JOURNAL OF COMPUTER AND SYSTEM SCIENCES 22, 407–420 (1981)

Explicit Constructions of Linear-Sized Superconcentrators

OFER GABBER AND ZVI GALIL*

School of Mathematical Sciences,
Tel Aviv University, Ramat Aviv, Tel Aviv, Israel

Received May 12, 1980; revised February 9, 1981

1. INTRODUCTION

In some cases people are interested in certain kinds of networks and want them to be of small size. Usually these kinds of networks are defined by certain requirements on the connectivity between their inputs and outputs. One trick that sometimes yields the desired networks is counting argument. One considers a certain family of graphs of size n and counts how many of these graphs do not satisfy the requirements (the bad ones). In case the number of bad ones is smaller than the number of graphs in the family, the existence of a good graph (the desired network) is established. In fact, in many of the cases one shows that most of the graphs in the family are good. (The fraction of bad graphs tends to zero as n grows.) The weakness of this approach is that it is nonconstructive: although one knows that many of these graphs are good, he cannot construct one such graph.

An (n, m, k) *concentrator* is a directed acyclic graph (dag) with n inputs, $m \leqslant n$ outputs, and at most kn edges, such that for every subset of m inputs there are m vertex disjoint paths going from these m inputs to the outputs. An (n, k) *superconentrator* (*s.c.*) is a dag with n inputs, n outputs and at most kn edges, such that for every $1 \leqslant r \leqslant n$ and any two sets of r inputs and r outputs there are r vertex disjoint paths connecting the two sets. A family of linear concentrators [superconcentrators] of density k is a set of $(n, m, k + o(1))$ concentrators [$(n, k + o(1))$ s.c.'s] for $1 \leqslant m \leqslant n < \infty$ [for $1 \leqslant n < \infty$].

In [6] Pinsker constructed a family of linear concentrators of density 29. His construction uses counting argument. Valiant [9] used Pinsker's linear concentrators to construct a family of linear s.c.'s of density 238. By doing so he disproved a conjecture that superconcentrators require more than a linear number of edges [1, p. 450, research problem 12.37].

Pippenger [7] has discovered a direct way to construct a family of linear s.c.'s of density 39. His construction used a certain type of graphs. the existence of which is

* The research of the second author was supported in part by the Israel Commission of Basic Research and by National Science Foundation grant number MCS78-2530.

0022-0000/81/030407–14$02.00/0

established by counting argument. However, the construction of explicit linear concentrators and superconcentrators remained open.

Margulis [5] made a major step forward. He found a way to construct explicit linear expanders defined below. An $(n, \theta, k, \alpha, c)$ *bounded strong concentrator* is a bipartite graph with n inputs, θn outputs and at most kn edges, such that if X is a set of inputs with $|X| \leqslant \alpha n$, then $|\Gamma_X| \geqslant c|X|$, where Γ_X is the set of outputs connected to X. We omit the word strong and the parameter c whenever $c=1$. An (n, k, d) *expander* is a bipartite graph with n inputs, n outputs and at most kn edges, such that for every subset X of inputs, $|\Gamma_X| \geqslant [1 + d(1 - |X|/n)]\,|X|$. Margulis described a family of explicit bipartite graphs $\{\hat{G}_n\}$ for $n = m^2$, $m = 1, 2, \ldots$, and proved:

THEOREM 1. *There exists a constant $d > 0$ such that for $n = m^2$ and $m = 1, 2, \ldots$, $\hat{G}_n$ is an $(n, 5, d)$ expander.*

Actually Margulis' theorem states that $\hat{G}_n$ is an $(n, 1, 5, \alpha, 1 + d(1 - \alpha))$ bounded strong concentrator for every $0 \leqslant \alpha \leqslant 1$. But the two statements are equivalent. Margulis' proof applied first a series of reductions and finally it used several deep theorems from the theory of group representations. Moreover, the constant d is not known. Possibly, one can compute it by tracing all the ε's in the proofs. But Margulis states explicitly that he does not know the constant. Angluin [2] has recently pointed out that Margulis' technique may yield $(n, 3, d')$ expanders. But d' is not known as well.

We construct a family of explicit graphs $\{G_n\}$ for $n = m^2$, $m = 1, 2, \ldots$, and our main result is the following theorem.

THEOREM 2. *For $n = m^2$, $m = 1, 2, \ldots$, G_n is an $(n, 5, d_0)$ expander, where $d_0 = (2 - \sqrt{3})/4$.*

The graphs G_n are similar to $\hat{G}_n$. But unlike Margulis' proof our proof (following several reductions) uses relatively elementary analysis and can be considered as self-contained. We give the proof of Theorem 2 in Section 2.

In Section 3 we explain how from a given family of linear expanders one can construct a family of certain linear bounded concentrators and how one can use the latter to construct a family of linear superconcentrators. The constructions depend on the value of d. That is why Margulis' result did not suffice. Using the graphs G_n of Theorem 2 we get a family of linear superconcentrators of density 504.

