106

ISRAEL JOURNAL OF MATHEMATICS, Vol. 73, No. 2, 1991

INDEPENDENT SETS IN REGULAR GRAPHS AND SUM-FREE SUBSETS OF FINITE GROUPS

BY

NOGA ALON†

Department of Mathematics

Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv, Israel

ABSTRACT

It is shown that there exists a function $\epsilon(k)$ which tends to 0 as k tends to infinity, such that any k-regular graph on n vertices contains at most $2^{(1/2+\epsilon(k))n}$ independent sets. This settles a conjecture of A. Granville and has several applications in Combinatorial Group Theory.

1. Introduction

All graphs considered here are finite, undirected and simple. For a graph $G = (V, E)$, let $I(G)$ denote the number of independent sets of G. During the 1988 Number Theory Conference at Banff, A. Granville (private communication from P. Erdös) conjectured that for any k-regular graph G on n vertices, $I(G) \leq 2^{(1/2+\epsilon(k))n}$, where $\epsilon(k)$ tends to 0 as k tends to infinity. Note that, since any k-regular bipartite graph on n vertices contains at least $2^{n/2+1} - 1$ independent sets, this conjecture, if true, is best possible, up to the actual behavior of the best possible error term $\epsilon(k)$.

In the present paper we settle Granville's conjecture by proving the following.

THEOREM 1.1 *For any k-regular graph G on n vertices,* $I(G) \leq 2^{(1/2+O(k^{-0.1}))n}$.

The estimate $O(k^{-0.1})$ can be easily improved, but since it seems that our method cannot supply the best possible estimate, we do not make any attempts to optimize our estimates here and throughout the paper. It is also worth noting that our method actually implies that if G is a graph on n vertices with minimum de-

†Research supported in part by the United States–Israel Binational Science Foundation and by a Bergmann Memorial Grant.

Received August 9, 1989 and in revised form October 18, 1990

gree δ and maximum degree Δ, then $I(G) \le 2^{(1/2+f(\delta,\Delta))n}$, where $f(\delta,\Delta)$ tends to zero when $\delta \to \infty$, $\Delta/\delta \to 1$. To simplify the presentation, we do not prove this stronger result (whose proof is analogous to that of Theorem 1.1 presented here) in detail.

By applying Theorem 1.1 to Cayley graphs, one can obtain several applications in Combinatorial Group Theory. For a finite group G and for a set $S \subseteq G$, we call a subset $A \subseteq G$ *S-free* if $AS \cap A = \emptyset$, i.e., if there are no $s \in S$ and $a_1, a_2 \in A$ such that $a_1 s = a_2$. Theorem 1.1 implies the following.

THEOREM 1.2. *Let G be a group of order n and suppose* $S \subseteq G$, $|S| = k$. *Then, the number of S-free subsets of G does not exceed* $2^{(1/2+O(k^{-0.1}))n}$.

Notice that if G has a subgroup H of index 2 and $S \subset G \backslash H$ then all the $2^{n/2}$ subsets of the coset $G \backslash H$ are S-free, showing that the last theorem is essentially best possible.

A subset A of a finite group G is called *sum-free* (or *product-free*) if $A \cdot A \cap A = \emptyset$, i.e., if there are no $a_1, a_2, a_3 \in A$ such that $a_1 a_2 = a_3$. As observed by Granville, Theorem 1.2 implies the following Corollary, which is, again, essentially best possible for any group containing a subgroup of index 2.

COROLLARY 1.3. *The number of sum-free subsets of any group G of order n is at most* $2^{(1/2+o(1))n}$, *where* $o(1)$ *tends to* 0 *as n tends to infinity.*

This result is closely related to some of the problems considered in [C],[CE]. See also [AK] and [WSW] for some related results.

