COMBINATORICA 6 (3) (1986) 207—219

EIGENVALUES, GEOMETRIC EXPANDERS, SORTING IN ROUNDS, AND RAMSEY THEORY

N. ALON

Received 6 June 1984

Expanding graphs are relevant to theoretical computer science in several ways. Here we show that the points versus hyperplanes incidence graphs of finite geometries form highly (nonlinear) expanding graphs with essentially the smallest possible number of edges. The expansion properties of the graphs are proved using the eigenvalues of their adjacency matrices.

These graphs enable us to improve previous results on a parallel sorting problem that arises in structural modeling, by describing an explicit algorithm to sort n elements in k time units using $O(n^{\alpha_k})$ parallel processors, where, e.g., $\alpha_2=7/4$, $\alpha_3=8/5$, $\alpha_4=26/17$ and $\alpha_5=22/15$.

Our approach also yields several applications to Ramsey Theory and other extremal problems in combinatorics.

1. Introduction

A graph G is called (n, α, β)-expanding, where $0<\alpha\leqq\beta\leqq n$, if it is a bipartite graph on the sets of vertices I (inputs) and O (outputs), where $|I|=|O|=n$, and every set of at least α inputs is joined by edges to at least β different outputs.

Expanding graphs with a small number of edges, which are the subject of an extensive literature, are relevant to theoretical computer science in several ways. Here we merely point out two examples. A family of linear expanders of density k and expansion d is a set $\{G_n\}_{n=1}^{\infty}$ of graphs, where G_n has $\leqq(k+o(1))n$ edges and is $(n, \alpha, \alpha(1+d(1-\alpha/n)))$-expanding for all $\alpha\leqq n/2$, where $d>0$ and k are fixed. Such a family is the basic building block used in the constructions of graphs with special connectivity properties and small number of edges (see, e.g., Chung [13]). An example of a graph of this type is an n-superconcentrator, which is a directed acyclic graph with n inputs and n outputs such that for every $1\leqq r\leqq n$ and every two sets A of r inputs and B of r outputs there are r vertex disjoint paths from the vertices of A to the vertices of B. Superconcentrators have been used in the construction of graphs that are hard to pebble (see Lengauer and Tarjan [29], Pippenger [34] and Paul, Tarjan and Celoni [36]), in the study of lower bounds (see Valiant [42]), and in the establishment of time space tradeoffs for computing various functions (Abelson [1], Ja'Ja' [27] and Tompa [40]).

A family of linear expanders is also essential in the recent parallel sorting network of Ajtai, Komlós and Szemerédi [2].

AMS subject classification (1980): 68 E 10, 68 E 05, 05 B 25, 05 C 55

It is not too difficult to prove the existence of a family of linear expanders using probabilistic arguments (Pinsker [32], see also Pippenger [33] and Chung [13]). However, for applications an explicit construction is desirable. Such a construction is far more difficult and was first given by Margulis [30] and modified by Gabber and Galil [20]. (See also [5], [6], [7] for a similar but more general construction.)

The expanding graphs used in [20] to construct superconcentrators and those used in the sorting network of [2] are (n, α, β)-expanding for some fixed (independent of n) ratio of β/α, i.e., they are rather weakly expanding. For some applications, however, a higher amount of expansion is necessary and $(n, \alpha(n), \beta(n))$-expanding graphs are needed, where $\beta(n)/\alpha(n) \to \infty$ as $n \to \infty$. A possible (and essentially the only known) method to obtain (explicitly) highly expanding graphs with a small number of edges is an "iteration" of the known expander of [20] (see Pippenger [35]). Unfortunately, this method is a poor substitute for the probabilistic construction since it supplies graphs with too many edges. This makes some of the applications impossible.

Here we use finite geometries to construct explicitly highly expanding graphs with essentially the smallest possible number of edges. Specifically, we show using the correspondence (proved independently by Tanner [39] and by Milman and the author [6]) between the eigenvalues of the adjacency matrix of a graph and its expansion properties, that the points versus hyperplanes incidence graph of a finite geometry of dimension d is an $(n, x, n-n^{1+1/d}/x)$-expanding graph, for all $0<x<n$. Our proof here is very similar to that of Tanner in [39]. In [3] we present a more elementary proof of this result, using a certain "second moment" method. We believe, however, that in view of the tight correspondence between the eigenvalues of a graph and its expansion properties (see [39], [6], [7], [4]) the method here is more natural.

One can check easily that any graph which is $(n, x, n-n^{1+1/d}/x)$-expanding for all $0<x<n$ must have at least $\Omega(n^{2-1/d})$ edges. The geometric expanders we consider have $(1+o(1))n^{2-1/d}$ edges; only a constant times the theoretical lower bound. The previous methods were not sufficient to construct graphs with this amount of expansion having $o(n^2)$ edges.

By a theorem of Singer ([23], p. 128), the edges of the geometric expanders can be defined by translations modulo n of a set of size $\simeq n^{1-1/d}$, in contrast to the result of Klawe [28] that asserts that no family of linear expanders can have this form. This reveals a difference between weakly expanding and highly expanding graphs.

From the expansion properties of the geometric expanders we deduce a certain strengthening of a theorem of de Bruijn and Erdős [9] on the number of lines determined by a set of points in a finite projective plane. We also obtain, using similar methods, several interesting results on Hadamard matrices and quadratic residues modulo a prime p, and construct explicitly some graphs relevant to Ramsey Theory. For example, a graph on n vertices with no cycle of length 4 and no independent set of size $>2n^{3/4}$.