Section 4 is devoted to improving the size of the superconcentrators constructed in Section 3. We observe that it is important to have d as large as possible. Making some changes in the first part of the proof of Theorem 2, we derive a new family of graphs $\{G'_n\}$ for $n = m^2$, $m = 1, 2, \ldots$, and a proof for the following theorem.

THEOREM 2'. *For $n = m^2$, $m = 1, 2, \ldots$, G'_n is an $(n, 7, d'_0)$ expander, where $d'_0 = 2d_0$.*

Applying the two constructions we derive a family of linear superconcentrators of density 273. In Appendix 1 we sketch a way how to reduce the density to approximately 271.8. Finally, Section 5 includes a list of some open problems.

2. The Proof of Theorem 2

Let $n = m^2$ and let A_m be $\{0, 1, \ldots, m-1\} \times \{0, 1, \ldots, m-1\}$. The bipartite graphs G_n are obtained from 5 permutations on A_m. (Each permutation defines m^2 edges in the obvious way.) The permutations are

$$\sigma_0(x, y) = (x, y),$$
$$\sigma_1(x, y) = (x, x+y),$$
$$\sigma_2(x, y) = (x, x+y+1),$$
$$\sigma_3(x, y) = (x+y, y),$$
$$\sigma_4(x, y) = (x+y+1, y),$$

where the + is modulo m.

The theorem follows from Lemma 1 proven below.

LEMMA 1. *For every* $X \subseteq A_m$, $\sum_{i=1}^{4} |\sigma_i(X) - X| \geqslant 4d_0 |X||X^c|/n$.

Proof of Theorem 2. By Lemma 1, for every $X \subseteq A_m$, there is an i such that $|\sigma_i(X) - X| \geqslant d_0 |X||X^c|/n = d_0 |X|(1 - |X|/n)$. But $\Gamma_X \supseteq X \cup \sigma_i(X)$ and $\Gamma_X - X \supseteq \sigma_i(X) - X$. ∎

We define A to be the $[0, 1) \times [0, 1)$ torus, and two automorphisms $\tau_i: A \to A$, $i = 1, 2$: $\tau_1(x, y) = (x, x+y)$, $\tau_2(x, y) = (x+y, y)$, where the + is modulo 1. Lemma 1 (the discrete version) follows from Lemma 2 (the continuous version) proven below.

LEMMA 2. *For every measurable* $X \subseteq A$, $\sum_{i=1}^{2} \mu(X - \tau_i^{-1}(X)) \geqslant 2d_0\mu(X)\mu(X^c)$, *where* $\mu(X)$ *is the Lebesgue measure of* X.

Proof of Lemma 1. Fix an $X \subseteq A_m$. For $(x, y) \in A_m$ let $A'_{(x,y)} = \{((x+u)/m, (y+v)/m) \mid 0 \leqslant u, v < 1\}$. Let $X' = \bigcup_{a \in X} A'_a$. Note that

$$\mu(X') = |X|/n \qquad \text{and} \qquad \mu(X'^c) = |X^c|/n. \tag{1}$$

For $p \in A'_{(x,y)}$, $p = ((x + u(p))/m, (y + v(p))/m)$. Let $a \in A_m$ and $p \in A'_a$. It follows from the definitions of τ_1, σ_1 and σ_2 that $\tau_1(p) \in A'_{\sigma_1(a)}$ if $u(p) + v(p) < 1$ and $\tau_1(p) \in A'_{\sigma_2(a)}$ otherwise. Therefore $p \in X' - \tau_1^{-1}(X')$ iff $[p \in X'$ and $\tau_1(p) \notin X']$ iff $[p \in A'_a$ for $a \in X$ and if $u(p) + v(p) < 1$ then $\sigma_1(a) \notin X$ else $\sigma_2(a) \notin X]$ iff $[p \in A'_a$ and if $u(p) + v(p) < 1$ then $a \in X - \sigma_1^{-1}(X)$ else $a \in X - \sigma_2^{-1}(X)]$. Since

$\mu(\{(u, v) | 0 \leqslant u + v < 1\}) = \frac{1}{2}$, $\mu(X' - \tau_1^{-1}(X')) = (1/2n)(|X - \sigma_1^{-1}(X)| + |X - \sigma_2^{-1}(X)|)$. Similarly for τ_2 and σ_3, σ_4. Hence

$$\sum_{i=1}^{2} \mu(X' - \tau_i^{-1}(X')) = \frac{1}{2n} \sum_{i=1}^{4} |X - \sigma_i^{-1}(X)|$$
$$= \frac{1}{2n} \sum_{i=1}^{4} |\sigma_i(X) - X| \tag{2}$$

(σ_i is a permutation). Applying Lemma 2 to X', substituting (2) and (1) for the left and right sides of the inequality of Lemma 2 yields the inequality of Lemma 1. ∎

Lemma 2 follows from Lemma 3 proven below.

