Lovász, vectors, graphs and codes

Dedicated to László Lovász, for his seventieth birthday

Noga Alon *

Abstract

A family of high-degree triangle-free pseudo-random Cayley graphs has been constructed in [2], motivated by a geometric question of Lovász. These graphs turned out to be useful in tackling a variety of additional extremal problems in Graph Theory and Coding Theory. Here we describe the graphs and their applications, and mention several intriguing related open problems. This is mainly a survey, but it contains several new results as well. One of these is a construction showing that the Lovász θ-function of a graph cannot be bounded by any function of its Shannon capacity.

1 Introduction

- What is the maximum possible (Euclidean) norm of a sum of n unit vectors so that any 3 of them contain 2 which are orthogonal ?
- What is the minimum possible size of the maxcut of a triangle-free graph with m edges ?
- What is the maximum possible number of words in a binary code of length n so that there is no Hamming ball of radius $(1/4 + \varepsilon)n$ containing more than two words ?

The first question is geometric, and was posed by Lovász motivated by the study of the θ-function of a graph. The second question is in Extremal Graph Theory, it was first considered by Erdős and Lovász. The third question is in Coding theory, and was first studied by Blinovskii, extending earlier results of Plotkin and Levenshtein. Somewhat surprisingly it turns out that all three questions, and several related ones, can be solved

*Department of Mathematics, Princeton University, Princeton, NJ 08544, USA and Schools of Mathematics and Computer Science, Tel Aviv University, Tel Aviv 69978, Israel. Email: nogaa@tau.ac.il. Research supported in part by an ISF grant and by a GIF grant.

asymptotically using a single construction of a family of triangle-free Cayley graphs with extremal spectral properties. Here we describe this construction, show how it is used in the solution of these problems and more, and describe their connection to Ramsey theory and to questions about the Shannon capacity of graphs.

2 The graphs

For a positive integer k, let $F_k = GF(2^k)$ denote the finite field with 2^k elements whose elements are represented, as usual, by binary vectors of length k. If a, b and c are three such vectors, let (a, b, c) denote their concatenation. Suppose k is not divisible by 3 and put $n = 2^{3k}$. Let W_0 be the set of all nonzero elements $\alpha \in F_k$ so that the leftmost bit in the binary representation of α^7 is 0, and let W_1 be the set of all nonzero elements $\alpha \in F_k$ for which the leftmost bit of α^7 is 1. Since 3 does not divide k, 7 does not divide $2^k - 1$ and hence $|W_0| = 2^{k-1} - 1$ and $|W_1| = 2^{k-1}$, as when α ranges over all nonzero elements of F_k so does α^7.

Let G_n be the Cayley graph of the elementary abelian 2-group Z_2^{3k} with the generating set $S = U_0 + U_1 = \{u_0 + u_1 : u_0 \in U_0, u_1 \in U_1\}$, where $U_0 = \{(w_0, w_0^3, w_0^5) : w_0 \in W_0\}$, and $U_1 = \{(w_1, w_1^3, w_1^5) : w_1 \in W_1\}$ with the powers computed in the finite field F_k.

The following theorem is proved in [2].

Theorem 2.1. *If k is not divisible by 3 and $n = 2^{3k}$ then G_n is a Cayley graph of Z_2^{3k}, it has n vertices, is regular of degree*

$$d_n = 2^{k-1}(2^{k-1} - 1) = (\frac{1}{4} + o(1))n^{2/3},$$

and satisfies the following properties

1. *G_n is triangle-free.*

2. *Every eigenvalue μ of G_n, besides the largest, satisfies*

$$-9 \cdot 2^k - 3 \cdot 2^{k/2} - 1/4 \leq \mu \leq 4 \cdot 2^k + 2 \cdot 2^{k/2} + 1/4.$$

The detailed proof can be found in [2]. Here is a sketch. The graph G_n is the Cayley graph of Z_2^{3k} with respect to the generating set $S = S_n = U_0 + U_1$, where U_i are defined as above. As the elements of $U_0 \cup U_1$ are the columns of the parity check matrix of a binary BCH-code of designed distance 7 (see, e.g., [40], Chapter 9), every set of six of them is

linearly independent. Therefore the elements of S_n are distinct and G_n is regular of degree $|S_n| = |U_0||U_1|$.

The fact that G_n is triangle-free is equivalent to the fact that the sum (in Z_2^{3k}) of any set of 3 elements of S_n is not the zero-vector. Let $u_0 + u_1$, $u'_0 + u'_1$ and $u"_0 + u"_1$ be three distinct elements of S_n, where $u_0, u'_0, u"_0 \in U_0$ and $u_1, u'_1, u"_1 \in U_1$. If the sum (modulo 2) of these six vectors is zero then, since every set of six members of $U_0 \cup U_1$ is linearly independent, every vector must appear an even number of times in the sequence $(u_0, u'_0, u"_0, u_1, u'_1, u"_1)$. However, since U_0 and U_1 are disjoint this implies that every vector must appear an even number of times in the sequence $(u_0, u'_0, u"_0)$ and this is clearly impossible. This proves part 1 of the theorem.

The proof of part 2 is based on the fact that the eigenvalues of G_n are given by the following character sums:

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

where χ ranges over all characters of the group Z_2^{3k}. Indeed, such an expression holds for any Cayley graph of an abelian group (see, e.g., [39]), where the eigenvectors are the characters. The bounds in part 2 can now be deduced from the known results about the weight distribution of dual BCH codes, proved using the Carlitz-Uchiyama bound (see [40], pages 280-281). The details can be found in [2].

