Smaller Explicit Superconcentrators

(Extended Abstract)

N. Alon * M. Capalbo †

August 14, 2002

Abstract

Using a new recursive technique, we present an explicit construction of an infinite family of N-superconcentrators of density 44. The most economical previously known explicit graphs of this type have density around 60.

1 Introduction

For an integer N, an N*-superconcentrator* Γ_N is a directed acyclic graph with a set X of N inputs (i.e., vertices with indegree 0) and a set Y of N outputs (i.e., vertices with outdegree 0), such that, for any subset S of X, and any subset T of Y satisfying $|S| = |T|$, there are $|S|$ vertex-disjoint directed paths in Γ_N from S to T. Superconcentrators have many applications in Computer Science, and the explicit construction of sparse graphs of this type has been a problem studied extensively. Gaber and Galil [4] presented the first explicit construction of N-superconcentrators with $O(N)$ edges (more precisely, about $270N$ edges). Since then, several researchers [2], [3], [5], [9], and [1] presented constructions of N-superconcentrators using fewer and fewer directed edges. The most economical construction before the one described in the present paper has been obtained from the technique presented in [1], combined with the Ramanujan graphs constructed in [8], and yields a family of N-superconcentrators that have about $60N$ edges. All of these constructions use the same recursive technique, and achieve improvements by using either better explicit expander constructions, or better analysis

*Department of Mathematics, Tel Aviv University, Tel Aviv 69978, Israel. E-mail: nogaa@post.tau.ac.il.
Research supported in part by a USA Israeli BSF grant, by a grant from the Israel Science Foundation and by the Hermann Minkowski Minerva Center for Geometry at Tel Aviv University.
†Institute for Advanced Study, Princeton, NJ 08540. Supported by NSF grant CCR98210-58. E-mail: mrc@ias.edu.

of known expander constructions. The best known lower bound for the number of edges of an N-superconcentrator is only $(5 - o(1))N$, proved by Lev and Valiant in [6].

In this paper we present a construction of a family of N-superconcentrators Γ_N with only $44N + O(1)$ edges. This is done by introducing a new recursive technique, and by combining it with appropriate extended double covers of Ramanujan expanders. In §2 we briefly describe the Ramanujan graphs needed here, and in §3 we give the construction of the graphs Γ_N. The proof of the main result, that each Γ_N is indeed an N-superconcentrator, is given in §4.

Our notation is mostly standard. For a graph $G = (V(G), E(G))$, and for a set $S \subseteq V(G)$, let $\mathcal{N}_G(S)$ denote the set of vertices in G that are adjacent in G to at least one vertex in S. If M is a matching in G, v is a vertex of G, and S is a subset of vertices of G, we say that M *covers* v if v is incident with an edge in M. M *saturates* S if it covers every vertex of S.

For an undirected graph $\Lambda = (X, E)$, where $X = \{x_1, ..., x_N\}$ is a set of N vertices, the *extended double cover* of Λ is the bipartite graph Λ' with parts $Y = \{y_1, ..., y_N\}$ and $Z = \{z_1, ..., z_N\}$, where $y_\iota z_{\iota'}$ is an edge in Λ' if and only if either $\iota = \iota'$, or $x_\iota x_{\iota'}$ is an edge in Λ. Thus, if Λ is k-regular, then its extended double cover Λ' is $k+1$-regular.

A graph is called *Ramanujan* if it is d-regular for some $d > 2$, and the absolute value of each eigenavlue of its adjacency matrix besides the largest one, is at most $2\sqrt{d-1}$.

For a group G and a subset Σ of G, where $\pi \in \Sigma$ if and only if $\pi^{-1} \in \Sigma$, the *Cayley graph* Λ' on G *with respect to* Σ is the $|\Sigma|$-regular graph whose vertex-set is G, and whose edge-set is $\{\{\nu, \pi\nu\} | \ \nu \in G$ and $\pi \in \Sigma\}$. The elements $\pi \in \Sigma$ are the *generators* of Λ', and Σ is the set of generators of Λ'. If Σ generates G, then Λ' is connected; otherwise, the components of Λ' are the right cosets of the subgroup S of G generated by Σ (i.e., the sets of the form $\{sg | s \in S\}$). If H is a subgroup of G, the *Schreier graph* $(G; G/H; \Sigma)$ is the graph whose vertices are the left cosets of H, where sH and $s'H$ are adjacent if there exists a $\pi \in \Sigma$ such that $\pi s H = s'H$.

