COMBINATORICA 7 (4) (1987) 343—355

# EXPANDERS OBTAINED FROM AFFINE TRANSFORMATIONS

S. JIMBO and A. MARUOKA

*Received 1 August 1985*
*Revised 22 June 1986*

A bipartite graph $G=(U, V, E)$ is an $(n, k, \delta, \alpha)$ expander if $|U|=|V|=n$, $|E|\leqq kn$, and for any $X\subseteq U$ with $|X|\leqq\alpha n$, $|\Gamma_G(X)|\geqq(1+\delta(1-|X|/n))|X|$, where $\Gamma_G(X)$ is the set of nodes in $V$ connected to nodes in $X$ with edges in $E$. We show, using relatively elementary analysis in linear algebra, that the problem of estimating the coefficient $\delta$ of a bipartite graph is reduced to that of estimating the second largest eigenvalue of a matrix related to the graph. In particular, we consider the case where the bipartite graphs are defined from affine transformations, and obtain some general results on estimating the eigenvalues of the matrix by using the discrete Fourier transform. These results are then used to estimate the expanding coefficients of bipartite graphs obtained from two-dimensional affine transformations and those obtained from one-dimensional ones.

## 1. Introduction

In the context of computational complexity, expanders have been studied as the basic building blocks in constructions of many types of graphs (or networks) such as superconcentrators, nonblocking networks and sorting networks. Because the optimal constructions of these graphs depend on constructions of expanders, obtaining good constructions of expanders becomes important. In this paper we adopt the following definitions of an expander: A bipartite graph $G=(U, V, E)$ is an $(n, k, \delta, \alpha)$ expander if $|U|=|V|=n$, $|E|\leqq kn$, and for any $X\subseteq U$ with $|X|\leqq\alpha n$, $|\Gamma_G(X)|\geqq(1+\delta(1-|X|/n))|X|$. Here $U$ and $V$ are disjoint sets of vertices, called the input set and output set, respectively, $E\subseteq U\times V$ is the set of edges, $\Gamma_G(X)$ denotes the set of outputs connected to inputs in $X$, and the notation $|\cdot|$ indicates cardinality. Explicit constructions of expanders are due to Margulis [10] and Gabber and Galil [6]. Margulis [10] gave an explicit construction of a family of $(n, 5, \delta, 1)$ expanders for $n=1^2, 2^2, 3^2, \ldots$ and proved that the constant $\delta$ is greater than zero. Slightly modifying Margulis's construction, Gabber and Galil [6] constructed families of $(n, 5, (2-\sqrt{3})/4, 1)$ expanders and $(n, 7, (2-\sqrt{3})/2, 1)$ expanders for $n=1^2, 2^2, 3^2, \ldots$. Alon and Milman [2] (using some result of Gabber and Galil) obtained a family of $(n, 13, 0.465, 1/2)$ expanders for $n=1^2, 2^2, 3^2, \ldots$. The proofs of

AMS subject classification (1980): 68 A 20.

expanding properties for these graphs are based on theorems from the theory of group representations or harmonic analysis. It would be satisfying to have an elementary proof of expansion.

In this paper, using relatively elementary analysis in linear algebra, we establish some general results to estimate the expanding coefficients of bipartite graphs whose edges are defined by a finite number of some affine transformations. Alon, Galil and Milman [3] obtained a result that gives a relation between the expanding coefficient $\delta$ of a bipartite graph and the second largest eigenvalue of a certain matrix related to the graph. In this paper a method for estimating the second largest eigenvalue of the matrix defined from affine transformations is developed. Combining these results we can obtain $(n, 9, 4/(\alpha+\sqrt{1+\alpha^2}), 1/2)$ expanders, where

$$\alpha = (2-5\sqrt{2}/8)/(2(1-5\sqrt{2}/8)) \approx 4.806,$$

from which, as Alon, Galil and Milman [3] show, we get superconcentrators with $122 \cdot 74n$ edgges. These are the best known explicit superconcentrators. These results should be compared with one, shown by Гassalygo [4] (improving [5], [11]) using a probabilistic argument, that superconcentrators with $36n+O(n)$ edges exist.

## 2. Relation between expanding coefficients and eigenvalues

Let $S$ denote $\{1, ..., n\}$. Let $\sigma_1, \sigma_2, ..., \sigma_q$ be permutations on $S$, and let $\xi$ (respectively, $\xi'$) be a bijection from $S$ onto $U$ (respectively, $V$). The bipartite graph $(U, V, E)$ obtained from $\{\sigma_1, ..., \sigma_q, I\}$ is defined as

$$E = \{(\xi(i), \xi'(j)) | \exists \sigma \in \{\sigma_1, ..., \sigma_q, I\},\ \sigma(i) = j\},$$

where $I$ is the identity map on $S$. The permutation matrix for $\sigma$, denoted by $M(\sigma)$, is the $n \times n$ matrix $[m_{ij}]$ such that $m_{ij} = \delta(\sigma(i), j)$, where $\delta$ is Kronecker's delta defined as

$$\delta(i, j) = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{otherwise.} \end{cases}$$

The transpose and the conjugate of a matrix $A$ are denoted by ${}^tA$ and $\bar{A}$, respectively, and the conjugate transpose of $A$ is denoted by $A^*$, that is $A^* = {}^t\bar{A}$. Let $\mathbf{0}$ and $\mathbf{1}$ denote column vectors of appropriate length with the elements 0 and 1, respectively. A square matrix $H$ is called Hermitian if $H^* = H$, and a square matrix $U$ is called unitary if $U^*U = E$, where $E$ denotes the identity matrix. Two square matrices $M$ and $M'$ are called similar if there exists a non-singular matrix $N$ such that $M = N^{-1}M'N$. Let $\mathbf{C}$ and $\mathbf{R}$ denote the set of complex numbers and the set of real numbers, respectively.