An (n, d, λ)-graph is a d regular graph on n vertices in which all eigenvalues but the first are of absolute value at most λ. This notation was introduced by the author in the late 80s, motivated by the fact that if λ is much smaller than d, then the graph exhibits strong pseudo-random properties. In particular, as shown in [8], the average degree of every induced subgraph on a set of xn vertices deviates from xd by less than λ. By considering the trace of the square of the adjacency matrix of any (n, d, λ)-graph, which is nd and is also the sum of squares of its eigenvalues, it is easy to see that $\lambda \geq \sqrt{d(n-d)/(n-1)}$ which is $\Omega(\sqrt{d})$ whenever, say, $d < n/2$. Thus the smallest possible value of λ is $\Theta(\sqrt{d})$. The graph $G = G_n$ described above is an (n, d, λ) where $d = \Theta(n^{2/3})$ and $\lambda = \Theta(\sqrt{d})$, that is, λ is as small as possible up to a constant factor. Note that by the above fact about the distribution of edges in subsets of (n, d, λ)-graphs, it follows that any set of $cn^{2/3}$ vertices of G spans many edges, provided $c > 36$, implying that such a graph with somewhat larger degrees which are still $\Theta(n^{2/3})$ cannot be triangle-free. Note also that in a random graph with degrees $\Theta(n^{2/3})$, every edge is typically contained in $\Theta(n^{1/3})$ triangles, that is, the graph includes lots of triangles. The fact that the graphs G_n are triangle-free and yet have strong pseudo-random properties derived from their spectrum make them useful in

tackling various extremal problems. Some of these are described in the following sections.

3 Shannon capacity and the Lovász θ-function

3.1 Shannon and Ramsey

The (and)-product of two undirected graphs $G = (V, E)$ and $G' = (V', E')$ is the graph whose vertex set is $V \times V'$ in which two distinct vertices (u, u') and (v, v') are adjacent iff (either $u = v$ or uv are adjacent in G) and (either $u' = v'$ or u', v' are adjacent in G'). The power G^n of G is defined with respect to this product. It is thus the graph whose vertex set is V^n in which two distinct vertices $(u_1, u_2, \ldots, u_n)$ and $(v_1, v_2, \ldots, v_n)$ are adjacent if and only if for all i between 1 and n either $u_i = v_i$ or $u_i v_i \in E$. The *Shannon capacity* $S(G)$ of G is the limit $\lim_{n\to\infty}(\alpha(G^n))^{1/n}$, where $\alpha(G^n)$ is the maximum size of an independent set of vertices in G^n. This limit exists, by super-multiplicativity, it is equal to the supremum over n of $(\alpha(G^n))^{1/n}$ and hence is always at least $\alpha(G)$. The Shannon capacity of a graph may be significantly larger than its independence number. In particular, there are graphs on n vertices with independence number smaller than $2\log_2 n$ and Shannon capacity at least $\sqrt{n}$, see [25], [12]. It is not known, however, if the Shannon capacity is bounded by any function of the independence number, that is, whether or not the maximum possible value of the Shannon capacity of a graph whose independence number is a constant c is finite. This is equivalent to a well known question on multicolored Ramsey numbers. Let $r(c+1:\ell)$ denote the maximum number r so that there is a coloring of the edges of the complete graph K_r on r vertices by ℓ colors with no monochromatic copy of K_{c+1}. As shown in [25], (see also [12]), the maximum possible value of $\alpha(G^\ell)$ as G ranges over all graphs with independence number c is exactly $r(c+1:\ell)$. It follows that the maximum possible Shannon capacity of a graph with independence number c is exactly the limit as ℓ tends to infinity of $r(c+1:\ell)^{1/\ell}$. In particular, the question of deciding whether or not the maximum possible Shannon capacity of a graph with independence number 2 is finite is equivalent to an old problem of Erdős (see, e.g., [17]) asking whether or not the Ramsey number $r(3:\ell)$ grows faster than any exponential in ℓ.

This question is wide open. Indeed, our understanding of the Shannon capacity of graphs is very limited. In view of this fact it is natural to replace in the question the Shannon capacity invariant by the best known upper bound for it, which is much better understood, and can be computed efficiently, namely by the Lovász θ-function of the graph.

3.2 The θ-function and nearly orthogonal vectors

If $G = (V, E)$ is a graph, an orthonormal labeling (also called orthogonal representation) of G is a family $(b_v)_{v \in V}$ of unit vectors in an Euclidean space so that if u and v are distinct non-adjacent vertices, then $b_u^t b_v = 0$, that is, b_u and b_v are orthogonal. The θ-function $\theta(G)$ of G is the minimum, over all orthonormal labelings b_v of G and over all unit vectors c (called here a handle), of

$$max_{v \in V} \frac{1}{(c^t b_v)^2}.$$

It is easy to check that for every G, $\alpha(G) \leq \theta(G)$. Indeed, in any orthonormal labeling of G the vectors b_v assigned to the vertices of any independent set are pairwise orthogonal, and therefore for any unit vector c the square of the inner product of at least one of them with c is at most the reciprocal of the size of the set. It is also not difficult to check that for any two graphs G and G', $\theta(G \cdot G') \leq \theta(G) \cdot \theta(G')$. (It is a bit more difficult to show that in fact equality holds, see [38].) This is proved by considering the tensor product of orthogonal representations of G and G' and the tensor product of the two handles. Therefore for every n, $\alpha(G^n) \leq (\theta(G))^n$ implying that the Shannon capacity of G satisfies $S(G) \leq \theta(G)$.

The following lemma is proved in [38].