The geometric expanders enable us to obtain an explicit algorithm for sorting n elements in two time units using $O(n^{7/4})$ parallel processors (and only direct implications). This improves results of Häggkvist and Hell [25], Bollobás and Rosenfeld [11] and Pippenger [35], who gave explicit algorithms to this problem using (13/30) (n^2-n), $(2/5)n^2+O(n^{3/2})$ and $O(n^{1,943\cdots}(\log n)^{0,943\cdots})$ processors, respectively.

We also improve the best known algorithms for sorting n elements in k time units, for all (fixed) $k \geq 4$. Very recently, Pippenger has found a better way of using the geometric expanders to get an explicit algorithm for sorting n elements in two time units using only $O(n^{26/15})$ parallel processors. His algorithm, however, uses indirect implications of arbitrary size.

The paper is organized as follows. In Section 2 we show how the eigenvalues of the adjacency matrix of a graph are related to its expansion properties, and use this to prove the expansion properties of the geometric expanders, i.e., the point-hyperplane incidence graphs in finite geometries. In Section 3 we describe how these geometric expanders can be applied to the problem of sorting in rounds. In Section 4 we obtain further results using similar methods and construct several graphs relevant to Ramsey Theory. Section 5 contains some concluding remarks.

2. The eigenvalue method and the geometric expanders

Relations between the expansion properties of a graph and the eigenvalues of certain matrices associated with it were proved, independently, by Tanner [39] and by Milman and the author ([6], [7], [4]).

For our purposes here we need a simple generalization of a result of Tanner [39]. Its proof is based on the ideas of [39].

Let G be a bipartite graph with classes of vertices U and V, where $|U|=n$, $|V|=m$. Suppose the degree of each $u \in U$ is k and the degree of each $v \in V$ is s. (Thus $kn=sm$). Let $A=(a_{uv})_{u \in U, v \in V}$ be the $n \times m$ adjacency matrix of G defined by

$$a_{uv} = \begin{cases} 1 & \text{if } u \text{ and } v \text{ are adjacent} \\ 0 & \text{otherwise.} \end{cases}$$

AA^T is a real symmetric positive semi-definite matrix and thus has real non-negative eigenvalues with orthogonal eigenvectors. Let $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$ be these eigenvalues and let $v_1, v_2, \ldots, v_n$ be a corresponding orthonormal set of eigenvectors. One can easily check that $\lambda_1 = ks$ and a possible choice for v_1 is $(1, 1, \ldots, 1)/\sqrt{n}$.

For $X \subseteq U$, let $N(X)$ denote the set of all neighbors of X in G. If $X=\{x\}$ we write $N(x)$ instead of $N(\{x\})$.

Theorem 2.1. *Suppose* $Z \subseteq V$, $|Z|=z$ *and assume* $b \leq kz/(2m)$. *Put* $X=\{u \in U: |N(u) \cap Z| \leq b\}$. *Then*

$$|X| \leq \frac{\lambda_2 n(m-z)}{ksz-2kbn+\lambda_2(m-z)+b^2n} \leq \left(\frac{\lambda_2 nm}{ksz-2kbn}\right).$$

Remark 2.2. For $X \subseteq U$, one can apply Theorem 2.1 with $Z=V-N(X)$ and $b=0$ to obtain that

$$|N(X)| \geq \frac{k^2|X|}{(ks-\lambda_2)|X|/n+\lambda_2}.$$

This is the main result of Tanner [39].

Proof of Theorem 2.1. Let f be the characteristic vector of X, and put $|X|=x$. The scalar product (f, v_1) is $x/\sqrt{n}$ and $(f,f)=x$. Therefore

$$(A^Tf, A^Tf) = (AA^Tf, f) = \sum_{i=1}^{n} \lambda_i (f, v_i)^2 \leqq ksx^2/n + \lambda_2(x - x^2/n).$$

$A^Tf=(g_v)_{v\in V}$ is a vector indexed by the outputs $v\in V$, where g_v is the number of neighbors of v in X. By the definition of X, $\sum\{g_v: v\in V-Z\}\geqq x(k-b)$. This and the convexity of the function y^2 imply

$$(A^Tf, A^Tf) = \sum_{v\in V} g_v^2 \geqq \sum_{v\in V-Z} g_v^2 \geqq x^2(k-b)^2/(m-z).$$

Thus

$$x\big(n(k-b)^2-(m-z)(ks-\lambda_2)\big) \leqq \lambda_2 n(m-z).$$

If $b\leqq(kz)/(2m)$ then $n(k-b)^2-(m-z)(ks-\lambda_2)=ksz-2nkb+\lambda_2(m-z)+b^2n>0$ and the assertion of the theorem follows. ∎

We can now describe the geometric expanders. Let $d, q>2$ be integers. Let U and V be, respectively, the sets of points and hyperplanes of a finite geometry of dimension d and order q. (As is well known, such a geometry always exists if q is a prime power, and has an easy explicit description—see [23], p. 128.) Let $G=G(q, d)$ denote the bipartite graph with classes of vertices U and V in which $p\in U$ is joined to $h\in V$ iff p is incident with h. The next theorem shows that $G(q, d)$ is a highly expanding graph.

Theorem 2.3. *Put* $n=(q^{d+1}-1)/(q-1)$, $k=(q^d-1)/(q-1)$.

