - \beta$.

The following two lemmas, which are both implicit in the work of Kleitman and Winston, summarise the above discussion. The first lemma gives a simple bound on the number of independent sets of a given size in a graph which satisfies a certain local density condition. The exact statement of this lemma is taken from [28]. The second lemma characterises the family of all independent sets in such a locally dense graph. The statement of this lemma is inspired by the statement of the main result of [7].

Lemma 1. *Let G be a graph on n vertices and assume that an integer q and reals R and $\beta \in [0, 1]$ satisfy*

$$R \geq e^{-\beta q} n. \quad (4)$$

Suppose that the number of edges induced in G by every set $U \subseteq V(G)$ with $|U| \geq R$ satisfies

$$e_G(U) \geq \beta \binom{|U|}{2}. \quad (5)$$

Then, for every integer m with $m \geq q$,

$$i(G, m) \leq \binom{n}{q} \binom{R}{m-q}. \quad (6)$$

Proof. Since there are exactly $\binom{n}{q}$ sequences (j_1, \dots, j_q) satisfying $j_1 + \dots + j_q \leq n$ and $j_s \geq 1$ for each s , the sum in the right-hand side of (2) has at most $\binom{n}{q}$ terms. Therefore, it suffices to show that for each sequence (j_1, \dots, j_q) that is outputted by the algorithm, the set $A(j_1, \dots, j_q)$ has at most R elements. If this were not the case, then there would be some sequence (j_1, \dots, j_q) such that for each $s \in \{1, \dots, q\}$, the set $A \setminus \{v_1, \dots, v_{j_s-1}\}$ in the s th iteration of the main loop of the algorithm (run on some input that results in this particular sequence) would have more than R elements and therefore induce in G a subgraph with edge density at least β . It follows from our discussion that each of the q iterations would shrink the set A by a factor of at most $1 - \beta$. Since $|A| = |V(G)| = n$ at the start of the algorithm, then, by (4),

$$|A(j_1, \dots, j_q)| \leq (1 - \beta)^q n \leq e^{-\beta q} n \leq R,$$

a contradiction. □

Lemma 2. *Let G be a graph on n vertices and assume that an integer q and reals R and D satisfy*

$$R + qD \geq n. \quad (7)$$

Suppose that the number of edges induced in G by every set $U \subseteq V(G)$ with $|U| \geq R$ satisfies

$$2e_G(U) \geq D|U|. \quad (8)$$

Then there exists a collection \mathcal{S} of q -element subsets of $V(G)$ and two mappings $g: \mathcal{I}(G) \rightarrow \mathcal{S}$ and $f: \mathcal{S} \rightarrow \mathcal{P}(V(G))$ such that $|f(S)| \leq R$ for each $S \in \mathcal{S}$ and $g(I) \subseteq I \subseteq f(g(I)) \cup g(I)$ for every $I \in \mathcal{I}(G)$ with at least q elements.

Proof. We define the mappings f and g and the family \mathcal{S} as follows. We simply run the algorithm with input I for each $I \in \mathcal{I}(G)$ with at least q elements and let $g(I)$ and $f(g(I))$ be the final sets S and A , respectively. Moreover, we let \mathcal{S} be the family of all such S , that is, the set of values taken by g . The discussion in the paragraph following the description of the algorithm should convince us that this is a valid definition of f , that $g(I) \subseteq I \subseteq f(g(I)) \cup g(I)$ for each I as above, and

that \mathcal{S} consists solely of q -element subsets of $V(G)$. It suffices to check that $|f(g(I))| \leq R$ for each such I . If this were not the case, then there would be some sequence (j_1, \dots, j_q) such that for each $s \in \{1, \dots, q\}$, the set $A \setminus \{v_1, \dots, v_{j_s-1}\}$ in the s th iteration of the main loop of the algorithm (run on an input I that generates this sequence) would have more than R elements and therefore induce in G a subgraph with average degree at least D . But then, each of the q iterations would remove from A at least $D + 1$ vertices. Since $|A| = |V(G)| = n$ at the start of the algorithm, then by (7),

$$|A(j_1, \dots, j_q)| \leq n - Dq \leq R,$$

a contradiction. \square

Before we close this section, let us make several final remarks. First, the conclusion of Lemma 2 is stronger than the conclusion of Lemma 1. This is simply because the existence of f and g as in the statement of the second lemma imply the bound on $i(G, m)$ asserted by the first lemma. Moreover, it should be clear from the proofs that the assumptions of the two lemmas are ‘interchangeable’ in the following sense. If a graph G satisfies the assumptions of Lemma 1 with some q , R , and β , then the conclusion of Lemma 2 holds for G with the same q and R ; and vice-versa, if a graph G satisfies the assumptions of Lemma 2 with some q , R , and D , then the conclusion of Lemma 1 holds for G with the same q and R . (The latter statement is redundant because, as we have already noted above, the conclusion of Lemma 2 is stronger than the conclusion of Lemma 1.)

3. APPLICATIONS

3.1. Independent sets in regular graphs. During a number theory conference at Banff in 1988, Granville conjectured (see [1]) that an n -vertex d -regular graph can have no more than $2^{(1+o(1))\frac{n}{2}}$ independent sets, where $o(1)$ is some function that tends to 0 as $d \rightarrow \infty$. A few years later, this was shown to be true by Alon [1], who proved that in fact

$$i(G) \leq 2^{(1+O(d^{-0.1}))\frac{n}{2}}$$

for every n -vertex d -regular graph G . As our first application of Lemma 1, we derive a somewhat stronger estimate, which was obtained several years later by Sapozhenko [37], using arguments very similar to those presented in Section 2.

Theorem 3 ([37]). *There is an absolute constant C such that every n -vertex d -regular graph G satisfies*

$$i(G) \leq 2^{\left(1+C\sqrt{\frac{\log d}{d}}\right)\frac{n}{2}}.$$

Alon [1] speculated that when n is divisible by $2d$, then the disjoint union of $\frac{n}{2d}$ complete bipartite graphs $K_{d,d}$ has the maximum number of independent sets among all d -regular graphs with n vertices. A slightly stronger statement (Theorem 4 below) was later conjectured by Kahn [24], who proved it under the additional assumption that G is bipartite, using a beautiful entropy argument. This assumption was recently shown to be unnecessary by Zhao [46], who gave a short and elegant argument showing that for every n -vertex d -regular graph G , there exists a $2n$ -vertex d -regular bipartite graph G' such that $i(G) \leq i(G')^{1/2}$. The results of Kahn and Zhao yield the following.

