EXPLICIT CONSTANT-DEGREE UNIQUE-NEIGHBOR EXPANDERS

Michael Capalbo *

August 14, 2002

Abstract

Here we solve a long-standing open problem by presenting the first explicit constructions of an infinite family $\mathcal{F}$ of bounded-degree 'unique-neighbor' expanders Γ; i.e., there are strictly positive constants α and ϵ, such that all $\Gamma = (X, Y, E(\Gamma)) \in \mathcal{F}$ satisfy the following properties. The output set Y has cardinality $21|X|/22$, and for each subset S of X with no more than $\alpha|X|$ vertices, there are at least $\epsilon|S|$ vertices in Y that are adjacent in Γ to exactly one vertex in S. Also, the construction of $\mathcal{F}$ is simple to specify, and each $\Gamma \in \mathcal{F}$ has fewer than $7|V(\Gamma)|/2$ edges. We then modify $\mathcal{F}$ to obtain explicit unique-neighbor expanders of maximum degree 3.

1 INTRODUCTION

We call a bipartite graph $\Gamma = (I, O, E)$, where $|I| = N$, and $|O|$ is less than, say, $399N/400$, a (α, ϵ)-*unique neighbor expander* if, for each subset S of I such that $|S| \leq \alpha|I|$, there are at least $\epsilon|S|$ vertices in O that are adjacent to exactly one vertex in S. (Call I the *input set* of Γ and O the *output set* of Γ.) Unique-neighbor expanders are useful in the construction of self-routing strict-sense nonblocking networks (see [2], [9]). However, or any strictly positive α and ϵ, the construction of an infinite family of bounded-degree (α, ϵ)-unique neighbor expanders has been a long-standing open question (see [2], [9]), perhaps because the 'second eigenvalue' method, which has been the main tool used in guaranteeing the expansion properties of a graph, does not appear to be strong enough to prove that an infinite family of bounded-degree graphs are unique-neighbor expanders (see [5]). However, here we answer this open question by presenting

*Department of Mathematical Sciences, The Johns Hopkins University, Baltimore, MD, and School of Mathematics, Institute for Advanced Study, Princeton, NJ. Supported by NSF grant CCR98210-58 and ARO grant DAAH04-96-1-0013. Email: mrc@ias.edu.

for strictly positive constants α and ϵ, an explicit infinite family $\mathcal{F}$ of bounded-degree unique-neighbor expanders, $\Gamma = (X, Y, E(\Gamma))$, where $|X| = 22|Y|/21$.

Each $\Gamma \in \mathcal{F}$ has no more than $7|V(\Gamma)|/2$ edges, and maximum degree 25. The construction of each $\Gamma = (X, Y, E(\Gamma)) \in \mathcal{F}$ is a simple graph product of a certain 'small' bipartite graph H with a 'large' graph Λ that has $|X|$ edges, and is in a certain explicit infinite family $\mathcal{H}$. The graph H is a bipartite graph that has 44 vertices on one side, 21 on the other, and a simple algebraic construction, while $\mathcal{H}$ is an infinite family of 44-regular Cayley Ramanujan graphs constructed in [6] and [7].

To show that each $\Gamma \in \mathcal{F}$ is a unique-neighbor expander, we first present properties of Λ that were established by N. Kahale [5], whose analysis uses the 'second eigenvalue' method. We later present H, and establish properties of H using analytic methods that work because H is so small. Then we show that the combined properties of Λ and H guarantee that Γ is indeed a unique-neighbor expander.

This work here is related to the work presented in [3], where the authors construct infinite families of unbalanced expanders of degree K (K fixed) and linear expansion $(1-\epsilon)K$, where the output side can be any constant fraction smaller than the input. However, we believe the constructions in this paper are of sufficient independent interest. The degrees of the constructions here are much lower, and the specifications are much simpler. Here we use only simple algebraic graph constructions that have been in the literature since the mid 1980's. The very recent extractor constructions that we use in [3] are not used at all here.

We now describe the layout of the rest of this paper. In §2 we present and analyze $\mathcal{H}$ and H. Then in §3 we use $\mathcal{H}$ and H to construct $\mathcal{F}$. We then analyze $\mathcal{F}$, and conclude that $\mathcal{F}$ is an infinite family of unique neighbor expanders. In §4 we lower the maximum degree to 3.