LEMMA 3. *For every measurable $X \subseteq A$,*

$$\sum_{i=1}^{2} \mu(X - \tau_i^{-2}(X)) \geqslant 4d_0 \mu(X)\, \mu(X^c).$$

Proof of Lemma 2. For every $X \subseteq A$,

$$X - \tau_i^{-2}(X) \subseteq [(X - \tau_i^{-1}(X)] \cup \tau_i^{-1}[X - \tau_i^{-1}(X)]$$

because $f(A) - f(B) \subseteq f(A - B)$ and $A - B \subseteq (A - C) \cup (C - B)$. Hence if X is measurable $\mu(X - \tau_i^{-2}(X)) \leqslant 2\mu(X - \tau_i^{-1}(X))$ because τ_i and τ_i^{-1} are measure preserving. This and Lemma 3 imply Lemma 2. ∎

If τ is an automorphism of A and f a function on A we define $\tilde{\tau}(f) \equiv f \circ \tau^{-1}$. Lemma 3 follows from Lemma 4 (the functional version) proven below.

LEMMA 4. *For every measurable function ϕ on A with*

$$\int_A \phi = 0, \tag{3}$$

and

$$\int_A |\phi|^2 < \infty, \tag{4}$$

we have:

$$\sum_{i=1}^{2} \int |\tilde{\tau}_i^2(\phi) - \phi|^2 \geqslant 8d_0 \int |\phi|^2.$$ [1]

[1] We will use the abbreviation $\int_A \psi$ for $\int_A \psi(x)\, d\mu(x)$.

A lemma similar to Lemma 4 (with different transformations and with a much smaller constant) was independently proven in [8] (Proposition 3.3).

Proof of Lemma 3. Fix a measurable $X \subseteq A$. Let $\phi = \chi_X - \mu(X)$, where χ is the characteristic function on A. So

$$\phi = \begin{cases} \mu(X^c) & \text{on } X, \\ -\mu(X) & \text{on } X^c. \end{cases}$$

Consequently, $\int_A \phi = 0$ and

$$\int_A |\phi|^2 = \mu(X)\,\mu(X^c) < \infty. \tag{4$'$}$$

So ϕ satisfies the assumptions of Lemma 4 and thus it satisfies its conclusion. Note that for every $Y \subseteq A$, $\tilde{\tau}(\chi_Y) = \chi_{\tau(Y)}$. Thus, $\tilde{\tau}_i^2(\phi) - \phi = \chi_{\tau_i^2(X)} - \chi_X$ and

$$|\tilde{\tau}_i^2(\phi) - \phi|^2 = \begin{cases} 1 & \text{on } (\tau_i^2(X) - X) \cup (X - \tau_i^2(X)), \\ 0 & \text{otherwise.} \end{cases}$$

Hence $\int_A |\tilde{\tau}_i^2(\phi) - \phi|^2 = \mu(\tau_i^2(X) - X) + \mu(X - \tau_i^2(X))$ (the two sets are disjoint). But $\mu(X - \tau_i^2(X)) = \mu(X) - \mu(X \cap \tau_i^2(X)) = \mu(\tau_i^2(X)) - \mu(X \cap \tau_i^2(X)) = \mu(\tau_i^2(X) - X) = \mu(X - \tau_i^{-2}(X))$. (Again we used the fact that τ_i^{-1} is measure preserving.) Hence

$$\int_A |\tilde{\tau}_1^2(\phi) - \phi|^2 = 2\mu(X - \tau_i^{-2}(X)). \tag{5}$$

Substituting (4)$'$ and (5) into the inequality of Lemma 4 yields the inequality of Lemma 3. ∎

Lemma 4 follows from Lemma 5 (the version dealing with infinite series of complex numbers) proven below.

LEMMA 5. *Let* $\{a_{m,n}\}_{-\infty < m,n < \infty}$ *be a system of complex numbers such that*

$$a_{0,0} = 0 \tag{3$'$}$$

and

$$\sum_{m,n} |a_{m,n}|^2 < \infty. \tag{4$''$}$$

Then

$$\sum_{m,n} |a_{m,n+2m} - a_{m,n}|^2 + \sum_{m,n} |a_{m+2n,n} - a_{m,n}|^2 \geqslant 8d_0 \sum_{m,n} |a_{m,n}|^2.$$

Proof of Lemma 4. By (4) $\phi \in \mathscr{L}^2(A)$. So, for $-\infty < m, n < \infty$, $a_{m,n}(\phi)$, the

Fourier coefficient of ϕ with respect to A, exists and $a_{m,n}(\phi) = \int_A \phi(p)\chi_{m,n}(p)\,d\mu(p)$, where $\chi_{m,n}(p) = e^{-2\pi i(mx+ny)}$ $(p = (x, y))$. Also

$$\begin{aligned} a_{m,n}(\bar{\tau}_1^2(\phi)) &= \int_A \phi(\tau_1^{-2}(p))\,\chi_{m,n}(p)\,d\mu(p) \\ &= \int_A \phi(p)\,\chi_{m+2n}(p)\,d\mu(p) \\ &= a_{m+2n,n}(\phi) \end{aligned} \tag{6}$$

because $\chi_{m,n} \circ \tau_1^2 = \chi_{m+2n,n}$. Similarly

$$a_{m,n}(\bar{\tau}_2^2(\phi)) = a_{m,n+2m}(\phi). \tag{7}$$

Consider Lemma 5 with $a_{m,n} \equiv a_{m,n}(\phi)$. By the Parseval equality $(\int |\phi|^2 = \sum_{m,n} |a_{m,n}|^2)$ and by the definition of $a_{0,0}$, (3)′ and (4)″ follow from (3) and (4) respectively. Consequently, the conclusion of Lemma 5 holds and substituting into it (6) and (7) (using the linearity of $a_{m,n}(\phi)$) and the Parseval equality yields the conclusion of Lemma 4. ∎