Theorem 4 ([24, 46]). *For every n -vertex d -regular graph G ,*

$$i(G) \leq i(K_{d,d})^{\frac{n}{2d}} = \left(2^{d+1} - 1\right)^{\frac{n}{2d}}.$$

We now derive Theorem 3 from Lemma 1.

Proof of Theorem 3. Let G be an n -vertex d -regular graph. We shall in fact estimate $i(G, m)$ for each m and deduce the claimed bound on $i(G)$ by summing over all m . Since $i(G) \leq 2^n$ and C is an arbitrary constant, we may assume that d is sufficiently large (and therefore n is sufficiently large). We consider two cases. First, if $m \leq n/10$, then we simply note that

$$i(G, m) \leq \binom{n}{\frac{n}{10}} \leq (10e)^{\frac{n}{10}} \leq 2^{0.48n}, \quad (9)$$

where we used the well-known inequality $\binom{a}{b} \leq (ea/b)^b$ valid for all a and b .

In the complementary case, $m > n/10$, we shall apply Lemma 1. To this end, let $B \subseteq V(G)$ and note that

$$d|B| = \sum_{v \in B} \deg_G(v) = 2e(B) + e(B, B^c) \leq 2e(B) + \sum_{v \in B^c} \deg_G(v) = 2e(B) + d(n - |B|). \quad (10)$$

Fix an arbitrary β , let $R = \frac{n}{2} + \frac{\beta n^2}{2d}$, and observe that if $|B| \geq R$, then (10) yields

$$e(B) \geq \frac{d}{2}(2|B| - n) \geq \frac{d}{2}(2R - n) \geq \frac{\beta n^2}{2} \geq \beta \binom{|B|}{2}. \quad (11)$$

Assume that $\beta > 10/n$ and let $q = \lceil 1/\beta \rceil$. By Lemma 1, since

$$e^{-\beta q} n \leq e^{-1} n \leq R,$$

then for every m with $m \geq \lceil n/10 \rceil \geq q$,

$$i(G, m) \leq \binom{n}{q} \binom{\frac{n}{2} + \frac{\beta n^2}{2d}}{m - q} \leq \left(\frac{en}{q}\right)^q \binom{\frac{n}{2} + \frac{\beta n^2}{2d}}{m - q} \leq (e\beta n)^{\lceil 1/\beta \rceil} \cdot \binom{\frac{n}{2} + \frac{\beta n^2}{2d}}{m - q}. \quad (12)$$

Summing (9) and (12) over all m yields

$$i(G) \leq 2^{0.49n} + 2^{\frac{n}{2} + \frac{\beta n^2}{2d} + \lceil 1/\beta \rceil \log_2(e\beta n)}$$

We obtain the claimed bound by letting $\beta = \frac{\sqrt{d \log d}}{n}$; we note that $\sqrt{d \log d} > 10$ as we assumed that d is large. \square

We ought to indicate here that one may significantly improve the upper bound given by Theorem 3 by a somewhat more careful analysis of the execution of the Kleitman–Winston algorithm than the one given in the proof of Lemma 1. The main reason why one should expect such an improvement to be possible is the crudeness of the second inequality in (11) in the case when $|B| - n/2$ is much larger than $R - n/2$. The proof of Lemma 1 uses (11) to show that in each step of the algorithm, the set A loses at least $\beta|A|$ elements whereas in reality A will lose many more elements as long as $|A|$ is not very close to $n/2 + \beta n^2/(2d)$. By considering the ‘evolution’ of $|A|$ partitioned into ‘dyadic’ intervals $(n/2 + n/2^{i+1}, n/2 + n/2^i]$, where $1 \leq i \leq \log_2 d - \log_2 \log_2 d$, one may prove that there is an absolute constant C such that every n -vertex d -regular graph G satisfies

$$i(G) \leq 2^{\left(1 + C \frac{(\log d)^2}{d}\right) \frac{n}{2}}.$$

One rigorous way of tracking this ‘evolution’ of $|A|$ is to repeatedly invoke Lemma 2 with $R_i = n/2 + n/2^{i+1}$ and $D_i = d/2^i$ for $i = 1, \dots, \log_2 d - \log_2 \log_2 d$. We leave filling in the details as an exercise for the reader.

3.2. Sum-free sets. The conjecture of Granville mentioned in the previous section was motivated by a problem posed by Cameron and Erdős at the same number theory conference. A set A of elements of an abelian group is called *sum-free* if there are no $x, y, z \in A$ satisfying $x + y = z$. Let $[n]$ denote the set $\{1, \dots, n\} \subseteq \mathbb{Z}$. Cameron and Erdős raised the question of determining the number $\text{SF}([n])$ of sum-free sets contained in the set $[n]$. They noted that any set containing either only odd integers or only integers greater than $n/2$ is sum-free, and that it is unlikely that there is another large collection of sum-free sets that are not essentially of one of the above two types. In view of this, they conjectured that $\text{SF}([n]) = O(2^{n/2})$. Soon afterwards, Alon [1] showed that the aforementioned conjecture of Granville implies the following weaker estimate on $\text{SF}([n])$, which will serve as a second example application of Lemma 1.

Theorem 5 ([1]). *The set $\{1, \dots, n\}$ has at most $2^{(1/2+o(1))n}$ sum-free subsets.*

The Cameron–Erdős conjecture was solved some fifteen years later by Green [19] and, independently, by Sapozhenko [39]. The solution due to Sapozhenko uses a method akin to the Kleitman–Winston algorithm presented in Section 2, while the one due to Green uses discrete Fourier analysis.² We do not discuss either of their arguments here, but instead refer the interested reader to the original papers. Finally, we mention that strong estimates on the number of sum-free subsets of $[n]$ with a given number of elements, which imply the conjecture, were recently obtained in [3]; the proof there employs the ideas presented in Section 2.