(i) *$G=G(q, d)$ is k-regular and $|U|=|V|=n$; thus G has $(1+o(1))n^{2-1/d}$ edges, (as $q\to\infty$ for fixed d).*

(ii) *If $X\subseteq U$, $|X|=x$ then*

$$|N(X)| \geqq n - \frac{(n-x)\big(n(q-1)+1\big)}{n(q-1)+1+(n-q-1)x} \geqq n - \frac{n^{1+1/d}}{x}.$$

Thus G is $(n, x, n-n^{1+1/d}/x)$-expanding for all $0<x<n$.

Proof. Part (i) is an easy well-known fact (see, e.g., [23], p. 128). To prove (ii), let $M=(m_{ph})_{p\in U, h\in V}$ be the $n\times n$ $0-1$ incidence matrix of U and V, i.e., $m_{ph}=1$ iff p is incident with h. By [23] (p. 128) $MM^T=\lambda J+(k-\lambda)I$, where $\lambda=(q^{d-1}-1)/(q-1)$, I is the $n\times n$ identity matrix and J is the $n\times n$ all 1's matrix. It follows that the eigenvalues of MM^T are $\lambda_1=\lambda n+k-\lambda=k^2$ and $\lambda_2=\ldots=\lambda_n=k-\lambda$. Let $X\subseteq I$, $|X|=x=\alpha n$. By Tanner's Theorem (see Remark 2.2)

$$|N(X)| \geqq \frac{k^2}{\alpha(k^2-k+\lambda)+k-\lambda}x = \frac{(n-1)^2\alpha n}{\alpha\big(n^2-n(q+1)\big)+n(q-1)+1}$$

$$= n - \frac{(n-x)\big(n(q-1)+1\big)}{n(q-1)+1+(n-q-1)x} \geqq n - \frac{n\big(n(q-1)+1\big)}{(n-q-1)x} \geqq n - \frac{nq}{x} \geqq n - \frac{n^{1+1/d}}{x}.$$ ∎

Remarks. 1. The known results about the distribution of primes (see e.g., [8]) clearly imply that for every fixed $d \geq 2$ and every integer n there exists a prime p such that $n \leq (p^{d+1}-1)/(p-1) \leq n + O(n^{1-1/(3d)})$. Any induced subgraph of $G(p, d)$ with n inputs and n outputs has $(1+o(1))n^{2-d^{-1}}$ edges and every set of x of its inputs is not joined to at most $(1+o(1))n^{1+1/d}x^{-1}$ outputs, i.e., has at least $n-(1+o(1))n^{1+1/d}x^{-1}$ neighbors. Thus we have for every $d \geq 2$, an explicit construction of a family of graphs $\{H(n, d)\}_{n=1}^{\infty}$ where $H(n, d)$ has $(1+o(1))n^{2-1/d}$ edges and is $(n, x, n-(1+o(1))n^{1+1/d}x^{-1})$-expanding for all $0 < x < n$.

2. Theorem 2.3 implies that if $P \subseteq U$, $|P| = q \leq n^{1/d}$ then $|N(P)| \geq n-(1/2)(n-q) \geq n/2$. Thus $G(q, d)$ is $(n, n^{1/d}, n/2)$-expanding. As noted by Pippenger [35], the well-known results about the problem of Zarankiewicz (see, e.g., [22]) supply lower bounds on the number of edges of expanding graphs. Using the results of [22] one can easily show that the number of edges of an $(n, n^{1/d}, n/2)$-expanding graph is at least $(1+o(1))(ln\, 2)n^{2-1/d}$. Note that the number of edges of $G(q, d)$ (or of $H(n, d)$) is $(1+o(1))n^{2-1/d}$ and thus these graphs have (up to a constant $1/ln2$) the smallest possible number of edges.

3. Let $PG(d, q)$ be the finite geometry of dimension d over the field $GF(q)$ and let $G(q, d)$ be the corresponding expander. Let n, k be as is Theorem 2.3. By Singer's Theorem ([23], p. 128) there exist $0 \leq a_1 < a_2 < \ldots < a_k < n$ such that $G(q, d)$ is isomorphic to the bipartite graph with classes of vertices $A = B = \{0, 1, 2, \ldots, n-1\}$ in which $a \in A$ is joined to $b \in B$ iff $b = (a + a_i) \pmod n$ for some $1 \leq i \leq k$. This contrasts with the result of [28] that implies that no family of linear expanders can have this form and thus shows a difference between highly expanding and weakly expanding graphs.

3. Sorting in rounds

Suppose we are given n elements with a linear order unknown to us. In the first round we ask m_1 simultaneous questions, each a binary comparison. Having the answers we deduce all implications and ask, in the next round, another m_2 questions, deduce their implications, and so on. A choice of our questions that guarantees that after r rounds we will know the complete order of the elements is an algorithm for sorting in r rounds. The need for such algorithms with fixed r arises in structural modeling (see Häggkvist and Hell [26]). Since all comparisons within a round are evaluated simultaneously, such algorithms have obvious connection to parallel sorting, as defined by Valiant [41], and seem to be practical in situations like testing consumer preferences (see Scheele [37]), where the communication between the sorting computer and the consumers is being performed by correspondence. Many results about sorting in rounds can be found in the survey article [10].