Lemma 3.1. *Let $G = (V, E)$ be a d-regular graph on n vertices and suppose that the most negative eigenvalue of the adjacency matrix A of G is at least $-\lambda$. Then*

$$\theta(G) \leq \frac{n\lambda}{d + \lambda}.$$

Proof: The matrix $B = (A + \lambda I)/\lambda$ is positive semi-definite and hence it is the gram matrix of vectors $(b_v)_{v \in V}$. It is easy to check that these vectors form an orthogonal representation of G. Define

$$c = \frac{\sum_{v \in V} b_v}{\| \sum_{v \in V} b_v \|}.$$

Then for every vector b_v

$$(c^t b_v)^2 = \frac{(1 + d/\lambda)^2}{n + nd/\lambda} = \frac{\lambda + d}{n\lambda},$$

completing the proof. □

By Theorem 2.1 and the above lemma, for the graph G_n in the theorem, $\theta(G_n) \leq (1 + o(1))36n^{2/3}$. The complement $\overline{G_n}$ of G_n is a graph with n vertices, and independence

number 2. Since the product $G_n \cdot \overline{G_n}$ contains an independent set of size n (consisting of all vertices (v, v) for $v \in V(G_n)$), it follows that

$$n \leq \alpha(G_n \cdot \overline{G_n}) \leq \theta(G_n \cdot \overline{G_n}) \leq \theta(G_n)\theta(\overline{G_n}) \leq (1 + o(1))36n^{2/3}\theta(\overline{G_n}).$$

Therefore $\theta(\overline{G_n}) \geq (1/36 + o(1))n^{1/3}$. We have thus shown that the maximum possible value of the θ-function of an n-vertex graph with independence number 2 is at least $\Omega(n^{1/3})$. This is tight, up to a multiplicative constant, answering a question of Lovász and improving earlier estimates of Konyagin [34] and of Kashin and Konyagin [32]. See [2] for more details.

The n unit vectors b_v described above have the following interesting geometric property. Among any three of them, some two are orthogonal (since the graph G_n is triangle-free). On the other hand, the square of the norm of their sum is $n+n\frac{d}{\lambda}$ where $d = (1/4+o(1))n^{2/3}$ and $\lambda = (9 + o(1))n^{1/3}$. This square norm is thus $(\frac{1}{36} + o(1))n^{4/3}$. Therefore the norm of this sum is $\Omega(n^{2/3})$ which is also tight, up to a multiplicative constant, improving the estimates in [34], [32].

Here is a quick proof of the tightness (see [34] for another proof). Let $v_1, \ldots, v_n$ be n unit vectors in an Euclidean space so that among any three of them some two are orthogonal. Let A be the gram matrix of these vectors an let $\lambda_1 \geq \cdots \geq \lambda_n \geq 0$ be its eigenvalues (which are all nonnegative as A is positive semi-definite). Then the square of the norm of the sum of the vectors is $j^t A j$ where j is the all 1 vector. This is at most $\lambda_1 n$. The assumption implies that the trace of $(A - I)^3$ is 0, that is, $\sum_i (\lambda_i - 1)^3 = 0$. As $\lambda_i - 1 \geq -1$ for all i this implies that $\lambda_1 \leq (n-1)^{1/3}$ implying the required bound.

3.3 Lovász and Shannon

As described above, for every graph G, $\alpha(G) \leq S(G) \leq \theta(G)$ where $\alpha(G)$ is the independence number of G, $S(G)$ is its Shannon capacity, and $\theta(G)$ is the Lovász θ-function of G. As mentioned it is not known whether or not the Shannon capacity $S(G)$ is bounded by any function of the independence number $\alpha(G)$. On the other hand by the discussion in the previous subsection the Lovász θ function is not bounded by any function of the independence number, and can be as large as $\Omega(n^{1/3})$ for an n-vertex graph with independence number 2. Can it be bounded by any function of the Shannon capacity $S(G)$? The next result shows that the answer is negative.

Theorem 3.2. *There is a sequence of graphs H_n with the following properties. H_n has n vertices, its Shannon capacity is 3 and its θ-function is at least $(1 + o(1))n^{1/4}$.*

Proof: Let $F = GF(2^k)$ be the finite field with $q = 2^k$ elements, and let $U = U_n$ be the set of all vectors $x = (x_0, x_1, x_2) \in F^3$ so that the sum $x_0+x_1+x_2$ (computed in F) is nonzero, and x is not of the form (y, y, y) for some $y \in F$. Define an equivalence relation on U by calling two vectors equivalent if one is a multiple of the other by a field element. The vertex set $V = V_n$ of the graph H_n is the equivalence classes of U with respect to this relation. Therefore $|V| = n = (q^3 - q^2 - q + 1)/(q - 1) = q^2 - 1$. Two vertices $x = (x_0, x_1, x_2)$ and $y = (y_0, y_1, y_2)$ are **not** connected iff $x_0y_0 + x_1y_1 + x_2y_2 = 0$, where the sum and product are computed in F and x, y are any two representatives of the corresponding equivalence classes. Note that this is an induced subgraph of the complement of the Erdős-Rényi graph (which is the polarity graph of a projective plane) considered in [26]. For our purpose here it is convenient to define it over a field of characteristic 2, see [9] for a close variant.

Claim 3.3. *The Shannon capacity of H_n is at most* 3.

Proof: We use a variant of the argument in [31],[5]. By definition we can assign to each vertex v of H_n a vector x_v in F^3 so that the inner product of each vector with itself (over F) is nonzero and for any two nonadjacent vertices u, v, the inner product of x_u and x_v is zero. By taking tensor powers this supplies, for every k, an assignment with similar properties for the vertices of the power H_n^k. For each vertex we get a vector in F^{3^k} so that the inner product of any vector with itself is nonzero and the inner product of any two vectors associated to non-adjacent vertices is 0. This implies that the vectors corresponding to an independent set are linearly independent and hence the size of each such set is at most 3^k, establishing the claim.