Proof of Theorem 5. Observe first that the number of all subsets of $[n]$ which contain fewer than $n^{2/3}$ elements from $\{1, \dots, \lceil n/2 \rceil - 1\}$ is at most $(n/2)^{n^{2/3}} 2^{n/2+1}$. Therefore, we may restrict our attention to sum-free sets that contain at least $n^{2/3}$ elements strictly smaller than $n/2$. For each such set A , let S_A be the set of $\lfloor n^{2/3} \rfloor$ smallest elements of A .

Given a set $S \subseteq \{1, \dots, \lceil n/2 \rceil - 1\}$, define an auxiliary graph G_S with vertex set $[n]$ by letting

$$E(G_S) = \{xy : x + s \equiv y \pmod{n} \text{ for some } s \in S \cup (-S)\}$$

and note that G_S is $2|S|$ -regular, as $n - (\lceil n/2 \rceil - 1) > \lceil n/2 \rceil - 1$ and hence S and $-S$ contain different residues modulo n . The crucial observation is that for every sum-free A as above, the set $A \setminus S_A$ is an independent set in the graph G_{S_A} . Indeed, otherwise there would be $x, y \in A \setminus S_A$ and an $s \in S_A \cup (-S_A)$ with $x + s \equiv y \pmod{n}$; since $1 \leq |s| < x, y \leq n$, this is only possible when $x + s = y$. In particular, for a given $S \subseteq \{1, \dots, \lceil n/2 \rceil - 1\}$, there are at most $i(G_S)$ sum-free sets A satisfying $S = S_A$. By Theorem 3, we conclude that

$$\text{SF}([n]) \leq (n/2)^{n^{2/3}} 2^{n/2+1} + \binom{n/2}{n^{2/3}} \cdot 2^{(1+O(n^{-1/3}\sqrt{\log n}))\frac{n}{2}} \leq 2^{(1/2+O(n^{-1/3}\log n))n}. \quad \square$$

Before closing this section, we remark that the paper of Alon [1] started a very successful line of inquiry into the closely related problem of determining the number of sum-free sets contained in an arbitrary finite abelian group; see, e.g., [2, 20, 21, 32, 38]. In many of these works, variations of the ideas presented in Section 2 play a prominent role.

3.3. Independent sets in regular graphs without small eigenvalues. Since every n -vertex bipartite graph G satisfies $\alpha(G) \geq n/2$ and hence it contains at least $2^{n/2}$ independent sets, the upper bounds for $i(G)$ proved in Section 3.1 are essentially best possible whenever G is bipartite.

²However, one might still argue that the general ‘philosophy’ behind Green’s proof is similar.

It is natural to ask whether these bounds can be improved when one assumes that G is ‘far’ from being bipartite. An affirmative answer to this question was given by Alon and Rödl [5].

Recall that the adjacency matrix of an n -vertex graph G is a real-valued symmetric $n \times n$ matrix and therefore it has n real eigenvalues. Denote these eigenvalues by $\lambda_1, \dots, \lambda_n$, where $\lambda_1 \geq \dots \geq \lambda_n$. It is well known that the quantity $\max\{|\lambda_2|, |\lambda_n|\}$, called the *second eigenvalue* of G , is closely tied with, among other parameters, the expansion properties of G . We shall be interested only in the smallest eigenvalue λ_n of G , which we denote by $\lambda(G)$. It was first proved by Hoffman [22] that every d -regular n -vertex graph G satisfies $\alpha(G) \leq \frac{-\lambda(G)}{d-\lambda(G)}n$. This was later significantly strengthened³ by Alon and Chung [4], who established the following relation between $\lambda(G)$ and the number of edges induced by large sets of vertices in G , cf. the expander mixing lemma (see, e.g., [23]).

Lemma 6 ([4]). *Let G be an n -vertex d -regular graph. For all $A \subseteq V(G)$,*

$$2e_G(A) \geq \frac{d}{n}|A|^2 + \frac{\lambda(G)}{n}|A|(n - |A|).$$

Alon and Rödl [5] were the first to prove that if $\lambda(G)$ is much larger than $-d$, then each such G has far fewer than $2^{n/2}$ independent sets. As our next application of Lemma 1, we derive a similar estimate, originally proved in [2].

Theorem 7 ([2]). *For every $\varepsilon > 0$, there exists a constant C such that the following holds. If G is an n -vertex d -regular graph with $\lambda(G) \geq -\lambda$, then*

$$i(G, m) \leq \binom{\left(\frac{\lambda}{d+\lambda} + \varepsilon\right)n}{m},$$

provided that $m \geq Cn/d$.

Proof of Theorem 7. Fix some $\varepsilon > 0$, let G be an n -vertex d -regular graph, and let $\lambda = -\lambda(G)$. We may assume that $\frac{\lambda}{d+\lambda} + \varepsilon < 1$ as otherwise there is nothing to prove. Let $U \subseteq V(G)$ be an arbitrary set with $|U| \geq \left(\frac{\lambda}{d+\lambda} + \frac{\varepsilon}{2}\right)n$. Lemma 6 implies that

$$2e_G(U) \geq \frac{d}{n}|U|^2 - \frac{\lambda}{n}|U|(n - |U|) = \frac{|U|}{n}((d + \lambda)|U| - \lambda n) \geq \frac{\varepsilon d}{2}|U| \geq \frac{\varepsilon d}{n} \binom{|U|}{2}.$$

Let $\beta = \frac{\varepsilon d}{n}$, $q = \left\lceil \frac{\log(2/\varepsilon)}{\varepsilon} \cdot \frac{n}{d} \right\rceil$, and $R = \left(\frac{\lambda}{d+\lambda} + \frac{\varepsilon}{2}\right)n$ and observe that $R \geq e^{-\beta q}n$. It follows from Lemma 1 that for every m with $m \geq q$,

$$i(G, m) \leq \binom{n}{q} \binom{R}{m-q}. \quad (13)$$

Let $r(t)$ denote the right-hand side of (13) with q replaced by t . We may clearly assume that $m \leq \alpha(G) \leq \frac{\lambda}{d+\lambda}n$, as otherwise $i(G, m) = 0$. An elementary calculation shows that

$$\frac{r(t+1)}{r(t)} = \frac{n-t}{t+1} \cdot \frac{m-t}{R-m+t+1} \leq \frac{nm}{(t+1)(R-m)} \leq \frac{2m}{\varepsilon(t+1)}$$

and hence

$$i(G, m) = r(q) = \prod_{t=0}^{q-1} \frac{r(t+1)}{r(t)} \cdot r(0) \leq \frac{(2m)^q}{\varepsilon^q q!} \cdot \binom{R}{m} \leq \left(\frac{2em}{\varepsilon q}\right)^q \cdot \left(\frac{R}{R + \varepsilon n/2}\right)^m \binom{R + \varepsilon n/2}{m},$$