Proof of Lemma 5. Let $S = \mathbf{Z} \times \mathbf{Z} - \{(0, 0)\}$, where $\mathbf{Z}$ denotes the set of integers. If $T \subseteq S$ let $l_2(T)$ be the set of complex functions f on T satisfying

$$\|f\|_T^2 \equiv \sum_{x \in T} |f(x)|^2 < \infty.$$

Define two permutations ω_1 and ω_2 on S by $\omega_1(m, n) = (m, n + 2m)$ and $\omega_2(m, n) = (m + 2n, n)$. Thus, Lemma 5 can be restated as

CLAIM 1. *For every* $f \in l_2(S)$,

$$\|f - f \circ \omega_1\|_S^2 + \|f - f \circ \omega_2\|_S^2 \geqslant (4 - 2\sqrt{3})\,\|f\|_S^2.$$

We partition S into the $\omega_i^{\pm 1}$ invariant sets $S_m = \{(a, b) \in S \mid gcd(a, b) = m\}$, $m \geqslant 1$ (where $gcd(0, a) = |a|$).

CLAIM 2. *For every real* $f \in l_2(S_1)$,

$$\|f - f \circ \omega_1\|^2 + \|f - f \circ \omega_2\|^2 \geqslant (4 - 2\sqrt{3})\,\|f\|^2 \qquad (\textit{where } \|\ \| = \|\ \|_{S_1}). \tag{8}$$

Claim 1 for a complex function f follows by applying Claim 2 to the real functions

$$(x, y) \mapsto \operatorname{Re} f(mx, my) \qquad \text{and} \qquad (x, y) \mapsto \operatorname{Im} f(mx, my)$$

on S_1 for every $m \geqslant 1$. For $f, g \in l_2(S_1)$, let $\langle f, g\rangle = \sum_{x \in S_1} f(x)\,g(x)$ be the usual inner product. The left-hand side of (8) equals $4\,\|f\|^2 - 2\langle f, f \circ \omega_1\rangle - 2\langle f, f \circ \omega_2\rangle$, so Claim 2 is equivalent to

CLAIM 3. *For every real function $f \in l_2(S_1)$,*

$$2(\langle f, f \circ \omega_1 \rangle + \langle f, f \circ \omega_2 \rangle) \leqslant 2\sqrt{3}\,\|f\|^2.$$

For any $x = (m, n) \in S_1$, define $\|x\| = \max(|m|, |n|)$. Let $\Sigma = \{\omega_1, \omega_1^{-1}, \omega_2, \omega_2^{-1}\}$. By a case analysis one shows

CLAIM 4. *If $\|x\| = 1$, then $\|\sigma(x)\| = \|x\|$ for two $\sigma \in \Sigma$ and $\|\sigma(x)\| > \|x\|$ for the other two. If $\|x\| > 1$, then $\|\sigma(x)\| < \|x\|$ for one $\sigma \in \Sigma$ and $\|\sigma(x)\| > \|x\|$ for the other three.*

Claim 4 implies

CLAIM 5. *For every $x \in S_1$, $\sum_{\sigma \in \Sigma} \lambda(x, \sigma(x)) \leqslant 2\sqrt{3}$, where*

$$\lambda(x, y) = \begin{cases} 1/\sqrt{3} & \text{if } \|x\| < \|y\|, \\ 1 & \text{if } \|x\| = \|y\|, \\ \sqrt{3} & \text{if } \|x\| > \|y\|. \end{cases}$$

Note that $\lambda(x, y)^{-1} = \lambda(y, x)\ \forall x, y \in S_1$.

Proof of Claim 3. If a, b, λ are real numbers and $\lambda > 0$ then $2ab \leqslant \lambda a^2 + b^2/\lambda$ since $(\sqrt{\lambda}\, a - b/\sqrt{\lambda})^2 \geqslant 0$. So $\forall x \in S_1$ and $\sigma \in \Sigma$,

$$2f(x)f(\sigma(x)) \leqslant \lambda(x, \sigma(x))f(x)^2 + \lambda(\sigma(x), \sigma^{-1}(\sigma(x))f(\sigma(x))^2.$$

Summing over $x \in S_1$ and $\sigma \in \{\omega_1, \omega_2\}$ we get

$$\begin{aligned} &2\langle f, f \circ \omega_1 \rangle + 2\langle f, f \circ \omega_2 \rangle \\ &\leqslant \sum_{\sigma \in \Sigma} \sum_{x \in S_1} \lambda(x, \sigma(x))f(x)^2 \\ &= \sum_{x \in S_1} \left(\sum_{\sigma \in \Sigma} \lambda(x, \sigma(x))f(x)^2 \right) \leqslant 2\sqrt{3}\,\|f\|^2 \end{aligned}$$

by Claim 5. ∎

Remark. This proof of Lemma 5 is different from the one we gave in the original version of our paper [4]. The present method enables us to show (in Appendix 2) that

(i) the constant $8d_0 = 4 - \sqrt{12}$ is best possible,

and

(ii) if $a_{m,n}$ are not all zero, then the inequality is strict.