Let $f_r(n)$ denote the minimum possible number of comparisons sufficient to sort n elements in r rounds. Clearly $f_1(n) = \binom{n}{2}$. Häggkvist and Hell [24, 25] and Bollobás and Thomason [12], used probabilistic arguments to obtain estimates of $f_r(n)$ for $r \geq 2$. In particular it is known that $f_2(n) = O(n^{3/2} \log n)$ and $f_2(n) = \Omega(n^{3/2})$, (see [12]). For practical applications, however, a probabilistic argument

is not enough and an explicit sorting algorithm is desirable. Häggkvist and Hell observed this fact and in [26] they gave explicit algorithms for sorting in k rounds with $O(n^{s_k})$ comparisons, where $s_k \to 1$ as $k \to \infty$ and, e.g., $s_3 = 8/5$, $s_4 = 20/13$ and $s_5 = 28/19$. It seems more difficult to find an efficient explicit sorting algorithm in two rounds. Häggkvist and Hell [25] gave such an algorithm with $(13/30)(n^2 - n)$ comparisons. A somewhat better algorithm was given by Bollobás and Rosenfeld in [11]—with $(2/5)n^2 + O(n^{3/2})$ comparisons. The only construction with $o(n^2)$ comparisons is due to Pippenger [35]—$O(n^{1,943\ldots}(\log n)^{0,943\ldots})$.

In some situations it may be undesirable to allow deducing all implications, since conclusions derived from relations themselves derived by transitivity may be unreliable. Thus one may be willing to allow only direct implications (i.e., if we find in the first round that $x < y$, $y < z$ and $z < t$ we conclude that $x < z$ and $y < t$ but not necessarily that $x < t$). In [12] a lower bound of $\Omega(n^{5/3})$ is proved for such an algorithm in 2 rounds. Here we use the geometric expanders arising from finite geometries of dimension 4 to obtain the following result.

Theorem 3.1. *By an explicit construction that uses only direct implications* $f_2(n) = O(n^{7/4})$.

Note that by the lower bound mentioned above this construction is not that far from being best possible. Theorem 3.1, together with the results of Häggkvist and Hell [26], Theorem 3, supply an explicit sorting algorithm in k rounds with $O(n^{\alpha_k})$ comparisons, where $\alpha_1 = 2$, $\alpha_2 = 7/4$ and $\alpha_k = \min (2(2^j - 1)\alpha_{k-j} - 2^j)/((2^j - 1)\alpha_{k-j} - 1)$, with the minimum taken over all j, $0 < j < k$, for which $\alpha_{k-j} \geq 2^j/(2^j - 1)$. This improves the results of [26] for all $k \geq 4$. In particular, one can easily check that $\alpha_4 = 26/17$ and $\alpha_5 = 22/15$, slightly better than the corresponding bounds $s_4 = 20/13$ and $s_5 = 28/19$ given in [26].

Proof of Theorem 3.1. Let A be the set of n objects we have to sort. Clearly we may assume that n is of the form $(q^5 - 1)/(q - 1)$ for some prime power q (otherwise, add $o(n)$ dummy objects to obtain an n of this form). Let $G = G(q, 4)$ be a geometric expander corresponding to a finite geometry of dimension 4 and order q. Let $U = \{u_1, u_2, \ldots, u_n\}$ and $V = \{v_1, v_2, \ldots, v_n\}$ be the sets of inputs and outputs of G, respectively. In the first round we compare the i-th element of A to the j-th element if $u_i v_j$ is an edge of G. There are $O(n^{7/4})$ such comparisons.

We proceed to show that even by deducing only direct implications we will have to compare in the second round only $O(n^{7/4})$ pairs.

For $X \subseteq A$ put $N(X) = \{y \in A : y$ is compared in the first round to some $x \in X\}$. We need the following two facts.

Fact 1. *If* $Z \subseteq A$, $|Z| = (3 + o(1))n^{3/4}$ *and* $X = \{x \in A : |N(x) \cap Z| \leq n^{1/2}\}$ *then* $|X| \leq (1 + o(1))n^{1/2}$.

This follows by substituting $m = n$, $\lambda_2 = (1 + o(1))n^{3/4}$, $k = s = (1 + o(1))n^{3/4}$, $z = (3 + o(1))n^{3/4}$ and $b = n^{1/2}$ in Theorem 2.1. (The fact that here $\lambda_2 = q^3 = ((1 + o(1))n^{3/4}$ appears in the proof of Theorem 2.3.) ∎

Fact 2. *If* $Y \subseteq A$, $|Y| > n^{1/2}$ *then* $|N(Y)| \geq n - n^{3/4}$.

This follows by substituting $x = n^{1/2}$ and $d = 4$ in Theorem 2.3. ∎

Define a partition of A into $l=[n^{1/4}/3]$ blocks $A_1, \ldots, A_l$, each of size $(3+o(1))n^{3/4}$, such that each A_i consists of consecutive objects (in the linear order we have to find) and the maximal element of A_i is smaller than the minimal element of A_{i+1}. Call an element $a \in A_{i+1}$ *bad* if $|N(a) \cap A_i| \leq n^{1/2}$, otherwise call it *good*. By Fact 1 the number of bad elements in A_{i+1} is $\leq (1+o(1))n^{1/2}$. Let $a \in A_{i+1}$ be good and suppose $b \in \cup \{A_j : 1 \leq j \leq i-1\}$. If

$$N(b) \cap N(a) \cap A_i \neq \emptyset \tag{3.1}$$

then, by direct implication from the first round, $b<a$. However, $|N(a) \cap A_i| > n^{1/2}$, and thus, by Fact 2 the number of b's that violate (3.1) is $\leq n^{3/4}$. It follows that the total number of comparisons of an element $a \in A_{i+1}$ to elements in $\cup \{A_j : 1 \leq j \leq i+1\}$ left for the second round is bounded by n (of course) if a is bad and by $|A_i| + |A_{i+1}| + n^{3/4} = (7+o(1))n^{3/4}$ if a is good. The total number of these comparisons is thus bounded by

$$l(1+o(1))n^{1/2}n + n(7+o(1))n^{3/4} = O(n^{7/4}).$$

Since the first round also requires $O(n^{7/4})$ comparisons, the total number of comparisons is $O(n^{7/4})$. ∎

Very recently Pippenger has shown that by using indirect implications of arbitrary length, the number of comparisons can be reduced to $O(n^{26/15})$. The first round of his algorithm uses the geometric expanders arising from finite geometries of dimensions 3.

