Constructive lower bounds for off-diagonal Ramsey numbers

Noga Alon [*] Pavel Pudlák [†]

February 22, 2002

Abstract

We describe an explicit construction which, for some fixed absolute positive constant ε, produces, for every integer $s > 1$ and all sufficiently large m, a graph on at least $m^{\varepsilon\sqrt{\log s/\log\log s}}$ vertices containing neither a clique of size s nor an independent set of size m.

1 Introduction

For two positive integers s and m, the Ramsey number $R(s,m)$ is the smallest integer R so that every graph on R vertices contains either a clique of size s or an independent set of size m. Equivalently, this is the smallest integer R so that in every 2-coloring of all edges of the complete graph on R vertices there is either a monochromatic clique of the first color on s vertices, or a monochromatic clique of the second color on m vertices. The fact that these numbers are finite for all s, m is a special case of Ramsey's well known theorem (see, e.g., [10]). In one of the first applications of the probabilistic method in combinatorics, Erdős [7] proved that $R(m,m) \geq \Omega(m2^{m/2})$. The problem of finding explicit edge colorings yielding a similar estimate is still open, despite a considerable amount of efforts by various researchers, and the best known explicit construction is due to Frankl and Wilson [9], who gave an explicit 2-edge coloring of the complete graph on $m^{(1+o(1))\frac{\log m}{4\log\log m}}$ vertices with no monochromatic clique on m vertices. See also [11], [2], for some multi-colored variations. These constructions do not supply any nontrivial explicit lower bounds for $R(s,m)$, where s is fixed and m grows. Such constructions for $s = 3$ appear in various papers, see [1], [6] (where it is shown that $R(3,m) \geq \Omega(m^{3/2})$ via an explicit construction) and their references. There is no known explicit construction that supplies an $\Omega(m^2)$ lower bound for $R(s,m)$, for any fixed s and large m, see, e.g., [3] for a construction that supplies a nearly quadratic bound.

In the present paper we describe larger explicit lower bounds for $R(s,m)$ for fixed s and large m. Our main result is the following.

Theorem 1.1 *There exists an $\varepsilon > 0$ and an explicit construction of graphs such that for every s and every sufficiently large m the construction produces a graph on at least $m^{\varepsilon\sqrt{\log s/\log\log s}}$ vertices containing neither a clique of size s nor an independent set of size m. This shows, constructively, that $R(s,m) > m^{\varepsilon\sqrt{\log s/\log\log s}}$.*

[*] Department of Mathematics, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv, Israel. Email: noga@math.tau.ac.il. Part of this work was done at the Institute for Advanced Study, Princeton, NJ 08540, USA. Research supported in part by a USA Israeli BSF grant, by a grant from the Israel Science Foundation and by the Hermann Minkowski Minerva Center for Geometry at Tel Aviv University.

[†] Mathematical Institute, Academy of Sciences of the Czech Republic, Prague, Czech Republic. Email: pudlak@math.cas.cz. Research supported in part by a grant A1019901 of the Academy of Sciences of the Czech Republic and by a cooperative research grant INT-9600919/ME-103 from the NSF (USA) and the MŠMT (Czech Republic)

The construction and the proof of its properties are given in the next section. The proof is not long, but combines several tools from various mathematical areas. These include some ideas from algebraic geometry obtained in [12], the well known bound of Weil on character sums, spectral techniques and their connection to the pseudo-random properties of graphs, the known bounds of [13] for the problem of Zarankiewicz and the well known Erdős-Rado bound for the existence of Δ-systems.

2 The construction and its properties

The proof of the theorem is based on the following general construction which can be applied to any graph G. The construction produces a graph which we shall call the clique graph of G. The clique graph has all cliques (of size at least 2) of G as vertices and two cliques K, L are connected by an edge if they are connected by an edge (u, v) in G such that (u, v) does not belong to neither of them, that is, $u \in K \setminus L$, $v \in L \setminus K$ and $(u, v) \in E(G)$. We shall use a subgraph of this graph consisting of all cliques of size exactly k, $k \geq 2$; it will be denoted by $CQ_k(G)$. The most interesting property of the k-clique graph of a graph is that it does not have a bigger independence number than that of the original graph G.