3. Construction of Linear Superconcentrators

The construction includes two parts. In the first we construct a certain kind of bounded concentrators: Let $p > 1$ be a fixed integer, and let $n > 0$ be any natural number such that $np/(p+1)$ is an even square. We construct a bipartite graph with n inputs and $np/(p+1)$ outputs. The inputs are partitioned into two disjoints parts, the big one of size $np/(p+1)$ and the small one of size $l \equiv n/(p+1)$. The big part and the outputs are connected by an $(np/(p+1),\ k,\ 2/(p-1))$ expander. (Since $np/(p+1)$ is a square, for $k=5$ and $p=31$ such an expander was constructed in the previous section because $d_0 \geqslant 1/15$.) Every output is connected to exactly one input in the small part: For every $j = 0,..., p-1$, outputs number $jl+1,..., (j+1)l$ are connected to inputs number $1,..., l$ in the small part.

Lemma 6. *The bipartite graph is an $(n, p/(p+1), k', \frac{1}{2})$ bounded concentrator, where $k' = (k+1)p/(p+1)$.*

Proof. Let A be the set of inputs and let S be the set of inputs in the big part. Let X be any set of inputs with $|X| \leqslant |A|/2$. Let $s = |X \cap S|$ and $t = |X \cap S^c|$. We now show that $|\Gamma_X| \geqslant |X|$. If $t \geqslant |X|/p$ it obviously holds. Otherwise $s \geqslant \lceil (p-1)/p \rceil |X|$. Let Y be any subset of $S \cap X$ of size

$$\hat{s} \equiv \left\lceil \frac{p-1}{p} |X| \right\rceil \leqslant \left\lceil \frac{p-1}{2p} |A| \right\rceil$$

$$= \left\lceil \frac{p^2-1}{2p^2} |S| \right\rceil \leqslant \tfrac{1}{2} |S| \qquad (|S| = np/(p+1) \text{ is even.})$$

By the definition of an expander,

$$|\Gamma_Y| \geqslant \left(1 + \frac{2}{p-1} \frac{1}{2}\right) |Y| = \frac{p}{p-1} \left\lceil \frac{p-1}{p} |X| \right\rceil \geqslant |X|. \quad \blacksquare$$

Lemma 7. *For **all** n we can construct an $(n, p/(p+1) + \varepsilon_n, k', \frac{1}{2})$ bounded concentrator, where $0 \leqslant \varepsilon_n = O(n^{-1/}2)$.*

Proof. Let n' be the smallest integer larger than n such that $n'p/(p+1)$ is an even square. Obviously $n' - n = O(n^{1/2})$. By Lemma 7, we can construct an $(n', p/(p+1), k', \frac{1}{2})$ bounded cocentrator. The desired concentrator is obtained by deleting $n' - n$ inputs (and their incident edges) from the small part. The ratio between the numbers of outputs and inputs is $p/(p+1) + \varepsilon_n$, where

$$0 \leqslant \varepsilon_n = O\left(\frac{n'-n}{n}\right) = O(n^{-1/2}). \quad \blacksquare$$

Using counting argument, Pippenger proved the existence of an $(n, \frac{2}{3}, 6, \frac{1}{2})$ bounded concentrator for n large enough. He then used the latter in a recursive construction to

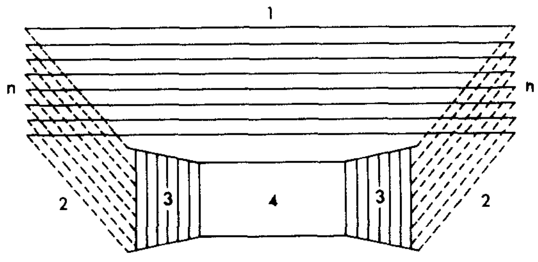

FIG. 1. The construction of the s.c. (1) n direct edges from inputs to outputs; (2) dotted lines represent identification of vertices not edges; (3) two $(n, \theta_n, k, \frac{1}{2})$ bounded concentrators; (4) an s.c. with $\theta_n \cdot n$ inputs and outputs constructed recursively.

derive a family of linear s.c.'s of density 39. An obvious generalization of his construction is stated in the following lemma.

LEMMA 8. *If we can construct for all n an $(n, \theta_n, k, \frac{1}{2})$ bounded concentrator, where $\theta_n = \theta + \varepsilon_n$, $0 \leqslant \theta < 1$, $\varepsilon_n = o(1)$, and $k > 1$, then we can construct a family of linear superconcentrators of density $(2k+1)/(1-\theta)$.*

Proof. The construction is essentially the recursive construction of [7]. Figure 1 describes how to construct an s.c. with n inputs and n outputs from an s.c. with $\theta_n \cdot n$ inputs and outputs. The correctness of the construction is the same as in [7]. Let $C(n)$ be the number of edges of this s.c. Then $C(n) = (2k+1)n + C(\theta_n \cdot n)$, and $C(n) \leqslant c$ for $n \leqslant n_0$. By induction $C(n) \leqslant ((2k+1)/(1-\theta) + \delta_n)n$, where $\delta_n = o(1)$. ∎

From Lemma 7 and 8 we derive the following theorem.