We give the next well known proposition without proof.

**Proposition 2.1.** (Rayleigh's principle). *Let $A$ be a Hermitian $n \times n$ matrix over* $\mathbf{C}$. *Let $\lambda_1$ and $\lambda_2$ be the first and second largest eigenvalues of $A$, respectively (among the $n$ eigenvalues with the proper multiplicities), and let $y$ be an eingenvector of $A$ with* *eigenvalue* $\lambda_1$. *Then*

$$\sup_{x\neq 0} \frac{x^*Ax}{x^*x} = \lambda_1,$$

$$\sup_{\substack{x\neq 0 \\ x^*y=0}} \frac{x^*Ax}{x^*x} = \lambda_2,$$

*where sup is over column vectors $x$ of length $n$ over* **C**. ▮

A doubly stochastic $n\times n$ matrix is a matrix $[a_{ij}]$ over **R** such that $a_{ij}\geqq 0$ and $\sum_k a_{ik}=\sum_k a_{kj}=1$ for $1\leqq i,j\leqq n$. We give the next well known proposition without proof.

**Proposition 2.2.** (i) *The product of two doubly stochastic matrices is a doubly stochastic matrix.*
(ii) *A doubly stochastic matrix has the eigenvector* **1** *with eigenvalue* 1.
(iii) *All eigenvalues of a doubly stochastic matrix have absolute value at most* 1. ▮

**Theorem 2.3.** (Alon, Galil and Milman [3]). *Let $\sigma_1, \sigma_2, \ldots, \sigma_q$ be permutations on $S$. Let $a_1, a_2, \ldots, a_q$ be positive real numbers with $\sum_i a_i=1$, and let $\lambda_2$ be the second largest eigenvalue (among the $n$ eigenvalues with proper multiplicities) of the Hermitian doubly stochastic $n\times n$ matrix $A$ defined as*

$$\sum_{i=1}^{q} \frac{1}{2} a_i(M(\sigma_i)+{}^tM(\sigma_i)).$$

*Then the bipartite graph obtained from $\{\sigma_1, \ldots, \sigma_q, \sigma_1^{-1}, \ldots, \sigma_q^{-1}, I\}$ is an $(n, 2q+1, 4/(\alpha+\sqrt{1+\alpha^2}), 1/2)$ expander, where $I$ denotes the identity map on $S$ and $\alpha=(2-\lambda_2)/(2(1-\lambda_2))$.*

By virtue of Theorem 2.3 the problem of estimating the expanding constant of a bipartite graph obtained from a finite number of permutations is reduced to the problem of estimating the second largest eigenvalue of the Hermitian doubly stochastic $n\times n$ matrix $A$ determined by the permutations. For the estimation of the second largest eigenvalue $\lambda_2$, we shall show that there exists a Hermitian $(n-1)\times(n-1)$ matrix whose largest eigenvalue is equal to $\lambda_2$.

**Proposition 2.4.** *Let $U=[u_{ij}]$ be a unitary $n\times n$ matrix such that $u_{1i}=u_{i1}=1/\sqrt{n}$ for $1\leqq i\leqq n$, and let $A$ be a Hermitian doubly stochastic $n\times n$ matrix. Then there exists a Hermitian $(n-1)\times(n-1)$ matrix $H$ such that* (i)

$$U^*AU=\left[\begin{array}{c|c} 1 & 0\ldots 0 \\ \hline 0 & \\ \vdots & H \\ 0 & \end{array}\right]$$

*and such that* (ii) *the second largest eigenvalue of $A$ (among the $n$ eigenvalues with the proper multiplicities) is equal to the largest eigenvalue of $H$.*

**Proof.** Since

$$(U^*AU)^* = U^*AU^{**} = U^*AU,$$

$U^*AU$, and hence $H$, is Hermitian. Let $A=[a_{ij}]$, $U=[u_{ij}]$ and $U^*AU=[b_{ij}]$. If $i=j=1$, then we have

$$b_{ij} = \sum_k \bar{u}_{k1}\Big(\sum_l a_{kl}u_{l1}\Big) = (1/n)\sum_k \sum_l a_{kl} = 1.$$

If $i=1$ and $j>1$, then we have

$$b_{ij} = \sum_k \bar{u}_{k1}\Big(\sum_l a_{kl}u_{lj}\Big) = \frac{1}{\sqrt{n}}\sum_l u_{lj}\Big(\sum_k a_{kl}\Big) = \sum_l \bar{u}_{l1}u_{lj} = 0.$$

Thus $U^*AU$ takes the form indicated in the proposition. Since similar metrices have the same eigenvalues and, by (iii) of Proposition 2.2, the largest eigenvalue of $A$ is 1, part (ii) of the proposition follows. ▌

## 3. Expanders obtained from affine transformations

Let $p$ and $m$ be positive integers and let $\mathbf{Z}_m$ denote the ring of residues modulo $m$. $\mathbf{Z}_m$ consists of classes of the form $\{i+mx \mid x\in\mathbf{Z}\}$, $0\leqq i\leqq m-1$, which we denote simply by $i$. Let $U$ and $H$ be as in Proposition 2.4. We shall show that, if we take the permutations $\sigma_1, \ldots, \sigma_q$ to be those determined by some affine transformations on $\mathbf{Z}_m \times \ldots \times \mathbf{Z}_m$ ($p$ times) and $U$ to be the discrete Fourier transform (DFT), then we can obtain a nontrivial upper bound on the largest eigenvalue of $H$.