4. Further results

The proof of Theorem 2.1 indicates that its conclusion will be of particular accuracy when applied to graphs that arise from block designs, since in this case all the eigenvalues except the largest one are equal. The graphs of the finite geometries that appear in Theorem 2.3 are one family of such examples. A second family of examples arises from Hadamard matrices. An Hadamard matrix H of dimension t is a t by t matrix over $\{1, -1\}$ in which every two distinct rows (and hence also every two distinct columns) are orthogonal. See, e.g., [23], Chapter 14 for the basic properties of Hadamard matrices. A submatrix of H is called monochromatic if all its entries have the same sign. The next theorem asserts that every relatively large submatrix of a Hadamard matrix is "balanced". Very recently, Frankl, Rödl and Wilson [18] have found several surprising extensions of it. A somewhat weaker version of this theorem can be proved using eigenvalues, as in Section 2. Here we present a very simple proof that uses a certain "second moment" method. A similar method is used in [3] to estimate the expansion properties of the geometric expanders.

Theorem 4.1. *Let $H=(h_{ij})$ be an Hadamard matrix of dimension t. Then both the number of $+1$'s and the number of -1's in every k by l submatrix of H are at least*

$$\frac{kl-(klt)^{1/2}}{2}.$$

In particular H contains no monochromatic square submatrix of dimension $>t^{1/2}$.

Remark. The last statement is sharp in the sense that for every $t=4^k$ there is a t by t Hadamard matrix H_k with a $\sqrt{t}\times\sqrt{t}$ submatrix all of whose entries are $+1$. Such an H_k is, e.g., the Kronecker product of k copies of

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

Proof. Let $(h_{ij})_{i\in A, j\in B}$ be a k by l submatrix of H, where $A, B\subseteq\{1, 2, \ldots, t\}$, $|A|=k$, $|B|=l$. By the convexity of the square and the orthogonality of the columns we obtain:

$$\frac{1}{k}\Big(\sum_{i\in A}\sum_{j\in B} h_{ij}\Big)^2 \leqq \sum_{i\in A}\Big(\sum_{j\in B} h_{ij}\Big)^2 \leqq \sum_{i=1}^{t}\Big(\sum_{j\in B} h_{ij}\Big)^2 =$$

$$= \sum_{j\in B}\sum_{i=1}^{t} h_{ij}^2 + 2\sum_{j,j'\in B, j<j'}\sum_{i=1}^{t} h_{ij}h_{ij'} = lt.$$

Thus

$$\Big|\sum_{j\in A}\sum_{j\in B} h_{ij}\Big| \leqq (klt)^{1/2}$$

and the desired result follows. ∎

A similar result can be proved for linear shift registers (=LFSR's). For $n\geqq 1$ let $N=2^n-1$ and let $a_0, a_1, \ldots, a_{N-1}$ be the output sequence of a binary maximal length LFSR with n cells. (See [21] for the basic properties of such sequences.) Define an $N\times N$ circulant 0-1 matrix $B=(b_{ij})$ by $b_{ij}=a_{(i+j)(\mathrm{mod}\,N)}$. One can show that the matrix

$$H=\begin{bmatrix} 1 & e \\ e^T & C \end{bmatrix},$$

where $C=(c_{ij})$ is given by $c_{ij}=(-1)^{b_{ij}}$ and e is the all 1 vector is an Hadamard matrix of dimension $N+1$, and thus Theorem 4.1 can be applied here. In particular, B contains no square submatrix of dimension $2^{n/2}$ all of whose entries are zero. This is sharp for any even n, since one can show that each such B contains a $(2^{n/2}-1)\times(2^{n/2}-1)$ submatrix all of whose entries are 0. We omit the details.

A similar proof establishes the following result about squares and nonsquares in finite fields.

Proposition 4.2. *Let $q=p^r$ be an odd prime power. Let A, B be two subsets of the finite field* GF(q), *where $|A|=k$, $|B|=l$, $k\leqq l$. Then*

$$\big|\{(a, b)\colon a\in A, b\in B \text{ and } a+b \text{ is a nonzero square}\}\big| \geqq f(q, k, l)$$

and

$$\big|\{(a, b)\colon a\in A, b\in B \text{ and } a+b \text{ is not a square}\}\big| \geqq f(q, k, l),$$

where

$$f(q, k, l)=\frac{1}{2}(kl-k-(kl(q-l))^{1/2}).$$

Proof. Let $\chi(x)$ be the character defined on $GF(q)$ where $\chi(0)=0$, $\chi(x)=+1$ if $x\neq 0$ is a square and $\chi(x)=-1$ if x is not a square.