2 An Auxiliary Construction

We need an infinite series of explicit 9-regular Ramanujan graphs $\Lambda_1, ..., \Lambda_l, \Lambda_{l+1}, ...$ such that Λ_{l+1} has exactly twice as many vertices as Λ_l. The construction in [9] gives us 9-regular Ramanujan graphs but not in the sizes that we need. Thus we present the following modification shown to us by A. Lubotzky.

Theorem 2.1 (A. Lubotzky [7]) *There exists an explicit family of 9-regular Ramanujan graphs on* $k \times 2^{l-1}$ *vertices, where* $k = 64 \times 65 \times 63 = 262,080$*, and* $l = 0, 1, 2, \ldots$.

Proof: We first construct an explicit family $\mathcal{H}'$ of 9-regular Ramanujan graphs on $k \times 2^{18l-18}$ vertices, for each integer l. Then we construct $\mathcal{H}$ from $\mathcal{H}'$.

To construct $\mathcal{H}'$, let $g(x)$ be an irreducible polynomial of degree 2 in $F_8[x]$, where F_8 denotes the field on 8 elements. For each nonnegative integer l, the graph $\Lambda_l' \in \mathcal{H}'$ is the Cayley graph on $H_l = PGL_2(K_l)$ where $K_l = F_8[x]/g^l(x)F_8[x]$ with respect to the set Σ_l of generators, specified below. The number of vertices of this graph is $k \times 2^{18l-18}$, where k is as above. To see this, note that K_1 is the finite field with 64 elements, and there are precisely $(64^2-1)(64^2-64)$ two by two invertible matrices over it. This is, therefore, the number of ways to choose the entries of an invertible two by two matrix over K_l modulo $g(x)$. Knowing these, there are $8^{(2l-2)4}$ ways to choose the actual entries, and this way we obtain all the invertible matrices over K_l. Since K_l contains $8^{2l} - 8^{2l-2}$ elements which are not divisible by $g(x)$, this implies that the cardinality of $PGL_2(K_l)$ is $(64^2-1)(64^2-64)8^{(2l-2)4}/(8^{2l}-8^{2l-2}) = k2^{18l-18}$.

To specify Σ_l, first fix a γ in F_8 such that the resulting polynomial $q(x) = x^2 + x + \gamma$ is irreducible in $F_8[x]$. Next, let β_l be a root of $q(x)$ in $F_8[x]/g^l(x)F_8[x] = K_l$ (we prove the existence of a root of $q(x)$ in each K_l in the Appendix). Let Σ_l be the following 9-element subset of H_l.

$$\Sigma_l = \left\{ \begin{pmatrix} 1 & \varepsilon + \delta\beta_l \\ (\varepsilon + \delta\beta_l + \delta)x & 1 \end{pmatrix} | \delta, \varepsilon \in F_8; \quad \varepsilon^2 + \varepsilon\delta + \delta^2\gamma = 1 \right\}. \tag{1}$$

It is easy to check that Σ_l has 9 elements and that each element of it is of order 2 in $PGL_2(K_l)$. This completes the description of all graphs $\Lambda_l' \in \mathcal{H}'$. By the proof in [9], each $\Lambda_l \in \mathcal{H}'$ is Ramanujan.

To construct $\mathcal{H}$ from $\mathcal{H}'$, we do the following. Let φ be the following mapping

$$\pi = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \mapsto \begin{pmatrix} a_{11}' & a_{12}' \\ a_{21}' & a_{22}' \end{pmatrix} \tag{2}$$

from H_{l+1} to H_l, where $a_{ij}' = a_{ij} \bmod g^l(x)$ for each $i, j \in \{1, 2\}$. Then φ is a surjective mapping and a group homomorphism, and the kernel of φ is H', where

$$H' = \left\{ \begin{pmatrix} 1 + g^l(x)s(x) & g^l(x)r(x) \\ t(x)g^l(x) & 1 \end{pmatrix} | r(x), s(x), t(x) \in F_8[x]/g(x)F_8[x] \right\}. \tag{3}$$

H' is a group, and is isomorphic to F_2^{18}, where addition in F_2^{18} corresponds to multiplication in H'. Thus, for each positive integer $c \leq 18$, there is a subgroup H_c of H with 2^c elements. Also, if π and π' are distinct elements in Σ_{l+1}, then $\varphi(\pi) \neq \varphi(\pi')$, as shown in the appendix.