Let ${}^t\mathbf{Z}_m^p$ denote the set of column vectors of length $p$ with elements from $\mathbf{Z}_m$. For $x, y\in{}^t\mathbf{Z}_m^p$ we define $\langle x, y\rangle$ as $\langle x, y\rangle = x^*y - \sum_i x_iy_i$, where $x={}^t(x_1, \ldots, x_p)$, $y={}^t(y_1, \ldots, y_p)$. Let $n=m^p$ so that $S$ denotes $\{1, \ldots, m^p\}$. Let $\nu$ be a bijection from $S$ onto ${}^t\mathbf{Z}_m^p$ such that $\nu(1)=\mathbf{0}$. In what follows $\nu$ is fixed so as to give a correspondance between elements in $S$ and those in ${}^t\mathbf{Z}_m^p$. Let $\Omega$ denote the matrix $[\omega_{ij}]$ such that $\omega_{ij}=m^{-p/2}\omega^{\langle\nu(i),\nu(j)\rangle}$, where $\omega=\exp\big(2\pi\sqrt{-1}/m\big)$. The map $\mathscr{F}$ from $C^{{}^tz_m^p}$ to $C^{{}^tz_m^p}$, defined as $\mathscr{F}(x)=\Omega x$, is the discrete Fourier transform.

**Proposition 3.1.** *$\Omega$ is unitary and $\omega_{1i}=\omega_{i1}=1/m^{p/2}$ for $1\leqq i\leqq m^p$.*

**Proof.** For any $x\in{}^t\mathbf{Z}_m^p$, $\langle\mathbf{0}, x\rangle=\langle x, \mathbf{0}\rangle=0$. Therefore by the definition of $\Omega=[\omega_{ij}]$

$$\omega_{1i} = \omega_{i1} = (1/m^{p/2})\omega^0 = 1/m^{p/2}$$

for any $1\leqq i\leqq m^p$. Let $\Omega^*\Omega=[v_{ij}]$, $\nu(i)=x$ and $\nu(j)=y$. Then we obtain

$$v_{ij} = \frac{1}{m^p}\sum_{z\in{}^t\mathbf{Z}_m^p}\omega^{-\langle x,z\rangle}\omega^{\langle z,y\rangle} =$$

$$= \frac{1}{m^p}\sum_{z\in{}^t\mathbf{Z}_m^p}\omega^{\langle y-x,z\rangle} =$$

$$= \frac{1}{m^p}\sum_{z_1\in\mathbf{Z}_m}\cdots\sum_{z_p\in\mathbf{Z}_m}\omega^{(y_1-x_1)z_1}\ldots\omega^{(y_p-x_p)z_p} =$$

$$= \frac{1}{m^p}\prod_{l=1}^{p}\Big(\sum_{z_l\in\mathbf{Z}_m}\omega^{(y_l-x_l)z_l}\Big),$$

where $x={}^t(x_1, \dots, x_p)$, $y={}^t(y_1, \dots, y_p)$ and $z={}^t(z_1, \dots, z_p)$. If $y_l \neq x_l$, then $\omega^{(y_l-x_l)} \neq 1$, so

$$\sum_{z_l \in \mathbf{Z}_m} \omega^{(y_l-x_l)z_l} = \frac{\omega^{m(y_l-x_l)}-1}{\omega^{(y_l-x_l)}-1} = 0.$$

If $x_l=y_l$, then

$$\sum_{z_l \in \mathbf{Z}_m} \omega^{(y_l-x_l)z_l} = m.$$

Therefore we conclude that for $1 \leqq i,\ j \leqq m^p$

$$v_{ij} = \delta(i,j) \quad ∎$$

From propositions 2.4 and 3.1, we have the next proposition.

**Proposition 3.2.**

$$\Omega^* A \Omega = \left[\begin{array}{c|c} 1 & 0 \dots 0 \\ \hline 0 & \\ \vdots & H \\ 0 & \end{array}\right]$$

*where $H$ is a Hermitian $(n-1)\times(n-1)$ matrix.* ∎

Thus the problem is now reduced to that of estimating the largest eigenvalue of $H$ in Proposition 3.2. Let $\mathbf{Z}_m^{p\times p}$ denote the set of $p\times p$ matrices whose elements are chosen from $\mathbf{Z}_m$. We define the sets $P$, $Q$ of permutations on $S$ as follows.

$P=\{\sigma\colon S\to S|$ There exists $B\in\mathbf{Z}_m^{p\times p}$ such that $B$ has an inverse $B^{-1}$ in $\mathbf{Z}_m^{p\times p}$ and $\sigma(i)=\nu^{-1}B\nu(i)\}$.

$Q=\{\sigma\colon S\to S|$ There exists $a\in{}^t\mathbf{Z}_m^p$ such that $\sigma(i)=\nu^{-1}(\nu(i)+a)\}$, where $v^{-1}Bv(i)=\nu^{-1}(B(\nu(i)))$ for $i\in S$.Let $\sigma_B$ denote the permutation on $S$ defined as

$$\sigma_B(i) = \nu^{-1}B\nu(i),$$

where $B\in\mathbf{Z}_m^{p\times p}$. Similarly, let $\sigma_a$ denote the permutation on $S$ defined as

$$\sigma_a(i) = \nu^{-1}(\nu(i)+a),$$

where $a\in{}^t\mathbf{Z}_m^p$.

We shall be concerned with the bipartite graphs obtained from permutations that can be written as products of permutations in $P\cup Q$. Then, for the estimation of the largest eigenvalue of $H$ for such bipartite graphs, we need the next four propositions.