THEOREM 3. *Assuming we can construct for every $n = m^2$ an $(n, k, 2/(p-1))$ expander, then we can construct a family of linear superconcentrators of density $(2k+3)p+1$.*

By the results of the previous section the assumption of the theorem is satisfied by taking $k = 5$, $p = 31$. Therefore we have a family of linear superconcentrators of density 504.

4. IMPROVING THE DENSITY

It follows from Theorem 3 that if expanders with larger d are used, then the superconcentrators will have fewer edges. (p is chosen to be the smallest positive integer with $d \geqslant 2/(p-1)$.) Considering the proof of Theorem 2 we see that we lost a factor of 2 going from Lemma 3 to Lemma 2. We now sketch a way to save this loss.

For $(x, y) \in A_m$ let

$$\begin{aligned}
\sigma_0'(x, y) &= (x, y),\\
\sigma_1'(x, y) &= (x, y + 2x),\\
\sigma_2'(x, y) &= (x, y + 2x + 1),\\
\sigma_3'(x, y) &= (x, y + 2x + 2),\\
\sigma_4'(x, y) &= (x + 2y, y),\\
\sigma_5'(x, y) &= (x + 2y + 1, y),\\
\sigma_6'(x, y) &= (x + 2y + 2, y),
\end{aligned}$$

where $+$ is mod m. These seven permutations yield the bipartite graph G_n'.

LEMMA 1'. *For every $X \subseteq A_m$,*

$$\sum_{\substack{i=1\\ i\neq 2,5}}^{6} |\sigma_i'(X) - X| + 2 \sum_{i=2,5} |\sigma_i'(X) - X| \geqslant 16 d_0 |X|\,|X^c|/n.$$

Lemma 1' follows from Lemma 3 of Section 2 in the same way Lemma 1 followed from Lemma 2. (In this case

$$\mu(X' - \tau_1^{-2}(X')) = (\tfrac{1}{4}\,|X - \sigma_1'(X)| + \tfrac{1}{2}\,|X - \sigma_2'(X)| + \tfrac{1}{4}|X - \sigma_3'(X)|)/n$$

because

$$\mu(\{(u, v) \mid 0 \leqslant v + 2u < 1\}) = \mu(\{(u, v) \mid 2 \leqslant v + 2u < 3\}) = \tfrac{1}{4}$$

and

$$\mu(\{(u, v) \mid 1 \leqslant v + 2u < 2\}) = \tfrac{1}{2},$$

and similarly for $\tau_2, \sigma_4', \sigma_5'$ and σ_6'.) Similarly, Theorem 2' stated in the introduction follows from Lemma 1' in the same way Theorem 2 followed from Lemma 1.

Using the expanders of Theorem 2' in Theorem 3 we get a family of linear s.c.'s of density 273 ($k = 7$, $p = 16$). In Appendix 1 we sketch a way to reduce the density to approximately 271.8. As we noted above, Angluin [2] has derived $(n, 3, d')$ expanders. Using Theorem 2', the best d' we could get is $d_0'/5$ and consequently we do not derive smaller superconcentrators.

5. OPEN PROBLEMS

1. Is there an elementary proof of Theorem 1 or 2 or a similar theorem (something like a clever induction)?

2. Given k, what is the largest d such that (n, k, d) expanders exist or such that we can explicitly construct them?

3. Is there a direct explicit construction for linear superconcentrators?

4. What is the smallest superconcentrator (constructive, and nonconstructive)?

5. Is there a direct construction of explicit linear (unbounded) concentrators, i.e., not using linear superconcentrators? (An obvious way to construct a concentrator is to prune enough edges from a larger superconcentrator.)

6. Is $\log n$ the best depth of a family of linear superconcentrators?

7. What is the size-depth tradeoff for superconcentrators?

8. Is there a linear routing algorithm for our s.c.'s? (i.e., an algrithm that finds the vertex disjoint paths connecting two given subsets of inputs and outputs.) For the routing we need to solve a matching problem, for which no linear time algorithm is known. But in our case, only special graphs arise for which it may be possible to find a better algorithm.

9. Can our techniques be used for other explicit constructions in other cases where the asymptotically best object (network or code) is nonconstructive?

Regarding Problem 4 above, F. R. K. Chung has recently improved the density of Pippenger's nonconstructive s.c.'s to 38.5 [3] and of our constructive s.c.'s to 263 (by improving the construction of Section 3), and, by using the ideas of Appendix 1, the density was further reduced to approximately 261.5.

Regarding Problem 9 above, N. Pippenger has told us that the expanders of Theorem 2′ can be used to give an explicit construction of $O(n \log n)$ nonblocking networks. (The existence of nonconstructive $O(n \log n)$ nonblocking networks is not new.) This bound matches the known lower bound.