Thus, for each positive integer $c \leq 18$, the Schreier graph $(H_{l+1}; H_{l+1}/H_c'; \Sigma_{l+1})$ is 9-regular, Ramanujan, and has $k \times 2^{18l-c}$ vertices. The construction of a 9-regular Ramanujan graph Λ_l on $k \times 2^l$ vertices for each $l \geq 0$ follows. ∎

3 Explicit Superconcentrators

Here we construct an infinite family of N-superconcentrators with $44N + O(1)$ edges for each N of the form $k \times 2^l$, and each nonegative integer l. Let Γ_k be any explicit k-superconcentrator from [1] or [5] (since $k = O(1)$, the exact size of Γ_k does not really matter). We next present the construction of Γ_N for each N of the form $k \times 2^l$, and each positive integer l.

THE CONSTRUCTION OF Γ_N.
Let X and Y be disjoint sets of N vertices each. The input and output sets of Γ are X and Y respectively. Let $X' = \{x'_1, ..., x'_N\}$ and $Y' = \{y'_1, ..., y'_N\}$ be disjoint sets of N vertices each.

The edges in Γ_N between X and X' form the extended double cover Λ_X of a 9-regular Ramanujan graph (explicitly constructed in Theorem 2.1), where each edge is directed from X to X'. Similarily, the edges in Γ_N from Y' to Y form the extended double cover Λ_Y of a 9-regular Ramanujan graph , where each edge is directed from Y' to Y. In addition, for each $\iota \in \{1, .., N/2\}$, the arcs $(x'_{\iota+N/2}, y'_\iota)$, $(x'_{\iota+N/2}, x'_\iota)$, $(x'_\iota, y_{\iota+N/2})$, and $(y'_\iota, y'_{\iota+N/2})$ are in Γ_N.

Put $X'' = \{x'_\iota \in X' | \iota \in \{1, ..., N/2\}\}$, and $Y'' = \{y'_\iota \in Y' | \ \iota \in \{1, ..., N/2\}\}$. The remaining edges of Γ_N form a digraph with input set X'' and output set Y'', which is isomorphic to $\Gamma_{N/2}$, and is vertex-disjoint from X, Y, $Y' \setminus Y''$, and $X' \setminus X''$.

The rest of this paper is devoted to proving the following theorem.

Theorem 3.1 *Γ_N has $44N + O(1)$ edges, and is an N-superconcentrator, with input set X and output set Y.*

4 The Proof of Theorem 3.1

By construction, the number of edges $f(N)$ of Γ_N satisfies $f(N) = (2 \cdot 10 + 2)N + f(N/2)$, implying the claim about the number of edges of Γ_N.

To prove the main part of Theorem 3.1, we use induction; that is, we assume that $\Gamma_{N/2}$ is an $N/2$-superconcentrator, and show that Γ_N is an N-superconcentrator. Let S be any subset of X, and let T be any subset of Y such that $|S| = |T|$. We first show that:
(A) there is a set $\mathcal{P}$ of vertex-disjoint directed paths in Γ_N in $X \cup X' \cup Y \cup Y'$ such that
(i) each vertex in $S \cup T$ is an endpoint of exactly one $P \in \mathcal{P}$, and
(ii) each $P \in \mathcal{P}$ is either (a) from S to T, or (b) from S to X'', or (c) from Y'' to T.
Then **(A)**, together with our inductive hypothesis that $\Gamma_{N/2}$ is an $N/2$-superconcentrator, imply that Γ_N is an N-superconcentrator.

We next show the existence of such a $\mathcal{P}$. We make the following claim.

Lemma 4.1 *Let S be any subset of X, and let T be any subset of Y where $|S| = |T|$. Suppose there exist matchings $M^*_S \subset \Lambda_X$ and $M^*_T \subset \Lambda_Y$ such that both M^*_S and M^*_T have $|S| = |T|$ edges, and M^*_S and M^*_T satisfy properties (1) and (2), stated below.*
(1) M^*_S saturates S, and M^*_T saturates T.
(2) Let ι be an arbitrary integer in $\{1, 2, ..., N/2\}$. Then if M^*_S covers both x'_ι and $x'_{\iota+N/2}$, then M^*_T covers at least one vertex of $\{y'_\iota, y'_{\iota+N/2}\}$. Similarly, if M^*_T covers both y'_ι and $y'_{\iota+N/2}$, then M^*_S covers at least one of $\{x'_\iota, x'_{\iota+N/2}\}$.

Then there exists a collection $\mathcal{P}$ of vertex-disjoint paths in Γ_N in $X \cup X' \cup Y' \cup Y$ that satisfies **(A)**.