Lemma 2.1 *For every graph G and every k, $\alpha(CQ_k(G)) \leq \alpha(G)$.*

Proof. Let X be an independent set in $CQ_k(G)$. Let $L_1, L_2, K \in X$ be three different cliques. Then the intersections $L_1 \cap K$, $L_2 \cap K$ are comparable by inclusion, because otherwise a vertex in $L_1 \setminus L_2$ would be connected to one in $L_2 \setminus L_1$ by an edge in K. Thus, for K, there exists the maximal intersection of the form $K \cap L$, $L \in X$ and $L \neq K$. Hence in each member K of X, there exists $v \in K$ which is not contained in any other clique of X. Taking one such vertex from each K we get an independent set in G whose size is equal to the size of X. □

In order to bound the maximal size of a clique in $CQ_k(G)$, we need to assume some special property of G. Namely, the graph must be sparse on all sufficiently big subsets.

Lemma 2.2 *Suppose $CQ_k(G)$ contains a clique of size $> k!(l-1)^k$. Then in G there is a subset of at most kl vertices on which there are at least $\binom{l}{2}$ edges.*

Proof. Let X be such a clique in $CQ_k(G)$. Think of X as a set system. By the well-known theorem of Erdős and Rado [8], there exists a Δ-system (=sunflower) with l petals (that is, l sets so that all intersections of a pair of them are identical) contained in X. Since the cliques in the sunflower are connected, there are $\binom{l}{2}$ edges on the vertices of the petals. □

In what follows we use the norm graphs of Kollár, Rónyai and Szabó [12]. (It is possible to get a slightly better bound using a modified version of these, described in [4], but this makes no essential difference for our purpose here.) The norm graphs are defined as follows. Let q be a power of a prime, $t > 1$; for these parameters the graph will be denoted by $NG_{q,t}$. Let N denote the norm of elements of the finite field GF_{q^t} over GF_q, that is, $N(x) = x^{\frac{q^t-1}{q-1}}$. The vertices of $NG_{q,t}$ are elements of GF_{q^t}, two vertices a and b are connected, if $N(a+b) = 1$. In order to obtain a regular graph we shall allow also loops, i.e., one loop at every vertex a such that $N(2a) = 1$. In our discussion here t is fixed and q is large (although everything here holds for general parameters as well). We need the following properties of the graph $NG_{q,t}$.

1. The number of vertices, denoted by n, is q^t.

2. The graph is regular of degree $\frac{q^t-1}{q-1}$ (which is asymptotically $n^{1-\frac{1}{t}}$).

3. $NG_{q,t}$ does not contain $K_{t,t!+1}$.

4. The largest eigenvalue of the graph is $\frac{q^t-1}{q-1}$, the absolute value of each other eigenvalue is bounded by $\frac{(q-2)q^{t/2}}{q-1}$ (which is $< \sqrt{n}$).

5. The independence number (of the graph obtained from $NG_{q,t}$ by omitting all loops) is $O(n^{\frac{1}{2}+\frac{1}{t}})$.

6. For each $k \le \lceil t/2 \rceil$, the number of cliques of size k in $NG_{q,t}$ is $(1+o(1))\frac{1}{k!}n^{k-\binom{k}{2}/t}$.

The first two properties follow from the definition. The third one is proved in [12] using some tools from algebraic geometry. The forth property is proved in the following.

Lemma 2.3 *The largest eigenvalue of $NG_{q,t}$ is $\frac{q^t-1}{q-1}$, the absolute value of each of the others is bounded by $\frac{(q-2)q^{t/2}}{q-1}$.*

Proof. Let χ be a character of the additive group of GF_{q^t}. Let A be the adjacency matrix of $NG_{q,t}$. We shall compute the vector $A\chi$, where we interpret χ as a column vector. The value of this vector on the a-th position is

$$\sum_{N(a+b)=1} \chi(b) = \sum_{N(c)=1} \chi(c-a) = \sum_{N(c)=1} \chi(c)\overline{\chi(a)},$$

thus $A\chi = (\sum_{N(c)=1} \chi(c))\overline{\chi}$. Whence

$$A^2\chi = (\sum_{N(c)=1} \chi(c))\overline{(\sum_{N(c)=1} \chi(c))}\chi = |\sum_{N(c)=1} \chi(c)|^2\chi.$$