The proof of Theorem 1.1 relies heavily on probabilistic arguments. In particular, it contains a somewhat surprising method presented in the next section of obtaining an exponentially small upper bound for the probability of a certain event. This method together with the well-known Kruskal–Katona theorem ([Kr],[Ka]) enables us to prove a variant of Theorem 1.1 for bipartite graphs. The general case is then deduced, in section 3, by applying the Lovász Local Lemma [EL]. In section 4 we describe the applications in Combinatorial Group Theory. The final section 5 contains some concluding remarks and open problems.

2. Almost regular bipartite graphs

In this section, which is the heart of the paper, we prove the following variant of Theorem 1.1 for bipartite graphs. (From now on, whenever we write $g = O(f)$ we mean that $g \le cf$ for some absolute positive constant c).

THEOREM 2.1. *Let G be a bipartite graph on n vertices in which the degree of each vertex is at least* $k - k^{5/8}$ *and at most* $k + k^{5/8}$. *Then* $I(G) \le 2^{(1/2+O(k^{-0.1}))n}$.

The proof of this theorem is presented in the rest of this section. In the proof we assume, whenever it is needed, that k is sufficiently large.

Let U and V denote the two vertex-classes of G. Put $|U| = l$, $|V| = m$, and assume, without loss of generality, that $l \le m$. Observe that by the assumptions on the degrees $l \cdot (k + k^{5/8}) \ge m \cdot (k - k^{5/8})$ and thus

$$l \le m \le \frac{n}{2}\left(1 + O(k^{-3/8})\right). \tag{2.1}$$

The total number of sets of vertices A satisfying $|A \cap U| \le lk^{-1/2}$ does not exceed

$$2^m \sum_{i \le lk^{-1/2}} \binom{l}{i} \le 2^{m + lH_2(k^{-1/2})} < 2^{n/2(1+O(k^{-0.1}))}, \tag{2.2}$$

where here $H_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function, $\log_2$ is the logarithm in base 2, and we applied the standard estimates for binomial distributions (see, e.g., [ES]) to conclude that

$$\sum_{i \le lk^{-1/2}} \binom{l}{i} \le 2^{lH_2(k^{-1/2})}.$$

It thus suffices to bound the number of independent sets of vertices containing at least $lk^{-1/2}$ members of U. For a subset $A \subseteq U$ let $N(A)$ denote the set of their neighbors in V. A is called an *s-set* if $|N(A)| = s$. Let $I(s,t)$ denote the number of s sets of cardinality t. The total number of independent sets in G is clearly

$$\sum_{t=0}^{l} \sum_{s=0}^{m} I(s,t) \cdot 2^{m-s}.$$

This is because if $A \subseteq U$ is an s-set there are precisely 2^{m-s} independent sets in G whose intersection with U is A. In view of (2.2) it suffices to consider the sets with at least $lk^{-1/2}$ vertices in U, i.e., to bound the sum

$$\sum_{lk^{-1/2} \le t \le l} \sum_{s=0}^{m} I(s,t) \cdot 2^{m-s}. \tag{2.3}$$

Put $t_0 = lk^{-1/2}$ and define $I'(s,t) = \sum_{i=1}^{s} I(i,t)$. Thus $I'(s,t)$ is the number of subsets of cardinality t in U which have at most s neighbors in V.

CLAIM 2.2.

$$I'(s,t_0) \le \binom{s+O(lk^{-1/7})}{t_0}.$$

PROOF. Since our graph is almost regular, $I(s,t_0)=0$ for, say, $s<\frac{1}{2}t_0$ and hence we may assume $s>\frac{1}{2}t_0$. (This is because for every subset B of U, $|N(B)| \ge |B|(k-k^{5/8})/(k+k^{5/8}) = |B|(1-O(k^{-3/8}))$.) Let us choose an ordered random subset $A=(v_1,v_2,\ldots,v_{t_0})$ of cardinality t_0 in U by choosing its elements, one by one, randomly and independently, where in each step an element of U is chosen randomly according to a uniform distribution among those members of U not chosen so far. Let us call the choice of v_i a *failure* if

$$|N(\{v_1,\ldots,v_{i-1}\})| \le s \quad \text{and} \quad |N(\{v_1,\ldots,v_i\})\setminus N(\{v_1,\ldots,v_{i-1}\})| \le k^{2/3}.$$

FACT 2.3. For every given fixed choice of $v_1,\ldots,v_{i-1}$, the conditional probability p that the choice of v_i is a failure is at most $s/l+ck^{-1/3}$, for some absolute positive constant c.