Proof: Let X'_S be the set of vertices $x' \in X'$ that are covered by an edge in M^*_S, and let Y'_T be the set of vertices $y' \in Y'$ that are covered by an edge in M^*_T. For each $\iota \in \{1, 2, ..., N/2\}$, let W_ι be the set of 4 vertices x'_ι, $x'_{\iota+N/2}$, y'_ι, $y'_{\iota+N/2}$. Because M^*_S and M^*_T satisfy (1), to prove Lemma 4.1, it suffices to prove the following statement.
For each W_ι, there exists a collection $\mathcal{P}_\iota$ of vertex-disjoint directed paths P (some of which may be of length 0) in $\Gamma_N \cap W_\iota$ such that
(i′) each vertex in $(X'_S \cup X'_T) \cap W_\iota$ is the endpoint of exactly one $P \in \mathcal{P}_\iota$,
(ii′) each $P_\iota \in \mathcal{P}_\iota$ is either (a) from X'_S to X'', or (b) from Y'' to Y'_T, or (c) from X'_S to X'_T.
This is easy to prove by exhaustive search, since W_ι has only 4 vertices. Indeed, one can easily check that unless either (*) $X'_T \cap W_\iota$ has 2 vertices and $X'_S \cap W_\iota$ none, or (**) $X'_S \cap W_\iota$ has 2 vertices and $X'_T \cap W_\iota$ none, there does exist such a $\mathcal{P}_\iota$. But because M^*_S and M^*_T satisfy (2), we are assured that neither (*) nor (**) happens, and so Lemma 4.1 follows. ∎

With Lemma 4.1 in mind, we devote the rest of this section to proving the following proposition.

Proposition 4.2 *Let S be any subset of X, and let T be any subset of Y where $|S| = |T|$. Then there exist matchings $M^*_S \subset \Lambda_X$ and $M^*_T \subset \Lambda_Y$ with $|S| = |T|$ edges each that satisfy (1) and (2) of Lemma 4.1.*

We first prove Lemma 4.3 stated below, and then use it to establish Proposition 4.2.

Lemma 4.3 *Let S and T be as in Proposition 4.2. Then there exist matchings M_S and M_T, and a subset I of $\{1, ..., N\}$ that satisfy the following properties.*
(1) Each edge in M_S is incident with a vertex in S, and each edge in M_T is incident with a vertex in T.
(2) Let X'_I denote the subset of X' of the form $\{x'_\iota | \iota \in I\}$, and let Y'_I denote the subset of Y' of the form $\{y'_\iota | \iota \in I\}$. Then M_S saturates X'_I and M_T saturates Y'_I.
(3) Let α be the number between 0 and 1 such that $|S| = |T| = \alpha|N|$. If α satisfies $1/4 \leq \alpha \leq 1/2$, then $|I|$ is at least $(\alpha - 1/4)N$. If α is larger than 1/2, then $|I|$ is at least $(\alpha - (1-\alpha)/2)N$.

The proof of Lemma 4.3 uses the following lemma.

Lemma 4.4 *Let $\bar{\Lambda}$ be the extended double cover of a 9-regular Ramanujan graph with N vertices, and let X and Y denote its parts, where $|X| = |Y| = N$. Let S be a subset of X, and let α be such that $|S| = \alpha N$. Then the following hold.*
If $\alpha \leq 1/4$, then $|\mathcal{N}_{\bar{\Lambda}}(S)|$ is at least $2|S|$.
If $1/4 \leq \alpha \leq 1/2$ then $|\mathcal{N}_{\bar{\Lambda}}(S)|$ is at least $|S| + N/4$.
If $1/2 \leq \alpha$ then $|\mathcal{N}_{\bar{\Lambda}}(S)|$ is at least $|S| + (1-\alpha)N/2$.

Lemma 4.4 is proved using the technique in [1]. The following lemma is a restatement of Theorem 2.1 in [1].