Hence χ is an eigenvector of A^2 with the eigenvalue $|\sum_{N(c)=1} \chi(c)|^2$. Since characters are orthogonal and their number is equal to the size of the group, they span the whole space and there are no other eigenvalues. The eigenvalues of A^2 are squares of the eigenvalues of A. Thus the largest eigenvalue of A is the one which corresponds to the trivial character, i. e., $\sum_{N(c)=1} 1 = \frac{q^t-1}{q-1}$ (the nonzero values of the norm are equally distributed among the nonzero elements of GF_q). The others (which are real, as A is symmetric) are among $\pm|\sum_{N(c)=1} \chi(c)|$ for nontrivial characters χ. We estimate those using Weil's bound on the character sums (see [15] Theorem 2E (i), page 44) and the simple fact that for each c, with $N(c) = 1$ there are exactly $q-1$ elements $d \in GF_{q^t}$ such that $d^{q-1} = c$ and for any x, $N(x^{q-1}) = x^{q^t-1} = 1$.

$$|\sum_{N(c)=1} \chi(c)| = |\frac{1}{q-1} \sum_{d \in GF_{q^t}} \chi(d^{q-1})| \le \frac{1}{q-1}(q-2)q^{t/2}.$$

□

To prove properties 5 and 6 we need the following lemma, which is Corollary 2.5 in Chapter 9 of [5].

Lemma 2.4 *Let H be a d-regular graph on n vertices in which the absolute value of every eigenvalue but the first is at most λ. Let B and C be two subsets of vertices, let $e_{B,C}$ be the number of ordered pairs (u,v) which are edges of H and $u \in B$, $v \in C$ (thus if $u, v \in B \cap C$, uv is an edge and $u \ne v$, it is counted twice, while loops contained in $B \cap C$ are counted once). Then*

$$|e_{B,C} - \frac{d}{n}|B| \cdot |C|| \le \lambda\sqrt{|B| \cdot |C|}.$$

To prove property 5 suppose, now, that B is a set of vertices of $NG_{q,t}$ containing no edges (besides, possibly, loops). Then, $e_{B,B} \leq |B|$ and we conclude, from the last lemma, that $|B|^2\frac{d}{n} - |B| \leq \lambda|B|$, where $d = (1+o(1))n^{1-1/t}$ and $\lambda = \sqrt{n}$, implying that $|B| \leq O(n^{1/2+1/t})$, as needed.

It is worth noting that the assertion of property 5 for graphs with no loops is known to follow from the bounds on the eigenvalues. This and the related result on the connection between the Shannon capacity of a graph and its eigenvalues appear in [14]). Since, however, our graph has loops (which are ignored in this property) we included the proof above. It is also worth noting that in fact for our purpose here this property provides only a little improvement of our bounds for the Ramsey graphs; we can use the trivial upper bound n on the independence number to prove the statement of Theorem 1.1.

We now turn to the proof of property 6, which supplies a lower bound to the number of k-cliques in $NG_{q,t}$. As the second eigenvalue of this graph is bounded in absolute value by $O(\sqrt{n})$, we can apply the well-known techniques for quasirandom graphs. These show that the number of small induced graphs is asymptotically the same as in a truly random graph with the same edge density (c.f., e.g. [5], Chapter 9). Since this was shown only for edge frequency 1/2 we have to check the proof for the norm graphs, where the edge frequency is $n^{-\frac{1}{t}}$. Instead of reproducing the original proof for this case we give a more direct one, based on Lemma 2.4 mentioned above.

Let G be a graph. We consider random one-to-one mappings of the set of vertices of G into the set of vertices of the norm graph $NG_{q,t}$. We denote by $A(G)$ the event that every edge of G is mapped on an edge of $NG_{q,t}$. In such a case we say that it is an embedding of G.

