Tough Ramsey graphs without short cycles

Noga Alon *
AT & T Bell Labs, Murray Hill, NJ 07974, USA
and Department of Mathematics
Raymond and Beverly Sackler Faculty of Exact Sciences
Tel Aviv University, Tel Aviv, Israel

Abstract

A graph G is t-tough if any induced subgraph of it with $x > 1$ connected components is obtained from G by deleting at least tx vertices. It is shown that for every t and g there are t-tough graphs of girth strictly greater than g. This strengthens a recent result of Bauer, van den Heuvel and Schmeichel who proved the above for $g = 3$, and hence disproves in a strong sense a conjecture of Chvátal that there exists an absolute constant t_0 so that every t_0-tough graph is pancyclic. The proof is by an explicit construction based on the tight relationship between the spectral properties of a regular graph and its expansion properties. A similar technique provides a simple construction of triangle-free graphs with independence number m on $\Omega(m^{4/3})$ vertices, improving previously known explicit constructions by Erdős and by Chung, Cleve and Dagum.

*Research supported in part by a United States Israel BSF Grant

Keywords: Eigenvalues, Ramsey graphs, tough graphs, girth, Cayley graphs.
Address for correspondence: Noga Alon, Department of Mathematics, Tel Aviv University, Ramat Aviv, Tel Aviv, Israel. Email address: noga@math.tau.ac.il.
AMS Subject Classification: 05C35, 05C38, 05C55, 05C25.

1 Introduction

The *toughness* $t(G)$ of a graph G is the largest real t so that for every positive integer $x \geq 2$ one should delete at least tx vertices from G in order to get an induced subgraph of it with at least x connected components. G is t-tough if $t(G) \geq t$. This parameter was introduced by Chvatál in [10], where he observed that Hamiltonian graphs are 1-tough and conjectured that 2-tough graphs are Hamiltonian. This conjecture is still open, despite a considerable amount of attention. Recall that a graph G on n vertices is *pancyclic* if it contains cycles of all lengths, from 3 to n. Another conjecture raised by Chvatál in [10] is the following.

Conjecture 1.1 ([10]) *There exists an absolute constant t_0 so that every t_0-tough graph is pancyclic.*

This conjecture has been recently disproved by Bauer, van den Heuvel and Schmeichel [8] who constructed, for every real t_0, a t_0-tough triangle-free graph. In this note we show, by explicit construction, that a much stronger result holds. Recall that the *girth* of a graph G is the length of a shortest cycle in it.

Theorem 1.2 *For every t and g there exists a t-tough graph of girth greater than g.*

This theorem can be proved by considering random graphs; one can show that for an appropriate $d = d(t)$ a random d-regular graph on n vertices is t-tough and has girth greater than g with positive probability, provided n is sufficiently large. The proof we present here is different and is by an explicit construction. We first apply some of the known results concerning the tight relationship between the spectral properties of regular graphs and their expansion properties (see [5], [23], [2]) to show that regular graphs with well separated eigenvalues are tough. This suffices to show that the Ramanujan graphs of [18], [19] with an appropriate choice of parameters provide explicit examples for proving Theorem 1.2.

One can easily check that t-tough graphs on n vertices cannot have an independent set of size greater than $n/(t+1)$. Therefore, tough graphs have small independence numbers and Theorem 1.2 is a strengthening of the well known fact, proved by Erdős in [14], that there are graphs of arbitrarily high girth, whose independence number is an arbitrarily small fraction of the number of vertices (implying that the corresponding chromatic numbers are arbitrarily high). The special case of girth 4 is a well studied Ramsey-type problem. Let $R(3, m)$ denote the maximum number of vertices of a triangle-free graph (i,e., a graph of girth at least 4) whose independence number is at most m. Erdős showed in [15], by a subtle probabilistic argument, that $R(3, m) \geq \Omega((m/\log m)^2)$, (see also [22] or [7] for a simpler proof). Ajtai, Komlós and Szemerédi proved in [1] that $R(3, m) \leq O(m^2/\log m)$, (see also [21] for an estimate with a better constant). The problem of finding an explicit construction of triangle-free graphs of independence number m and many vertices seems more difficult. Erdős

[16] gave an explicit construction of such graphs with

$$\Omega(m^{(2\log 2)/3(\log 3-\log 2)}) = \Omega(m^{1.13})$$

vertices. This has been improved by Cleve and Dagum [12], and improved further by Chung, Cleve and Dagum in [11], where the authors present a construction with

$$\Omega(m^{\log 6/\log 4}) = \Omega(m^{1.29})$$

vertices.