APPENDIX 1: SUPERCONCENTRATORS, THERMODYNAMICS AND SELF-REPRODUCING SYSTEMS

We sketch a way to slightly improve the s.c.'s of Section 3. Although the improvement is small, we include it because of the following reason. The construction of Section 3 does not make full use of d_0' $(=2d_0)$. We chose $p = 16$ since this is the smallest integer such that $d_0' \geqslant 2/(p-1)$. The construction required p to be integer. If p could be any real number, then we could choose p such that $d_0' = 2/(p-1)$ and would get density 271.7794... $((2k+3)p+1)$. N. Pippenger asked whether one can modify the construction and achive this density, thus making full use of d_0'. We will sketch below a partial answer to this question. In this case we get density 271.7819.... The reason that even a full use of d_0' would not improve the density by much is that d_0' is very close to 2/15 (0.139... versus 0.1333...). One possible way to improve the density is by improving Theorem 2′, i.e., by constructing (k, d, n) expanders with better k and d. Possibly, we would not be able to get so close to the better d with $2/(p-1)$ for an integer p. In that case the improvement suggested here might be much more useful.

We show how to construct from the expanders of Theorem 2′ an $(n, \theta, \bar{k}, \frac{1}{2})$ bounded concentrator, where $\theta = p'/(p'+1)$, $\bar{k} = (k+1)p'/(p'+1)$ and $15 < p' < 16$. By Theorem 3, we obtain a family of s.c.'s with density $(2k+3)p' + 1 < 273$ ($k = 7, p' < 16$). As in Section 3, the inputs will be divided into a big part of size $np'/(p'+1)$ and small part of size $n/(p'+1)$ and the connection will be done similarly. The only difference is that since p' is not integral, only part of the inputs in the small part will be connected to 16 different outputs. The rest will be connected to only 15.

Consider any set of inputs X with $x \equiv |X|/n \leqslant \frac{1}{2}$. Let $x = x_0 + x_1$, where $x_0 = |X \cap S|/n$ (S is the big part). So $0 \leqslant x_0 \leqslant \theta$ and $0 \leqslant x_1 \leqslant 1 - \theta$. $|\Gamma_{X \cap S}|/n \geqslant x_0[1 + 2d_0(1 - x_0/\theta)] \equiv g_{d_0,\theta}(x_0)$. Also $|\Gamma_{X \cap S^c}|/n = \sup\{15x_1,\ 16x_1 - (16 - 17\theta)\} \equiv f(x_1)$. The first term in the supremum is due to the fact that all inputs in the small part are connected to 15 outputs. The second term is due to the fact that the number of inputs that are not connected to 16 outputs is $(16 - 17\theta)n$ $(16(1-\theta)n - \theta n)$. So in order that this network will be an $(n, \theta, k, \frac{1}{2})$ bounded concentrator, we need the following:

$$\forall x\ 0 \leqslant x \leqslant \tfrac{1}{2}$$

$$\forall x_0, x_1\ x = x_0 + x_1, \qquad 0 \leqslant x_0 \leqslant \theta, \qquad 0 \leqslant x_1 \leqslant 1 - \theta,$$

we have

$$\sup\{f(x_1), g_{d_0,\theta}(x_0)\} \geqslant x. \tag{1}$$

If $f(x_1) \geqslant x$ then (1) holds. Otherwise $f(x_1) < x$, $x_1 < f^{-1}(x)$ and $x_0 > x - f^{-1}(x)$. By choosing θ such that

$$g_{d_0,\theta}(x - f^{-1}(x)) \geqslant x \tag{2}$$

we will have (1). We look for θ_0, the minimal θ that satisfies (2). It turns out that $\theta_0 = 0.9403275$, $p' = 15.92834$ and the density of the s.c. is 271.7819.

By showing that 273 is not the best density, we disprove a possible connection (suggested by Nick Pippneger) between s.c.'s, thermodynamics (−273°C is the absolute zero) and reproduction (273 is the average number of days in pregnancy).

APPENDIX 2: Lemma 5 is Best Possible

We now show that

(i) the constant $8d_0 = 4 - \sqrt{12}$ is best possible,

and

(ii) if $a_{m,n}$ are not all zero, then the inequality is strict.

Proof of (i). We construct a sequence of nonzero real functions f_n, $n \geqslant 1$, in $l_2(S)$ such that

$$\|f_n - f_n \circ \omega_1\|_S^2 + \|f_n - f_n \circ \omega_2\|_S^2 = [4 - 2\sqrt{3} + o(1)]\, \|f_n\|_S^2. \qquad (*)$$

Consequently, Lemma 5 is false for a constant $>8d_0$. The function f_n will vanish outside S_1. As in the reduction of Claim 2 to Claim 3, (*) holds iff

$$Q(f_n) \equiv \langle f_n, f_n \circ \omega_1 \rangle + \langle f_n, f_n \circ \omega_2 \rangle = (\sqrt{3} - o(1))\, \|f_n\|^2.$$

