Eigenvalues and expansion of bipartite graphs

Høholdt, Tom; Janwa, Heeralal

[Link back to DTU Orbit](#)

Eigenvalues and expansion of bipartite graphs

Tom Høholdt · Heeralal Janwa

Abstract We prove lower bounds on the largest and second largest eigenvalue of the adjacency matrix of connected bipartite graphs and give necessary and sufficient conditions for equality. We give several examples of classes of graphs that are optimal with respect to the bounds. We prove that BIBD-graphs are characterized by their eigenvalues. Finally we present a new bound on the expansion coefficient of (c, d)-regular bipartite graphs and compare that with with a classical bound.

1 Introduction

An expander graph is a highly connected "sparse" graph (see, for example [28]). Expander graphs have numerous applications including those in communication science, computer science (especially complexity theory), network design, cryptography, combinatorics and pure mathematics (see the books and articles in the Bibliography).

T. Høholdt
Department of Mathematics, Technical University of Denmark, Copenhagen, Denmark
e-mail: T.Hoeholdt@mat.dtu.dk

H. Janwa (✉)
Department of Mathematics, University of Puerto Rico, Rio Piedras, Puerto Rico
e-mail: heeralal.janwa@gmail.com

Expander graphs have played a prominent role in recent developments in coding theory (LDPC codes, expander codes, linear time encodable and decodable codes, codes attaining the Zyablov bound with low complexity of decoding) (see [3,8,11,15–18,20,27,30–32,34,37], and others).

We shall consider graphs $\mathcal{X} = (V, E)$, where V is the set of vertices and E is the set of edges of $\mathcal{X}$. We will assume that the graph is undirected and connected and we shall only consider finite graphs. For $F \subset V$, the *boundary* ∂F is the set of edges connecting F to $V \backslash F$. The *expanding constant*, or *isoperimetric constant* of $\mathcal{X}$ is defined as,

$$h(\mathcal{X}) = \min_{\emptyset \neq F \subset V} \frac{|\partial F|}{\min\{|F|, |V \backslash F|\}}.$$

Moreover if $\mathcal{X}$ is viewed as the graph of a communication network, then $h(\mathcal{X})$ measures the "quality" of the network as a transmission network. In all applications, the larger the $h(\mathcal{X})$ the better, so we seek graphs (or families of graphs) with $h(\mathcal{X})$ as large as possible with some fixed parameters.

In [32] Tanner introduced another notation for the expansion coefficient. Let as before $\mathcal{X} = (V, E)$, be a graph where V is the set of vertices and E is the set of edges of $\mathcal{X}$. Let $X \subseteq V$ with $|X| \leq \alpha |V|$, then

$$c(\alpha) = \min_{\emptyset \neq X \subset V} \frac{|\partial X|}{\min\{|X|, |V \backslash X|\}}.$$

It is well-known that the expansion properties of a graph are closely related to the eigenvalues of the *adjacency matrix* A of the graph $\mathcal{X} = (V, E)$; it is indexed by pairs of vertices x, y of $\mathcal{X}$ and A_{xy} is the number of edges between x and y. When $\mathcal{X}$ has n vertices, A has n real eigenvalues, repeated according to multiplicities that we list in decreasing order

$$\mu_0 \geq \mu_1 \geq \cdots \geq \mu_{n-1}.$$

It is also known that if $\mathcal{X}$ is D-regular, i.e. all vertices have degree D, then $\mu_0 = D$ and if moreover the graph is connected $\mu_1 < D$. Also $\mathcal{X}$ is bipartite if and only if $-\mu_0$ is an eigenvalue of A. We recall the following

Theorem 1 [7] *Let $\mathcal{X}$ be a finite, connected , D-regular graph then*

$$(D - \mu_1)/2 \leq h(\mathcal{X}) \leq \sqrt{2D(D - \mu_1)}.$$

And

Theorem 2 [7] *Let $(\mathcal{X}_m)_{m \geq 1}$ be a family of finite connected, D-regular graphs with $|V_m| \to +\infty$ as $m \to \infty$. Then*

$$\liminf_{N \to \infty} \mu_1(\mathcal{X}_m) \geq 2\sqrt{D - 1}.$$

This leads to the following

Definition 1 A finite connected, D-regular graph $\mathcal{X}$ is *Ramanujan* if, for every eigenvalue μ of A other than $\pm D$, one has

$$\mu \leq 2\sqrt{D - 1}.$$

We will also need

Definition 2 (*Bipartite Ramanujan Graphs*) Let $\mathcal{X}$ be a (c, d)-regular bipartite graph. Then $\mathcal{X}$ is called a Ramanujan graph if

$$\mu_1(\mathcal{X}) \leq \sqrt{(c - 1)} + \sqrt{(d - 1)}.$$

It is known that computing the expansion coefficient of arbitrary graphs is an NP-complete problem. Thanks to the work of Tanner, and Alon and Millman, one can derive bounds on the expansion coefficient in terms of μ_1. The complexity of determining μ_1 is still difficult if the number of vertices is large (for example of the order 10^6 for LDPC codes).

In this article we derive bounds on μ_1 for arbitrary bipartite graph $\mathcal{X}$ in terms of the number of edges, the maximum degree $\mu_{\max}$, and the rank r_χ of the transfer matrix of $\mathcal{X}$. Since effective upper bounds exist on $\mu_{\max}$, and r_χ, [5] we thus obtain a bound that is easily computable. We also demonstrate that our bound is met with equality by bipartite graphs derived from six families of graphs that have played prominent role in the coding theory and sequence design (especially in the efficient construction of LDPC codes) (for example bipartite graphs of finite geometries, from N-gons, the $D(n, q)$ graphs, graphs from finite analog of upper half-planes, from BIBD, and from projective coset graph of codes). Our bounds provide explanations as to why the corresponding LDPC codes from these bipartite work so well in practice. We analyze the bipartite graphs of BIBD's and show that the graphs are bipartite Ramanujan graphs and are optimal in that they meet our bound. Furthermore, we demonstrate that eigenvalues, in some sense, characterize BIBD's. Finally we present a new bound on the expansion coefficient of (c, d)-regular bipartite graphs and compare that with a classical bound.

2 Eigenvalue bounds

We recall that a matrix A with rows and columns indexed by a set X is called irreducible when it is not possible to find a proper subset S of X so that $A(x, y) = 0$ whenever $x \in S$ and $y \in X \backslash S$. Equivalently, A is not irreducible if and only if it is possible to apply a simultaneous row and column permutation on A to get a matrix in a square block form so that one of the blocks is a zero block. For the following lemma, see for example ([14], p. 363).