³In particular, Lemma 6 implies that $e_G(A) > 0$ for every A with more than $\frac{-\lambda(G)}{d-\lambda(G)}n$ vertices.

where we used the inequalities $a! > (a/e)^a$ and $\binom{a}{c} \geq (a/b)^c \binom{b}{c}$ valid whenever $a \geq b \geq c \geq 0$. Finally, if K is sufficiently large (as a function of ε) and $C \geq K \cdot \left\lceil \frac{\log(2/\varepsilon)}{\varepsilon} \right\rceil$, then for every m with $m \geq Cn/d \geq Kq$,

$$\left(\frac{2em}{\varepsilon q}\right)^{q/m} \cdot \frac{R}{R + \varepsilon n/2} \leq \left(\frac{2Ke}{\varepsilon}\right)^{1/K} \cdot \left(1 - \frac{\varepsilon}{2}\right) \leq 1,$$

which completes the proof of the theorem. \square

We close this section with several remarks. First, the constant $\frac{\lambda}{d+\lambda}$ in the assertion of the theorem is optimal as for many values of n , d , and α , there are n -vertex d -regular graphs with $\alpha(G) = \frac{-\lambda(G)}{d-\lambda(G)}n = \alpha n$. Second, the assumption that $m \geq Cn/d$ cannot be relaxed as for every $\varepsilon > 0$, every n -vertex d -regular graph G satisfies $i(G, m) \geq \binom{(1-\varepsilon)n}{m}$ whenever $m \leq \varepsilon n/(d+1)$. (To see this, consider the greedy process of constructing an independent set which repeatedly picks an arbitrary vertex of G and removes it and all of its neighbours from G .) Third, the above theorem implies the conjecture of Granville stated in Section 3.1 as $\lambda(G) \geq -d$ for every d -regular graph G . Finally, we refer the interested reader to [2] and [5], where Theorem 7 was used to obtain upper bounds on the number of sum-free sets in abelian groups of even order and lower bounds on some multicolor Ramsey numbers, respectively.

3.4. The number of C_4 -free graphs. As our next example, we present the main result from one of the papers of Kleitman and Winston [27] which introduced the methods described in Section 2. Call a graph C_4 -free if it does not contain a cycle of length four and let $\text{ex}(n, C_4)$ denote the maximum number of edges in a C_4 -free graph with n vertices. A classical result of Kővári, Sós, and Turán [31] together with a construction due to Brown [11] and Erdős, Rényi, and Sós [17] imply that

$$\text{ex}(n, C_4) = \left(\frac{1}{2} + o(1)\right) n^{3/2}.$$

Let $f_n(C_4)$ be the number of (labeled) C_4 -free graphs on the vertex set $\{1, \dots, n\}$. Since each subgraph of a C_4 -free graph is itself C_4 -free, we have

$$2^{\text{ex}(n, C_4)} \leq f_n(C_4) \leq \sum_{m=0}^{\text{ex}(n, C_4)} \binom{\binom{n}{2}}{m} = 2^{\Theta(\text{ex}(n, C_4) \log n)},$$

which yields

$$\text{ex}(n, C_4) \leq \log_2 f_n(C_4) \leq O(\text{ex}(n, C_4) \log n). \quad (14)$$

Answering a question of Erdős, Kleitman and Winston [27] showed that the lower bound in (14) is tight up to a constant factor.

Theorem 8 ([27]). *There is a positive constant C such that*

$$\log_2 f_n(C_4) \leq Cn^{3/2}.$$

Before we continue with the proof of the theorem, let us make a few comments. In fact, Erdős asked whether $\log_2 f_n(H) = (1 + o(1))\text{ex}(n, H)$ for an arbitrary H that contains a cycle. This was shown to be the case by Erdős, Frankl, and Rödl [16] under the assumption that $\chi(H) \geq 3$. Very recently, Morris and Saxton [34] proved that $\log_2 f_n(C_6) \geq 1.0007 \cdot \text{ex}(n, C_6)$ for infinitely many n . But the notoriously difficult problem of determining whether or not $\log_2 f_n(H) = O(\text{ex}(n, H))$ for every bipartite H that is not a forest remains unsolved, apart from the following two special

cases: H is a cycle length four [27], six [25], or ten [34] or H is an unbalanced complete bipartite graph [8, 9]. More exactly, it is proved in [9] and [34] that $\log_2 f_n(K_{s,t}) = O(n^{2-1/s})$ whenever $2 \leq s \leq t$ and that $\log_2 f_n(C_{2\ell}) = O(n^{1+1/\ell})$ for every $\ell \geq 2$, respectively. As it is commonly believed that $\text{ex}(n, K_{s,t}) = \Omega(n^{2-1/s})$ whenever $s \leq t$ and that $\text{ex}(n, C_{2\ell}) = \Omega(n^{1+1/\ell})$, both these results are most likely best possible. Finally, we mention that the proofs of most of the results mentioned in this paragraph use either a variant of Lemma 1 or extensions of the ideas presented in Section 2 to hypergraphs, see Section 4.2.

Proof of Theorem 8. Note that one can order the vertices of every n -vertex graph G as v_1, \dots, v_n in such a way that for every $i \in \{2, \dots, n\}$, letting $G_i = G[\{v_1, \dots, v_i\}]$,

$$\delta(G_{i-1}) \geq \deg_{G_i}(v_i) - 1.$$

Indeed, one may obtain such an ordering by iteratively letting v_i be a minimum-degree vertex of $G - \{v_{i+1}, \dots, v_n\}$ for $i = n, \dots, 2$. In particular, every labeled n -vertex graph G can be constructed in the following way. First, choose an ordering v_1, \dots, v_n of the vertices and let G_1 be the empty graph with vertex set $\{v_1\}$. Second, for each $i \in \{2, \dots, n\}$, build a graph G_i by adding to the graph G_{i-1} a vertex labeled v_i in such a way that its degree d_i (in G_i) satisfies $d_i \leq \delta(G_{i-1}) + 1$. Finally, we let $G = G_n$. Observe that G is C_4 -free if and only if G_i is C_4 -free for each i .