**Proposition 3.3.** *Let $B$ be a matrix in $\mathbf{Z}_m^{p\times p}$ that has the inverse $B^{-1}$ in $\mathbf{Z}_m^{p\times p}$. Then*

$$\Omega^* M(\sigma_B)\Omega = M(\sigma_{{}^tB^{-1}}).$$

**Proof.** The element in the $i$-th row and $j$-th column of matrix $\Omega^* M(\sigma_B)\Omega$ is expressed as

$$(3.1)\qquad \big(\Omega^* M(\sigma_B)\Omega\big)(i,j) =$$

$$= \frac{1}{m^p}\sum_k\sum_l \overline{\omega^{\langle v(i),\, v(k)\rangle}}\,\delta\big(v^{-1}Bv(k),\, l\big)\omega^{\langle v(l),\, v(j)\rangle} =$$

$$= \frac{1}{m^p}\sum_k \omega^{\langle Bv(k),\, v(j)\rangle - \langle v(i),\, v(k)\rangle},$$

where $\delta(\cdot,\ \cdot)$ is Kronecker's delta. On the other hand we have

$$(3.2)\qquad \langle Bv(k), v(j)\rangle = {}^t\big(Bv(k)\big)v(j) = {}^tv(k){}^tBv(j) = \langle v(k), {}^tBv(j)\rangle.$$

From (3.1) and (3.2) we have $\big(\Omega^* M(\sigma_B)\Omega\big)\ (i,j) = \frac{1}{m^p}\sum_k \omega^{\langle {}^tBv(j) - v(i),\, v(k)\rangle} = = \delta\big(v^{-1}{}^tB^{-1}v(i), j\big) = \delta\big(\sigma_{{}^tB^{-1}}(i), j\big) = M(\sigma_{{}^tB^{-1}})(i, j)$ as is shown in the proof of Proposition 3.1. ▮

**Proposition 3.4.** *Let $a \in {}^t\mathbf{Z}_m^p$. Then $\Omega^* M(\sigma_a)\Omega$ is the diagonal matrix whose i-th diagonal element is $\omega^{\langle a,\, v(i)\rangle}$.*

**Proof.** The element in the $i$-th row and $j$-th column of matrix $\Omega^* M(\sigma_a)\Omega$ is expressed as

$$\big(\Omega^* M(\sigma_a)\Omega\big)(i,j) = \frac{1}{m^p}\sum_k\sum_l \overline{\omega^{\langle v(i),\, v(k)\rangle}}\,\delta\big(v^{-1}(v(k)+a),\, l\big)\omega^{\langle v(l),\, v(j)\rangle} =$$

$$= \frac{1}{m^p}\sum_k \omega^{\langle v(k)+a,\, v(j)\rangle - \langle v(i),\, v(k)\rangle} =$$

$$= \omega^{\langle a,\, v(j)\rangle}\frac{1}{m^p}\sum_k \omega^{\langle v(k),\, v(j) - v(i)\rangle} = \omega^{\langle a,\, v(j)\rangle}\delta(i,j) = \omega^{\langle a,\, v(i)\rangle}\delta(i,j) \quad ▮$$

The principle of the next proposition is due to Gabber and Galil [6].

**Proposition 3.5.** *Let $A = [a_{ij}]$ be a symmetric $n \times n$ matrix over $\mathbf{R}$ such that if $i \neq j$ then $a_{ij} \geqq 0$, and let $\lambda$ be the largest eigenvalue of $A$. Let $\gamma_{ij}$, $1 \leqq i, j \leqq n$, be real numbers such that $\gamma_{ij} > 0$ and $\gamma_{ij} = 1/\gamma_{ji}$ for $1 \leqq i, j \leqq n$. Then*

$$\lambda \leqq \max_i \sum_j \gamma_{ij} a_{ij}.$$

**Proof.** Let $y = {}^t(y_1, \dots, y_n)$ be an arbitrary column vector in ${}^t\mathbf{C}^n$ such that $y^* y = 1$, where ${}^t\mathbf{C}^n$ denote the set of column vectors of length $n$ with elements from $\mathbf{C}$. Since for arbitrary $\lambda > 0$ and $a, b \in \mathbf{R}$,

$$\big(\sqrt{\lambda}a - b/\sqrt{\lambda}\big)^2 = \lambda a^2 + b^2/\lambda - 2ab \geqq 0,$$

and hence $2ab \leqq \lambda a^2 + b^2/\lambda$, we have

$$\begin{aligned} v^*Ay &= \sum_i \sum_j a_{ij}\bar{y}_i y_j = \\ &= \frac{1}{2}\sum_i \sum_j a_{ij}(\bar{y}_i y_j + y_i \bar{y}_j) \leqq \\ &\leqq \frac{1}{2}\sum_i \sum_j 2a_{ij}|y_i|\,|y_j| \leqq \\ &\leqq \frac{1}{2}\sum_i \sum_j a_{ij}(\gamma_{ij}|y_i|^2 + \gamma_{ji}|y_j|^2) = \\ &= \frac{1}{2}\sum_i \sum_j (a_{ij}\gamma_{ij}|y_i|^2 + a_{ji}\gamma_{ji}|y_j|^2) = \\ &= \sum_i \sum_j a_{ij}\gamma_{ij}|y_i|^2 = \\ &= \sum_i (\sum_j a_{ij}\gamma_{ij})|y_i|^2 \leqq \\ &\leqq (\max_i \sum_j a_{ij}\gamma_{ij})(\sum_i |y_i|^2) = \\ &= \max_i \sum_j \gamma_{ij}a_{ij}. \end{aligned}$$

Thus, by Proposition 2.1, we conclude that

$$\lambda = \sup_{\substack{x \in {}^t\mathbf{C}^n \\ x \neq 0}} \frac{x^*Ax}{x^*x} \leqq \max_i \sum_j \gamma_{ij}a_{ij}. \quad \blacksquare$$

**Proposition 3.6.** *Let $A = [a_{ij}]$ be a Hermitian $n \times n$ matrix over $\mathbf{C}$ and let $B = [b_{ij}]$ be a symmetric $n \times n$ matrix over $\mathbf{R}$. Let $\lambda_B$ be the maximal eigenvalue of $B$. If $|a_{ij}| \leqq b_{ij}$ for $1 \leqq i, j \leqq n$, then $|\lambda| \leqq \lambda_B$ for any eigenvalue $\lambda$ of $A$.*