Lemma 4.5 *Let $G = (V, E)$ be a d-regular graph on N vertices, and suppose that the second largest eigenvalue of the adjacency matrix of G is at most λ. Define $a = \frac{d-\lambda}{2d}$, $b = \frac{1+2a}{4a}$. Let $S \subset V$ be a set of vertices of G, and let $W = \mathcal{N}_G(S) - S$ be the set of all neighbors of S that lie outside S. Put $|S| = \alpha N$ and $|W| = wN$. Then*

$$w^2 - 2(1 - 2\alpha - b)w - 4\alpha(1-\alpha) \geq 0. \tag{4}$$

Note that if G is as in Lemma 4.5, and H is the extended double cover of G, then for every set of vertices $S \subset X$ satisfying $|S| = \alpha N$ and $|\mathcal{N}_H(S)| = (\alpha + w)N$ the inequality (4) holds. In Lemma 4.4 we start with a 9-regular Ramanujan graph on N vertices. As it is Ramanujan, its second largest eigenvalue is at most $2\sqrt{8}$. Therefore, in the notation of Lemma 4.5, $a = \frac{9-2\sqrt{8}}{18} = 0.18573$ and $b = \frac{1+2a}{4a} = 1.846038$. Let S and W be as in Lemma 4.5, suppose $|S| = \alpha N$ and $|W| = wN$. Substituting in (4) we get:

$$w^2 + (1.6920754 + 4\alpha)w - 4\alpha(1-\alpha) \geq 0. \tag{5}$$

Therefore, in order to complete the proof of Lemma 4.4 it suffices to prove the following.

Lemma 4.6 *Let α and w be two reals in $[0, 1]$ and suppose (5) holds. Then:*
(i) If $\alpha \leq 1/4$ then $w \geq \alpha$.
(ii) If $1/4 \leq \alpha \leq 1/2$ then $w \geq 1/4$.
(iii) If $\alpha \geq 1/2$ then $w \geq \frac{1-\alpha}{2}$.

Proof: For every fixed $\alpha \in [0, 1]$ the left hand side of (5), which is

$$f(w) = w^2 + (1.6920754 + 4\alpha)w - 4\alpha(1-\alpha)$$

is a strictly increasing function of w for $w \in [0, 1]$. Therefore, it suffices to prove the following:
(i') If $0 \leq \alpha \leq 1/4$, then

$$f(\alpha) = \alpha^2 + (1.6920754 + 4\alpha)\alpha - 4\alpha(1-\alpha) \leq 0. \tag{6}$$

(ii') If $1/4 \le \alpha \le 1/2$ then

$$f(1/4) = 1/16 + (1.6920754 + 4\alpha)1/4 - 4 \cdot \alpha(1-\alpha) \le 0. \tag{7}$$

(iii') If $1/2 \le \alpha \le 1$, then

$$f(\frac{1-\alpha}{2}) = (\frac{1-\alpha}{2})^2 + (1.6920754 + 4\alpha)\frac{1-\alpha}{2} - 4\alpha(1-\alpha) \le 0. \tag{8}$$

These inequalities can be checked routinely. The left hand side of (6) is non-positive for all $\alpha \in [0, 0.2564]$ (and hence for all $\alpha \in [0, 1/4]$) the left hand side of (7) is non-positive for all $\alpha \in [0.236314, 0.51368]$ (and hence for all $\alpha \in [1/4, 1/2]$), and the left hand side of (8) is non-positive for all $\alpha \in [0.4872, 1]$ (and hence for all $\alpha \in [1/2, 1]$). This completes the proof, and hence implies the assertion of Lemma 4.4 as well. ∎

We now use Lemma 4.4 together with Menger's Theorem to prove the existence of I, M_S and M_T that satisfy (1)–(3) of Lemma 4.3, and then this lemma will follow. Let $U' = \{u'_1, ..., u'_N\}$ and $V' = \{v'_1, ..., v'_N\}$ be disjoint sets, each of N vertices. Let G' be the following graph on $S \cup U' \cup V' \cup T$. Every edge in G' is either directed from S to U', or from U' to V', or from V' to T. First, $G[S \cup X']$ is isomorphic to $\Lambda_X[S \cup X']$; (x, u'_ι) in an edge in G' if and only if (x, x'_ι) is in Γ_N (and $x \in S$). Secondly, $G'[U' \cup V']$ is a matching; $(u'_\iota, v'_{\iota'})$ is an edge in G' if and only if $\iota = \iota'$. Thirdly, $G[Y' \cup T]$ is isomorphic to $\Lambda_Y[Y' \cup T]$; (v'_ι, y) is an edge in G' if and only if (y'_ι, y) is an edge in Γ_N (and $y \in T$). Note that the maximum possible number of vertex-disjoint paths from S to T is the maximum possible cardinality of I in Lemma 4.3. By Menger's Theorem

(*) the maximum possible size of I is equal to the minimum possible cardinality of a set of vertices C that separates S and T in G'.

Let C be a minimum size separating set, and let $a, b, c, d \in [0, 1]$ satisfy $|C \cap S| = aN$; $|C \cap U'| = bN$; $|C \cap V'| = cN$, and $|C \cap T| = dN$.