We now specify notation. For each positive integer ι, let $\mathbf{N}_\iota$ denote the set of ι nonnegative integers smaller than than ι. All graphs in this paper are *undirected* and simple. For any subset V' of $V(G)$, let $G[V']$ denote the induced subgraph of G on V', and let $\mathcal{N}_G(V')$ denote the set of vertices adjacent to at least one vertex in V'. Similarily, for any vertex v of G, let $\mathcal{N}_G(v) = \mathcal{N}_G(\{v\})$, and define $\delta_G(v)$ to be $|\mathcal{N}_G(v)|$, or equivalently, the degree of v in G. Also, we define a $q+1$-regular graph Λ to be *Ramanujan* if all but one of the eigenvalues of the adjacency matrix of Λ are no larger than $2\sqrt{q}$. Now suppose we are given a group G and a subset Σ of G, where $\pi \in \Sigma$ if and only if $\pi^{-1} \in \Sigma$. We define the *Cayley graph* Λ' on G *with respect to* Σ to be the $|\Sigma|$-regular graph whose vertex-set is G, and whose edge-set is $\{\{\nu, \pi\nu\}|\ \nu \in G$ and $\pi \in \Sigma\}$. (Call the elements $\pi \in \Sigma$ the *generators* of Λ'.) If Σ generates G, then Λ' is connected; otherwise, the components of Λ' are the right cosets of the subgroup of G generated by Σ.

2 AN AUXILIARY CONSTRUCTION

Theorem 2.1 *Let $\mathcal{H}$ be the infinite family of 44-regular Cayley Ramanujan graphs on N vertices, explicitly constructed by A. Lubotsky, R. Phillips, and P. Sarnak [7], [6], pp. 96–98, and M. Morgenstern [8]. Then $\mathcal{H}$ satisfies the following property* **(*)**.
(*): *There exists strictly positive α and ϵ, such that, for any $\Lambda = (V, E) \in \mathcal{H}$, and any subset E' of E such that $|E'| \leq \alpha|E|$, there are at least $\epsilon|E'|$ vertices in Λ that are incident to at least 1, but no more than 7, edges in E'.*

That $\mathcal{H}$ satisfies **(*)** is a direct corollary of the following theorem, proved by N. Kahale.

Theorem 2.2 *[4], [5] Let $\Lambda = (V, E)$ be a k-regular Ramanujan graph. Then for all $\epsilon > 0$, and for any nonempty subset X of size at most $k^{-1/\epsilon}|V|$, the average degree d of $\Lambda[X]$ satisfies*

$$d \leq (1 + \sqrt{k-1})(1 + O(\epsilon)). \tag{1}$$

■

The next graph H that we present is a modified graph from that constructed in [1].

Proposition 2.3 *Let $H = (W, T, E_H)$ be the bipartite graph with parts $W = \{w_0, ..., w_{43}\}$ and $T = \{t_0, ..., t_{20}\}$, where $w_{\iota'}$ is adjacent to t_ι in H if and only if either (I) or (II) holds.*

(I) $\iota' \leq 24$, and either (a) $\iota = 20$, or (b) $\lfloor \frac{\iota'}{5} \rfloor \lfloor \frac{\iota}{5} \rfloor \equiv \iota - \iota'$ (mod 5).

(II) $\iota' \geq 25$, and $\iota' - 25 = \iota$.

Then H satisfies property **(**)**: *if U is any nonempty subset of W that has no more than 7 vertices, there is at least one vertex in T that is adjacent in H to exactly one vertex in U.*

Proof: Let W' denote the subset of W consisting of the 25 vertices $w_{\iota'}$; $\iota' \leq 24$. Then if $U \cap W'$ contains exactly one vertex w, then w is the only vertex in U adjacent in H to t_{20}. Also, if $U \cap W'$ is empty, then there are $|U|$ vertices in T adjacent to exactly one vertex in U since the induced subgraph of H on $(W \setminus W') \cup T$ is a matching that saturates $W \setminus W'$. So we now assume that $|U \cap W'|$ is at least 2. We then show that (*) there are at least $8 - |U \cap W'|$ vertices in T that are adjacent to exactly one vertex in $U \cap W'$. Since each vertex in $W \setminus W'$ is adjacent to only one vertex in T, Proposition 2.3 will follow.

For all $\iota \in \mathbf{N}_{25}$, set $a_\iota = \lfloor \iota/5 \rfloor$. Then, for each $\iota' \in \mathbf{N}_{25}$, we may think of $\mathcal{N}_H(w_{\iota'}) \setminus \{t_{20}\}$ as the 'line' that covers all points t_ι where ι is such that $a_{\iota'} \in \{0, 1, 2, 3\}$, and $\iota = \iota' + a_\iota a_{\iota'}$, where addition and multiplication done in the 5-element field F_5. Thus, if we prove the following lemma, then we have shown (*), and Proposition 2.3 will then follow.