**Proof.** Let $\lambda_1(\lambda_n)$ be the maximal (minimal) eigenvalue of $A$. Then it suffices to show that $|\lambda_1| \leqq \lambda_B$ and $|\lambda_n| \leqq \lambda_B$. Since $b_{ij} \geqq 0$ for $1 \leqq i, j \leqq n$ and $B = [b_{ij}]$ is a symmetric matrix over $\mathbf{R}$, we have by Proposition 2.1

$$\lambda_B = \sup_{\substack{x \in {}^t\mathbf{C}^n \\ x \neq 0}} \frac{x^*Bx}{x^*x} = \sup_{\substack{y_1, \ldots, y_n \geqq 0 \\ \Sigma y_i^2 = 1}} \sum_i \sum_j b_{ij}y_i y_j.$$

On the other hand, since $A$ is Hermitian, we have by Proposition 2.1

$$\lambda_1 = \sup_{\substack{x \in {}^t\mathbf{C}^n \\ x \neq 0}} \frac{x^*Ax}{x^*x} = \sup_{\substack{y_1, \ldots, y_n \in \mathbf{C} \\ \sum_i |y_i|^2 = 1}} \sum_i \sum_j a_{ij}\bar{y}_i y_j.$$

Moreover,

$$\lambda_n = -\sup_{\substack{x \in {}^t\mathbf{C}^n \\ x \neq 0}} \frac{x^*(-A)x}{x^*x} = -\sup_{\substack{y_1, \dots, y_n \in \mathbf{C} \\ \sum_i |y_i|^2 = 1}} \Big(-\sum_i \sum_j a_{ij}\bar{y}_i y_j\Big)$$

because the maximal eigenvalue of $-A$ is the minimal eigenvalue of $A$ multiplied by $-1$. Therefore,

$$|\lambda_1| = \Big|\sup_{\substack{y_1, \dots, y_n \in \mathbf{C} \\ \sum_i |y_i|^2 = 1}} \sum_i \sum_j a_{ij}\bar{y}_i y_j\Big| \leqq \sup_{\substack{y_1, \dots, y_n \in \mathbf{C} \\ \sum_i |y_i|^2 = 1}} \sum_i \sum_j |a_{ij}|\,|y_i|\,|y_j| \leqq$$

$$\leqq \sup_{\substack{y_1, \dots, y_n \geqq 0 \\ \sum_i y_i^2 = 1}} \sum_i \sum_j b_{ij} y_i y_j = \lambda_B,$$

and similarly $|\lambda_n| \leqq \lambda_B$. ▮

## 4. Two-dimensional affine transformations

Let $p=2$. The permutations $\tilde{\varrho}_1, \tilde{\varrho}_2, \tilde{\varphi}_1$ and $\tilde{\varphi}_2$ on ${}^tZ_m^2$ are defined as

$$\tilde{\varrho}_1({}^t(x_1, x_2)) = {}^t(x_1 + 2x_2, x_2),$$

$$\tilde{\varrho}_2({}^t(x_1, x_2)) = {}^t(x_1, x_2 + 2x_1),$$

$$\tilde{\varphi}_1({}^t(x_1, x_2)) = {}^t(x_1 + 1, x_2),$$

$$\tilde{\varphi}_2({}^t(x_1, x_2)) = {}^t(x_1, x_2 + 1).$$

The permutations $\varrho_i$ and $\varphi_i$, $1 \leqq i \leqq 2$, on $S$ are defined as

$$\varrho_i = \nu^{-1}\tilde{\varrho}_i \nu,$$

$$\varphi_i = \nu^{-1}\tilde{\varphi}_i \nu.$$

Then, from the definitions of $P$ and $Q$, $\varrho_1, \varrho_2 \in P$ and $\varphi_1, \varphi_2 \in Q$. For $x \in {}^t\mathbf{Z}_m^2$, we define $\|x\|$ as

$$\|x\| = \mathcal{R}e(\omega^{x_1} + \omega^{x_2}) = \mathcal{R}e(\omega^{x_1}) + \mathcal{R}e(\omega^{x_2}),$$

where ${}^tx = (x_1, x_2)$, $\omega = \exp(2\pi/\sqrt{-1}/m)$ and the notation $\mathcal{R}e(\cdot)$ indicates real part.

The proofs of the next two lemmas are straightforward examinations of cases. These proofs are given in Appendix.

**Lemma 4.1.** *For* $z \in {}^t\mathbf{Z}_m^2$ *with* $z \neq \mathbf{0}$, *let* $J = \{\tilde{\varrho}_1(z), \tilde{\varrho}_1^{-1}(z), \tilde{\varrho}_2(z), \tilde{\varrho}_2^{-1}(z)\}$, $s_d = |\{x \in J \mid \|x\| > \|z\|\}|$, *and* $s_u = |\{x \in J \mid \|x\| < \|z\|\}|$. *Then* $s_d \leqq 2$ or $s_u \geqq 1$.

**Lemma 4.2.** *Let* $z$, $s_d$ *and* $s_u$ *be as in Lemma* 4.1. *If* $\|z\| > 0$, *then* $s_d \leqq 1$ *and* $s_u - s_d \geqq 2$.

Using the results mentioned so far, we can obtain families of expanders. The set of permutations we use to construct the expanders are $\{\varrho_1, \varrho_2, \varphi_1\varrho_1, \varphi_2\varrho_2, I\}$.