Here we combine our eigenvalue technique with known results about the Hamming weights of words of an appropriate dual BCH code to obtain a very simple explicit cnstruction with $\Omega(m^{4/3})$ vertices, improving the above mentioned bounds. The simple triangle-free graph we construct has several additional interesting properties, and its construction can be extended to yield simple explicit graphs with small indepedence numbers and no short odd cycles.

The rest of this note is organized as follows. In Section 2 we establish the connection between the spectral properties of a regular graph and its toughness and apply it to prove Theorem 1.2. In Section 3 we construct triangle free graphs that show explicitly that $R(3,m) \geq \Omega(m^{4/3})$.

2 Eigenvalues and toughness

It is easy and well known that the largest eigenvalue of (the adjacency matrix of) a d-regular graph is d. An (n,d,λ)-*graph* is a d-regular graph on n vertices, in which every eigenvalue μ besides the largest satisfies $|\mu| \leq \lambda$. It is well known (see, e.g., [5], [23], [2], [7] Chapter 9) that (n,d,λ)-graphs, with λ much smaller than d have certain pseudo-random properties. In this section we show that the toughness of each such graph is high. This is shown in the next proposition, in which we make no attempt to optimize the constant factors.

Proposition 2.1 *Let $G=(V,E)$ be an (n,d,λ)-graph. Then the toughness $t=t(G)$ of G satisfies*

$$t > \frac{1}{3}\left(\frac{d^2}{\lambda d+\lambda^2} - 1\right). \tag{1}$$

In the proof of the above proposition we need the following simple lemma implicit in [3] (see [7], page 122 for the proof).

Lemma 2.2 *Let $G=(V,E)$ be an (n,d,λ)-graph, and let B be a set of vertices of G. For a vertex $v \in V$ let $N(v)$ denote the set of all neighbors of v. Then*

$$\sum_{v\in V}(|N(v)\cap B| - d|B|/n)^2 \leq \lambda^2|B|\left(1-\frac{|B|}{n}\right). \qquad \square$$

Corollary 2.3 *Let $G = (V, E)$ be an (n, d, λ)-graph and let A, B be two subsets of vertices of G so that there is no edge of G joining a vertex of A with a vertex of B. Then*

$$|A| \cdot |B| \leq \frac{\lambda^2}{d^2} n(n - |B|). \tag{2}$$

Proof. By Lemma 2.2, since $|N(v) \cap B| = 0$ for all $v \in A$,

$$|A| \frac{d^2 |B|^2}{n^2} \leq \lambda^2 |B| \frac{n - |B|}{n},$$

implying the desired result. □

Proof of Proposition 2.1. Let W be a set of vertices of G and suppose that $G - W$ has $x \geq 2$ connected components and that $|W| \leq tx$. We must show that t satisfies (1). Let $C_1, C_2, \ldots, C_x$ be the sets of vertices of the connected components of $G - W$ and suppose that $|C_1| \leq |C_2| \leq \cdots \leq |C_x|$. Define $A = \cup_{i \leq \lfloor x/2 \rfloor} C_i$ and $B = \cup_{i > \lfloor x/2 \rfloor} C_i$. Let y denote the number of vertices in A. Clearly $|B| \geq |A| = y \geq \lfloor x/2 \rfloor$. By (2)

$$y^2 \leq |A| \cdot |B| \leq \frac{\lambda^2}{d^2} n(n - |B|) < \frac{\lambda^2}{d^2} n^2,$$

and hence

$$y < \frac{\lambda}{d} n. \tag{3}$$

In addition, since $|A| = y \geq \lfloor x/2 \rfloor \geq x/3$ it follows that $|W| \leq tx \leq 3ty$. Thus $|B| = n - |A| - |W| \geq n - (3t+1)y$ and $n - |B| \leq (3t+1)y$. Substituting in (2) this implies that

$$y(n - (3t+1)y) \leq |A| \cdot |B| \leq \frac{\lambda^2}{d^2} n(n - |B|) \leq \frac{\lambda^2}{d^2} n(3t+1)y,$$