Lemma 2.4 *Let T' be a set of 20 points of the form (a,b); $a \in F_5 \setminus \{4\}$; $b \in F_5$, and let W' be the set of 25 lines, each line parameterized by the ordered pair (a',b'); $a',b' \in F_5$, where the line parameterized by (a',b') contains points in T' precisely of the form $(a',b') : b = b' + aa'$, where all operations are done in the field F_5. Next, for any subset U' of W' and any point $p \in T'$, let $\varphi_{U'}(p)$ be the number of lines $l \in U'$ such that $p \in l$. Now let U' be any subset of at least 2 lines of W'. Then there are at least $8 - |U'|$ points p in T' such that $\varphi_{U'}(p)$ is exactly 1.*

Proof: For each $j = 0,1,2,3$, let A_j denote the set of 5 points of T' of the form (j,b), where $b \in F_5$. So each line in W' intersects each A_j exactly once. These two facts will be useful.

Fact 1: Let l and l' be distinct lines in W'. Then l and l' intersect at at most 1 point in T'.

Fact 2: Let $l, l' \in W'$. Suppose that l intersects A_{j_1} at (j_1, η_1), and A_{j_2} at (j_2, η_2), and that l' intersects A_{j_1} at (j_1, η_1'), and A_{j_2} at (j_2, η_2'), where j_1 and j_2 are distinct elements of F_5. Now let j_3 be any element of F_5. Then, if l intersects A_{j_3} at (j_3, η_3), and l' intersects $A_{j_3'}$ at (j_3, η_3'), then η_3' and η_3 must satisfy

$$\eta_3' - \eta_3 = \sigma_1 + (j_3 - j_1)(\sigma_2 - \sigma_1)(j_2 - j_1)^{-1}, \tag{2}$$

where $\sigma_1 = \eta_1' - \eta_1$, and $\sigma_2 = \eta_2' - \eta_2$.

We now use these facts to prove Lemma 2.4 for when $|U'| = 6$. Write the lines of U' as $l_1, ..., l_6$. For each line l_i, let $(0, \eta_i)$ denote the point in A_0 covered by l_i; $(1, \eta_i')$ denote the point in A_1 covered by l_i; $(2, \eta_i'')$ the point in A_2 covered by l_i, and $(3, \eta_i''')$ the point in A_3 covered by l_i. We now break the proof of this lemma for when $|U'| = 6$ into two cases.

Case 1: $\varphi_{U'}(p) \leq 2$ for each point $p \in T'$.

Then since each line in W' covers exactly one point in each A_j, we may assume that the lines in U' together cover exactly 3 points p in A_0, and that $\varphi_{U'}(p)$ is exactly 2 for each such p $\in A_0$. Let us assume without loss of generality that l_1 and l_2, l_3 and l_4, and l_5 and l_6, cover the same point in A_0, or in other words,

(A) $\eta_1 = \eta_2$; $\eta_3 = \eta_4$, and $\eta_5 = \eta_6$, but η_1, η_3, and η_5 are necesarily distinct.

Similarily, we may assume that

(A$'$) the lines in U' together cover exactly 3 points p in A_1 and 3 points p in A_2, and that $\varphi_{U'}(p)$ is exactly 2 for each such p.

Therefore, since l_5 and l_6 intersect at A_0 (and at A_0 only by Fact 1), we may assume that l_1, l_2, l_3, l_4 cover exactly 3 points in A_1 and 3 points in A_2. By Fact 1, l_1 and l_2 intersect in neither A_1 nor A_2, and similarily for l_3 and l_4. Therefore, for the rest of Case 1, we may assume without loss of generality that

(B) $\eta_1' = \eta_3'$, and $\eta_4' \notin \{\eta_1', \eta_2', \eta_3'\}$, or equivalently, l_3 intersects l_1 at a point in A_1, but l_4 intersects none of l_1,l_2, l_3 in A_1.

We may also assume without loss of generality that besides (B), either events (1) or (2), stated below, happen.

Event (1): $\eta_3'' = \eta_2''$, and $\eta_4'' \notin \{\eta_1'', \eta_2'', \eta_3''\}$, or equivalently, l_3 intersects l_2 in A_2, and l_4 does not intersect any of l_1,l_2,l_3 in A_2.