**Theorem 4.3.** *Let* $\sigma_1=\varrho_1$, $\sigma_2=\varrho_2$, $\sigma_3=\varphi_1\varrho_1$, $\sigma_4=\varphi_2\varrho_2$. *And let*

$$A=\sum_{i=1}^{4}(1/8)\big(M(\sigma_i)+{}^{t}M(\sigma_i)\big)$$

*and* $\lambda$ *be the second largest eigenvalue of* $A$. *Then*

$$\lambda \leqq 5\sqrt{2}/8.$$

**Corollary.** (Alon, Galil and Milman [3]) *The bipartite graph obtained from* $\{\sigma_1, \ldots, \sigma_4, \sigma_1^{-1}, \ldots, \sigma_4^{-1}, I\}$ *is an* $(n, 9, 4/(\alpha+\sqrt{1+\alpha^2}), 1/2)$ *expander, where* $\alpha=(2-\sqrt{5}\,2/8)/(2(1-5\sqrt{2}/8))$.

**Proof of Corollary.** The Corollary follows from Theorem 2.3 and Theorem 4.3. ▮

**Proof of Theorem 4.3.** Let

$$\Omega^*A\Omega=\left[\begin{array}{c|c} 1 & 0\ldots0 \\ \hline 0 & \\ \vdots & H \\ 0 & \end{array}\right].$$

By Proposition 3.2, $H$ is a Hermitian $(n-1)\times(n-1)$ matrix. Let $H=[h_{ij}]$, $1\leqq j$, $j\leqq n-1$. Then, by Theorem 2.3 and Proposition 3.6, it suffices to show that there exists a symmetric $(n-1)\times(n-1)$ matrix $C=[c_{ij}]$ over $\mathbf{R}$ such that $c_{ij}\geqq|h_{ij}|$ for $1\leqq i$, $j\leqq n-1$ and such that the largest eigenvalue $\lambda_C$ of $C$ satisfies that

$$\lambda_C \leqq 5\sqrt{2}/8.$$

Since ${}^{t}M(\sigma)=M(\sigma^{-1})$ and $M(\sigma)M(\sigma')=M(\sigma'\sigma)$ for any permutations $\sigma$ and $\sigma'$ on $S$, $A$ can be written as

$$A=\frac{1}{8}\{(E+M(\varphi_1))M(\varrho_1)+(E+M(\varphi_1^{-1}))M(\varrho_1^{-1})+$$
$$+(E+M(\varphi_2))M(\varrho_2)+(E+M(\varphi_2^{-1}))M(\varrho_2^{-1}),$$

where $E$ denotes the identity matrix. Recall that $v$ gives the correspondence between elements in $S$ and those in ${}^{t}\mathbf{Z}_m^2$. We define the bijection $v_C$ from $S\setminus\{n\}$ to ${}^{t}Z_m^2\setminus\{0\}$ by $v_C(i)=v(i+1)$ for $1\leqq i\leqq n-1$. Let $C=[c_{ij}]$ denote the symmetric $(n-1)\times\times(n-1)$ matrix over $\mathbf{R}$ such that for $1\leqq i, j\leqq n-1$

$$c_{ij}=\frac{1}{8}\{|1+\omega^{i_1}|\big(\delta(\varrho_2(i), j)+\delta(\varrho_2^{-1}(i), j)\big)+$$
$$+|1+\omega^{i_2}|\big(\delta(\varrho_1(i), j)+\delta(\varrho_1^{-1}(i), j)\big)\},$$

where $\omega=\exp\big(2\pi\sqrt{-1}/m\big)$ and ${}^{t}v_C(i)=(i_1, i_2)\in\mathbf{Z}_m^2$. Let $D_1$ and $D_2$ denote the $2\times 2$ matrices over $\mathbf{Z}_m$ that define $\varrho_1$ and $\varrho_2$, respectively; $v\varrho_1 v^{-1}(x)=D_1x$ and

$\nu Q_2 \nu^{-1}(x) = D_2 x$ for $x \in {}^t\mathbf{Z}_2^m$. Since

$$D_1 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad D_2 = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$$

so that ${}^tD_1 = D_2$, it follows from Propositions 3.3 and 3.4 that for $1 \leqq i, j \leqq n-1$ $c_{ij} \geqq |h_{ij}|$. For $1 \leqq i, j \leqq n-1$ we define $\gamma_{ij}$ as

$$\begin{aligned} \gamma_{ij} &= 1/\sqrt{2} && \text{if} \quad \|v_C(i)\| > \|v_C(j)\|, \\ \gamma_{ij} &= 1 && \text{if} \quad \|xv_C(i)\| = \|v_C(j)\|, \\ \gamma_{ij} &= \sqrt{2} && \text{if} \quad \|v_C(i)\| < \|v_C(j)\|. \end{aligned}$$

Put

$$\alpha = \max\{|1+\omega^{i_1}|/2,\ |1+\omega^{i_2}|/2\}$$

$$\beta = \min\{|1+\omega^{i_1}|/2,\ |1+\omega^{i_2}|/2\}.$$

Then clearly $0 \leqq \beta \leqq \alpha \leqq 1$. Let $i$ be an arbitrary index in $\{1, \ldots, m-1\}$. From Lemma 4.2, if $\|v_C(i)\| > 0$, then we have

$$\sum_j \gamma_{ij} c_{ij} \leqq \frac{1}{4}\left(\sqrt{2} + \frac{3}{\sqrt{2}}\right) = 5\sqrt{2}/8.$$

Assume that $\|v_C(i)\| \leqq 0$. From the definition of $c_{ij}$ and Lemma 4.1 we have

$$\text{(4.1)} \qquad \sum_j \gamma_{ij} c_{ij} \leqq \frac{1}{4} \max\left\{2\sqrt{2}\alpha + 2\beta,\ \sqrt{2}(2\alpha+\beta) + \frac{\beta}{\sqrt{2}}\right\} = \frac{1}{4\sqrt{2}}(4\alpha + 3\beta).$$