i.e.,

$$n \leq (3t+1)(y + \frac{\lambda^2}{d^2} n).$$

Hence, by (3),

$$n < (3t+1)(\frac{\lambda}{d} n + \frac{\lambda^2}{d^2} n),$$

implying that

$$(3t+1) > \frac{d^2}{d\lambda + \lambda^2},$$

and completing the proof. □

In [18], [19] the authors describe explicitly, for every $d = p + 1$ where $p \equiv 1 (mod\ 4)$ is a prime, and for every $n = q(q^2 - 1)/2$ where $q \equiv 1 (mod\ 4)$ is a prime and p is a quadratic residue modulo q, (n, d, λ) graphs G_n with $\lambda = 2\sqrt{d-1}$, where the girth of G_n is at least $2 \log_p q \geq \frac{2}{3} \log_{d-1} n$. By Proposition 2.1 and by the known results about the distribution of primes in arithmetic progressions (see, e.g., [13]) this supplies, for any integer $g \geq 3$, infinitely many values of n with an explicit graph G_n on n vertices with girth at least g and toughness at least $n^{c/g}$, for some absolute positive constant c. We have thus proved the following.

Corollary 2.4 *There exists a positive constant c so that for every integer $g \geq 3$ there are infinitely many values of n with an explicit graph G_n on n vertices whose girth is at least g so that $t(G_n) \geq n^{c/g}$.* □

The assertion of Theorem 1.2 is an immediate consequence of Corollary 2.4. □
Note that the last corollary is tight, up to the constant factor c. Indeed, if G is a t-tough graph on n vertices which is not a complete graph, then the minimum degree in G is at least $2t$. Thus, if the girth of G is $g > 2r$, an easy known argument (see, e.g., [9], Chapter 3), implies that $n > (2t-1)^r$. The last corollary provides explicit triangle-free graphs with n vertices and toughness n^{ϵ} for some absolute positive ϵ. For this special case larger toughness (as a function of the number of vertices) can be obtained using a simpler construction. This is done in the next section, where the connection to the Ramsey numbers $R(3,m)$ is also discussed.

3 Constructive lower bound for the Ramsey numbers $R(3,m)$

In this section we construct a family of graphs, which we call the *code graphs*. These graphs, whose construction is extremely simple, have several interesting properties, that follow from the eigenvalue technique and some known results in the theory of Error Correcting Codes.

For a positive integer k, let $F_k = GF(2^k)$ denote the finite field with 2^k elements. The elements of F_k are represented, as usual, by binary vectors of length k. If a and b are two such vectors, let (a,b) denote their concatenation, i.e., the binary vector of length $2k$ whose first k coordinates are those of a and whose last k coordinates are those of b. Let G_k be the graph whose vertices are all $n = 2^{2k}$ binary vectors of length $2k$, where two vectors u and v are adjacent if and only if there exists a non-zero $z \in F_k$ so that $u + v = (z, z^3)$, where here $u+v$ is the sum modulo 2 of u and v, and where the power z^3 is computed in the field F_k. The following theorem summerizes some of the properties of these graphs.

Theorem 3.1 *For every $k > 1$, G_k is a $d_k = 2^k - 1$-regular graph on $n_k = 2^{2k}$ vertices with the following properties.*

1. *G_k is triangle-free and has diameter 3.*
2. *Every eigenvalue μ of G_k, besides the largest, satisfies*
$$|\mu| \leq 2 \cdot 2^{k/2} + 1.$$
3. *The independence number of G_k is at most*
$$\frac{2 \cdot 2^{k/2} + 1}{2^k + 2 \cdot 2^{k/2}} n_k < \frac{2}{2^{k/2}} n_k = 2n_k^{3/4},$$
and hence its chromatic number is at least $\frac{1}{2} n_k^{1/4}$.