Consider two possible cases.

Case 1: $1/4 \le \alpha \le 1/2$. Then we may assume that both a and d are no larger than $\alpha - 1/4$, or we are done by **(*)**. Thus, by Lemma 4.4, if C is indeed a cut-set, then $2\alpha - a - d - 1/2$ must be no larger than $b + c$. (Proof: any subset $\tilde{S}$ of S having $(\alpha - a)|N|$ vertices must have at least $(\alpha - a + 1/4)N$ neighbors in G' in U'. Similarily, any subset $\tilde{T}$ of T having $(\alpha - d)|N|$ vertices must have at least $(\alpha - d + 1/4)N$ neighbors in V'. Thus $C \cap (U' \cup V')$ must have at least $(\alpha - a + 1/4)N + (\alpha - d + 1/4)N - N$ vertices if C indeed separates S and T in G'.) But this implies that $a + b + c + d$ must be a least $2(\alpha - 1/4)$, showing that $|C|$ must be at least $2(\alpha - 1/4)N$. By **(*)** the assertion of Lemma 4.3 follows in this case.

Case 2: $1/2 \le \alpha$. In this case we may assume that both $\alpha - a$ and $\alpha - d$ are at least $(1-\alpha)/2$. Then $2\alpha - a - d + (1 - \alpha) - 1$ must be no larger than $b + c$. (Proof: It follows from Lemma 4.4 that if $\tilde{S}$ is any subset of S of at least $(1 - \alpha)N/2$ vertices, then there must be at least

$|\tilde{S}| + (1-\alpha)N/2$ neighbors in G' of $\tilde{S}$ in U'. Similarily, if $\tilde{T}$ is any subset of T with at least $(1-\alpha)N/2$ vertices, then there must be at least $|\tilde{T}| + (1-\alpha)N/2$ neighbors in G' of $\tilde{T}$ in V'. The desired estimate follows as in Case 1.) This implies that $\alpha \le a+b+c+d$. Thus, by **(*)**, the assertion of Lemma 4.3 follows in this case as well, and so Lemma 4.3 follows. ∎

We now use Lemma 4.3 to complete the proof of Proposition 4.2. We prove that there exist matchings $M_S^* \subset \Lambda_X$ and $M_T^* \subset \Lambda_Y$ with $|S| = |T|$ edges each that satisfy (1) of Lemma 4.1, and that satisfy (A) and (B), stated below.

(A) M_S^* saturates X_I', and M_T^* saturates Y_I'.

(B) Let ι be an arbitrary integer in $\{1,...,N/2\}$ such that neither ι nor $\iota + N/2$ is in I. Then M_S^* covers at most one of x_ι', $x_{\iota+N/2}'$, and M_T^* covers at most one of y_ι', $y_{\iota+N/2}'$.

Then M_S^* and M_T^* will satisfy (2) of Lemma 4.1 as well, and Proposition 4.2 will follow.

Now let M_S, M_T, and I satisfy (1)–(3) of Lemma 4.3, and let X_I' and Y_I' be as in (2) of Lemma 4.3. To show that there exist M_S^* and M_T^* as needed, let G be the graph $\Lambda_X[S \cup X']$. Next, let $\hat{\Lambda}_X$ be the graph formed from G by identifying x_ι' with $x_{\iota+N/2}'$ if and only if neither the integer ι nor $\iota + N/2$ is in I. Construct $\hat{\Lambda}_Y$ in an analogous fashion. Thus, matchings in $\hat{\Lambda}_X$ and $\hat{\Lambda}_Y$ that saturate both S and X_I' simultaneously, and T and Y_I' simultaneously respectively, correspond to matchings in Λ_X and Λ_Y with $|S|$ edges each that satisfy both (1) of Lemma 4.1 and (A) and (B), and thus, (2) of Lemma 4.1. Hence, to finish the proof of Proposition 4.2, it suffices to prove that

(C) there exist matchings in $\hat{\Lambda}_X$ and $\hat{\Lambda}_Y$ that saturate both S and X_I' simultaneously, and T and Y_I' simultaneously, respectively.

This is done next. We first show a statement that seems a priori weaker than (C), namely

(D) there exist matchings in $\hat{\Lambda}_X$ and $\hat{\Lambda}_Y$ that saturate S and T respectively, and there exist (a possibly different set of) matchings in $\hat{\Lambda}_X$ and $\hat{\Lambda}_Y$ that saturate X_I' and Y_I' respectively.