Let G be the directed graph on vertex set S_1 having set of edges $E = \{(x, \sigma(x)) \mid x \in S_1,\ \sigma \in \Sigma,\ \|x\| < \|\sigma(x)\|\}$. (Recall $\Sigma = \{\omega_1, \omega_1^{-1}, \omega_2, \omega_2^{-1}\}$.) G contains exactly eight vertices x with $\|x\| = 1$: $V_0 = \{(\pm 1, 0), (0, \pm 1), (\pm 1, \pm 1)\}$. By Claim 4, each $x \in V_0$ is connected to two distinct vertices with $\|x\| > 1$, and the resulting 16 vertices are roots of complete infinite ternary trees. For all $i > 0$ let V_i be the set of vertices in the $(i-1)$st level of these trees (at distance i from V_0); so $|V_i| = 16 \cdot 3^{i-1}$. Given $n > 0$ define $f_n \colon S_1 \to \mathbf{R}$ (the real numbers)

$$f_n(x) = \begin{cases} |V_i|^{-1/2} & \text{if } x \in V_i,\quad 1 \leqslant i \leqslant n, \\ 0 & \text{otherwise.} \end{cases}$$

$$\|f_n\|^2 = \sum_{i=1}^{n} \sum_{x \in V_i} f_n(x)^2 = \sum_{i=1}^{n} |V_i|\, |V_i|^{-1} = n,$$

and

$$Q(f_n) = \sum_{i=2}^{n} \sum_{\substack{(y,x) \in E \\ x \in V_i, y \in V_{i-1}}} f(x) f(y).$$

The inner sum consists of $|V_i|$ terms each of which equals $|V_i|^{-1/2}\, |V_{i-1}|^{-1/2}$, so it equals $\sqrt{3}$ ($|V_{i-1}| = |V_i|/3$) and $Q(f_n) = (n-1) \cdot \sqrt{3} = [\sqrt{3} - o(1)] \cdot \|f_n\|^2$. ∎

Proof of (ii). By arguing as in the reduction to Claim 3, it suffices to show that if $0 \neq f \in l_2(S_1)$, then the inequality of Claim 3 is strict. If $\exists \xi \in V_0$ with $f(\xi) \neq 0$ then using $\sum_{\sigma \in \Sigma} \lambda(\xi, \sigma(\xi)) = 2 + 2/\sqrt{3} < 2\sqrt{3}$ we see that the final inequality in the proof of Claim 3 is strict. If $f|_{V_0} = 0$ but $f \neq 0$ then since every vertex of G can be reached by a directed path from a vertex in V_0, we see that there exists a pair $(x, \omega_i(x))$ ($i = 1$ or 2) such that exactly one of $f(x)$, $f(\omega_i(x))$ is 0. Then the inequality $(\sqrt{\lambda(x, \omega_i(x)} f(x) - f(\omega_i(x))/\sqrt{\lambda(x, \omega_i(x))})^2 \geqslant 0$, which contributes to the first inequality in the proof of Claim 3, is strict. ∎

ACKNOWLEDGMENTS

Originally we proved Lemma 5 with $d_0 = 1/16$, and later noted that it could be slightly improved. The fact that d_0 could be improved was observed independently also by Nick Pippenger and Andy Odlyzko. Originally, the construction of the s.c.'s depended quadratically on p (or $1/d$) and N. Pippenger conjectured that the dependence should be linear. Subsequently the authors verified his conjecture. He also asked whether it might be possible to use fully d_0'. (Note that $d_0' > 2/15$.) Appendix 1 gives a partial answer to his question. We also thank the referee who suggested how to organize better the proof of Lemma 5.

References

1. A. V. Aho, J. E. Hopcroft, and J. D. Ullman, "The Design and Analysis of Computer Algorithms," Addison-Wesley, Reading, Mass., 1974.
2. D. Angluin, A note on a construction of Margulis, *Inform. Process. Lett.* **8** (1979), 17–19.
3. F. R. K. Chung, On Concentrators, superconcentrators, generalized, and nonblocking networks, *Bell. Sys. Tech. J.* **58** (1978), 1765–1777.
4. O. Gabber and Z. Galil, Explicit constructions of linear size superconcentrators, *in* "Proceedings, 20th Annual IEEE Symposium on Foundations of Computer Science, San Juan, Puerto Rico, November 1979," pp. 364–370.
5. G. A. Margulus, Explicit construction of concentrators, *Problemy Peredači Informacii* **9**, No. 4 (1973), 71–80. (English translation in *Problems Inform. Transmission* (1975).)
6. M. S. Pinsker, On the complexity of a concentrator, *in* "Proceedings, 7th International Telegraffic Conference, Stockholm, June 1973," pp. 318/1–318/4.
7. N. Pippenger, Superconcentrators, *SIAM J. Comput.* **6** (1972), 298–304.
8. K. Schmidt, "Asymptotically Invariant Sequences and an Action of SL(2, Z)," manuscript, Math.Inst., University of Warwick, Coventry, 1979.
9. L. G. Valiant, On nonlinear lower bounds in computational complexity, *in* "Proceedings, 7th Annual ACM Symposium on Theory of Computing, Albuquerque, N.M., May 1975," pp. 45–53.