Event (2): $\eta_4'' = \eta_2''$, and $\eta_3'' \notin \{\eta_1'', \eta_2'', \eta_4''\}$, or equivalently, l_4 intersects l_2 in A_2, and l_3 does not intersect any of l_1, l_2, l_3 in A_2.

Thus, we now break up Case 1 into two subcases.

Subcase 1: $\eta_3'' = \eta_2''$, and $\eta_4'' \notin \{\eta_1'', \eta_2'', \eta_3''\}$, or equivalently, Event (1) happens. In this case we prove that, for some $j \in \{1, 2\}$, the lines of U' cover at least 4 points in A_j. Then this implies that there are at least 2 points $p \in A_j$ where $\varphi_{U'}(p) = 1$, because each line covers exactly one point of A_j.

Let $\sigma_0 = \eta_1 - \eta_3$, and let $\sigma = \eta_1' - \eta_4'$. Then by Fact 2, $\eta_1'' = \eta_4'' + \sigma_0 + 2(\sigma - \sigma_0)$ or equivalently,

$$\eta_1'' = \eta_4'' + 2\sigma - \sigma_0. \tag{3}$$

However, by assumption of Event (1), $\eta_2'' = \eta_3''$. Since $\eta_2 = \eta_1$ by (A), $\eta_2' = \eta_3' + \sigma_0/2$ by Fact 2. Also, $\eta_1' = \eta_3'$ by (A), so $\eta_2' = \eta_1' + 3\sigma_0$. Equivalently, by definition of σ,

$$\eta_2' = \eta_4' + \sigma + 3\sigma_0. \tag{4}$$

Now (A′) and (B) imply that one of l_5 and l_6, say l_6, must intersect l_4 in A_1 and l_1 in A_2, and that the other, say l_5, must intersect l_2 in A_1 and l_4 in A_2 (or equivalently, $\eta_6' = \eta_4'$ and $\eta_6'' = \eta_1''$, and $\eta_5' = \eta_2'$, and $\eta_5'' = \eta_4''$). On the other hand, $2(\eta_6' - \eta_5')$ must equal $\eta_6'' - \eta_5''$ by Fact 2, since $\eta_5 = \eta_6$. Since $\eta_6' = \eta_4'$, $\eta_5' = \eta_2'$, $\eta_6'' = \eta_1''$, and $\eta_5'' = \eta_4''$, this implies that (a) $2(\eta_4' - \eta_2')$ must equal $\eta_1'' - \eta_4''$. But from Equation (4), $2(\eta_4' - \eta_2') = 2(-3\sigma_0 - \sigma) = 3\sigma - \sigma_0$. However, this and (a) imply that $3\sigma - \sigma_0 = \eta_1'' - \eta_4''$, which implies, by Equation (3) that $3\sigma - \sigma_0 = 2\sigma - \sigma_0$. This implies that $\sigma = 0$. But if σ is 0, then so is $\eta_3' - \eta_4'$, since $\eta_1' = \eta_3'$ by assumption. But if $\eta_3' - \eta_4'$ is 0, then l_3 and l_4 intersect at A_1 as well as A_0, which is impossible by Fact 1. So l_5 and l_6 cannot cover these points in A_1 and A_2. So we are done with Subcase 1.

Subcase 2: $\eta_4'' = \eta_2''$, and $\eta_3'' \notin \{\eta_1'', \eta_2'', \eta_4''\}$, or equivalently, Event (2) happens. We handle this case in the following fashion. Let $\sigma_0 = \eta_1 - \eta_3$, and $\tilde{\sigma_0} = \eta_3 - \eta_5$. We assume that we cannot reduce to Subcase 1. Then we use Fact 2 to show that at most 2 pairs of lines in U' can intersect in A_3, finishing Subcase 2.

By (A′) and (B), we may assume that l_5 intersects l_2 in A_1, and l_3 in A_2, and that l_6 intersects l_4 in A_1 and l_1 in A_2, or equivalently, (c) $\eta_5' = \eta_2'$, $\eta_5'' = \eta_3''$, $\eta_6' = \eta_4'$, and $\eta_6'' = \eta_1''$, or we could reduce to Subcase 1. (Indeed, if, say, l_5 intersects l_2 in A_1 and l_1 in A_2, then we could reduce to Subcase 1 using l_1, l_2, l_5, l_6.) Then by Fact 2, $\eta_3' - \eta_5' = (\eta_3 - \eta_5)/2 = \tilde{\sigma_0}/2$, and $\eta_2' - \eta_4' = \sigma_0/2$, since $\eta_3'' = \eta_5''$, and $\eta_2'' = \eta_4''$. Thus, for every l_i, $l_{i'}$ in U', we have now calculated $\eta_i' - \eta_{i'}'$ in terms of σ_0 and $\tilde{\sigma_0}$. Indeed, $\eta_1' = \eta_3'$ by (A), and by (c), $\eta_2' = \eta_5'$, and $\eta_4' = \eta_6'$.