PROOF. If $N(\{v_1,\ldots,v_{i-1}\})>s$ then $p=0$ and the Fact follows. Otherwise, there are at least $m-s$ vertices in $V\setminus N(\{v_1,\ldots,v_{i-1}\})$. For each such vertex u, the probability that it is a neighbor of the new chosen vertex v_i is precisely $d_G(u)/(l-i+1) \ge (k-k^{5/8})/l$, where $d_G(u)$ is the degree of u in G. It follows that the expected value of

$$Y=|N(\{v_1,\ldots,v_i\})\setminus N(\{v_1,\ldots,v_{i-1}\})|$$

is at least

$$\frac{m-s}{l}(k-k^{5/8}) \ge \left(1-\frac{s}{l}\right)(k-k^{5/8}).$$

Since the random variable Y is never more than $k+k^{5/8}$ it follows that

$$pk^{2/3}+(1-p)(k+k^{5/8}) \ge \left(1-\frac{s}{l}\right)(k-k^{5/8}).$$

Therefore $p \le s/l+O(k^{-1/3})$, establishing Fact 2.3. ■

Returning to the proof of Claim 2.2, observe that if for $A=(v_1,,\ldots,,v_{t_0})$ we have

$$|N(\{v_1,,\ldots,,v_{t_0}\})| \le s$$

then

$$|N(\{v_1,,\ldots,,v_i\})\backslash N(\{v_1,,\ldots,,v_{i-1}\})| \ge k^{2/3}$$

for no more than $s/k^{2/3}$ values of i. Thus, the number of failures is at least $t_0 - s/k^{2/3} \ge t_0 - O(t_0 k^{-1/6})$, where here we used the fact that $s \le m$ and $t_0 = lk^{-1/2}$. By Fact 2.3, the conditional probability of every failure, given all the previous choices, is small. Hence, the probability of having at least $t_0 - O(t_0 k^{-1/6})$ failures is at most

$$\binom{t_0}{O(t_0 k^{-1/6})}\left(\frac{s}{l} + ck^{-1/3}\right)^{t_0 - O(t_0 k^{-1/6})}. \tag{2.4}$$

Since

$$\binom{t_0}{O(t_0 k^{-1/6})} \le (1 + O(k^{-1/7}))^{t_0},$$

and since, as $s/l > t_0/2l = 1/2\sqrt{k}$, we have

$$\left(\frac{s}{l} + ck^{-1/3}\right)^{-O(t_0 k^{-1/6})} \le (1 + O(k^{-1/7}))^{t_0},$$

the quantity (2.4) is at most

$$\left(\frac{s}{l} + O(k^{-1/7})\right)^{t_0} \le \left(\frac{s - t_0 + O(lk^{-1/7})}{l}\right)^{t_0}$$

$$\le \binom{s + O(lk^{-1/7})}{t_0} \cdot \frac{t_0!}{l^{t_0}}.$$

We have thus proved that the probability that an ordered random subset A of cardinality t_0 in U has at most s neighbors in V does not exceed

$$\binom{s + O(lk^{-1/7})}{t_0} \cdot \frac{t_0!}{l^{t_0}}.$$

Since there are $l(l-1)\cdot \ldots \cdot (l - t_0 + 1)$ possibilities for choosing an ordered set A of t_0 vertices, and since any unordered set of cardinality t_0 is counted in this manner $t_0!$ times, we conclude that

$$I'(s, t_0) \le \frac{l(l-1)\cdot\ldots\cdot(l-t_0+1)}{t_0!}\binom{s+O(lk^{-1/7})}{t_0} \cdot \frac{t_0!}{l^{t_0}} \le \binom{s+O(lk^{-1/7})}{t_0}.$$