Let $u, s, t \in \mathbf{R}$ be such that

$$\omega^{i_1} = u + s\sqrt{-1},$$

$$\omega^{i_2} = v + t\sqrt{-1}.$$

Then by the assumption we have

$$\text{(4.2)} \qquad \alpha^2 + \beta^2 = \frac{1}{4}(|1+\omega^{i_1}|^2 + |1+\omega^{i_2}|^2) =$$

$$= \frac{1}{4}(u^2 + s^2 + v^2 + t^2 + 2(u+v) + 2) = 1 + \frac{1}{2}\|v_C(i)\| \leqq 1.$$

Hence by the Canchy—Schwarz inequality

$$\text{(4.3)} \qquad 4\alpha + 3\beta \leqq \sqrt{4^2+3^2} \cdot \sqrt{\alpha^2+\beta^2} \leqq 5.$$

By (4.1) and (4.3) we obtain

$$\sum_j \gamma_{ij} c_{ij} \leqq 5\sqrt{2}/8.$$

Thus from Proposition 3.5 we conclude

$$\lambda_C \leqq 5\sqrt{2}/8. \quad \blacksquare$$

As shown in Alon, Galil and Milman [3], we can obtain a family of superconcentrators with density about 122.74, the smallest density explicitly known, using the expanders in Theorem 4.3.

To mention another result, we define the expanding coefficient $\delta_\alpha(G)$ of a bipartite graph $G$ with $n$ inputs and $n$ outputs as

$$\delta_\alpha(G) = \sup \{\delta\in\mathbf{R} | \forall X \subseteqq U \text{ with } |X| \leqq \alpha n, |\Gamma_G(X)| \geqq (1+\delta-|X|/n)|X|\}.$$

where $\alpha\in\mathbf{R}$ is a constant such that $0<\alpha\leqq 1$. Klawe [8], [9] conjectured that $\delta_1(G_n)$ is bounded below by $\Omega(1/\log n)$ for a family of bipartite graphs $G_n$ defined by some one-dimensional affine transformations on the set $\mathbf{Z}_m$. By employing our methods we can construct a family of bipartite graph $G_n$ obtained by one-dimensional affine transformations with $\delta_1(G_n)=\Omega(1/(\log \mathrm{n})^2)$. One of the referees noticed us that Maass [12] established a stronger results by short combinatorial arguments: There exists a family of bipartite graphs $G_n$ obtained by one-dimensional affine transformations with $\delta_1(G_n)=\Omega(1/\log n)$; Maass's proof can be easily modified to give this estimate even to our graphs above.

**Acknowledgments.** We wish to thank the referees for providing a list of comments which improved the presentation of the paper and simplified the proofs of Lemma 5.1 and 5.2.

## 5. Appendix

**Proof of Lemma 4.1.** Let $z={}^t(z_1, z_2)\in{}^t\mathbf{Z}_m^2$, then

$$\tilde{\varrho}_1(z) = (z_1+2z_2, z_2),$$
$$\tilde{\varrho}_1^{-1}(z) = (z_1-2z_2, z_2),$$
$$\tilde{\varrho}_2(z) = (z_1, z_2+2z_1) \quad \text{and}$$
$$\tilde{\varrho}_2^{-1}(z) = (z_1, z_2-2z_1).$$

Let $\omega^{z_1}=u+s\sqrt{-1}$, $\omega^{z_2}=v+t\sqrt{-1}$, where $u$, $v$, $s$ and $t$ are real real numbers. Note that $u^2+s^2=1$ and $v^2+t^2=1$ because $\omega=\exp(2\pi\sqrt{-1}/m)$, and therefore

$$\omega^{-z_1} = 1/(u+s\sqrt{-1}) = u-s\sqrt{-1},$$
$$\omega^{-z_2} = 1/(v+t\sqrt{-1}) = v-t\sqrt{-1}.$$

By the definition of $\|\cdot\|$, we have

$$\text{(A.1)} \qquad \|\tilde{\varrho}_1(z)\|-\|z\| = \mathscr{Re}(\omega^{z_1+2z_2})-\mathscr{Re}(\omega^{z_1}) =$$
$$= \mathscr{Re}\big((u(v^2-t^2)-2stv)+(s(v^2-t^2)+2tuv)\sqrt{-1}\big)-u =$$
$$= u(v^2-t^2)-2stv-u =$$
$$= u(v^2+t^2)-2ut^2-2stv-u =$$
$$= -2t^2u-2stv.$$

Similarly we can derive the following equations:

(A.2) $$\|\tilde{\varrho}_1^{-1}(z)\| - \|z\| = -2t^2u + 2stv,$$

(A.3) $$\|\tilde{\varrho}_2(z)\| - \|z\| = -2s^2v - 2stu \quad \text{and}$$

(A.4) $$\|\tilde{\varrho}_2^{-1}(z)\| - \|z\| = -2s^2v + 2stu.$$

If $s=0$, $\|\tilde{\varrho}_2(z)\| - \|z\| = 0$ and $\|\tilde{\varrho}_2^{-1}(z)\| - \|z\| = 0$, which implies $s_d \leqq 2$. If $t=0$, $\|\tilde{\varrho}_1(z)\| - \|z\| = 0$ and $\|\tilde{\varrho}_1^{-1}(z)\| - \|z\| = 0$, which also implies $s_d \leqq 2$. Therefore, we can assume that $s \neq 0$ and $t \neq 0$. Now, we assume that $s_u = 0$. From the assumption the values of (A.1), ..., (A.4) are all non-negative. Therefore, $-2t^2u \geqq 0$, namely $u \leqq 0$, and $-2s^2v \geqq 0$, namely $v \leqq 0$. Therefore, we have $|tu| \geqq |sv|$ and $|sv| \geqq |tu|$, from which $|tu| = |sv|$. Therefore we conclude that

$$\|\tilde{\varrho}_1(z)\| - \|z\| = 0 \quad \text{or} \quad \|\tilde{\varrho}_1^{-1}(z)\| - \|z\| = 0 \quad \text{and}$$
$$\|\tilde{\varrho}_2(z)\| - \|z\| = 0 \quad \text{or} \quad \|\tilde{\varrho}_2^{-1}(z)\| - \|z\| = 0.$$