So the only pairs of lines in U' that have not intersected in A_0, A_1, or A_2 are the pairs (l_1, l_5), (l_2, l_3),(l_2, l_6), (l_4, l_5), (l_3, l_4), (l_1, l_4). So by Fact 1, these are the only pairs that can intersect in A_3. We can now use Fact 2 to give necessary conditions on σ_0 and $\tilde{\sigma_0}$ for each of these pairs to intersect in A_3. Suppose that l_5 and l_1 intersect in A_3. Then by Fact 2,

$$\eta_1 - \eta_5 + 3((\eta_1' - \eta_5') - (\eta_1 - \eta_5)) = 0. \tag{5}$$

From (B) and (c), $\eta_1' - \eta_5' = \tilde{\sigma_0}/2$. Now $\eta_1 - \eta_5 = \sigma_0 + \tilde{\sigma_0}$ by definition of σ_0 and $\tilde{\sigma_0}$. Thus, Equation (5) holds only if $\sigma_0 = \tilde{\sigma_0}$. So l_5 and l_1 will intersect in this case only if $\tilde{\sigma_0} = \sigma_0$. By a similar calculation, l_2 and l_6 intersect in A_3 only if $\sigma_0 = \tilde{\sigma_0}$. However, l_1 and l_4, and l_3 and l_2, intersect in A_3 only if $\sigma_0 = 3\tilde{\sigma_0}$. Furthermore, l_4 and l_5, and l_3 and l_6, intersect in A_3 only if $\sigma_0 = 2\tilde{\sigma_0}$. Thus in this subcase there can be only two intersections in A_3, so and thus, at there must exist at least 2 points $p \in A_3$ where $\varphi_{U'}(p) = 1$. Thus, we are done with Subcase 2, and thus, Case 1. So we next consider Case 2.

Case 2: There exists a point $p = (j, \tilde{\eta})$ in T where $\varphi_{U'}(p) \geq 3$. We break case 2 up into two cases.

Subcase 1: $\varphi_{U'}((j, \tilde{\eta})) = 3$. Then assume that $(j, \tilde{\eta})$ is contained in each of l_1, l_2, and l_3 in U', but none of l_4, l_5, and l_6 in U'. Then we may assume that there exists another point $(j, \tilde{\eta}')$ in A_j contined in both l_4 and l_5 in U' or there are at least 2 points p' in A_j where $\varphi_{U'}(p') = 1$. So let j' be any element in $F_5 \setminus \{4, j\}$, and each integer $i \in \{1, 2, 3, 4, 5\}$, let $(j', \tilde{\eta}_i)$ be the point in $A_{j'}$ covered by l_i.

Since each line intesects each $A_{\tilde{j}}$ at exactly one point, we may assume that, for each $j'' \in F_5 \setminus \{4, j\}$, l_4 and l_5 each intersect a l_i; $i \in \{1, 2, 3\}$, otherwise there are at least 2 points $p' \in A_{j''}$ where $\varphi_{U'}(p') = 1$. However, by Fact 2, we may assume that at least one of events (a) or (b) happen. (a) There exists j_1, j_2, $j_3 \in F_5 \setminus \{j, 4\}$ such that l_4 intersects l_1, and l_5 intersects l_2 in A_{j_1}; l_4 intersects l_2, and l_5 intersects l_3 in A_{j_2}; and l_4 intersects l_3, and l_5 intersects l_1. (b) There exists j_1, $j_2 \in F_5 \setminus \{j, 4\}$ such that l_4 intersects l_1 and l_5 intersects l_2 in A_{j_1}, and l_4 intersects l_2, and l_5 intersects l_1 in A_{j_2}.