This completes the proof of Claim 2.2. ■

For a family $\mathfrak{F}$ of t_1-sets and for $t_1 \geq t_2$, the *t_2-shadow of* $\mathfrak{F}$, denoted $\partial^{(t_2)}(\mathfrak{F})$, is defined by $\partial^{(t_2)}(\mathfrak{F}) = \{B : |B| = t_2$ and $B \subseteq F$ for some $F \in \mathfrak{F}\}$. We need the following well-known result.

PROPOSITION 2.4 (A special case of the Kruskal–Katona theorem; see [Kr],[Ka]). *If $t_1 \geq t_2$, $\mathfrak{F}$ is a family of t_1-sets and $|\mathfrak{F}| \geq \binom{x}{t_1}$ then $|\partial^{(t_2)}(\mathfrak{F})| \geq \binom{x}{t_2}$.* ■

COROLLARY 2.5. *For every t, $t_0 \leq t \leq l$, and for every s, $1 \leq s \leq m$,*

$$I'(s,t) \leq \binom{s + O(lk^{-1/7})}{t}.$$

PROOF. Define $\mathcal{A}_t = \{A : A \subseteq U, |A| = t$ and $|N(A)| \leq s\}$. By Claim 2.2,

$$|\mathcal{A}_{t_0}| \leq \binom{s + O(lk^{-1/7})}{t_0}.$$

Clearly, for every $t \geq t_0$, $\partial^{(t_0)}(\mathcal{A}_t) \subseteq \mathcal{A}_{t_0}$. The result now follows from Proposition 2.4. ■

We can now complete the proof of Theorem 2.1. By the last Corollary, the sum given in (2.3) is at most

$$\begin{aligned}
\sum_{lk^{-1/7} \leq t \leq l} \sum_{s=0}^{m} \binom{s + O(lk^{-1/7})}{t} 2^{m-s} &= \sum_{s=0}^{m} 2^{m-s} \sum_{lk^{-1/7} \leq t \leq l} \binom{s + O(lk^{-1/7})}{t} \\
&\leq \sum_{s=0}^{m} 2^{m-s} \cdot 2^{s+O(lk^{-1/7})} \\
&= m 2^{m+O(lk^{-1/7})} \\
&\leq 2^{(1/2+O(k^{-0.1}))n},
\end{aligned}$$

where the last inequality follows from inequality (2.1). This completes the proof of Theorem 2.1. ■

3. General regular graphs

In this section we show how to derive Theorem 1.1 from Theorem 2.1. This is done by applying the Lovász Local Lemma, proved in [EL] (see also, e.g., [GRS]), which is the following.

LEMMA 3.1 (The Lovász Local Lemma [EL]). *Let $A_1, A_2, \ldots, A_n$ be events in a probability space. Suppose that each event A_i is mutually independent of all the other events but at most d and that $\Pr(A_i) \leq p$ for all $1 \leq i \leq n$. If $ep(d+1) <$*

1, *where* $e = 2.718\ldots$ *is the basis of the natural logarithm, then with positive probability no event* A_i *holds.* ■

The following simple corollary is very similar to Lemma 2.4 in [AA].

COROLLARY 3.2. *Every k-regular graph* $G = (V, E)$ *where, say,* $k \geq 100$, *contains a spanning bipartite subgraph H in which the degree of each vertex is at least* $k/2 - 2\sqrt{k \log k}$ *and at most* $k/2 + 2\sqrt{k \log k}$.