We need the easy, known fact that for every $0\neq c\in GF(q)$

$$\sum_{x\in GF(q)} \chi(x)\chi(x+c) = -1. \tag{4.1}$$

Indeed

$$\sum_{x\in GF(q)} \chi(x)\chi(x+c) = \sum_{0\neq x\in GF(q)} \chi(x)\chi(x)\left(1+\frac{c}{x}\right) = \sum_{0\neq x\in GF(q)} \chi\left(1+\frac{c}{x}\right) = -1.$$

Combining (4.1) with the convexity of the square we obtain

$$\frac{1}{k}\Big(\sum_{a\in A}\sum_{b\in B}\chi(a+b)\Big)^2 \leqq \sum_{a\in A}\Big(\sum_{b\in B}\chi(a+b)\Big)^2 \leqq$$

$$\leqq \sum_{a\in GF(q)}\Big(\sum_{b\in B}\chi(a+b)\Big)^2 = |B|(q-1)-|B|(|B|-1) = l(q-l).$$

Since $\big|\{(a,b): a\in A,\ b\in B \text{ and } a+b=0\}\big|\leqq k$ the desired result follows. ∎

Next we consider some constructions of graphs related to Ramsey Theory. Let H_1 and H_2 be two families of graphs. The Ramsey number $r(H_1, H_2)$ is the maximal number of vertices of a graph G, such that G contains no subgraph isomorphic to a member of H_1 and its complement $\bar{G}$ contains no copy of a member of H_2. Usually it is much easier to obtain lower bounds to $r(H_1, H_2)$ using probabilistic arguments, than to explicitly construct a graph G demonstrating this bound. Thus, e.g., the problem of constructing an explicit graph G showing that $r(K_m, K_m) > c^m$ for some $c>1$, where K_m is the complete graph on m vertices, is still open (see [14], [19]), while the existence of such a constant c is proved very easily using probabilistic arguments. Here we apply Theorems 2.3 and 4.1 to bound, by explicit constructions, two families of Ramsey numbers.

For $k\geqq 2$, let k_t denote a topological complete graph on k vertices, i.e., a graph obtained from the complete graph on k vertices K_k by replacing some of the edges by internally vertex disjoint paths. Thus 2_t is a path and 3_t is a cycle. Erdős and Hajnal [16] proved that there exists a constant $c>0$ such that in any two-coloring of the edges of K_n there is a monochromatic $(c\sqrt{n})_t$. They also proved, using probabilistic methods, that there exists a constant $d>0$ and a two-coloring of the edges of K_n with no monochromatic $(d\sqrt{n})_t$. Theorem 4.1 supplies an explicit construction of such a coloring. Indeed, let $H=(h_{ij})$ be an $n\times n$ symmetric Hadamard matrix. (E.g., the matrix mentioned in the remark following Theorem 4.1, or the matrix constructed using the LFSR.) Color the edges of K_n by the colors ± 1 according to H, i.e., the color of $\{i,j\}$ is h_{ij}. We claim that in this coloring there is no monochromatic $(3\sqrt{n})_t$. Indeed, suppose this is false and let Z be the set of vertices of a monochromatic $(3\sqrt{n})_t$ of color $+1$ (say). By Theorem 4.1 the induced graph on Z contains at least $\frac{1}{4}(3^2-3)(1+o(1))n > n$ edges of color -1. Each such edge has to be replaced by a path and all these paths have to be internally disjoint. However, this is impossible since the total number of vertices is only n.

The second construction is related to the Ramsey number $r=r(C_4, K_n)$, which is the maximal number of vertices of a graph G that contains no 4-cycle and no independent set of size n. It is known [15], [38] that $c_1 n^{1+c_2} \leqq r \leqq c_3 n^2/\log(n)$ for some $c_1, c_2, c_3 > 0$. However, the lower bound is probabilistic and there is no known explicit construction of a graph G on $\Omega(n^{1+\delta})$ vertices with the desired properties. Theorem 2.3 supplies such an example (with $\delta = 1/3$). It is worth noting that this example is still not as good as the probabilistic lower bound—$\Omega(n/\log n)^{3/2}$—given by Spencer [38]. The explicit example we consider is a well known graph $G=(V, E)$, first constructed by Erdős and Rényi ([17], see also [8], p. 314). Let q be a prime power, and let V be the set of points of the projective plane $\mathrm{PG}(2, q)$ over the field of order q ($|V|=q^2+q+1$). A point (x, y, z) is joined to all the points on its polar with respect to the conic $x^2+y^2+z^2=0$. Thus (x, y, z) and (a, b, c) are joined iff $ax+by+cz=0$, that is, iff the point (x, y, z) lies on the line (a, b, c). Clearly G contains no 4-cycle, since any two points in $\mathrm{PG}(2, q)$ lie in exactly one common line. By Theorem 2.3, every set of $|V|^{3/4}$ points in $\mathrm{PG}(2, q)$ is incident with at least $|V|-|V|^{3/4}$ lines. Thus G contains no independent subset of size $>2|V|^{3/4}$. Substituting $n=2|V|^{3/4}$ we conclude that G is an explicit example showing $r(C_4, K_n) > c_1 n^{4/3}$. (Using Theorem 2.1 one can replace the constant 2 here by $(1+\varepsilon)$.) We note that a similar nonlinear explicit lower bound for $r(C_6, K_n)$ can be described analogously, using generalized n-gons.