Claim 3.4. *The θ-function of H_n is at least $\sqrt{q} > n^{1/4}$.*

Proof: The complement of H_n is an induced subgraph of the polarity graph of the projective plane of order q. The eigenvalues of this polarity graph are easy to compute, as for its adjacency matrix A, $A^tA = qI + J$ where I is the identity matrix and J is the all 1 matrix. Thus the eigenvalues of A^tA are $q+1+q^2+q = (q+1)^2$ (with multiplicity 1) and q (with multiplicity $q^2 + q$). It follows that the smallest eigenvalue of A is $-\sqrt{q}$, and by eigenvalues interlacing, the smallest eigenvalue of the adjacency matrix of the complement of H_n is at least $-\sqrt{q}$. It is not difficult to check that this complement is regular of degree q. Thus, by Lemma 3.1,

$$\theta(\overline{H_n}) \leq \frac{n\sqrt{q}}{q + \sqrt{q}}.$$

It follows that

$$\theta(H_n) \geq \frac{q + \sqrt{q}}{\sqrt{q}} = \sqrt{q} + 1 > n^{1/4}.$$

This completes the proof of the claim, which together with the previous claim imply the assertion of the theorem. □

4 Ramsey graphs and Maxcut

4.1 The Ramsey number $r(3, m)$

Let $r(3, m)$ denote the maximum number of vertices of a triangle-free graph whose independence number is at most m. The problem of determining or estimating this function is a well studied Ramsey type problem. Ajtai, Komlós and Szemerédi proved in [1] that $r(3, m) \leq O(m^2/\log m)$, (see also [43] for an estimate with a better constant). Improving a result of Erdős who showed in [22] that $r(3, m) \geq \Omega((m/\log m)^2)$, Kim [33] proved that the upper bound is tight up to a constant factor, that is: $r(3, m) = \Theta(m^2/\log m)$. Proofs providing a better constant appear in [14], [28]. All these lower bound proofs are probabilistic, and do not supply any explicit construction of the corresponding graphs.

The problem of finding an explicit construction of triangle-free graphs of independence number m and many vertices has also received a considerable amount of attention. Erdős [23] 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 [16], and further improved by Chung, Cleve and Dagum in [15], where the authors present a construction with

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

vertices. A better explicit construction is given in [3], where the number of vertices is $\Omega(m^{4/3})$.

The graphs G_n described in Section 2 provide the best known explicit construction, as shown in [2]. Indeed, the graph G_n is triangle-free, and as described in the previous section its Shannon capacity is at most $m = O(n^{2/3})$, where n is the number of its vertices. As the Shannon capacity is an upper bound for the independence number, these are explicit graphs showing that $r(3, m) \geq \Omega(m^{3/2})$. A different construction providing the same asymptotic bound has been given a few years later in [18]. See also [35], [19] for more recent variants.

4.2 Maxcut in triangle-free graphs

For a graph G, let $f(G)$ denote the maximum number of edges in a bipartite subgraph of G, that is, the size of the maxcut of G. Edwards [20], [21] proved that for any graph G with m edges,

$$f(G) \geq \frac{m}{2} + \frac{-1+\sqrt{8m+1}}{8} = \frac{m}{2} + \Omega(m^{1/2}).$$

This is tight for every $m = \binom{s}{2}$ where s is an integer.

Erdős and Lovász (see [24]) showed that if G is a triangle-free graph with m edges, then

$$f(G) \geq m/2 + \Omega(m^{2/3}(\frac{\log m}{\log\log m})^{1/3}).$$

This has been improved by a logarithmic factor by Poljak and Tuza [41], and further improved by Shearer [44], who proved that if G is a triangle-free graph with m edges then

$$f(G) \geq \frac{m}{2} + \Omega(m^{3/4}). \tag{1}$$

In [4] the exponent $3/4$ is improved to $4/5$. Moreover, it is shown that this is tight up to the multiplicative constant in the error term. That is, there exists a constant $C > 0$ so that for every m there exists a triangle-free graph G with m edges satisfying

$$f(G) \leq \frac{m}{2} + Cm^{4/5}.$$

This is proved using the graphs G_n described in Section 2 together with the following simple lemma, whose proof can be found, for example, in [4].

Lemma 4.1. *Let $G = (V, E)$ be a d-regular graph with n vertices and $m = nd/2$ edges, and let $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$ be the eigenvalues of G. Then*

$$f(G) \leq (d - \lambda_n)n/4 = \frac{m}{2} - \lambda_n n/4.$$

The graph $G = G_n$ is triangle-free, has n vertices, is $d = (\frac{1}{4} + o(1))n^{2/3}$-regular and its most negative eigenvalue is $\lambda_n = -\lambda$ where $\lambda \leq (9 + o(1)n^{1/3}$. Therefore the number of edges of G is $m = \Theta(n^{5/3})$ and

$$f(G) \leq \frac{m}{2} + O(n^{4/3}) = \frac{m}{2} + O(m^{4/5}).$$

5 List decodable zero-rate codes

A binary code $C \subset \{0,1\}^n$ is $< L$-list decodable with normalized radius τ if any Hamming ball with radius τn contains less than L codewords.