4. The toughness $t(G_k)$ satisfies

$$t(G_k) \geq \Omega(n_k^{1/4}).$$

Proof. The graph G_k is the Cayley graph of Z_2^{2k} with respect to the generating set $S_k = \{(z, z^3) : \quad 0 \neq z \in F_k\}$. It is obvious that G_k has 2^{2k} vertices and that it is $|S_k| = 2^k - 1$ regular. Let A_k be the $2k$ by $2^k - 1$ binary matrix whose columns are all the vectors in S_k. This matrix is the parity check matrix of a binary BCH-code of designed distance 5 (see, e.g., [20], Chapter 9). The fact that G_k is triangle-free is equivalent to the fact that the sum (modulo 2) of any set of at most 3 columns of A_k is not the zero-vector. But this is simply the statement that the distance of the above code is greater than 3, which is, of course, correct. The diameter of G_k cannot be 2 by simple counting, as the number of vertices of distance at most 2 from a given vertex is at most $1 + d_k + \binom{d_k}{2} < n_k$. The fact that it is at most 3 is equivalent to the statement that every vector in Z_2^{2k} is a sum of at most 3 members of S_k, which is proved in [20], pages 279-280. (In the language of Coding Theory this is simply the fact that the corresponding BCH-code is quasi-perfect, or that its covering raduis is 3.) This proves part 1 of the theorem.

In order to prove part 2 we argue as in the last section of [6]. Recall that the eigenvalues of Cayley graphs of abelian groups can be computed easily in terms of the characters of the group. This result, decsribed in, e.g., [17], implies that the eigenvalues of the graph G_k are all the numbers

$$\sum_{s \in S_k} \chi(s),$$

where χ is a multiplicative character of Z_2^{2k}. It follows that these eigenvalues can be expressed in terms of the Hamming weights of the linear combinations (over $GF(2)$) of the rows of the matrix A_k. Each such linear combination of Hamming weight w corresponds to the eigenvalue $d_k - 2w$. However, the linear combinations of the rows of A_k are simply all words of the code whose generating matrix is A_k, which is the dual of the BCH-code whose parity-check matrix is A_k. It is known (see [20], pages 280-281) that the Carlitz-Uchiyama bound implies that the Hamming weight w of each non-zero codeword of this dual code satisfies

$$2^{k-1} - 2^{k/2} \leq w \leq 2^{k-1} + 2^{k/2}.$$

Since the zero vector corresponds to the largest eigenvalue of G_k this implies that every eigenvalue μ of G_k besides the largest satisfies

$$-2 \cdot 2^{k/2} - 1 \leq \mu \leq 2 \cdot 2^{k/2} - 1,$$

implying the assertion of part 2 of the theorem.

Part 3 follows easily from part 2 as follows. In [3], Lemma 2.3 it is shown that the number of edges of any induced subgraph on αn vertices in an (n, d, λ)-graph deviates from $d\alpha^2 n/2$ by at most $\lambda\alpha(1-\alpha)n/2$. Thus, if there is an independent set of size αn in such a graph then

$$\lambda\alpha(1-\alpha)n/2 \geq d\alpha^2 n/2,$$

implying that $\alpha \leq \lambda/(d+\lambda)$. By part 2, G_k is an $(n_k, 2^k-1, 2\cdot 2^{k/2}+1)$-graph and the assertion of part 3 follows.

Part 4 is an immediate consequence of part 2 and Proposition 2.1. This completes the proof of the theorem. □

Theorem 3.1 shows that the code-graph G_k is an explicit triangle-free graph on n_k vertices whose chromatic number exceeds $0.5n_k^{1/4}$. In addition, the graphs G_k are explicit examples showing that $R(3,m) \geq \Omega(m^{4/3})$.

The construction above can be extended by applying BCH codes with designed distance $2h+1 > 5$ in the obvious way. This gives an explicit family of graphs $G_{k,h}$, for all $k, h > 1$, where $G_{k,h}$ is a 2^k-1-regular graph on $n_{k,h} = 2^{kh}$ vertices which contains no odd cycle of length at most $2h-1$. Every eigenvalue of $G_{k,h}$ besides the largest is, in absolute value, at most $2(h-1)\cdot 2^{k/2}+1$ and hence it is $\Omega(2^{k/2}/(h-1))$-tough and has no independent set of size at least

$$\frac{2(h-1)}{2^{k/2}} n_{k,h} = 2(h-1) n_{k,h}^{1-\frac{1}{2h}}.$$

It is possible to use other (binary and nonbinary) error correcting codes to construct other graphs in a similar manner. In [6] it is shown that by applying some of the codes constructed in [4] one can construct graphs with high expansion properties, and other codes may very well yield additional graphs with interesting properties.