Lemma 1 *Let D be a finite graph. Then the adjacency matrix of A is irreducible if and only if D is connected.*

We shall also need

Proposition 1 (Perron-Frobenius) *Let A be an irreducible non-negative matrix. Then, there is up to scalar multiples, a unique non-negative eigenvector $\mathbf{a} := (a_1, a_2, \ldots, a_n)$ all of whose coordinates a_i are strictly positive. The corresponding eigenvalue μ_0 (called the dominant eigenvalue of A) has algebraic multiplicity 1 and $\mu_0 \geq \mu_i$ for any eigenvalue μ_i of A.*

We recall the following special case of Courant-Fisher Theorem (called the Raleigh-Ritz Theorem) (see for example, ([14], Theorem 4.2.2))

Theorem 3 *Let A be an $n \times n$ Hermitian matrix over the complex field $\mathcal{C}$, then it is known that all its eigenvalues are real, with maximum eigenvalue $\mu_{\max}$ (i.e. the spectral radius of A). For $\mathbf{0} \neq X \in \mathcal{C}^n$, define the Raleigh quotient $R_X := \frac{X^{*T} A X}{X^{*T} X}$. Then $\mu_{\max} = \max_{X \neq \mathbf{0}} R_X$. Furthermore, $R_X \leq \mu_{\max}$ with equality if and only if X is an eigenvector corresponding to the eigenvalue $\mu_{\max}$.*

Definition 3 *Let $\mathcal{X}$ be a bipartite graph with average left degree $\overline{c}$ and average right degree $\overline{d}$. Define $v := |E|/\overline{c}$ and $b := |E|/\overline{d}$. Let $\mu_1 := \max_\gamma\{|\gamma| | \gamma \neq \mu_{\max}\}$, where the maximization is over the eigenvalues of $\mathcal{X}$, and $\mu_{\max}$ is the maximum eigenvalue of the adjacency matrix of $\mathcal{X}$.*

Theorem 4 *Let $\mathcal{X}$ be a connected bipartite graph with average left degree $\overline{c}$ and average right degree $\overline{d}$ and maximum eigenvalue $\mu_{\max}$. Then $\sqrt{\overline{c}\overline{d}} \leq \mu_{\max}$ with equality if and only is $\mathcal{X}$ is a (c, d)-regular bipartite graph.*

Proof If $\mathcal{X}$ is a (c, d)-regular bipartite graph, with adjacency matrix

$$A = \begin{bmatrix} \mathbf{0} & H \\ H^T & \mathbf{0} \end{bmatrix}$$

then it is easy to see that $[1, 1, \ldots, 1, \tau, \ldots, \tau]$ where $\tau = \sqrt{\frac{d}{c}}$ is an eigenvector corresponding to the eigenvalue $\sqrt{cd}$ and then the inequality and equality follow from the Perron-Frobenius theorem (Proposition 1). Conversely, assume that $\mathcal{X}$ is a connected bipartite graph on v left vertices of average degree $\overline{c}$ and b right vertices of average degree $\overline{d}$ and maximum eigenvalue $\mu_{\max}$. Define $Z := [1, 1, \ldots, 1, \tau, \ldots, \tau]^T$, in which the first v component are 1, and where $\tau := \sqrt{\frac{\overline{d}}{\overline{c}}}$

Then one can see that $R_Z = \sqrt{\overline{c}\overline{d}}$ and therefore $\sqrt{\overline{c}\overline{d}} \leq \mu_{\max}$. If we have equality then $R_Z = \mu_{\max}$, and from the Courant-Fisher Theorem Z is an eigenvector corresponding to the maximal eigenvalue R_Z. Therefore, $AZ = \mu_{\max}Z$. By assumption, then $AZ = \sqrt{\overline{c}\overline{d}}Z$.

By solving the simultaneous equations, we get that $c_{v_i} = \overline{c}$ for every left vertex v_i, and $d_{b_j} = \overline{d}$ for every right vertex b_j. Consequently, $\mathcal{X}$ is a (c, d) regular graph. $\qquad\square$

Theorem 5 *Let $\mathcal{X}$ be a connected graph such that both $\pm\mu_{\max}$ are eigenvalues (i.e. it is a bipartite graph with say v left vertices and b right vertices). Suppose that*

$$\left(\frac{1}{2v}\sum_{\mu_i}\mu_i{}^2\right) \cdot \left(\frac{1}{2b}\sum_{\mu_i}\mu_i{}^2\right) = \mu_{\max}^2.$$

Then $\mathcal{X}$ is a (c, d)-regular graph, where $c := |E|/v$ and $d := |E|/b$

Proof By definition of the adjacency matrix, $Trace(AA^T) = 2|E|$. But $Trace(AA^T) = \sum_{\mu_i}\mu_i{}^2$ Since, $\overline{c} := |E|/v$ and $\overline{d} = |E|/b$, by assumption we get $\overline{c}\overline{d} = \mu_{\max}^2$ and therefore by Theorem 4, $\mathcal{X}$ is a (c, d) regular graph with $c := |E|/v$ and $d := |E|/b$. $\qquad\square$

Theorem 6 *Let $\mathcal{X}$ be a connected bipartite graph with average left degree $\overline{c}$ and average right degree $\overline{d}$. Let $v := |E|/\overline{c}$ and $b := |E|/\overline{d}$ (we assume $b \geq v$) and maximum eigenvalue $\mu_{\max}$ (i.e. the spectral radius of $\mathcal{X}$), and $r_\chi :=$ rank of the transfer matrix of the bipartite graph $\mathcal{X}$. Then*

$$\mu_1 \geq \left(\frac{|E| - \mu_{\max}^2}{r_\chi - 1}\right)^{1/2}$$

with equality if and only if the eigenvalues are $\pm\mu_{\max}$ (with multiplicity 1), $\pm\mu_1$ (with multiplicity $r_\chi - 1$), and 0 with multiplicity $b + v - 2r_\chi$. Indeed equality holds if and only if the bipartite graph has four nonzero eigenvalues and a possible 0 eigenvalue.