We conclude this section with a certain strengthened version of the de Bruijn—Erdős theorem. Let M be a projective plane of order q, and let P denote the set of its q^2+q+1 points. For $X \subseteq P$, let $L(X)$ denote the set of all lines determined by X, (i.e., the set of lines containing at least two points of X.) Similarly, for $X_1, X_2 \subset P$, let $L(X_1, X_2)$ denote the set of lines that intersect both X_1 and X_2. de Bruijn and Erdős [9] proved that if X is not collinear then $|L(X)| \geqq |X|$. Meshulam [31] showed that if $X_1 \cup X_2$ is not collinear and $|X_1| = |X_2|$ then $|L(X_1, X_2)| \geqq |X_1|$. Our results supply an improvement of these results for relatively large sets of points. Indeed, Theorem 2.3 for $d=2$ implies that a set of x points in M is incident with at least $(q+1)^2 x/(q+x)$ lines. This gives the exact result for $x=0, 1, 2$ and $x \geqq q^2$ and implies that if $X_1, X_2 \subseteq P$ satisfy $|X_1| = |X_2| = cq$, where $c > 1$, then

$$|L(X_1, X_2)| \geqq q + \frac{c-1}{c+1}(q+1)^2.$$

In particular, if $X \subseteq M$ and $|X| = 2cq$, where $c > 1$ then

$$|L(X)| \geqq q + \frac{c-1}{c+1}(q+1)^2.$$

However, here one can prove directly the following stronger result:

If $X \subseteq M$, $|X| = q+1+r$, *where* $q \geqq r \geqq 1$ *then*

$$|L(X)| > \frac{rq + r^2(q+1-r)/2}{q+1+r}. \tag{4.2}$$

Note that (4.2) implies that if $|X| = (1+\varepsilon)(q+1)$, where $\varepsilon > 0$ then

$$|L(X)| > \frac{\varepsilon^2(1-\varepsilon)}{2+2\varepsilon}(q+1)^2.$$

To prove (4.2), partition X into $k=\lceil(q+1+r)/r\rceil$ parts, $X_1, \ldots, X_k$, each of size $\leqq r$. Let $N(X_i)$ denote the set of lines incident with points of X_i. One can easily check that $|N(X_i)| \geqq (q+1)+q+\ldots+(q+2-|X_i|)$ and thus

$$\sum_{i=1}^{k} |N(X_i)| > (q+1-r/2)(q+1+r) = (q^2+q+1)+q+\frac{r}{2}(q+1-r).$$

Put

$$T = \{(l, x_i): 1 \leqq i \leqq k, l \text{ is a line of } M \text{ and } l \in N(X_i)\}.$$

Clearly

$$|T| > (q^2+q+1)+q+\frac{r}{2}(q+1-r)$$

and since no line occurs in more than k pairs of T, there are more than $\left(q+(r/2)(q+1+r)\right)/(k-1)$ lines that belong to $\geqq 2N(X_i)$'s. Since $k-1 < (q+1+r)/r$, (4.2) follows. Corresponding results to higher dimensions can be proved analogously.

5. Concluding remarks

1. There are certain algorithmic problems that can be solved using networks whose existence is proved using probabilistic arguments. In some cases, however, an explicit construction is desirable. Expanding graphs share some of the properties of random graphs and can thus sometimes replace the "random" components of these networks by explicit ones. Indeed, the problem of existence of superconcentrators with a linear number of edges was first solved using probabilistic methods (see [42], [33]) and only afterwards was an explicit construction given using a small variation of the expanding graphs of [30], (see [20]). The first version of the sorting network of [2] also used random graphs (see [2], page 1) and again expanding graphs supplied an explicit construction.

The existence of a two round sorting algorithm using $o(n^2)$ comparisons was proved in [12], [25] using probabilistic arguments. As shown in [35] and in Section 3, here, once more, expanding graphs supply an explicit construction of such an algorithm. Notice that there still exists a gap between what is done probabilistically in [12] and the known explicit constructions. It would be nice to close this gap, and also to decide whether $f_2(n)$ is closer to $O(n^{3/2}\log n)$ or to $O(n^{3/2})$.

As mentioned in [3] the geometric expanders are useful also in explicit constructions of efficient superconcentrators of limited depth.

2. More results about the correspondence between the eigenvalues of a graph and its expansion properties appear in [39], [3], [6], [7]. In particular, in [6] this correspondence is combined with some results on group representations to obtain, by explicit construction, many linear families of expanders.

Added in proof: Some recent lower and upper bounds for sorting in rounds appear in [43]. Better explicit parallel sorting algorithms, that use the expanders constructed in [44], appear in [45].

References

[1] H. ABELSON, A note on time space tradeoffs for computing continuous functions, *Infor. Proc. Letters* **8** (1979), 215—217.

[2] M. AJTAI, J. KOMLÓS and E. SZEMERÉDI, Sorting in $c \log n$ parallel steps, *Combinatorica* **3** (1983), 1—9.

[3] N. ALON, Expanders, sorting in rounds and superconcentrators of limited depth, *Proc.* **17***th Annual ACM Symp. on Theory of Computing, Providence, RI* (1985), 98—102.

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

[5] N. ALON, Z. GALIL and V. D. MILMAN, Better expanders and superconcentrators, *J. of Algorithms, to appear.*

[6] N. ALON and V. D. MILMAN, λ_1, isoperimetric inequalities for graphs and superconcentrators, *J. Combinatorial Theory Ser. B*, **38** (1985), 73—88.

[7] N. ALON and V. D. MILMAN, Eigenvalues, expanders and superconcentrators, *Proc.* **25***th Annual Symp. on Foundations of Comp. Sci.*, Florida (1984), 320—322.

[8] B. BOLLOBÁS, *Extremal Graph Theory*, Academic Press, London and New York (1978).

[9] N. G. DE BRUIJN and P. ERDŐS, On a combinatorial problem, *Indagationes Math.* **20** (1948), 421—423.

[10] B. BOLLOBÁS and P. HELL, Sorting and Graphs, in: *Graphs and Order*, (I. Rival, ed.) D. Reidel (1985), 169—184.

[11] B. BOLLOBÁS and M. ROSENFELD, Sorting in one round, *Israel J. Math.* **38** (1981), 154—160.