It would be interesting to determine or estimate, for every t and g, the smallest possible $n = n(t,g)$ for which there are t-tough graphs on n vertices whose girth is at least g. Using the techniques of Section 2 we can show that there are two positive constants c_1 and c_2 so that for all $t > 1$ and $g \geq 3$,

$$t^{c_1 g} \leq n(t,g) \leq t^{c_2 g}.$$

The problem of finding an accurate estimate remains open.

Acknowledgment I would like to thank Jan van den Heuvel for helpful discussions.

References

[1] M. Ajtai, J. Komlós and E.Szemerédi, *Lower bounds for some Ramsey numbers*, Discrete Math. 2 (1972), 289-293.

[2] N. Alon, *Eigenvalues and expanders*, Combinatorica 6(1986), 83-96.

[3] N. Alon and F. R. K. Chung, *Explicit construction of linear sized tolerant networks*, Discrete Math. 72(1988), 15-19; (Proc. of the First Japan Conference on Graph Theory and Applications, Hakone, Japan, 1986.)

[4] N. Alon, O. Goldreich, J. Hastad and R. Peralta, Simple constructions of almost k-wise independent random variables, Proc. 31^{st} IEEE FOCS, St. Louis, Missouri, IEEE (1990), 544-553. See also: Random Structures and Algorithms 3 (1992), 289-304.

[5] N. Alon and V. D. Milman, λ_1, *isoperimetric inequalities for graphs and superconcentrators*, J. Comb. Theory, Ser.B, 38 (1985), 73-88. See also: *Eigenvalues, expanders and superconcentrators*, Proc. 25^{th} IEEE FOCS, Singer Island, Florida, IEEE(1984), 320-322.

[6] N. Alon and Y. Roichman, *Random Cayley graphs and expanders*, Random Structures and Algorithms, in press.

[7] N. Alon and J. H. Spencer, **The Probabilistic Method**, Wiley, 1991.

[8] D. Bauer, J. van den Heuvel and E. Schmeichel, *Toughness and triangle-free graphs*, to appear.

[9] B. Bollobás, **Extremal Graph Theory**, Academic Press, 1978.

[10] V. Chvátal, *Tough graphs and hamiltonian circuits*, Discrete Mathematics 5 (1973), 215-218.

[11] F. R. K. Chung, R. Cleve and P. Dagum, *A note on constructive lower bounds for the Ramsey numbers* $R(3,t)$, J. Combinatorial Theory Ser. B 57 (1993), 150-155.

[12] R. Cleve and P. Dagum, *A constructive* $\Omega(t^{1.26})$ *lower bound for the Ramsey number* $R(3,t)$, Inter. Comp. Sci. Inst. Tech. Rep. TR-89-009, 1989.

[13] H. Davenport, **Multiplicative Number Theory**, Springer Verlag, 1980 (Second Edition).

[14] P. Erdős, *Graph Theory and Probability*, Canad. J. Math. 11 (1959), 34-38.

[15] P. Erdős, *Graph Theory and Probability, II*, Canad. J. Math. 13 (1961), 346-352.

[16] P. Erdős, *On the construction of certain graphs*, J. Combinatorial Theory 17 (1966), 149-153.

[17] L. Lovász, **Combinatorial Problems and Exercises**, North Holland, Amsterdam, 1979, Problem 11.8.

[18] A. Lubotzky, R. Phillips and P. Sarnak, *Explicit expanders and the Ramanujan conjectures*, Proc. 18^{th} ACM STOC (1986), 240-246. See also: *Ramanujan graphs*, Combinatorica 8 (1988), 261-277.

[19] G. A. Margulis, *Explicit group-theoretical constructions of combinatorial schemes and their application to the design of expanders and superconcentrators*, Problemy Peredachi Informatsii 24(1988), 51-60 (in Russian). English translation in Problems of Information Transmission 24(1988), 39-46.

[20] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, North Holland, Amsterdam, 1977.

[21] J. B. Shearer, *A note on the independence number of a triangle-free graph*, Discrete Math. 46 (1983), 83-87.

[22] J. Spencer, *Asymptotic lower bounds for Ramsey functions*, Discrete Math. 20 (1977), 69-76.

[23] R. M. Tanner, *Explicit construction of concentrators from generalized N-gons*, SIAM J. Alg. Disc. Meth. 5 (1984), 287-293.