Lemma 2.5 *Let G be a graph on less than $\frac{t}{2}+1$ vertices with r edges. Then*

$$Pr(A(G)) = (1+o(1))n^{-\frac{r}{t}}.$$

Proof. We prove the lemma by induction on the number of vertices and edges. The base case ($r=0$) is trivial. Suppose the lemma holds for all smaller graphs than a given graph G with r edges and $s < \frac{t}{2}+1$ vertices. Let $G_{u,v}$ be the graph on the same set of vertices with the edge (u,v) deleted. Let G_u (G_v, respectively) be the restriction of G to the set of vertices $V(G)\setminus\{v\}$ ($V(G)\setminus\{u\}$, respectively), let G' be the restriction of G to the set of vertices $V(G)\setminus\{u,v\}$. Let r' be the number of edges of G' and note that $r - r' < 2(\frac{t}{2}-1)+1 = t-1$. We have $Pr(A(G_{u,v})) = Pr(A(G_{u,v})|A(G'))\cdot Pr(A(G'))$. Thus, by the induction assumption

$$Pr(A(G_{u,v})|A(G')) = (1+o(1))n^{-\frac{r-1-r'}{t}}.$$

For an embedding f' of G', let $\nu(u,f')$ be the number of extensions of f' to an embedding of G_u; $\nu(v,f')$ denotes the same for v. Clearly, the number of extensions of f' to an embedding of $G_{u,v}$ is at least $\nu(u,f')\nu(v,f') - \min(\nu(u,f'),\nu(v,f'))$ and at most $\nu(u,f')\nu(v,f')$. Thus we have

$$\frac{\nu(u,f')\nu(v,f') - \min(\nu(u,f'),\nu(v,f'))}{(n-s+2)(n-s+1)} \leq Pr(A(G_{u,v})|f') \leq \frac{\nu(u,f')\nu(v,f')}{(n-s+2)(n-s+1)}.$$

Taking expectation over all embeddings f' the middle term becomes $Pr(A(G_{u,v})|A(G'))$, which is $(1+o(1))n^{-\frac{r-1-r'}{t}}$. Note that by our choice of the parameters, $n^2 n^{-\frac{r-1-r'}{t}} = n^p$ with $p > 1$. Hence the term $\min(\nu(u,f'),\nu(v,f'))$ ($\leq n$) is negligible and we get

$$E_{f'}(\nu(u,f')\nu(v,f')|\ A(G')) = (1+o(1))n^2 n^{-\frac{r-1-r'}{t}}.$$

Now let f be a random one-to-one mapping of $V(G)$ into the norm graph. Let f' be a fixed embedding of G'. Then

$$Pr_f(A(G)|\ f|_{V(G)\setminus\{u,v\}} = f') = n^{-\frac{1}{t}}\frac{\nu(u,f')\nu(v,f')}{(n-s+2)(n-s+1)} + \delta,$$

where $|\delta| \le \sqrt{n}\frac{\sqrt{\nu(u,f')\nu(v,f')}}{(n-s+2)(n-s+1)}$. This follows from Lemma 2.4, where we take the possible images of u as the set B and the possible images of v as the set C. Averaging over embeddings f' we get $Pr(A(G)|A(G'))$ on the left hand side. On the right hand side we get $(1+o(1))n^{-\frac{r-r'}{t}}$ from the first term plus the expectation of the error term δ. By Jensen's inequality, the absolute value of this expectation is bounded by

$$\sqrt{n}\frac{\sqrt{E(\nu(u,f')\nu(v,f'))}}{(n-s+2)(n-s+1)} = (1+o(1))n^{-\frac{1}{2}-\frac{r-1-r'}{2t}}.$$

The exponent is less than $-\frac{r-r'}{t}$, by our choice of the parameters. Hence the expectation of the error term is negligible and we get $Pr(A(G)|A(G')) = (1+o(1))n^{-\frac{r-r'}{t}}$. Whence $Pr(A(G)) = (1+o(1))n^{-\frac{r}{t}}$. □

The assertion of property 6 follows from the last lemma, as it implies that for $k \le \lceil t/2 \rceil$ the number of cliques of size k is $\binom{n}{k}Pr(A(K_k)) = (1+o(1))\frac{1}{k!}n^{k-\binom{k}{2}/t}$.