Now, given integers d and i with $d \leq i$, let $g_i(d)$ denote the maximum number of ways to attach a vertex of degree d to an i -vertex C_4 -free graph with minimum degree at least $d - 1$ in such a way that the resulting graph remains C_4 -free. This number is well defined as clearly $g_i(d) \leq \binom{i}{d}$. Moreover, let $g_i = \max\{g_i(d) : d \leq i\}$. The argument given in the previous paragraph proves that

$$f_n(C_4) \leq n! \cdot n! \cdot \prod_{i=2}^n g_{i-1}. \quad (15)$$

Indeed, there are $n!$ ways to order $[n]$ as v_1, \dots, v_n and for each such ordering, there are at most $n!$ choices for the sequence d_2, \dots, d_n of degrees. In view of (15), the following claim easily implies the assertion of the theorem.

Claim. There exists a constant C such that $g_n \leq \exp(C\sqrt{n})$ for all n .

Without loss of generality, we may assume that n is large. Thus, if $d \leq \sqrt{n}/\log n$, then

$$g_n(d) \leq \binom{n}{d} \leq \left(\frac{n}{\frac{\sqrt{n}}{\log n}} \right) \leq (e\sqrt{n} \log n)^{\frac{\sqrt{n}}{\log n}} \leq \exp(\sqrt{n}).$$

Therefore, we shall from now on assume that $d > \sqrt{n}/\log n$. Let G be a C_4 -free graph on n vertices with $\delta(G) \geq d - 1$. Let H be the square of G , that is, the graph with $V(H) = V(G)$ and

$$E(H) = \{xy : xz, yz \in E(G) \text{ for some } z \in V(G)\}.$$

Crucially, observe that adding v to G will result in a C_4 -free graph if and only if the neighbourhood of v is an independent set in H . Hence, $i(H, d)$ is an upper bound on the number of C_4 -free extensions of G by a vertex of degree d . We shall estimate $i(H, d)$ using Lemma 1.

To this end, we show that subgraphs of H induced by large subsets of $V(H)$ have reasonably high density. Since G is C_4 -free, every edge xy of H corresponds to a unique vertex $z \in V(G)$ such that xz and yz are edges of G . Therefore, for each $B \subseteq V(H)$,

$$e_H(B) = \sum_{z \in V(G)} \binom{\deg_G(z, B)}{2} \geq n \cdot \binom{\sum_z \deg(z, B)/n}{2},$$

where the last inequality is Jensen's inequality applied to the convex function $x \mapsto \binom{x}{2}$. Since

$$\sum_{z \in V(G)} \deg_G(z, B) = \sum_{x \in B} \deg_G(x) \geq |B| \cdot \delta(G) \geq (d-1)|B|,$$

then assuming that $|B| \geq \frac{2n}{d-1}$ implies

$$e_H(B) \geq n \cdot \frac{(d-1)|B|}{2n} \left(\frac{(d-1)|B|}{n} - 1 \right) \geq \frac{(d-1)^2}{2n} \binom{|B|}{2}.$$

Finally, let $R = \frac{2n}{d-1}$, $\beta = \frac{(d-1)^2}{2n}$, and $q = \lceil 3(\log n)^3 \rceil$. Since $d > \sqrt{n}/\log n$ and n is large, then $\beta q \geq \log n$ and therefore $e^{-\beta q n} \leq 1 \leq R$. It follows from Lemma 1 that

$$i(H, d) \leq \binom{n}{q} \binom{\frac{2n}{d-1}}{d-q} \leq e^{4 \log^4 n} \cdot \left(\frac{2en}{(d-q)^2} \right)^{d-q} \leq \sup_{k>0} \left(\frac{e\sqrt{n}}{k} \right)^{2k} = e^{2\sqrt{n}},$$

where we used the assumption that n is large and the fact that $\sup \left\{ \left(\frac{e}{x} \right)^x : x > 0 \right\} = e$. \square

3.5. Roth's theorem in random sets. As our final example, we present a short proof of a well-known result of Kohayakawa, Łuczak, and Rödl [29]. Recall that $[n]$ denotes the set $\{1, \dots, n\}$. A famous theorem of Roth [35] asserts that for every positive δ , any set of at least δn integers from $[n]$ contains a 3-term arithmetic progression (3-term AP), provided that n is sufficiently large (as a function of δ only). Given a positive δ , we shall say that a set $A \subseteq \mathbb{Z}$ is δ -Roth if each $B \subseteq A$ satisfying $|B| \geq \delta|A|$ contains a 3-term AP. We may now restate Roth's theorem as follows. For every positive δ , there exists an n_0 such that the set $[n]$ is δ -Roth whenever $n \geq n_0$. With the aim of showing that there exist 'smaller' and 'sparser' δ -Roth sets Kohayakawa, Łuczak, and Rödl [29] proved the following result.

Theorem 9 ([29]). *For every positive δ , there exists a constant C such that if $C\sqrt{n} \leq m \leq n$, then the probability that a uniformly chosen random m -element subset of $\{1, \dots, n\}$ is δ -Roth tends to 1 as $n \rightarrow \infty$.*

We shall deduce Theorem 9 as an easy corollary of the following upper bound for the number of subsets of $[n]$ of a given cardinality that do not contain a 3-term AP, originally proved in [7] and [40] in a much more general form. This upper bound will be derived from Roth's theorem using Lemma 2 with one additional twist which was previously considered in [2].