We claim that (D) implies (C). Indeed, suppose M_1 is a matching in $\hat{\Lambda}_X$ that saturates S and M_2 a matching that saturates X_I'. Let C be a component of the union $M_1 \cup M_2$, and let P be the set of edges of $M_1 \cup M_2$ incident to a vertex in C. It is not difficult to check that there is a subset S_C of edges of P that saturates $C \cap (X_I' \cup S)$. The union $\cup_C S_C$, where C ranges over the components of $M_1 \cup M_2$, is a matching that covers every vertex of X_I' and S. A similar statement holds in $\hat{\Lambda}_Y$. Thus (D) implies (C).

Having shown that (D) implies (C), we now prove (D). Since M_S, M_T, and I satisfy (1) and (2) of Lemma 4.3, there exist matchings in $\hat{\Lambda}_X$ and $\hat{\Lambda}_Y$ that saturate X_I' and Y_I' respectively. Therefore, to prove (D), all we need to show now is that there exist matchings in $\hat{\Lambda}_X$ and $\hat{\Lambda}_Y$ that saturate S and T respectively. We do this next, using the fact that I satisfies (3) of Lemma 4.3 as well. By Hall's Theorem, there exist such matchings if, for each subset S_0 of S, and each subset T_0 of T, $|\mathcal{N}_{\hat{\Lambda}_X}(S_0)| \ge |S_0|$, and $|\mathcal{N}_{\hat{\Lambda}_Y}(T_0)| \ge |T_0|$. But we note that

$$|\mathcal{N}_{\hat{\Lambda}_X}(S_0)| \geq |\mathcal{N}_{\Lambda_X}(S_0) \cap X'_I| + |\mathcal{N}_{\Lambda_X}(S_0) \cap (X' \setminus X'_I)|/2. \tag{9}$$

We now consider 2 cases.

Case 1: $\alpha \leq 1/2$, where $|S| = \alpha N$, as before. The case when $|S_0|$ is no larger than $N/4$ can be handled easily using Lemma 4.4. If $|S_0|$ is at least $N/4$, then by Lemma 4.4, $|\mathcal{N}_{\Lambda_X}(S_0)|$ is at least $|S_0| + N/4$. Also, $|I|$ is at least $(\alpha - 1/4)N$ because I satisfies (3) of Lemma 4.3. So $|\mathcal{N}_{\Lambda_X}(S_0) \cap X'_I| \geq |S_0| - N/4$, because at most $N/4$ vertices in S are not matched by M_S to a vertex in X'_I (as M_S and I satisfy (1) and (2) of Lemma 4.3). Together these imply that $|\mathcal{N}_{\hat{\Lambda}_X}(S_0)| \geq |S_0|$. Similarily, $|\mathcal{N}_{\hat{\Lambda}_X}(T_0)| \geq |T_0|$. This implies (D) for the case $\alpha \leq 1/2$.

Case 2: $\alpha \geq 1/2$. Then we may assume that $|S_0| \geq (1-\alpha)|N|/2$. By Lemma 4.4, we see that $|\mathcal{N}_{\Lambda_X}(S_0)|$ is at least $|S_0| + (1-\alpha)N/2$. Also, $|I|$ is at least $(\alpha - (1-\alpha)/2)N$ because I satisfies (3) of Lemma 4.3. So $|\mathcal{N}_{\Lambda_X}(S_0) \cap X'_I| \geq |S_0| - (1-\alpha)N/2$ because at most $(1-\alpha)N/2$ vertices in S are not matched by M_S to a vertex in X'_I (because M_S and I satisfy (1) and (2) of Lemma 4.3). Together these imply that $|\mathcal{N}_{\hat{\Lambda}_X}(S_0)| \geq |S_0|$. Similarily, $|\mathcal{N}_{\hat{\Lambda}_Y}(T_0)| \geq |T_0|$. This implies (D) for the case when $\alpha \geq 1/2$ as well, and so (D) follows.

As we have shown, (D) implies (C), which implies Proposition 4.2 by (**). ■

Proposition 4.2 and Lemma 4.1 imply Theorem 3.1. ■

Acknowledgment We would like to thank Alex Lubotzky for helpful discussions.

References

[1] N. Alon, Z. Galil, V.D. Milman, Better expanders and superconcentrators, *J. Algorithms* 8 (1987), 337–347.

[2] N. Alon, V.D. Milman, λ_1, isoperimetric inequalities for graphs and superconcentrators, *J. Combinatorial Theory* **B** 38 (1985), 77–88.