[12] B. BOLLOBÁS and A. THOMASON, Parallel sorting, *Discrete Appl. Math.* **6** (1983), 1—11.

[13] F. R. K. CHUNG, On concentrators, superconcentrators, generalizers, and nonblocking networks, *Bell Sys. Tech. J.* **58** (1978), 1765—1777.

[14] P. ERDŐS, Problems and results in Graph Theory, *in: Proc. Inter. 4th Conf. on the theory and applications of graphs* (G. Chartrand et al. eds.), Kalamazoo, Michigan (1980), pp. 331—341.

[15] P. ERDŐS, Extremal problems in Number Theory, *Combinatorics and Geometry, Proc. Inter. Conf. in Warsaw*, 1983, to appear.

[16] P. ERDŐS and A. HAJNAL, On complete topological subgraphs of certain graphs, *Ann. Univ. Sci. Budapest, Eötvös Sect. Math.* **7** (1964), 143—149.

[17] P. ERDŐS and A. RÉNYI, On a problem in the theory of graphs, *Publ. Math. Inst. Hungar. Acad. Sci.* **7** (1962), 215—235 (in Hungarian).

[18] P. FRANKL, V. RÖDL and R. M. WILSON, The number of submatrices of given type in a Hadamard martrix, *J. of Combinatorial Theory B, to appear.*

[19] P. FRANKL and R. M. WILSON, Intersection theorems with geometric consequences, *Combinatorica* **1** (1981), 357—368.

[20] O. GABBER and Z. GALIL, Explicit construction of linear sized superconcentrators, *J. Comp. and Sys. Sci.* **22** (1981), 407—420.

[21] S. GOLOMB, *Shift Register Sequences*, Holden Day, Inc., San Francisco, 1967.

[22] R. K. GUY and S. ZNAM, A problem of Zarankiewicz, in: *Recent Progress in Combinatorics* (W. T. Tutte, ed.) Academic Press, 1969, 237—243.

[23] M. HALL, JR., *Combinatorial Theory*, Wiley and Sons, New York and London, 1967.

[24] R. HÄGGKVIST and P. HELL, Graphs and parallel comparison algorithms. *Congr. Num.* **29** (1980), 497—509.

[25] R. HÄGGKVIST and P. HELL, Parallel sorting with constant time for comparisons, *SIAM J. Comp.* **10**, (1981), 465—472.

[26] R. HÄGGKVIST and P. HELL, Sorting and merging in rounds, *SIAM J. Alg. and Disc. Meth.* **3** (1982), 465—473.

[27] J. JA'JA, Time space tradeoffs for some algebraic problems, *Proc.* **12***th Ann. ACM Symp. on Theory of Computing*, 1980, 339—350.

[28] M. KLAWE, Non-existence of one-dimensional expanding graphs, *Proc.* **22***nd Ann. Symp. Found.* Comp. Sci. Nashville (1981). 109—113.

[29] T. LENGAUER and R. E. TARJAN, Asymptotically tight bounds on time space trade-offs in a pebble game, *J. ACM* **29** (1982), 1087—1130.

[30] G. A. MARGULIS, Explicit constructions of concentrators, *Prob. Per. Infor.* **9** (1973), 71—80, (English translation in *Problems of Infor. Trans.* (1975), 325—332).

[31] R. MESHULUAM, A geometric construction of a superconcentrator of depth 2, *preprint.*

[32] M. PINSKER, On the complexity of a concentrator, *7th International Teletraffic Conference*, Stockholm, June 1973, 318/1—318/4.

[33] N. PIPPENGER, Superconcentrators, *SIAM J. Computing* **6** (1977), 298—304.
[34] N. PIPPENGER, Advances in pebbling, Internat. *Colloq. on Autom. Lang. and Prog.* **9** (1982), 407—417.
[35] N. PIPPENGER, Explicit construction of highly expanding graphs, *preprint.*
[36] W. J. PAUL, R. E. TARJAN and J. R. CELONI, Space bounds for a game on graphs, *Math. Sys. Theory* **20** (1977), 239—251.
[37] S. SCHEELE, *Final report to office of environmental education,* Dept. of Health, Education and Welfare, Social Engineering Technology, Los Angeles, CA 1977.
[38] J. SPENCER, Asymtotic lower bounds for Ramsey functions, *Discrete Math.* **20** (1977), 69—76.
[39] R. M. TANNER, Explicit construction of concentrators from generalized N-gons, *SIAM J. Alg. Discr. Meth.*, **5** (1984), 287—293.
[40] M. TOMPA, Time space tradeoffs for computing functions, using connectivity properties of their circuits, *J. Comp. and Sys. Sci.* **20** (1980), 118—132.
[41] L. G. VALIANT, Parallelism in comparison networks. *SIAM J. Comp.* **4** (1975), 348—355.
[42] L. G. VALIANT, Graph theoretic properties in computational complexity, *J. Com. and Sys. Sci.* **13** (1976), 278—285.
[43] N. ALON, Y. AZAR, and U. VIZHKIN, Tight complexity bounds for parallel comparison sorting, *Proc. 27th FOCS, to appear.*
[44] A. LUBOTZKY, R. PHILLIPS, and P. SARNAK, Ramanujan graphs, *to appear.*
[45] N. PIPPENGER, Sorting and selecting in rounds, *preprint.*

Noga Alon

Department of Mathematics
Tel Aviv University, Ramat Aviv, Tel Aviv
Israel
and
Bell Communications Research
Morristown, N.J. 07960, U.S.A.