Proof Since the rank of the transfer matrix of the bipartite graph is r_χ, and the rank of its transpose is the same, we conclude that the rank of the adjacency matrix of the graph is $2r_\chi$. Therefore, 0 appears as an eigenvalue of the graph with multiplicity $b + v - 2r_\chi$ and non-zero eigenvalues appear $2r_\chi$ times. Since $\mathcal{X}$ is a connected bipartite graph, the set of eigenvalues is $S(\mathcal{X}) := \{\pm\mu_{\max}, \pm\mu_1, \pm\mu_2, \pm \cdots \pm \mu_{r_\chi-1}, 0\}$ with $2r_\chi$ non-zero eigenvalues, where the absolute values are in decreasing order.

Since $AA^T = A^2 = \begin{bmatrix} HH^T & \mathbf{0} \\ \mathbf{0} & H^T H \end{bmatrix}$ we get by taking the trace, $Trace(A^2) = Trace(HH^T) + Trace(H^T H) = v\bar{c} + b \cdot \bar{d} = |E| + |E| = 2|E|$. Therefore, $2|E| = Trace(A^2) = 2\mu_{\max}{}^2 + 2\mu_1{}^2 + 2\sum_{i=2}^{r_\chi - 1}\mu_i^2 \le 2\mu_{\max}{}^2 + 2(r_\chi - 1)\mu_1{}^2$. Hence

$$\mu_1 \ge \left(\frac{|E| - \mu_{\max}^2}{r_\chi - 1}\right)^{1/2}.$$

It is clear that equality occurs if and only if the eigenvalues are $\pm\mu_{\max}$ with multiplicity 1, $\pm\mu_1$ with multiplicity $(r_\chi - 1)$, and 0 with multiplicity $b - r_\chi$. The last statement can be derived from the Perron-Frobenius theorem which gives that a graph is bipartite if and only if λ is an eigenvalue with multiplicity m_λ, then $-\lambda$ also is an eigenvalue with the same multiplicity. $\qquad\square$

Finding tight upper bounds on the spectral radius ($\mu_{\max}$) is one of the most important problems in graph theory and several tight bounds are known, for example in terms of the degree sequence (see, the recent book [6] and scores references therein). In our theorem, one can replace $\mu_{\max}$ with any of these upper bounds, thus avoiding computation of the spectral radius to obtain the bound. Similarly one can replace r_χ with an upper bound, for example $r_\chi \le v$. With such a replacement, the equality condition is only necessary but not sufficient anymore. The rank r_χ problem is related to the problem of "nullity of graphs" that has many important applications in Chemistry, Biology and other disciplines (see [6] for references). The complexity of determining μ_1 is difficult if the number of vertices is large (for example of the order 10^6 for LDPC codes). We thus derive a bound that is easily computable. Indeed, in the next section, we demonstrate that our bound is met with equality by μ_1 of bipartite graphs derived from six families of graphs that have played prominent role in the coding theory and sequence design (especially in the efficient construction of LDPC codes). We thus provide explanations as to why the corresponding LDPC codes based on these bipartite graphs work so well in practice. A simple bound on μ_1 of d-regular graph has been known for a long time (see [4] or [22].)

If we do not have information about the rank r_χ of the incidence matrix of the bipartite graph, then since $r_\chi \le v$,

$$\left(\frac{|E| - \mu_{\max}^2}{r_\chi - 1}\right)^{1/2} \ge \left(\frac{|E| - \mu_{\max}^2}{v - 1}\right)^{1/2}$$

and we obtain the following result.

Corollary 1 *Let $\mathcal{X}$ be a connected bipartite graph with average left degree $\bar{c}$ and average right degree $\bar{d}$. Let $v := |E|/\bar{c}$ and $b := |E|/\bar{d}$ (we assume $b \ge v$) and maximum eigenvalue $\mu_{\max}$. Then*

$$\mu_1 \ge \left(\frac{|E| - \mu_{\max}^2}{v - 1}\right)^{1/2}$$

with equality if the eigenvalues are $\pm\mu_{\max}$ (with multiplicity 1), $\pm\mu_1$ (with multiplicity $(v-1)$), and 0 (with multiplicity $b - v$).

However, determination of the rank r_χ or bounding it is one of the important problems in graph theory. In fact, as we will show by several examples in Sect. 2.1 that the bound is substantially improved by a knowledge of r_χ, as the following observation shows.

Corollary 2 *Let $\mathcal{X}$ be a connected bipartite graph with average left degree $\overline{c}$ and average right degree $\overline{d}$, and vertices $v \leq b$. Then the bound in Theorem 6 improves upon the bound in Corollary 1 by $\left\lceil \sqrt{(v - r_\chi)/(r_\chi - 1)} \right\rceil \times 100$ percent.*

As we will see in Example 1 below, we some times get as much as 100 percentage improvement.

Corollary 3 *Let $\mathcal{X}$ be a connected (c, d)-regular bipartite graph with rank of the incidence matrix r_χ. Define $v := |E|/c$ and $b := |E|/d$. Then $\mu_{\max} = \sqrt{c \cdot d}$, and*

$$\mu_1 \geq \left(\frac{|E| - cd}{r_\chi - 1} \right)^{1/2}$$

with equality if and only if the eigenvalues are $\pm\mu_{\max}$ (with multiplicity 1), $\pm\mu_1$ (with multiplicity $(r_\chi - 1)$), and 0 (with multiplicity $b - r_\chi$).

Corollary 4 *Let $\mathcal{X}$ be a connected (c, d)-regular bipartite graph. Define $v := |E|/c$ and $b := |E|/d$. Then*

$$\mu_1 \geq \left(\frac{|E| - cd}{v - 1} \right)^{1/2}$$

with equality if the eigenvalues are $\pm\mu_{\max}$ (with multiplicity 1), $\pm\mu_1$ (with multiplicity $(v - 1)$), and 0 (with multiplicity $b - v$.)

2.1 Examples of bipartite graphs attaining the bound on μ_1

In this section we give some examples of classes of graphs where the bound on μ_1 in Theorem 6 is met with equality.

The first group contains graphs derived from the so-called Kasami, Welch and Niho binary linear codes. These have important applications in sequence design and cryptography.

The second group contain some Cayley graphs from subgroups of $PGL(2, I\!\!F_q)$ constructed by Terras [33] and many coauthors and their spectra was analyzed by Li and Meemark [23].