PROOF. Let $f: V \to \{0,1\}$ be a random function, i.e., a random two-coloring of V obtained by choosing, for each $u \in V$ independently, a color $f(u) \in \{0,1\}$ according to a uniform distribution on $\{0,1\}$. For each vertex $u \in V$, let A_u be the event that u has more than $k/2 + 2\sqrt{k \log k}$ neighbors having the same color. By the standard estimates for the probability in the tail of the binomial distribution (see, e.g., [ES]), it is easy to check that for every $u \in V$

$$\Pr(A_u) \leq k^{-3}.$$

However, each event A_u is mutually independent of all the other events A_v, besides those vertices v that have a common neighbor with u. Since there are at most $k(k-1)$ such vertices v, Lemma 3.1 implies that with positive probability no event A_u holds. Put $V_0 = f^{-1}(0)$ and $V_1 = f^{-1}(1)$ and let H be the spanning bipartite subgraph of G on the classes of vertices V_0 and V_1 whose edges are all edges of G joining vertices from distinct classes. Clearly H satisfies the conclusion of Corollary 3.2. ■

PROOF OF THEOREM 1.1. Let G be a k-regular graph on n vertices. By Corollary 3.2, if k is sufficiently large G has a spanning bipartite subgraph H in which the degree of each vertex is at least $k/2 - (k/2)^{5/8}$ and at most $k/2 + (k/2)^{5/8}$. Since any independent set in G is also independent in H, $I(G) \leq I(H)$. However, by Theorem 2.1

$$I(H) \leq 2^{(1/2 + O(k^{-0.1}))n},$$

and hence

$$I(G) \leq 2^{(1/2 + O(k^{-0.1}))n},$$

completing the proof. ■

4. Combinatorial group theory

Let G be a finite group. As defined in section 1, for a set $S \subseteq G$ (which does not contain the identity of G) and for $A \subseteq G$, A is called *S-free* if $AS \cap A = \emptyset$. Recall that the *Cayley graph* $H(G,S)$ of G with respect to S is the graph whose set of vertices consists of all elements in G, in which g and g' are adjacent if and only if there is an $s \in S$ such that $gs = g'$ or $g's = g$. Clearly $H(G,S)$ is l-regular where $l = |S \cup S^{-1}|$. It is also obvious that every S-free set is an independent set in $H(G,S)$. Therefore, one can apply Theorem 1.1 to $H(G,S)$ and conclude that the number of S-free subsets of G is at most

$$2^{(1/2+O(|S|^{-0.1}))|G|},$$

as asserted in Theorem 1.2. ■

To prove Corollary 1.3 we argue as follows. Let G be a group of order n. The total number of subsets of cardinality at most, say, $\log n$ of G is

$$\sum_{i=0}^{\log n} \binom{n}{i} = 2^{o(n)}.$$

It thus suffices to bound the number of sum-free subsets of G containing at least $\log n$ elements. Let us order the elements of G arbitrarily. For each sum-free subset A of G containing at least $\log n$ elements, let $S = S_A$ be the set of the first $\log n$ elements of A, according to our chosen order. Clearly A is an S-free subset of G. Thus, by Theorem 1.2, for each fixed S there are at most

$$2^{(1/2+O((\log n)^{-0.1}))n} = 2^{(1/2+o(1))n}$$

possible choices for A. As there are

$$\binom{n}{\log n} = 2^{o(n)}$$

possible sets S, it follows that the total number of sum-free subsets in G does not exceed $2^{(1/2+o(1))n}$. This establishes Corollary 1.3. ■

Note that the upper bound in Corollary 1.3 holds even if we define a sum-free set to be any set A such that there are no $a_1, a_2, a_3 \in A$ satisfying $a_1 a_2 = a_3$, where a_2 belongs to the first, say, $\log n$ elements of A. It is also worth noting that an easy modification in the last proof yields the following result, which was, in fact, Granville's original motivation for raising his conjecture on regular graphs.