[3] M. Buck, Expanders and diffusers, *SIAM J. Algebraic and Disc. Meth.* 7 (1986), 282–304.

[4] O. Gabber and Z. Galil, Explicit construction of linear-sized superconcentrators, *FOCS* 1979, 364–370.

[5] A. Jimbo and A. Maruoka, Expanders obtained from affine transformations, *Combinatorica* 7 (1987), 343–345.

[6] G. Lev and L. G. Valiant, Size bounds for superconcentrators, *Theoret. Comput. Sci.* 22 (1983), 233–251.

[7] A. Lubotzky, personal communication.

[8] A. Lubotzky, R. Phillips, and P. Sarnak, Ramanujan graphs, *Combinatorica* 8 (1988), 261–277.

[9] M. Morgenstern, Existence and explicit Construction of q+1-regular Ramanujan graphs for every prime power q, *J. Comb Theory B* 62 (1994), 44–62.

5 Appendix

For completeness, we include here the proofs of a few simple results mentioned in §2.

Proposition 5.1 *Let $q(x) = x^2 + x + \gamma$ be an irreducible polynomial in $F_8[x]$, and let $g(x)$ be any other irreducible polynomial of degree 2 in $F_8[x]$. Then for each positive integer l, there is a root β_l of $q(x)$ in the ring $K_l = F_8[x]/g^l(x)F_8[x]$. Furthermore, we can find such a β_l efficiently.*

Proof: Observe, first, that as $K_1 = F_8[x]/g(x)F_8[x]$ is the unique finite field with $8^2 = 64$ elements, it contains the roots of every irreducible polynomial of degree 2 over F_8, and hence contains a root β_1 of $q(x)$ in the field K_1.

To complete the proof of Proposition 5.1, apply induction on l. Let l be any positive integer. We assume that there exists a root β_l of $q(x)$ in K_l, or equivalently, there exists a $\beta_l \in F_8[x]$ such that $q(\beta_l) \equiv 0 \bmod g^l(x)$. Now let β_{l+1} be the element in $F_8[x]$ such that $\beta_{l+1} = \beta_l + r(x)g^l(x)$, where $r(x) = r$ is a polynomial of degree at most 1 in $F_8[x]$ to be determined later. Then

$$q(\beta_{l+1}) = q(\beta_l) + r(x)g^l(x) + r^2(x)g^{2l}(x). \tag{10}$$

But if l is positive, then $2l \geq l+1$. Also, as $q(\beta_l) \equiv 0 \bmod g^l(x)$, it follows that $q(\beta_l) \equiv \tilde{r}(x)g^l(x) \bmod g^{l+1}(x)$ for some $\tilde{r}(x)$ in $F_8[x]$ of degree at most 1. Set $r(x) = \tilde{r}(x)$ to conclude that $q(\beta_{l+1}) \equiv 0 \;\; mod \;\; g^{l+1}(x)$. Obviously, this proof yields an efficient algorithm as well. ■

Claim: Let Σ_{l+1} and φ be as in §2. If π and π' are distinct elements in Σ_{l+1}, then $\varphi(\pi) \neq \varphi(\pi')$.
Proof: For any two polynomials $s(x), t(x) \in F_8[x]$, say that $t(x)$ is a *multiple* of $s(x)$ if $t(x) = r(x)s(x)$, for some polynomial $r(x) \in F_8[x]$. Let π and π' be two distinct elements in Σ_{l+1} and suppose that $\varphi(\pi) = \varphi(\pi')$. Then for some $\delta, \epsilon \in F_8$, where at least one is nonzero, $\epsilon + \delta\beta_{l+1}$ is a multiple of $g^l(x)$. We may assume that δ is nonzero, and by dividing, if needed, that $\delta = 1$. Hence $\beta_{l+1} + \epsilon$ is a multiple of $g^l(x)$. Now let us write $q(x) = (x + \epsilon)x + r(x)$, where $r(x)$ is a polynomial in $F_8[x]$ that has degree at most 1. Because q is irreducible in $F_8[x]$, $r(x)$ is not a multiple of $x + \epsilon$. However, then $r(\beta_{l+1})$ is a multiple of $g^l(x)$ because $q(\beta_{l+1})$ is a multiple of $g^l(x)$ (by the definition of β_{l+1}) and so is $\beta_{l+1} + \epsilon$. But since $r(x)$ is not a multiple of $x + \epsilon$, this implies that ϵ' is a multiple of $g^l(x)$ for some nonzero $\epsilon' \in F_8$, which is impossible.