Returning to the proof of Theorem 1.1 take $k = \lceil \frac{t}{2} \rceil$. We first bound the maximum size of a clique in $CQ_k(NG_{q,t})$. To this end we use the well-known fact [13] that for every t there exists a constant C_t such that every graph with m vertices and at least $C_t m^{2-\frac{1}{t}}$ edges contains $K_{t,t!+1}$ as a subgraph (where $C_t = (1+o(1))\frac{t}{2e}$). If we take $l(1-\frac{t}{l}) > (2C_t)^t k^{2t-1}$, then $\binom{l}{2} > C_t(kl)^{2-\frac{1}{t}}$. Hence, by Lemma 2.2, $CQ_k(NG_{q,t}))$ does not contain a clique of size $> k!(l-1)^k$.

Since $k = \lceil \frac{t}{2} \rceil$, there are, by property 6, $n^{c_{q,t}t}$ k-cliques in $NG_{q,t}$, where $c_{q,t} \to 3/8$ as $q,t \to \infty$. For this choice of parameters, the graph obtained has $n^{\Omega(t)}$ vertices, contains no independent set of size larger than $O(n^{1/2+1/t})$ (by property 5 and Lemma 2.1), and contains no clique of size $s = k!l^k$, for some $l < t^{3t}$. This shows, by an explicit construction, that

$$R(s,m) \ge m^{\Omega\left(\sqrt{\frac{\log s}{\log\log s}}\right)}.$$

This proves Theorem 1.1 for infinitely many values of m. Since prime powers, in fact already primes, occur frequently, we can claim the statement for all sufficiently large m. □

3 Concluding remarks

The graphs described here show, constructively, that $R(s,m) > m^{\varepsilon\sqrt{\log s/\log\log s}}$. Using probabilistic arguments it is known that in fact for every fixed s, $R(s,m)$ is much bigger and satisfies

$$R(s,m) \ge \Omega\left(\left(\frac{m}{\log m}\right)^{(s+1)/2}\right).$$

It will be very interesting to find an explicit construction of a graph with at least $m^{\Omega(s)}$ vertices containing neither a clique of size s nor an independent set of size m.

Acknowledgment: We would like to thank Vojta Rödl for helpful discussions.

References

[1] N. Alon, *Explicit Ramsey graphs and orthonormal labelings*, The Electronic Journal of Combinatorics, 1 (1994), R12, 8pp.

[2] N. Alon, *The Shannon Capacity of a union,* Combinatorica 18 (1998), 301-310.

[3] N. Alon, M. Krivelevich, *Constructive bounds for a Ramsey-type problem*, Graphs and Combinatorics 13 (1997), 217-225.

[4] N. Alon, L. Rónyai, T. Szabó, *Norm-graphs: variations and applications,* J. Combinatorial Theory, Ser. B 76 (1999), 280-290.

[5] N. Alon, J.H. Spencer, *The Probabilistic Method,* Wiley, 1992.

[6] B. Codenotti, P. Pudlák, G. Resta, *Some structural properties of low rank matrices related to computational complexity,* Theor. Comput. Sci., to appear.

[7] P. Erdős, *Some remarks on the theory of graphs,* Bulletin of the Amer. Math. Soc. **53** (1947), 292–294.

[8] P. Erdős, R. Rado, *Intersection theorems for systems of sets,* J. London Math. Soc. **35** (1960), 85-90.

[9] P. Frankl, R. Wilson, *Intersection theorems with geometric consequences*, Combinatorica 1 (1981), 259–286.

[10] R. L. Graham, B. L. Rothschild, J. H. Spencer, *Ramsey Theory*, Second Edition, Wiley, New York, 1990.

[11] V. Grolmusz, *Superpolynomial size set systems with restricted intersections mod* 6 *and explicit Ramsey graphs,* Combinatorica, to appear. (Preliminary version in: Lecture Notes in Computer Science Vol. 1276, 1997, 82-90.)

[12] J. Kollár, L. Rónyai, T. Szabó, *Norm-graphs and bipartite Turán numbers,* Combinatorica 16 (1996), 399-406.

[13] T. Kövari, V.T. Sós, P. Turán, *On a problem of K. Zarankiewicz,* Colloquium Math., 3 (1954), 50-57.

[14] L. Lovász, *On the Shannon capacity of a graph*, IEEE Transactions on Information Theory IT-25, (1979), 1-7.

[15] W.G. Schmidt, *Equations over Finite Fields An Elementary Approach,* Springer LNM 536, 1976.