PROPOSITION 4.1. *The number of sum-free subsets of the set of integers* $\{1,2,\ldots,n\}$ *(with respect to usual addition) is at most* $2^{(1/2+o(1))n}$. ■

This result, with a somewhat worse estimate for the error term than the one that follows from our proof, has recently been proved also by Erdös and Granville, and, independently, by N. Calkin [C]. This solves one of the questions raised by Cameron in [Ca], as it easily implies that the Hausdorff dimension of the set of all sum-free sets of positive integers is $\frac{1}{2}$. Cameron (see [CE]) conjectured that in fact the number in the Proposition does not exceed $O(2^{n/2})$. Our method does not suffice to prove this stronger assertion but it yields the upper bound $2^{(1/2+o(1))n}$ even if we define a set A to be sum-free if there are no $a_1, a_2, a_3 \in A$ with $a_1 + a_2 = a_3$, where a_2 belongs to the smallest $f(n)$ elements of A, for any function $f(n)$ that tends to infinity with n.

5. Concluding remarks and open problems

The disjoint union of $n/2k$ complete k-regular bipartite graphs is a k-regular graph G on n vertices satisfying

$$I(G) = (2^{k+1} - 1)^{n/2k} = 2^{(1/2+\theta(1/k))n}.$$

It seems plausible that this graph has the maximum possible number of independent sets among all k-regular graphs on n vertices.

The number of sum-free sets in the group $G = (Z_2)^n$, which has order $N = 2^n$, is at least $2^{N/2+\Omega(n)} = 2^{N/2+\Omega(\log N)}$, since for each fixed non-zero vector $\epsilon = (\epsilon_1, \ldots, \epsilon_n) \in G$, any set of vectors whose scalar product (modulo 2) with ϵ is 1 is sum-free. This shows that the $o(n)$ term in the exponent in Corollary 1.3 is needed. It would be interesting to obtain a best possible version of Corollary 1.3.

An extension of Theorem 1.1 to hypergraphs may also be interesting.

ACKNOWLEDGEMENT

I would like to thank P. Erdös and Zs. Tuza for many helpful comments.

REFERENCES

[AA] I. Algor and N. Alon, *The star-arboricity of graphs*, Discrete Math. **75** (1989), 11–22.

[AK] N. Alon and D. J. Kleitman, *Sum-free subsets*, in *A Tribute to Paul Erdös* (A. Baker, B. Bollobás and A. Hajnal, eds.), Cambridge Univ. Press, 1990, pp. 13–26.

[C] N. J. Calkin, *On the number of sum-free sets*, to appear.

[Ca] P. J. Cameron, *Portrait of a typical sum-free set*, in *Surveys in Combinatorics 1987* (C. Whitehead, ed.), London Math. Soc. Lecture Notes **123**, Cambridge Univ. Press, 1987, pp. 13–42.

[CE] P. J. Cameron and P. Erdös, *On the number of sets of integers with various properties*, in *Proceedings of the 1988 Canadian Number Theory Conference at Banff* (R. Mollin, ed.), to appear.

[EL] P. Erdös and L. Lovász, *Problems and results on 3-chromatic hypergraphs and some related questions*, in *Infinite and Finite Sets* (A. Hajnal *et al.*, eds.), North-Holland, Amsterdam, 1975, pp. 609–628.

[ES] P. Erdös and J. Spencer, *Probabilistic Methods in Combinatorics*, Akadémiai Kiadó, Budapest, 1974, p. 18.

[GRS] R. L. Graham, B. L. Rothschild and J. H. Spencer, *Ramsey Theory*, Wiley, New York, 1980.

[Ka] G. O. H. Katona, *A theorem on finite sets*, in *Theory of Graphs* (P. Erdös and G. O. H. Katona, eds.), Akadémiai Kiadó, Budapest, 1968, pp. 187–207.

[Kr] J. B. Kruskal, *The number of simplices in a complex*, in *Mathematical Optimization Techniques*, Univ. of California Press, Berkeley, 1963, pp. 251–278.

[WSW] W. D. Wallis, Anne Penfold Street and Jennifer Seberry Wallis, *Combinatorics, Room Squares, Sum-free Sets, Hadamard Matrices*, Lecture Notes in Mathematics **292**, Springer-Verlag, Berlin, Heidelberg and New York, 1972, Part 3, pp. 123–277.