The third group contains the so-called $D(m, q)$ graphs that were constructed from affine transformations over finite fields by Lazebnik and Ustimenko [21]. These graphs have yielded high performance LDPC codes. For example, recently, using $D(m, q)$ as the Tanner graph, Kim et al. [19] constructed and studied the associated LDPC code $LU(m, q)$. Sin and Xiang [29] determined the dimension of the code $LU(3, q)$ for odd q, and Anslan [2] very recently settled the case of even q.

Li et al. [23] have determined the eigenvalues of $D(m, 2)$ and their multiplicities, and partial information about $D(3, m)$. From their results we see that the bound of Theorem 6 again is met with equality which gives a theoretical explanation of the high performance of the corresponding LDPC codes.

The fourth group contains the generalized 4-gons. The generalized N-gons yield connected bipartite graphs of optimal girth and have many applications in group theory, combinatorics, and coding theory (see for example, [26] and [35], and comprehensive references therein). They are highly symmetric and from a theorem of Feit and Higman they can only exist for $N = 2, 3, 4, 6, 8$. Fortunately, each of them form a class of different regularity. Moreover these graphs have also been used in the construction of very efficient LDPC codes. (see for example [35], and several references therein).

The fifth group mentions graphs from balanced incomplete block designs, which are treated in the next section, and the sixth group recalls a generalization of these by Gunnells in [10].

Example 1 (Graphs from Codes) Let C be a binary linear code of length n, with minimum distance $d \geq 3$, then one can define the projective coset graph $\mathcal{X}_P(C)$ using C, where the eigenvalues of the adjacency matrix are precisely $\{n - 2w(c)|c \in C^{\perp}\}$, where $C^{\perp}$ is the dual code of C. In particular if $C^{\perp}$ contains the vector 1^n, then the $\mathcal{X}_P$ is a bipartite graph (see [18]). To get a particular class of codes, let α be a *primitive* element of $\mathbb{F}_{2^m}$ (i.e., α is a generator for the multiplicative group $\mathbb{F}_{2^m}^*$) and let $m_r(x)$ denote the minimal polynomial of α^r over $\mathbb{F}_2$. Let $n = 2^m - 1$. Let $\mathcal{C}_r$ be the cyclic code of length $2^m - 1$ over $\mathbb{F}_2$ generated by $m_1(x)m_r(x)$ (i.e., the vector space $\frac{x^n-1}{\langle m_1(x)m_r(x)\rangle}$).

If $r = 2^i + 1$, or $r = 2^{2i} - 2^i + 1$. Then, $\mathcal{C}_r^{\perp}$ has three non-zero weights, namely $2^{m-1}, 2^{m-1} \pm 2^{(m+e-2)/2}$, when m/e is odd, where $e = $ G.C.D.(m, i) (see [25] and [24]).

The graph $\mathcal{X}(\mathcal{C}_r)$ is a $K = (2^m - 1)$-regular graph on $N = (K + 1)^2$ vertices and $\mu_1(\mathcal{X}(\mathcal{C}_r)) = 2^{e/2}\sqrt{K + 1}$.

It follows that for m-odd and $e = 1$, we get optimal Ramanujan graphs (i.e, they meet the lower bound on the second eigenvalue of Theorem 6. The weight distribution of these graphs was determined by Kasami and Niho. They are: 0 with multiplicity 1, 2^{m-1} with multiplicity $n(2^{m-1}-1)$, and $2^{m-1}\pm2^{(m-1)/2}$ with respective multiplicity $n(2^{m-2}\pm2^{(m-3)/2})$. If we consider the extended code C^{ext} by adding a parity check we get a code of length $2^m = N$, then $\mathcal{X}_P(C^{ext})$ is a bipartite graph on 2^{2m+1} vertices with eigenvalues $\pm2^m$ with multiplicity 1, $\pm2^{(m+1)/2}$ with multiplicity $(N-1)2^{(m-1)}$, and 0 with multiplicity $2(N-1)(2^{m-1}+1)$.

These graphs also satisfy the bound in Theorem 6. Here $r_\chi = 1 + 2^{m-1}(2^m - 1)$, and $v = 2^{2m}$. We also see from Corollary 2 that, since v is approximately $2r_\chi$, Theorem 6 improves upon the bound in Corollary 1 by nearly 100 percent.

Example 2 (Projective Graphs of $PGL(2, \mathbb{F}_q)$) Let H be a subgroup of $PGL(2, \mathbb{F}_q)$. Then for a double coset HsH which is its own inverse (i.e., symmetric) and which is the disjoint union of $|H|$ right H-cosets, consider the Cayley graph $X_{HsH} = Cay(G/H, HsH/H)$, called an H-graph. It is undirected and $|H|$-regular. (When $H = K$, where K is this non-split torus, this is a Terras graph.) If one considers $H = U$ to be the subgroup of $PGL(2, \mathbb{F}_q)$ which is the subgroup of upper triangular matrices inside $SL(2, \mathbb{F}_q)$, then the eigenvalues of the graphs X_{UsU} is q-regular bipartite Ramanujan graph with eigenvalues $\pm q$ with multiplicity 1, ±1 with multiplicity q, and $\sqrt{q}$ of multiplicity $(q + 1)(q - 3)/2$. For these graphs, the bound in Theorem 6 is essentially an equality. The graphs X_{U_t} which are the Cayley graph $Cayley(G/U, U/U_t)$ defined in [23] have similar spectral characterization.

Example 3 (The $D(m, q)$ Graphs) The graphs were defined by [21] as follows.

Fixed a finite field $\mathbb{F}_q$, the graph is a q-regular bipartite graphs $D(q)$ with left vertices $X = \{x = [x, x_1, x_2, ...] : x, x_i \in \mathbb{F}_q$ for $i \geq 1\}$ and right vertex set $Y = \{y = [y, y_1, y_2, ...] : y, y_i \in \mathbb{F}_q$ for $i \geq 1\}$; a vertex $\mathbf{x}$ in X and a vertex $\mathbf{y}$ in Y are adjacent if their coordinates satisfy the following relations:

$$y_1 = xy + x_1, \ y_2 = xy_1 + x_2, \ y_3 = yx_1 + x_3, \ y_4 = yx_2 + x_4,$$

and for $i \geq 1$, $y_{4i+1} = xy_{4i-1} + x_{4i+1}, \ y_{4i+2} = xy_{4i} + x_{4i+2}, \ y_{4i+3} = yx_{4i+1} + x_{4i+3}, \ y_{4i+4} = yx_{4i+2} + x_{4i+4}$

By deleting all except the first m coordinates of the vertices, one obtains a truncation graph $D(m, q)$, which is q-regular bipartite of size $2q^m$. Each $D(m + 1, q)$ is a q-fold unramified

cover of $D(m, q)$. So they form an infinite tower of covering graphs. It was shown in [21] that for ≥ 3, the girth of $D(m, q)$ is large, at least $m + 5$.