Define

$$\tau_L = \frac{1}{2} - \frac{\binom{2k}{k}}{2^{2k+1}} \quad \text{if } L = 2k \text{ or } L = 2k+1. \tag{2}$$

Blinovskii [13] proved that for any fixed radius $\tau < \tau_L$ the largest possible $< L$-list decodable code with normalized radius τ in $\{0,1\}^n$ is exponentially large in n, that is of size at least 2^{bn} for some $b = b(\tau, L) > 0$. On the other hand he showed that for any fixed radius $\tau > \tau_L$ the largest $< L$-list decodable code with normalized radius τ (of any length n) is of constant size, that is, of size at most some $b' = b'(\tau, L)$. Therefore, the maximum possible rate is positive for $\tau < \tau_L$, and is zero for $\tau > \tau_L$. How large can C be when τ is just above the threshold τ_L ? Let $m(L, \varepsilon)$ denote the maximum possible size of a $< L$ list decodable code with normalized radius at least $\tau_L + \varepsilon$, where the maximum is taken over all values of the length n.

Levenshtein [36] showed that the so-called Plotkin bound is sharp in the unique decoding case ($L = 2$), namely

$$m(2, \varepsilon) = \frac{1}{4\varepsilon} + O(1).$$

For larger values of L the situation is more complicated. The result of [13] is proved by iterating Ramsey's theorem, providing a very large (finite) bound for $m(L, \varepsilon)$. In a recent paper with Bukh and Polyanskiy [7] it is proved that for every even L, $m(L, \varepsilon) = \Theta(1/\varepsilon)$. This implies that for every L, $m(L, \varepsilon) \geq \Omega(1/\varepsilon)$. In addition, the value of $m(3, \varepsilon)$ is determined up to a constant factor, as stated in the following theorem.

Theorem 5.1 ([7])**.**

$$m(3, \varepsilon) = \Theta(\frac{1}{\varepsilon^{3/2}}).$$

The lower bound is proved using the graphs described in Section 2. Here is the argument.

Proof of the lower bound: Let $G = G_m = (V, E)$ be the graph described in Section 2, where m is the number of its vertices. Recall it is a Cayley graph of an elementary abelian 2-group Z_2^r, let A be its adjacency matrix, and let $d = \lambda_1 \geq \lambda_2 \geq \cdots \lambda_m = -\lambda$ be its eigenvalues, where d is the degree of regularity and $-\lambda$ is the smallest eigenvalue. Thus $d = (1/4 + o(1))m^{2/3}$, $\lambda = (9 + o(1))m^{1/3}$ and G is triangle-free. As it is a Cayley graph of an elementary abelian 2-group, it has an orthonormal basis of eigenvectors $v_1, v_2, ..., v_m$

in which each coordinate of each vector is in $\{-1/\sqrt{m}, 1/\sqrt{m}\}$. Indeed, the eigenvectors are simply the (normalized) characters of the group. Define $B = (A + \lambda I)/\lambda$ where I is the m-by-m identity matrix. Then B is a positive semidefinite matrix, its diagonal is the all-1 vector, its eigenvalues are $\mu_i = (\lambda_i + \lambda)/\lambda$ and the corresponding eigenvectors are the vectors v_i. Let P be the m-by-m orthogonal matrix whose columns are the vectors v_i, and note that the first v_1 is the constant vector $1/\sqrt{m}$. Let D be the diagonal matrix whose diagonal entries are the eigenvalues μ_i and let $\sqrt{D}$ denote the diagonal matrix whose entries are $\sqrt{\mu_i}$. Then $P^t B P = D$ and thus $B = (P\sqrt{D})(\sqrt{D}P^t)$.

The rows of the matrix $P\sqrt{D}$ are vectors $x_1, x_2, \ldots, x_m$ where $x_i = (x_{i1}, x_{i2}, \ldots, x_{im})$. Note that for each j, $x_{ij} \in \{-\sqrt{\mu_j/m}, \sqrt{\mu_j/m}\}$ for all i, and that x_{i1} is positive for all i. In addition $x_i^t x_j = B_{ij}$ for all i, j implying that the ℓ_2-norm of each vector x_i is 1 and that among any three vectors x_i there is an orthogonal pair. Let y_i be the vector obtained from x_i by removing its first coordinate (the one which is $\sqrt{\mu_1/m} = \sqrt{(d+\lambda)/m\lambda}$). Then each y_i is a vector of ℓ_2-norm $\sqrt{1 - \mu_1/m}$ and among any three of them there is a pair with inner product $-\mu_1/m$. We can normalize the vectors by dividing each entry by $\sqrt{1 - \mu_1/m}$ to get m unit vectors $z_1, z_2, \ldots, z_m$, where any three of them contain a pair with inner product $-\delta$, where $\delta = \mu_1/(m - \mu_1)$. Moreover, for the vectors $z_i = (z_{ij})$, for each fixed j the absolute value of all z_{ij} is the same for all i. Denote this common value by t_j. We can now use the vectors z_i to define functions mapping $[0, 1]$ to $\{1, -1\}$ as follows. Split $[0, 1]$ into disjoint intervals I_j of length t_j^2 and define f_i to be $\mathrm{sign}(z_{ij})$ on the interval I_j. It is clear that the ℓ_2-norm of each f_i is 1 and the inner product between f_i and f_j is exactly that between z_i and z_j. In particular, each three functions f_i contain a pair whose inner product is at most $-\delta$.

One can replace the functions by vectors of $1, -1$ with essentially the same property, using an obvious rational approximation to the lengths of the intervals. Let n denote the length of these vectors.