This means that $s_d \leqq 2$. ▌

**Proof of Lemma 4.2.** Let $z, z_1, z_2, u, v, s$ and $t$ be as in the proof of Lemma 4.1. $\|z\| = u + v > 0$ implies that $\max(u, v)$ is positive and is larger than or equal to the absolute value of $\min(u, v)$. Considering the symmetry of the expressions, we may assume that $u = \max(u, v)$, namely

(A.5) $$u > 0 \quad \text{and} \quad u \geqq |v|.$$

Then if $v \leqq 0$, then

(A.6) $$u > |v| = -v.$$

Assume $s=0$. Then we have $u=1$ because $u^2+s^2=1$. Therefore $v \neq -1$ because $\|z\| = u+v > 0$. On the other hand, since $z \neq {}^t(0, 0)$ from the assumption of the lemma, it is not the case that both $u=1$ and $v=1$ hold. Therefore $-1 < v < 1$. Hence $t \neq 0$ because $v^2 + t^2 = 1$. Therefore $t^2u > 0$. Thus we have from (A.1), ..., (A.4)

$$\|\tilde{\varrho}_1(z)\| - \|z\| < 0,$$
$$\|\tilde{\varrho}_1^{-1}(z)\| - \|z\| < 0,$$
$$\|\tilde{\varrho}_2(z)\| - \|z\| = 0,$$
$$\|\tilde{\varrho}_2^{-1}(z)\| - \|z\| = 0,$$

which imply the assertion of the lemma. Therefore, we may assume that $s \neq 0$, namely $|s| > 0$.

*Case 1.* $v \leqq 0$.

In this case we have from (A.6) $|t| = \sqrt{1-|v|^2} > \sqrt{1-|u|^2} = |s|$. Therefore we have $|t^2u| > |stv|$ and $|stu| > |s^2v|$. Thus

$$\|\tilde{\varrho}_1(z)\| - \|z\| < 0,$$
$$\|\tilde{\varrho}_1^{-1}(z)\| - \|z\| < 0 \quad \text{and}$$
$$\|\tilde{\varrho}_2(z)\| - \|z\| < 0 \quad \text{or} \quad \|\tilde{\varrho}_2^{-1}(z)\| - \|z\| < 0,$$

which imply the assertion of the lemma.

*Case 2.* $v>0$.

Note that from (A.5) $|t|=\sqrt{1=|v|^2}\geqq\sqrt{1-|u|^2}=s$. If $|tu|>|sv|$, then

$$\|\tilde{\varrho}_1(z)\|-\|z\| < 0,$$

$$\|\tilde{\varrho}_1^{-1}(z)\|-\|z\| < 0 \quad \text{and}$$

$$\|\tilde{\varrho}_2(z)\|-\|z\| < 0 \quad \text{or} \quad \|\tilde{\varrho}_2^{-1}(z)\|-\|z\| < 0,$$

which imply the assertion of the lemma. If $|tu|=|sv|$, then

$$\|\tilde{\varrho}_1(z)\|-\|z\| < 0 \quad \text{or} \quad \|\tilde{\varrho}_1^{-1}(z)\|-\|z\| < 0 \quad \text{and}$$

$$\|\tilde{\varrho}_2(z)\|-\|z\| < 0 \quad \text{or} \quad \|\tilde{\varrho}_2^{-1}(z)\|-\|z\| < 0,$$

because $|tu|=|sv|\neq 0$. Thus the lemma follows. ▌

## References

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

[2] N. Alon and V. D. Milman, Eigenvalues, expanders and superconcentrators, *Proc. 25th Ann. IEEE Symp. on Found. of Comput. Sci.*, (1984), 320—322.

[3] N. Alon, Z. Galil and V. D. Milman, Better expanders and superconcentrators", to appear in *J. of Algorithms.*

[4] L. A. Bassalygo, Asymptotically optimal switching ciruits, *Problems of Infor. Trans.* **17** (1981) 206—211.

[5] F. R. K. Chung, On concentrators, superconcentrators, and nonblocking networks, *Bell System Tech. J.*, **58** (1979), 1765—1777.

[6] O. Gabber and Z. Galil, Explicit constructions oflinear-sized superconcentrators, *J. Comput. System Sci.*, **22** (1981), 407-420.

[7] S. Jimbo and A. Maruoka, Expanders obtained from affine transformations, *Proc. 17th Ann. ACM Symp. on Theory of Computing*, (1985), 88—97.

[8] M. Klawe, Nonexistence of one-dimensional expanding graphs, *Proc. 22nd Ann. Symp. on Found. of Comput. Sci.*, (1981), 109—113.

[9] M. Klawe, Limitations on explicit constructions of expanding graphs, *SIAM J. Comput.* **13** (1984), 156—166.

[10] G. A. Margulis, Explicit construction of concentrators, *Prob. Info. Trans.*, 9 (1975), 325—332.

[11] N. Pippenger, Superconcentrators, *SIAM J. Comput.* **6** (1977), 298—304.

[12] W. Maass, Combinatorial lower bound arguments for deterministic and nondeterministic Turing machines, *Trans. AMS.* **292** (1985), 675—693.

Shuji Jimbo

*Oki Electric Industry*
*Shibaura, Minato-ku,*
*Tokyo, 108 Japan*

Akira Maruoka

*Faculty of Engineering,*
*Tohoku University*
*Sendai, 980 Japan*