Lemma 1 [36] *The eigenvalues of D(m, q) are $\pm q$ of multiplicity one, zero of multiplicity $2q - 2$, and $\pm\sqrt{q}$ of multiplicity $q^2 - q$. Consequently, they are optimal Ramanujan graphs.*

These graphs also show why the bound in Theorem 6 is stronger than the one in Corollary 1.

Example 4 (Graphs from generalized 4-gons) The 4-gons give $(s + 1, r + 1)$-regular graphs on $[n, m]$ vertices, with eigenvalues $\pm\sqrt{(s + 1)(r + 1)}$, $\pm\sqrt{s + r}$, and 0, with $n = sr^2 + sr + r + 1 = (r + 1)(sr + 1)$.

Since $(s + 1)n = (r + 1)m$, we conclude that $m = (s + 1)/r + 1)n = (s + 1)(sr + 1)$. They are known to exist for $(s, r) = (q, q), (q, q^2), (q^2, q^3), (q - 1, q + 1)$ and $q \neq 2$.

Example 5 (BIBD Graphs) In the next section we show that BIBD graphs yield optimal Ramanujan graphs.

Example 6 (Graphs of Gunnells from Grassmanians) One can consider generalizations of the BIBD graphs from finite geometries to construct bipartite graphs $B(k, n)$ by taking points as k-spaces and blocks as $n - k$ spaces and incidence is by containment. Or one can consider bipartite graphs where the incidence is defined when the intersection is a fixed s-dimensional subspace. In some cases, the eigenvalues and their multiplicities have been obtained by [10], and these yield optimal eigenvalue expander graphs. In the case where $k = 1$ we are back in the BIBD case.

3 Bipartite graphs from balanced incomplete block designs

Unless otherwise specified, for background on block designs, we follow Hall [12].

Definition 4 A *balanced incomplete block design* (BIBD) $\mathcal{D}$ with parameters (v, b, r, k, λ) is an incidence structure with a set $\mathcal{V}$ of v distinct varieties (or objects) denoted $a_1, \ldots, a_v$ and a set $\mathcal{B}$ of b distinct blocks denoted $B_1, \ldots, B_b$, such that each of the b blocks is incident with k varieties, and each of the v varieties is incident with r blocks, and every pair of varieties is incident with precisely λ blocks. The design is called *symmetric* if $b = v$ and its parameters are denoted by (v, k, r).

Proposition 2 *For a (BIBD) $\mathcal{D}$ with parameters (v, b, r, k, λ),*

1. $b \cdot k = v \cdot r$
2. $r(k - 1) = \lambda(v - 1)$

Remark 1 For a BIBD, Fisher's inequality implies that $b \geq v$ and hence $r \geq k$ and for symmetric designs $b = v$, and $r = k$. Furthermore, in any (v, k, r) symmetric block design, every pair of blocks is incident with precisely λ varieties, and if v is even then $k - \lambda$ is a square.

Definition 5 A BIBD can be described by a $v \times b$ *incidence matrix* $H := (h_{ij})$, where for $1 \leq i \leq v$ and $1 \leq j \leq b$, $h_{ij} = 1$ if a_i is incident with B_j, and $h_{ij} := 0$ else.

Then $\mathcal{D}$ is a block design if and only if the following system of equations hold.

$$B := HH^T = (r - \lambda)I + \lambda J_v \qquad (1^v)^T H = k1^b \qquad (1)$$

where J_v is the $v \times v$ all 1's matrix, and 1^v and 1^b are all 1's vectors of appropriate lengths.

3.1 The bipartite graph of a BIBD

Definition 6 Let $\mathcal{D}$ be a BIBD. The bipartite graph $\mathcal{X}_\mathcal{D}$ has left set of vertices $\mathcal{V}$ and right set of vertices $\mathcal{B}$ and the adjacency of the left and right vertices is defined by the incidence structure of the design.

It is clear that the left vertices of $\mathcal{X}_\mathcal{D}$ all have degree r and the right vertices all have degree k so the graph is what is called (r, k)-*regular*. In the symmetric case all vertices have degree r so the graph is r-*regular*.

The adjacency matrix of the bipartite graph $\mathcal{X}_\mathcal{D}$ is then,

$$A = \begin{bmatrix} \mathbf{0} & H \\ H^T & \mathbf{0} \end{bmatrix} \tag{2}$$

We cite from [13]

Theorem 7 *The adjacency matrix of the A of the bipartite graph $\mathcal{X}_\mathcal{D}$ of a (v, b, r, k, λ) BIBD has characteristic polynomial $P_A(x) = (x - \sqrt{k \cdot r})(x + \sqrt{k \cdot r})(x - \sqrt{r - \lambda})^{v-1} (x + \sqrt{r - \lambda})^{v-1} x^{b-v}$, and minimal polynomial $m_A(x) = (x - \sqrt{k \cdot r})(x + \sqrt{k \cdot r}) (x - \sqrt{r - \lambda})(x + \sqrt{r - \lambda})x$. In particular, the eigenvalues are $\sqrt{k \cdot r}$ with multiplicity 1, $\sqrt{r - \lambda}$ with multiplicity $v - 1$, 0 with multiplicity $b - v$, $-\sqrt{r - \lambda}$ with multiplicity $v - 1$, and $-\sqrt{k \cdot r}$ with multiplicity 1.*

and

Theorem 8   (I) *The bipartite graph $\mathcal{X}_\mathcal{D}$ of a (v, b, r, k, λ) BIBD is an (r, k)-regular bipartite Ramanujan graph with $\mu_1 = \sqrt{r - \lambda}$.*
(II) *The r-regular graph of a symmetric BIBD is an r-regular bipartite Ramanujan graph with $\mu_1 = \sqrt{r - \lambda}$.*

It is also clear that for these graphs the bound in Theorem 6 is satisfied with equality.

We will next show that the eigenvalues in some sense characterize the graphs coming from BIBD's.