Put, say, $\varepsilon = \frac{\delta}{4.01}$. Plugging $d = (1/4 + o(1)m^{2/3}$ and $\lambda = (9 + o(1)m^{1/3}$ we get $\varepsilon = \Theta(m^{-2/3})$ and hence the number of vectors is $m = \Theta\big((1/\varepsilon)^{3/2}\big)$. This gives a binary code with $m = \Theta\big((1/\varepsilon)^{3/2}\big)$ codewords of length n so that among any three codewords there are two such that the Hamming distance between them exceeds $(1/2 + 2\varepsilon)n$. Thus no Hamming ball of radius $(1/4 + \varepsilon)n = (\tau_3 + \varepsilon)n$ can contain three vectors, completing the proof. $\square$

6 Extensions and open problems

As described in the previous sections, if G is a graph with independence number $\alpha(G)$, Shannon capacity $S(G)$ and θ-function $\theta(G)$, then $\alpha(G) \leq S(G) \leq \theta(G)$. Already in his original paper introducing $S(G)$ Shannon [42] proved that if $\chi^*(\overline{G})$ is the fractional chromatic number of the complement of G, and $\chi(\overline{G})$ is the chromatic number of this complement, then $S(G) \leq \chi^*(\overline{G}) \leq \chi(\overline{G})$. Lovász showed that $\theta(G) \leq \chi^*(\overline{G})$. Therefore, for every graph G,

$$\alpha(G) \leq S(G) \leq \theta(G) \leq \chi^*(\overline{G}) \leq \chi(\overline{G}).$$

As mentioned in Section 3, it is not known whether or not $S(G)$ can be bounded by any function of $\alpha(G)$. On the other hand, for any other pair of invariants among the above five, the larger one is not bounded by any function of the smaller one. Indeed as shown in Section 3, there are graphs G on n vertices where $\theta(G) \geq \Omega(n^{1/4})$ and $S(G) \leq 3$, and graphs G on n vertices with $\theta(G) = \Theta(n^{1/3})$ and $\alpha(G) = 2$.

We next show that for any $\varepsilon > 0$ there is a $\delta > 0$ and n-vertex graphs for which $\chi^*(\overline{G}) \geq n^\delta$ and $\theta(G) \leq (2 + \varepsilon)$. Such graphs are constructed in [10], based on a theorem of Frankl and Rödl [29].

For a pair of integers $q > s > 0$ let $G(q, s)$ denote the graph on $n = \binom{2q}{q}$ vertices corresponding to all q-subsets of the $2q$-element set $Q = \{1, 2, \ldots, 2q\}$, where two vertices are adjacent iff the intersection of their corresponding subsets is of cardinality precisely s. By the main result of Frankl and Rödl in [29], for every $\gamma > 0$ there is a $\mu = \mu(\gamma) > 0$ so that if $(1 - \gamma)q > s > \gamma q$ then every family of more than $2^{2q(1-\mu)}$ subsets of cardinality q of Q contains some pair of subsets whose intersection is of cardinality s. This means that the independence number of the graph $G(q, s)$ for q and s that satisfy $(1 - \gamma)q > s > \gamma q$ satisfies

$$\alpha(G(q, s)) \leq n^c \tag{3}$$

for some $c = c(\gamma) < 1$, where $n = \binom{2q}{q}$ is the number of vertices. Therefore, the fractional chromatic number of $G(q, s)$ is at least $n^{1-c} = n^\delta$.

It is shown in [10] that the parameter γ can be chosen to ensure that $\theta(G(q, s)) \geq \frac{n}{2+\varepsilon}$, where n is the number of vertices of $G(q, s)$. Lovász proved in [38] that if a graph has a vertex transitive automorphism group then the product of its θ-function with that of its complement is the number of vertices. Since the graph $G(q, s)$ is clearly vertex transitive, this implies that the θ-function of its complement is at most $2 + \varepsilon$. Thus, this complement is a graph showing that θ may be fixed (in fact close to 2) while the fractional chromatic number of the complement grows as a small fixed power of the number of vertices.

The existence of graphs with a fixed fractional chromatic number and large chromatic number is well known. Here the gap can be only logarithmic in the number of vertices. The Kneser graphs provide examples of graphs with fractional chromatic number $2+\varepsilon$ and chromatic number $\Omega(\log n)$ where n is the number of vertices. The Kneser graph $K(m,r)$ is the graph whose vertices are all subsets of cardinality r of an m-element set, where two are adjacent if they are disjoint. Lovász proved in [37] that the chromatic number of $K(m,r)$ is $m-2r+2$, and it is easy to see that its fractional chromatic number is m/r. Taking $r=\frac{m}{2+\varepsilon}$ we get the required example.

It will be interesting to find a construction of K_k-free graphs with extremal spectral properties for $k>3$, extending that of the graphs G_n described in Section 2. It is not difficult to show (see [9]) that if $d^{k-1} > n^{k-2}\lambda$ then any (n,d,λ)-graph G contains a clique of size k. Therefore, if $\lambda = O(\sqrt{d})$ and G contains no copy of K_k, then

$$d \leq O(n^{1-\frac{1}{2k-3}}).$$

This is tight for $k=3$, as shown by the graphs G_n. Is it tight for larger values of k as well?

What is the largest possible value of the θ-function of an n vertex graph with independence number smaller than k ? In [10] it is shown that this maximum is at most $O(n^{1-2/k})$. This is tight for $k=3$ but is not known to be tight for any larger value of k. The results in [27] imply that this maximum is at least $\Omega(n^{1-O(1/\log k)})$. It will be interesting to close the gap here. In a somewhat different direction it is proved in [10] that if the odd girth of the complement of an n vertex graph G exceeds $2s+1$, then its θ-function is at most $O(n^{1/(2s+1)})$. As mentioned in [10], this is tight for all values of s, by a natural extension of the construction of the graphs G_n.