Theorem 10. *For every positive ε , there exists a constant D such that if $D\sqrt{n} \leq m \leq n$,*

$$|\{A \subseteq [n] : |A| = m \text{ and } A \text{ contains no 3-term AP}\}| \leq \binom{\varepsilon n}{m}.$$

Proof of Theorem 9. Fix a positive δ , let $\varepsilon = \delta/6$, and let D be the constant from the statement of Theorem 10. Let $C = D/\delta$ and suppose that $C\sqrt{n} \leq m \leq n$. Since $\lceil \delta m \rceil \geq D\sqrt{n}$, Theorem 10 implies that the set \mathcal{A} defined by

$$\mathcal{A} = \{A \subseteq [n] : |A| = \lceil \delta m \rceil \text{ and } A \text{ contains no 3-term AP}\}$$

has at most $\binom{\varepsilon n}{\lceil \delta m \rceil}$ elements. Now, let R be an m -element subset of $[n]$ chosen uniformly at random. Clearly,

$$\begin{aligned} \Pr(R \text{ is not } \delta\text{-Roth}) &= \Pr(R \supseteq A \text{ for some } A \in \mathcal{A}) \leq \sum_{A \in \mathcal{A}} \Pr(R \supseteq A) \leq \sum_{A \in \mathcal{A}} \left(\frac{m}{n}\right)^{|A|} \\ &= |\mathcal{A}| \cdot \left(\frac{m}{n}\right)^{\lceil \delta m \rceil} \leq \binom{\varepsilon n}{\lceil \delta m \rceil} \cdot \left(\frac{m}{n}\right)^{\lceil \delta m \rceil} \leq \left(\frac{\varepsilon n}{\lceil \delta m \rceil} \cdot \frac{m}{n}\right)^{\lceil \delta m \rceil} \leq 2^{-\delta m}. \quad \square \end{aligned}$$

Our proof of Theorem 10 will use the following simple consequence of Roth's theorem, observed first by Varnavides [45], as a 'black box'.

Proposition 11 ([35, 45]). *For every positive δ , there exist an integer n_0 and a positive β such that if $n \geq n_0$, then every set of at least δn integers from $\{1, \dots, n\}$ contains at least βn^2 3-term APs.*

Proof of Theorem 10. Fix a positive ε , let n_0 and β be the constants from the statement of Proposition 11 invoked with $\delta = \varepsilon/2$, and suppose that $n \geq n_0$. Given an arbitrary set $B \subseteq [n]$ and integers m and n' , let

$$\begin{aligned} a(B, m) &= |\{I \subseteq B: |I| = m \text{ and } I \text{ contains no 3-term AP}\}|, \\ a(n', m) &= \max \{a(B, m): B \subseteq [n] \text{ with } |B| = n'\}. \end{aligned}$$

Our aim is to show that $a([n], m) = a(n, m) \leq \binom{\varepsilon n}{m}$, provided that $m \geq C\sqrt{n}$ for some constant C which depends only on ε . This inequality will follow from the trivial observation that $a(n', m) \leq \binom{n'}{m}$ for all n' and m and the following claim.

Claim. If $n' \geq \varepsilon n/2$ and $m \geq 2\lfloor \sqrt{n} \rfloor$, then $a(n', m) \leq 2\binom{n}{\lfloor \sqrt{n} \rfloor}^2 \cdot a(n' - \lfloor \beta n/12 \rfloor, m - 2\lfloor \sqrt{n} \rfloor)$.

Let \mathcal{H} be the 3-uniform hypergraph with vertex set $[n]$ whose edges are all triples of numbers which form a 3-term AP. Let B be an arbitrary n' -element subset of $[n]$. By Proposition 11, $e_{\mathcal{H}}(B) \geq \beta n^2$. Let $Z \subseteq B$ be the set of all vertices of $\mathcal{H}[B]$, the subhypergraph of \mathcal{H} induced by B , whose degree is at least βn . In other words, Z is the set of all numbers in B that belong to at least βn three-term APs contained in B . Since the maximum degree of \mathcal{H} is at most $2n$, we have $|Z| \geq \beta n$.

We first estimate the number of m -element subsets of B with no 3-term AP that contain fewer than \sqrt{n} elements of Z . Since each such set A may be partitioned into A_1 and A_2 , where $|A_1| = \lfloor \sqrt{n} \rfloor$ and $A_2 \subseteq B \setminus Z$, there are at most $\binom{n}{\lfloor \sqrt{n} \rfloor} \cdot a(n' - \lfloor \beta n \rfloor, m - \lfloor \sqrt{n} \rfloor)$ such sets. We may therefore focus on counting subsets of B that contain at least \sqrt{n} elements of Z . We shall obtain a suitable upper bound for their number using Lemma 2.

Let W be an arbitrary subset of Z and consider the auxiliary graph G_W with vertex set B whose edges are all pairs $\{x, y\}$ such that $\{x, y, z\} \in \mathcal{H}$ for some $z \in W$. Since for a given pair $\{x, y\} \subseteq [n]$, there are at most three different z such that $\{x, y, z\} \in \mathcal{H}$, it follows that $e(G_W) \geq |W|\beta n/3$ and the maximum degree of G_W is no more than $3|W|$. It follows that for an arbitrary subset U of B with at least $n' - \beta n/12$ elements,

$$e_{G_W}(U) \geq e(G_W) - |B \setminus U| \cdot \Delta(G_W) \geq \frac{\beta n |W|}{3} - \frac{\beta n}{12} \cdot 3|W| = \frac{\beta n |W|}{12}. \quad (16)$$

Observe crucially that if some set $I \cup W$ contains no 3-term APs, then I is an independent set in the graph G_W .

Let $w = \lfloor \sqrt{n} \rfloor$ and fix some $W \subseteq Z$ with $|W| = w$. We shall prove an upper bound on the number of ways one can extend W to an m -element subset of B that contains no 3-term APs. By our above discussion, if $I \cup W$ is such a set, then I is an independent set of G_W with $m - w$ elements. Let \mathcal{S} be the family of sets and let f and g be the maps whose existence is postulated by Lemma 2 with $G = G_W$, $q = \lfloor \sqrt{n} \rfloor$, $R = n' - \lceil \beta n / 12 \rceil$, and $D = \beta w / 6$. Note that the assumptions of the lemma are satisfied by our discussion above, see (16). Since clearly for each extension I of W to an m -element subset of B with no 3-term APs, $I \cap f(g(I))$ contains no 3-term APs, the number E_W of extensions of W satisfies

$$E_W \leq \sum_{S \in \mathcal{S}} a(f(S), m - w - q) \leq \binom{n}{q} \cdot a(R, m - w - q).$$

We conclude that

$$\begin{aligned} a(B, m) &\leq \binom{n}{\lfloor \sqrt{n} \rfloor} \cdot a(n' - \lceil \beta n \rceil, m - \lfloor \sqrt{n} \rfloor) + \sum_{W \subseteq Z: |W|=w} E_W \\ &\leq \binom{n}{\lfloor \sqrt{n} \rfloor}^2 \cdot a(n' - \lceil \beta n \rceil, m - 2\lfloor \sqrt{n} \rfloor) + \binom{n}{w} \binom{n}{q} \cdot a(n' - \lceil \beta n / 12 \rceil, m - 2\lfloor \sqrt{n} \rfloor) \\ &\leq 2 \binom{n}{\lfloor \sqrt{n} \rfloor}^2 \cdot a(n' - \lceil \beta n / 12 \rceil, m - 2\lfloor \sqrt{n} \rfloor), \end{aligned}$$

which, since B was an arbitrary n' -element subset of $[n]$, proves the claim.