Theorem 9 *Given numbers (b, v, r, k, λ) where b and v are positive integers with $b \geq v$ that satisfy*

$$bk = vr \quad and \quad \lambda(v - 1) = r(k - 1)$$

and a bipartite graph $\mathcal{X}$ on $v + b$ vertices where the adjacency matrix A has eigenvalues

. $\pm\sqrt{kr}$ *with multiplicity* 1.
.. $\pm\sqrt{k - \lambda}$ *with multiplicity* $v - 1$
... 0 *with multiplicity* $b - v$

then r, k, λ are integers and the graph comes from a (b, v, r, k, λ) block design.

Proof Since $2|E| = Trace(A^2)$ we get $|E| = kr + (v-1)(r-\lambda) = kr + r(v-1) - \lambda(v-1) = kr + rv - r - r(k - 1) = rv$. It now follows from Theorem 4 that $\mathcal{X}$ is a (r, k)-regular graph and in particular the numbers r and k are integers.

Let $X = [\sqrt{r}, \sqrt{r}, \ldots, \sqrt{r}, \sqrt{k}, \sqrt{k}, \ldots, \sqrt{k}]$, where the multiplicity of $\sqrt{r}$ is v, and $\sqrt{k}$ is b.

Then we can verify that $AX = \sqrt{r \cdot k}X$.

Therefore,

$$A^T A X = \sqrt{r \cdot k} A X = (rk) X \tag{3}$$

Let $B = HH^T$, where H is the left-right incidence matrix of the bipartite graph, and let $Q = H^T H$.

Hence, from the definition of H, we can confirm that $BY = r \cdot kY$, where $Y = [\sqrt{r}, \sqrt{r}, \ldots, \sqrt{r}]^T$. Consequently $Z = [1, 1, \ldots, 1]^T$ is an eigenvector corresponding to the eigenvalue $r \cdot k$.

Then by ([9], p. 186), B has eigenvalues $\alpha = r \cdot k$ with multiplicity 1, $r - \lambda$ with multiplicity $(v - 1)$.

Therefore, the minimal polynomial of B is $m_B(x) = (x - rk)q(x)$, where $q(x) = (x - (r - \lambda))$. (Since B is real symmetric, it is diagonalizable by an orthonormal basis, and therefore its minimal polynomial is composed of distinct factors).

Substituting B for X, we have $Bq(B) = r \cdot kq(B)$. Since rk is a simple eigenvalue of B with eigenvector Z, $q(B)$ has columns that are multiples of Z. However $q(B)$ is symmetric, as B is symmetric, we conclude that all the column multiples are the same scalar c, i.e.

$$q(B) = cJ,$$

where J is the $v \times v$ matrix of all 1's.

Hence $B - (\sqrt{r - \lambda})^2 I_v = B - (r - \lambda)I_v = c \cdot J$. Hence, $B = (r - \lambda)I_v + c \cdot J_v$.

By taking Trace both sides, and since $Trace(B) = Trace(HH^T) = rv$, we conclude that $c = \lambda$. Hence

$$B = HH^T = (r - \lambda)I + \lambda J,$$

and $1^v H = k.1^b$ since the graph is a bipartite graph. From the equation, one can also deduce that λ is also an integer, which is the number of times a pair of vertices are incident with the same vertex on the right. Therefore, H is the incidence matrix of a (v, b, r, k, λ) BIBD. □

4 Ramanujan graphs from BIBD's of finite geometries and other constructions

Several authors (See [20] and scores of citations) have constructed high performance LDPC codes from graphs from the Tanner graphs of incidence matrices of some configurations in the projective geometries $PG(n, q)$ and and affine geometries $AG(n, q)$.

The point as varieties and s spaces as blocks yield BIBD's whose parameters are determined, for example, in Hall [12]. Therefore, those graphs would yield optimal eigenvalue expanding graphs, and their second eigenvalue meets the bound in Theorem 6 and thus they are optimal. Thus we give a theoretical explanation of why those graphs yield high performance LDPC codes.

As mentioned before, generalizations of these graphs to construct bipartite graphs $B(k, n)$ has been considered by Gunnells [10] by taking points as k-spaces and blocks as $n - k$ spaces and incidence is by containment. Or one can consider bipartite graphs where the incidence is defined when the intersection is a fixed s-dimensional subspace. In some cases, the eigenvalues and their multiplicities have been obtained and those also lead to optimal eigenvalue expander graphs.

5 Combinatorial bounds on the expansion coefficient

In [32] Tanner proved for a (c, d)-regular bipartite graph the following

Theorem 10

$$c(\alpha) \geq \frac{c^2}{\alpha cd + \mu_1{}^2(1 - \alpha)} \tag{4}$$

with μ_1 as before.

In the case where $c = d$ we can use the following result from [1] to get another bound.

Proposition 3 (Alon and Chung) *Let* $G = (V, E)$ *be a d-regular graph on n vertices. Let* $S \subset V$ *with* $|S| = \gamma n$ *for some real number* γ, $0 < \gamma < 1$. *Then*

$$|e(S) - \frac{1}{2}d\gamma^2 n| \leq \frac{1}{2}\mu(1 - \gamma)\gamma n$$

Here $e(S)$ denotes the number of edges contained in the induced subgraph of G on the vertex set S.

Let $G = (V, E)$ be a d-regular bipartite connected graph on n vertices with $V = V_1 \cup V_2$ where $|V_1| = |V_2| = \frac{n}{2} = N$. let $S_1 \subseteq V_1$ with $|S_1| = \alpha N$, $T = \partial S_1$ and $S = S_1 \cup T$. With $|T| = t$ we have $|S| = \alpha N + t$ so $|S| = \gamma 2N$ where $\gamma = \frac{\alpha N + t}{2N}$ and $e(S) = e(S_1, T)$ and therefore $|e(S)| = \alpha Nd$.