What is the maximum possible Euclidean norm of a sum of n unit vectors in an Euclidean space (of any dimension) so that among any k of them some two are orthogonal ? This extends the question discussed in subsection 3.2 and is closely related to the question about the maximum possible θ-function of a graph on n vertices with independence number smaller than k. Denote this maximum possible norm by $f(n,k)$. It is clear that $f(n,2) = \sqrt{n}$ and as discussed in Section 3, $f(n,3) = \Theta(n^{2/3})$. In [10] it is shown that $f(n,k) \leq O(n^{1-1/k})$ for all k. The following theorem can be proved following the approach in [27].

Theorem 6.1. *For any $k > k_0$, $n > n(k)$,*

$$f(n,k) \geq n^{1-O(1/\log k)}.$$

Here is an outline of the proof. Let $t = 4p$, p a prime, and let $\mathcal{F}$ be the set of all vectors in $\{-1, 1\}^t$ with an even number of -1 entries which is at most $n/3$. Let $\mathcal{G}$ denote the tensor product of s copies of $\mathcal{F}$, normalized to be unit vectors. Each vector in $\mathcal{G}$ has projection at least $(1/3)^s$ in the direction of the all 1 vector. Put $q = 2^{-0.85st}$ and let X be a random subset of $\mathcal{G}$ obtained by taking each member of $\mathcal{G}$, randomly and independently, to be a member of X with probability q. Let n denote the number of vectors in X. Clearly their sum is of norm at least $n/3^s$, and n is at least $2^{st/25}$ (say), with high probability. By a result of [30], any set of more than $2^{H(1/4)t}$ vectors in $\mathcal{F}$ contains an orthogonal pair. Now any set in the tensor power of s copies of $\mathcal{F}$ that contains no such pair is a subset of a product of its projections on the copies of $\mathcal{F}$, namely of a box of the form $\mathcal{F}_1 \times \mathcal{F}_2 \cdots \times \mathcal{F}_s$, with $\mathcal{F}_i \subset \mathcal{F}$ with no pair of orthogonal vectors. The number of choices for such a product is smaller than $2^{2^t s}$ and the probability that for, say, $k = 30 \cdot 2^t/t$, k members of such a product belong to X is small, by the union bound, as

$$2^{2^t s}\binom{2^{H(1/4)ts}}{k}q^k < 1.$$

This completes the proof. □

As described in Section 4, every triangle free graph with m edges contains a bipartite subgraph with at least $\frac{m}{2} + cm^{4/5}$ edges. The graphs G_n show that this is tight up to the absolute constant c. It is natural to extend the question for other forbidden graphs H. Let $f(G)$ denote the maximum number of edges in a bipartite subgraph of G and let $f(m, H)$ denote the minimum possible value of $f(G)$, as G ranges over all H-free graphs with m edges. It is proved in [11] that $f(m, H) = \frac{m}{2} + c(H)m^{4/5}$ for all graphs H obtained by joining a vertex to all vertices of any nontrivial forest, and this is tight up to the value of $c(H)$. Here, too, the tightness follows from the graphs G_n. It is also proved in the same paper that

$$f(m, C_{2r}) \geq \frac{m}{2} + c(r)m^{\frac{r}{r+1}} \tag{4}$$

for every even cycle C_{2r}, and this is tight for $2r \in \{4, 6, 10\}$. For complete bipartite graphs with 2 or 3 vertices in the smaller color class it is shown that

$$f(m, K_{2,s}) \geq \frac{m}{2} + c(s)m^{5/6}$$

and

$$f(m, K_{3,s}) \geq \frac{m}{2} + b(s)m^{4/5}$$

and both results are tight up to the constants $c(s), b(s)$. See also [6] for some related results. An intriguing conjecture raised in [6] is that for every fixed graph H there is an

$\varepsilon = \varepsilon(H)$ so that $f(m, H) \geq \frac{m}{2} + \Omega(m^{3/4+\varepsilon})$. This, as well as the conjecture that for every even cycle the estimate (4) is tight, remain open.

Recall that the function $m(L, \varepsilon)$ defined in Section 5 is the maximum possible size of a binary code (of any length) in which every Hamming ball of normalized radius $\tau_L + \varepsilon$ contains less than L codewords. Here τ_L, defined in (2), is the threshold normalized radius between positive and zero rate for $< L$-list decodable codes. While it is proved in [7] that for every even L, $m(L, \varepsilon) = \Theta_L(1/\varepsilon)$ and that $m(3, \varepsilon) = \Theta(1/\varepsilon^{3/2})$, the problem of determining or estimating $m(L, \varepsilon)$ for odd values of $L > 3$ is open. The lower bound is $\Omega_L(1/\varepsilon)$ and the upper bound is an iterated exponential in $1/\varepsilon$. It seems plausible to conjecture that $m(n, \varepsilon)$ is bounded by a polynomial in ε, for any fixed L. This remains open.

Thucydides, who is widely considered to be the father of scientific history, wrote in the introduction to his book on the History of the Peloponnesian War between Sparta and Athens (431-404 BC): "With reference to the speeches in this history; some I heard myself, others I got from various quarters; it was in all cases difficult to carry them word for word in one's memory, so my habit has been to make the speakers say what was in my opinion demanded of them by the various occasions."

In analogy, let me conclude this short paper stating that many of the results described here are due to Lovász, others are inspired by his questions and proofs. Regarding the statements that are difficult to derive directly by following his work word for word, my habit has been to try to find out how Laci would have established them. I hope this has been at least somewhat successful.

References

[1] M. Ajtai, J. Komlós and E. Szemerédi, A note on Ramsey numbers, J. Combinatorial Theory Ser. A 29 (1980), 354-360.