Let $K = \lceil (12 - 6\varepsilon) / \beta \rceil$ and suppose that $m \geq \sqrt{n}$. We recursively invoke the claim K times to obtain

$$a(n, m) \leq 2^K \binom{n}{\lfloor \sqrt{n} \rfloor}^{2^K} \binom{\varepsilon n / 2}{m - 2K \lfloor \sqrt{n} \rfloor} \leq 2^K \binom{2Kn}{2K \lfloor \sqrt{n} \rfloor} \binom{\varepsilon n / 2}{m - 2K \lfloor \sqrt{n} \rfloor}. \quad (17)$$

As in the proof of Theorem 7, denote by $r(t)$ the right-hand side of (17) with $2K \lfloor \sqrt{n} \rfloor$ replaced by t . We may clearly assume that $m < \varepsilon n / 4$ as otherwise $a(n, m) = 0$ by Roth's theorem (we may assume that n is sufficiently large). An elementary calculation shows that

$$\frac{r(t+1)}{r(t)} = \frac{2Kn - t}{t+1} \cdot \frac{m-t}{\varepsilon n / 2 - m + t + 1} \leq \frac{2Knm}{(t+1)(\varepsilon n / 2 - m)} \leq \frac{8Km}{\varepsilon(t+1)}$$

and hence, letting $T = 2K \lfloor \sqrt{n} \rfloor$,

$$a(n, m) \leq r(T) \leq 2^K \cdot \frac{(8Km)^T}{\varepsilon^T T!} \cdot \binom{\varepsilon n / 2}{m} \leq 2^K \cdot \left(\frac{8eKm}{\varepsilon T} \right)^T \cdot \left(\frac{1}{2} \right)^m \binom{\varepsilon n}{m}.$$

Finally, if D is sufficiently large as a function of K and ε , then for every m with $m \geq D\sqrt{n} \geq D/(2K) \cdot T$, we have

$$2^{K/m} \cdot \left(\frac{8eKm}{\varepsilon T} \right)^{T/m} \leq 2,$$

which completes the proof of the theorem. \square

4. CONCLUDING REMARKS AND FURTHER READING

4.1. Other applications of the Kleitman–Winston method. There have been quite a few successful applications of the Kleitman–Winston method other than the ones presented in Section 3. In particular, variants of Lemma 1 were used in the following works: Kleitman and Wilson [25] proved that the number of n -vertex graphs with girth larger than 2ℓ is $2^{O(n^{1+1/\ell})}$; Dellamonica, Kohayakawa, Lee, Rödl, and the author [14, 15, 28] proved sharp bounds on the number of subsets of $[n]$ with a given cardinality which contain no non-trivial solutions to the equation $a_1 + \dots + a_h = b_1 + \dots + b_h$ for every $h \geq 2$; Balogh, Das, Delcourt, Liu, and Sharifzadeh [6] and Gauy, Hàn, and Oliveira [18] proved sharp bounds for the number of intersecting families of k -element subsets of $[n]$ with a given cardinality and for the typical size of the largest intersecting subfamily contained in a random collection of k -element subsets of $[n]$; Bansal, Pendavingh, and van der Pol [10] proved strong bounds on the number of matroids on n elements.

4.2. Extensions of the Kleitman–Winston method to hypergraphs. It seems natural to seek a generalisation of the Kleitman–Winston method that would yield non-trivial upper bounds for the number of independent sets in a hypergraphs of higher uniformity. Perhaps somewhat surprisingly, such generalisations were considered only fairly recently. To the best of our knowledge this was first done in [8, 9], where sharp upper bounds for the number of n -vertex graphs which do not contain a copy of a fixed complete bipartite subgraph were proved using a generalisation of the argument presented in Section 3.4. Around the same time, similar ideas were developed by Saxton and Thomason, who used them to establish lower bounds for the list chromatic number of regular uniform hypergraphs [41]. Inspired by the groundbreaking work of Conlon and Gowers [13] and Schacht [42], these efforts culminated in far-reaching generalisations of the Kleitman–Winston method to arbitrary uniform hypergraphs, obtained independently by Saxton and Thomason [40], and by Balogh, Morris, and the author [7]. For further details, we refer the interested reader to [7, 12, 13, 36, 40, 42].

Acknowledgments. I would like to thank Noga Alon, Józsi Balogh, Domingos Dellamonica, Yoshi Kohayakawa, Sang June Lee, Rob Morris, and Vojta Rödl for many interesting discussions on the topics of independent sets in graphs and the Kleitman–Winston method and its applications over the past several years. These discussions have greatly influenced the content of this paper. I would also like to thank David Conlon, Asaf Ferber, and Rob Morris for their careful reading of an earlier version of this manuscript and many valuable comments which helped me improve the exposition and saved me from making several embarrassing mistakes. Finally, special thanks to Jarik Nešetřil for his encouragement to write this survey.

REFERENCES

1. N. Alon, *Independent sets in regular graphs and sum-free subsets of finite groups*, Israel J. Math. **73** (1991), 247–256.
2. N. Alon, J. Balogh, R. Morris, and W. Samotij, *Counting sum-free sets in abelian groups*, Israel J. Math. **199** (2014), 309–344.
3. ———, *A refinement of the Cameron–Erdős conjecture*, Proc. Lond. Math. Soc. (3) **108** (2014), 44–72.
4. 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.
5. N. Alon and V. Rödl, *Sharp bounds for some multicolor Ramsey numbers*, Combinatorica **25** (2005), 125–141.