The proposition above now gives

$$\alpha Nd - dN\frac{(\alpha N + t)^2}{4N^2} \leq \frac{\mu_1}{4N}(2N - (\alpha N + t))(\alpha N + t)$$

and hence

$$0 \leq (d - \mu_1)(\alpha N + t)^2 + \mu_1(\alpha N + t)2N - 4\alpha N^2 d$$

and therefore

$$\alpha N + t \geq \frac{-2N\mu_1 + \sqrt{4N^2\mu_1{}^2 + 16N^2\alpha d(d - \mu_1)}}{2(d - \mu_1)}$$

so

$$c(\alpha) \geq \frac{t}{\alpha N} \geq \frac{-\mu_1 + \sqrt{\mu_1{}^2 + 4\alpha d(d - \mu_1)}}{(d - \mu_1)\alpha} - 1 \tag{5}$$

We can get yet another lower bound by using a proposition from [17]

Proposition 4 (Janwa and Lal) *Let* G *be a* (c, d)-*regular graph with vertex set* $V_1 \cup V_2$ *with* $|V_1| = m$ *and* $|V_2| = n$. *For* $S \subset V_1$ *and* $T \subset V_2$ *let* $e(S, T)$ *denote the number of edges from the set S to the set T. Then*

$$|e(S, T) - \frac{d|S||T|}{m}| \leq \frac{\mu_1}{2}\left(|S| + |T| - \frac{|S|^2}{m} - \frac{|T|^2}{n}\right)$$

We will use this lemma in the situation where $S \subset V_1$ and $T = \partial S$ with $|S| = \alpha m$, $|T| = t$ so we know that $e(S, T) = |S|c$.

We get

$$\alpha mc - \frac{d\alpha mt}{m} \leq \frac{\mu_1}{2}\left(\alpha m + t - \frac{\alpha^2 m^2}{m} - \frac{t^2}{n}\right)$$

which gives

$$t \geq \frac{\mu_1 n + 2dn\alpha - \sqrt{(\mu_1 n + 2dn\alpha)^2 + 4\mu_1(\mu_1\alpha mn - \mu_1\alpha^2 mn - 2\alpha mnc)}}{2\mu_1}$$

and therefore

$$c(\alpha) \geq \frac{\mu_1 n + 2dn\alpha - \sqrt{(\mu_1 n + 2dn\alpha)^2 + 4\mu_1(\mu_1\alpha mn - \mu_1\alpha^2 mn - 2\alpha mnc)}}{2\mu_1\alpha m} \tag{6}$$

using $mc = nd$ and some manipulation this gives

Proposition 5

$$c(\alpha) \geq \frac{\mu_1 c + 2cd\alpha - \sqrt{(\mu_1 c + 2cd\alpha)^2 + 4\mu_1 dc(\mu_1(\alpha - \alpha^2) - 2c\alpha)}}{2d\alpha\mu_1}$$

To get a more transparent bound we use that

$$A - A\sqrt{1 - x} \geq A - A\left(1 - \frac{x}{2}\right)$$

for $0 \leq x \leq 1$ to get:

$$c(\alpha) \geq \frac{2\mu_1 \frac{2\alpha c^2 d + \mu_1\alpha^2 cd - \mu\alpha cd}{\mu_1 c + 2cd\alpha}}{2\mu_1\alpha d}$$

and therefore

Theorem 11

$$c(\alpha) \geq \frac{2c - \mu_1(1 - \alpha)}{\mu_1 + 2d\alpha}$$

6 Comparison of the three bounds on the expansion coefficients

The bound in (5) is only valid in the case where the graph is regular (i.e. $c = d$) and in this case it can be shown to be inferior to the bounds of Theorem 10 and Theorem 11. We will compare those last two. We first note that the bound of Theorem 11 only gives something interesting in the case where $2c - \mu_1(1 - \alpha) \geq 0$. Also if equality holds in either Theorem 6 or the corollaries it is true that $\mu_1 \leq 2c$. However it is easy to prove

Lemma 2

$$\frac{c^2}{\alpha cd + \mu_1^2(1 - \alpha)} \geq \frac{2c - \mu_1(1 - \alpha)}{\mu_1 + 2d\alpha}$$

Proof The above inequality is the same as

$$c^2\mu_1 + 2c^2 d\alpha \geq (2c - \mu_1(1 - \alpha))(cd\alpha + \mu_1^2(1 - \alpha))$$

which is the same as

$$0 \geq -(\mu_1(1 - \alpha) - c)^2 - \alpha(1 - \alpha)cd$$

$\square$

Since the approximation we used in deriving Theorem 11 is very crude for $x \geq \frac{1}{2}$ one could hope that the bound in Proposition 5 would improve on Theorem 10, but we have

Lemma 3

$$\frac{c^2}{\alpha cd + \mu_1{}^2(1-\alpha)} \geq \frac{\mu_1 c + 2cd\alpha - \sqrt{(\mu_1 c + 2cd\alpha)^2 + 4\mu_1 dc(\mu_1(\alpha - \alpha^2) - 2c\alpha)}}{2d\alpha\mu_1}$$

Proof This is easy to see if $\alpha = 0, 1$ and when $\alpha \neq 0, 1$ a straightforward but tedious calculation shows that the inequality is equivalent to:

$$\mu_1{}^4(1-\alpha)^2 - 2\mu_1{}^3 c(1-\alpha) + \mu_1{}^2(c^2 + 2cd\alpha(1-\alpha)) - \mu_1 2c^2 d\alpha + c^2 d^2 \alpha^2 \geq 0$$

The left side of this can be rewritten as

$$(\mu_1{}^2(1-\alpha) - \mu_1 c)^2 + cd\alpha[2\mu_1{}^2(1-\alpha) + cd\alpha - 2c\mu_1]$$

As a function of μ_1 it has a minimum for $\mu_1 = \frac{c}{2(1-\alpha)}$ if $c \leq 4d\alpha(1-\alpha)$ and if $c > 4d\alpha(1-\alpha)$ the minimum is obtained at $\mu_1 = \frac{c+\sqrt{c^2-4cd\alpha(1-\alpha)}}{2(1-\alpha)}$. In the first case the value of the function at the minimum is clearly positive if $c \leq 2d\alpha(1-\alpha)$ and if $2d\alpha(1-\alpha) < c < 4d\alpha(1-\alpha)$ the same can be seen to hold by inserting $c = Ad\alpha(1-\alpha)$ with $2 < A < 4$. In the second case we put $c = Ad\alpha(1-\alpha)$ with $A \geq 4$ and $x = \sqrt{1 - \frac{4}{A}}$ and then the minimum is obtained when $\mu_1 = \frac{Ad\alpha(1+x)}{2}$ and the minimum value is

$$A^2(1-\alpha)^2\alpha^4 d^4 \left[A^2(1+x)^2 \left(\frac{1+x}{4} - \frac{1}{2} \right)^2 + A \left(\frac{(1+x)^2}{2} \right) + 1 - A(1+x) \right]$$

The discriminant of the second degree polynomial is $-\frac{3x^2}{4}$ so the minimum value is positive. $\square$

The lesson learnt here is that in order to get a bound that improves on Theorem 10 one needs a better estimation of $e(S, T)$ in Proposition 5. The two theorems do give results that are quite close for a range of parameters. Theorem 11 has one advantage in its derivation and expression. The techniques we used are bound to lead to further improvements. For example, for the bipartite graph of edge-vertex graphs, the following improvement of Theorem 10 has been obtained in [16].