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

[3] N. Alon, Tough Ramsey graphs without short cycles, J. Algebraic Combinatorics 4 (1995), 189-195.

[4] N. Alon, Bipartite subgraphs, Combinatorica 16 (1996), 301-311.

[5] N. Alon, The Shannon capacity of a union, Combinatorica 18 (1998), 301-310.

[6] N. Alon, B. Bollobás, M. Krivelevich and B. Sudakov, Maximum cuts and judicious partitions in graphs without short cycles, J. Combinatorial Theory, Ser. B 88 (2003), 329-346.

[7] N. Alon, B. Bukh and Y. Polyanskiy, List-decodable zero-rate codes, arXiv:1710.10663

[8] N. Alon and F. R. K. Chung, Explicit construction of linear sized tolerant networks, Discrete Math. 72(1988), 15-19.

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

[10] N. Alon and N. Kahale, Approximating the independence number via the θ-function, Math. Programming 80 (1998), 253-264.

[11] N. Alon, M. Krivelevich and B. Sudakov, MaxCut in H-free graphs, Combinatorics, Probability and Computing 14 (2005), 629-647.

[12] N. Alon and A. Orlitsky, Repeated communication and Ramsey graphs, IEEE Transactions on Information Theory 41 (1995), 1276-1289.

[13] V. M. Blinovskiĭ, Bounds for codes in decoding by a list of finite length, Problemy Peredachi Informatsii 22 (1986),11–25.

[14] T. Bohman and P. Keevash, Dynamic Concentration of the Triangle-Free Process, The Seventh European Conference on Combinatorics, Graph Theory and Applications, 489–495, CRM Series, 16, Ed. Norm., Pisa, 2013.

[15] 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.

[16] 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.

[17] F. Chung and R. L. Graham, **Erdős on Graphs: His Legacy of Unsolved Problems**, A. K. Peters, Ltd., Wellesley, MA, 1998.

[18] B. Codenotti, P. Pudlák, and G. Resta, Some structural properties of low-rank matrices related to computational complexity, Theoret. Comput. Sci. 235 (2000), 89–107.

[19] D. Conlon, A sequence of triangle-free pseudorandom graphs, Combin. Probab. Comput. 26 (2017), no. 2, 195-200.

[20] C. S. Edwards, Some extremal properties of bipartite subgraphs, Canadian Journal of Mathematics 3 (1973), 475-485.

[21] C. S. Edwards, An improved lower bound for the number of edges in a largest bipartite subgraph, Proc. 2^{nd} Czechoslovak Symposium on Graph Theory, Prague, (1975), 167-181.

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

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

[24] P. Erdős, Problems and results in Graph Theory and Combinatorial Analysis, in: *Graph Theory and Related Topics*, J. A. Bondy and U. S. R. Murty (Eds.), Proc. Conf. Waterloo, 1977, Academic Press, New York, 1979, 153-163.

[25] P. Erdős, R. J. McEliece and H. Taylor, Ramsey bounds for graph products, Pacific Journal of Mathematics, 37 (1971),45–46.

[26] P. Erdős and A. Rényi, On a problem in the theory of graphs (in Hungarian), Publ. Math. Inst. Hungar. Acad. Sci. 7 (1962), 215–235.

[27] U. Feige, Randomized graph products, chromatic numbers, and the Lovász θ-function, Proc. of the 27th ACM STOC, ACM Press (1995), 635-640.

[28] G. Fiz Pontiveros, S. Griffiths and R. Morris, The triangle-free process and R(3,k), arXiv:1302.6279

[29] P. Frankl and V. Rödl, Forbidden intersections, Trans. AMS 300 (1987), 259–286.

[30] P. Frankl and R. Wilson, Intersection theorems with geometric consequences, Combinatorica 1 (1981), 259-286.

[31] W. Haemers, An upper bound for the Shannon capacity of a graph, Colloq. Math. Soc. János Bolyai 25, Algebraic Methods in Graph Theory, Szeged, Hungary (1978), 267–272.

[32] B. S. Kashin and S. V. Konyagin, On systems of vectors in a Hilbert space, Trudy Mat. Inst. imeni V. A. Steklova 157 (1981), 64-67. English translation in: Proc. of the Steklov Institute of Mathematics (AMS 1983), 67-70.

[33] J. H. Kim, The Ramsey number $R(3,t)$ has order of magnitude $t^2/\log t$, Random Structures Algorithms 7 (1995), 173-207.

[34] S. V. Konyagin, Systems of vectors in Euclidean space and an extremal problem for polynomials, Mat. Zametki 29 (1981), 63-74. English translation in: Mathematical Notes of the Academy of the USSR 29 (1981), 33-39.

[35] S. Kopparty, A constructive lower bound on R(3,k), see: http://sites.math.rutgers.edu/ sk1233/courses/graphtheory-F11/cayley.pdf

[36] V. I. Levenshtein, The application of Hadamard matrices to a problem in coding, Problemy Kibernetiki, 5 (1961), 123–136. English translation in Problems of Cybernetics 5, 1964 pp. 166–184.

[37] L. Lovász, Kneser's conjecture, chromatic number, and homotopy, J. Combin. Theory Ser. A 25 (1978), no. 3, 319-324.

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

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

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

[41] S. Poljak and Zs. Tuza, Bipartite subgraphs of triangle-free graphs, SIAM J. Discrete Math. 7 (1994), 307-313

[42] C. E. Shannon, The zero–error capacity of a noisy channel, IRE Trans. Inform. Theory 2 (1956), 8–19.

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

[44] J. B. Shearer, A note on bipartite subgraphs of triangle-free graphs, Random Structures and Algorithms 3 (1992), 223-226.