6. J. Balogh, S. Das, M. Delcourt, H. Liu, and M. Sharifzadeh, *The typical structure of intersecting families of discrete structures*, arXiv:1408.2559 [math.CO].
7. J. Balogh, R. Morris, and W. Samotij, *Independent sets in hypergraphs*, to appear in J. Amer. Math. Soc.
8. J. Balogh and W. Samotij, *The number of $K_{m,m}$ -free graphs*, *Combinatorica* **31** (2011), 131–150.
9. ———, *The number of $K_{s,t}$ -free graphs*, *J. Lond. Math. Soc. (2)* **83** (2011), 368–388.
10. N. Bansal, R. A. Pendavingh, and J. G. van der Pol, *On the number of matroids*, to appear in *Combinatorica*.
11. W. G. Brown, *On graphs that do not contain a Thomsen graph*, *Canad. Math. Bull.* **9** (1966), 281–285.
12. D. Conlon, *Combinatorial theorems relative to a random set*, arXiv:1404.3324 [math.CO].
13. D. Conlon and W. T. Gowers, *Combinatorial theorems in sparse random sets*, arXiv:1011.4310 [math.CO].
14. D. Dellamonica Jr., Y. Kohayakawa, S. Lee, V. Rödl, and W. Samotij, *The number of B_3 -sets of a given cardinality*, submitted.
15. ———, *On the number of B_h -sets*, to appear in *Combin. Probab. Comput.*
16. P. Erdős, P. Frankl, and V. Rödl, *The asymptotic number of graphs not containing a fixed subgraph and a problem for hypergraphs having no exponent*, *Graphs Combin.* **2** (1986), 113–121.
17. P. Erdős, A. Rényi, and V. T. Sós, *On a problem of graph theory*, *Studia Sci. Math. Hungar.* **1** (1966), 215–235.
18. M. M. Gausy, H. Hàn, and I. C. Oliveira, *Erdős–Ko–Rado for random hypergraphs: asymptotics and stability*, arXiv:1409.3634 [math.CO].
19. B. Green, *The Cameron–Erdős conjecture*, *Bull. London Math. Soc.* **36** (2004), 769–778.
20. B. Green and I. Z. Ruzsa, *Counting sumsets and sum-free sets modulo a prime*, *Studia Sci. Math. Hungar.* **41** (2004), 285–293.
21. ———, *Sum-free sets in abelian groups*, *Israel J. Math.* **147** (2005), 157–188.
22. A. J. Hoffman, *On eigenvalues and colorings of graphs*, *Graph Theory and its Applications (Proc. Advanced Sem., Math. Research Center, Univ. of Wisconsin, Madison, Wis., 1969)*, Academic Press, New York, 1970, pp. 79–91.
23. S. Hoory, N. Linial, and A. Wigderson, *Expander graphs and their applications*, *Bull. Amer. Math. Soc. (N.S.)* **43** (2006), 439–561 (electronic).
24. J. Kahn, *An entropy approach to the hard-core model on bipartite graphs*, *Combin. Probab. Comput.* **10** (2001), 219–237.
25. D. J. Kleitman and D. B. Wilson, *On the number of graphs which lack small cycles*, manuscript, 1996.
26. D. J. Kleitman and K. J. Winston, *The asymptotic number of lattices*, *Ann. Discrete Math.* **6** (1980), 243–249, *Combinatorial mathematics, optimal designs and their applications (Proc. Sympos. Combin. Math. and Optimal Design, Colorado State Univ., Fort Collins, Colo., 1978)*.
27. ———, *On the number of graphs without 4-cycles*, *Discrete Math.* **41** (1982), 167–172.
28. Y. Kohayakawa, S. Lee, V. Rödl, and W. Samotij, *The number of Sidon sets and the maximum size of Sidon sets contained in a sparse random set of integers*, *Random Structures & Algorithms* **46** (2015), 1–25.
29. Y. Kohayakawa, T. Łuczak, and V. Rödl, *Arithmetic progressions of length three in subsets of a random set*, *Acta Arith.* **75** (1996), 133–163.
30. Ph. G. Kolaitis, H. J. Prömel, and B. L. Rothschild, *K_{l+1} -free graphs: asymptotic structure and a 0-1 law*, *Trans. Amer. Math. Soc.* **303** (1987), 637–671.
31. T. Kővari, V. T. Sós, and P. Turán, *On a problem of K. Zarankiewicz*, *Colloquium Math.* **3** (1954), 50–57.
32. V. F. Lev, T. Łuczak, and T. Schoen, *Sum-free sets in abelian groups*, *Israel J. Math.* **125** (2001), 347–367.
33. W. Mantel, *Problem 28*, *Wiskundige Opgaven* **10** (1907), 60–61.
34. R. Morris and D. Saxton, *The number of $C_{2\ell}$ -free graphs*, arXiv:1309.2927 [math.CO].
35. K. F. Roth, *On certain sets of integers*, *J. London Math. Soc.* **28** (1953), 104–109.
36. W. Samotij, *Stability results for random discrete structures*, *Random Structures Algorithms* **44** (2014), 269–289.
37. A. A. Sapozhenko, *On the number of independent sets in extenders*, *Diskret. Mat.* **13** (2001), 56–62.
38. ———, *Asymptotics of the number of sum-free sets in abelian groups of even order*, *Dokl. Akad. Nauk* **383** (2002), 454–457.
39. ———, *The Cameron–Erdős conjecture*, *Dokl. Akad. Nauk* **393** (2003), 749–752.
40. D. Saxton and A. Thomason, *Hypergraph containers*, arXiv:1204.6595 [math.CO].
41. ———, *List colourings of regular hypergraphs*, *Combin. Probab. Comput.* **21** (2012), 315–322.
42. M. Schacht, *Extremal results for random discrete structures*, submitted.
43. E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression*, *Acta Arith.* **27** (1975), 199–245.

44. P. Turán, *Eine Extremalaufgabe aus der Graphentheorie*, Mat. Fiz. Lapok **48** (1941), 436–452.
45. P. Varnavides, *On certain sets of positive density*, J. London Math. Soc. **34** (1959), 358–360.
46. Y. Zhao, *The number of independent sets in a regular graph*, Combin. Probab. Comput. **19** (2010), 315–320.

SCHOOL OF MATHEMATICAL SCIENCES, TEL AVIV UNIVERSITY, TEL AVIV 69978, ISRAEL; AND TRINITY COLLEGE,
CAMBRIDGE CB2 1TQ, UK

E-mail address: `samotij@post.tau.ac.il`