Theorem 12 *Let $G(V(G), E(G))$ be a d-regular graph on n vertices. Let H be the corresponding edge-vertex bipartite graph. Then*

$$c(\alpha) \geq \frac{4}{\mu + \sqrt{\mu^2 + 4\alpha(d-\mu)d}}$$

References

1. Alon N., Chung F.R.K.: Explicit construction of linear sized tolerant networks. Discret. Math. **72**, 15–19 (1988).
2. Arslan O.: The dimension of LU(3,q) codes. J. Comb. Theory A **116**(5), 1073–1079 (2009).
3. Barg A., Zemor G.: Error exponent of expander codes. IEEE Trans. Inform. Theory **48**(6), 1725—1729 (2002).
4. Chung F.G.: Spectral Graph Theory. (Revised and Improved Edition). http://www.math.ucsd.edu-fan.
5. Cvetkovic D.M., Doob M., Sachs H.: Spectra of Graphs: Theory and Applications. Academic Press (1979).
6. Cvetkovic D., Rowlinson P., Simic S.: An introduction to the theory of graph spectra. Cambridge University Press (2010).
7. Davidoff G., Sarnak P., Valette A.: Elementary Number Teory, Group Theory, and Ramanujan Graphs. London Mathematical Society Student Texts 55 (2003).
8. Forney G.D.: Codes on graphs: recent progress. Phys. A **302**(104), 1–13 (2001).
9. Godsil C.D.: Algebraic Combinatorics. Chapman and Hall (1993).
10. Gunnells P.E.: Some elementary Ramanujan graphs. Geometriae Dedicata **112**, 51–63 (2005).
11. Guruswami V., Indyk P.: Expander-based construction of efficiently decodable codes. 42nd IEEE Symposium on Foundation of Computer Science, October 14–17, 658 (2001).
12. Hall M. Jr.: Combinatorial Theory, 2nd edn. Wiley Interscience in discrete Mathematics.
13. Høholdt T., Janwa H.: Optimal bipartite Ramanujan graphs from balanced incomplete block designs: their characterizations and applications to expander/LDPC codes. In: Bras-Amoros M., Høholdt T. (eds.) Proceedings of AAECC-18. Springer Lecture Notes in Computer Science, vol. 5527, pp. 53–64 (2009).
14. Horn Roger A., Johnson, C.R.: Matrix Analysis. Cambridge University Press, (1992).
15. Hoory S., Linial N., Wigderson A.: Expander graphs and their applications. Bull. Am. Math. Soc. (N.S.), 43(4), 439–561 (2006).
16. Janwa H., Lal A.K.: On Expander Graphs: Parameters and Applications. submitted, January 2001. (see arXiv:cs.IT/04060-48v1).
17. Janwa H., Lal A.K.: On tanner codes: parameters and decoding. Appl. Algebra Eng. Commun. Comput. **13**, 335–347 (2003).
18. Janwa H., Moreno O.: Strongly Ramanujan graphs from codes, polyphase-sequences, and Combinatorics. Proceedings of the International Symposium on Information Theory, 1997 (ISIT-97) Ulm, Germany, pp. 408–408 (1997).
19. Kim J.L., Peled U.N., Perepelitsa I., Pless V., Friedl S.: Explicit construction of families of LDPC codes with no 4-cycles. IEEE Trans. Inform. Theory **50**, 2378–2388 (2004).
20. Kou Y., Lin S., Fossorier M.P.C.: Low-density parity-check codes based on finite geometries: a rediscovery and new results. IEEE Trans. Inform. Theory **47**(7), 2711–2736 (2001).
21. Lazebnik F., Ustimenko V.A.: Explicit construction of graphs with arbitrary large girth and of largh size. Discret. Appl. Math. **60**, 275–284 (1997).
22. Li W.W.: Character sums and abelian Ramanujan graphs. J. Number Theory **41**, 199–217 (1992).
23. Li W.W., Meemark Y.: Ramanujan graphs on cosets of $PGL_2(\mathbf{F}_q)$. Finite Fields Their Appl. **11**(3), pp. 511–543
24. MacWilliams F.J., Sloane N.J.A.: The theory of error-correcting codes. North Holland (1998).
25. Niho Y.: Multi-valued cross-correlation functions between two maximal linear recursive sequences. Ph.D. dissetrtation, Unvi. Southern California, Los Angeles, CA (1972).
26. Payne S.E., Thas J.A.: Finite Generalized Quadrangles, 2nd edn. European Mathematical Society, April 15 (2009).
27. Rosenthal J., Vontobel P.O.: Construction of LDPC codes using ramanujan graphs and ideas from margulis. Allerton Conference (2000).
28. Sarnak P.: What is...an Expander. Notices AMS **51**(7), 762—763 (2004).
29. Sin P., Xiang Q.: On the dimensions of certain LDPC codes based on q-regular bipartite graphs. IEEE Trans. Inform. Theory **52**, 3735–3737 (2006).
30. Sipser M., Spielman D.A.: Expander codes. Codes and complexity. IEEE Trans. Inform. Theory **42**(6), part 1, 1710–1722 (1996).
31. Spielman D.A.: Linear-time encodable and decodable error-correcting codes. IEEE Trans. Inform. Theory **42**(6), 1710–1722 (1996).
32. Tanner R.M.: Explicit concentrators from generalized N-gons. SIAM J. Discret. Appl. Math. **5**, 287–329 (1984).
33. Terras A.: Home page of Audrey Terras. http://math.ucsd.edu/~aterras.

34. Tanner R.M.: Minimum-distance bounds by graph analysis. IEEE Trans. Inform. Theory **47**(2), 808–821 (2001).
35. Vanderndriessche P.: Some low-density parity-check codes derived from finite geometries. Des. Codes Cryptogr. **54**(3), 287–297 (2010).
36. Wang C.: Analysis of finite-length low-density parity-check codes. Thesis, Pen State University, USA (2010).
37. Zemor G.: On expander codes. IEEE Trans. Inform. Theory. **IT-47**(2), 835–837 (2001).