Suppose event (a) happens. On one hand, by Fact 2, $\tilde{\eta}_{i'} - \tilde{\eta}_i = \tilde{\eta}_5 - \tilde{\eta}_4$ if l_5 intersects $l_{i'}$ and if l_4 intersects l_i in $A_{j''}$, for any $i, i' \in \{1, 2, 3\}$, and any $j'' \in F_5 \setminus \{4, j\}$. On the other hand, note that $(\tilde{\eta}_1 - \tilde{\eta}_3) + (\tilde{\eta}_3 - \tilde{\eta}_2) + (\tilde{\eta}_2 - \tilde{\eta}_1) = 0$. Thus, if (a) happens then this would imply that $3(\tilde{\eta}_1 - \tilde{\eta}_3)$ is 0, since then $(\tilde{\eta}_1 - \tilde{\eta}_3) = (\tilde{\eta}_3 - \tilde{\eta}_2) = (\tilde{\eta}_2 - \tilde{\eta}_1) = (\tilde{\eta}_5 - \tilde{\eta}_4)$. But this is impossible, since $\tilde{\eta}_1 - \tilde{\eta}_3$ is nonzero by Fact 1. So (a) cannot happen. By a similar line of reasoning, (b) cannot happen either. Thus, there must exist at least one $j' \in F_5 \setminus \{j, 4\}$ such that the lines of U' cover at least 4 points in $A_{j'}$. So there must be at least 2 points $p' \in A_{j'}$ where $\varphi_{U'}(p') = 1$.

Subcase 2: There is a point $p = (j, \tilde{\eta})$ where $\varphi_{U'}(p) \geq 4$. Then for each $j' \in F_5 \setminus \{j, 4\}$, the lines of U' must cover at least 4 points of $A_{j'}$ by Fact 1. Since each line in U' covers at most 1 point of $A_{j'}$, we are done for this subcase as well.

Thus we have shown that there are at least 2 points in $p \in T'$ where $\varphi_{U'}(p) = 1$ when $|U'| = 6$. We now show that Lemma 2.4 holds for when $|U'| = 7$. Suppose it does not. Then in each A_j, there are at most 3 points covered by the lines in U'; since each line intersects each A_j, there must be at least one point in A_j covered by 3 lines of U', and another covered in A_j by at least 2 lines of U'. So fix a $j \in F_5 \setminus \{4\}$. Then by mimicing the proof in Case 2 in the proof of Lemma 2.4, we can see that there is at least one $j'' \in F_5 \setminus \{4, j\}$ such that 4 points of $A_{j''}$ are covered by a line in U', and thus, at least one of those 4 points in $p \in A_{j''}$ must satisfy $\varphi_{U'}(p) = 1$, so Lemma 2.4 indeed holds for when $|U'| = 7$.

The proofs that there are at least $8 - |U'|$ points in T' that are covered by exactly one line of U' for the cases when $|U'| = 2, 3, 4$, and 5 follow the lines of reasoning used to prove the cases when $|U'|$ is 6 and 7, but are easier, and will not be given here. Thus, Lemma 2.4 follows. ■

Proposition 2.3 follows from Lemma 2.4. ■

3 CONSTRUCTION AND ANALYSIS OF $\mathcal{F}$

In this section we construct $\mathcal{F}$ from $\mathcal{H}$ and H, presented in Theorem 2.1 and Proposition 2.3, respectively. We do this by presenting, for an arbitrarily large integer N, a bipartite graph Γ with parts X and Y, where $|X| = N = 22|Y|/21$. We then prove, via Theorem 3.1, stated below, that Γ is a unique-neighbor expander.

Let $\Lambda = (V, X)$ be the (Cayley) graph in $\mathcal{H}$ with N edges, and let $\Sigma = \{\pi_0, ...\pi_{44}\}$ be the set of 44 generators of Λ. (so $X = \{\nu, \pi\nu' | \ \nu \in V$ and $\pi \in \Sigma\}$). Next, let $W = \{w_0, ..., w_{43}\}$, $T = \{t_0, ..., t_{20}\}$, and H be as in Proposition 2.3. The input set of Γ is X and the output set is $Y = V\times$ [21], where $\gamma \in X$ and $\langle \nu, \iota \rangle \in Y$ are adjacent in Γ if and only if both (1) γ is incident to ν in Λ, and (2) there exists an $\iota' \in \{0, 1, ..., 43\}$ where both $w_{\iota'}$ is adjacent to t_ι in H, and γ is incident to $\pi_{\iota'}\nu$ in Λ. ■

First, since Λ is 44-regular, $|E| = |X| = 22|V| = 22|Y|/21$, so indeed $|X| = 22|Y|/21$. So we next prove that, for each subset S of X such that $|S| \leq \alpha|X|$, there are at least $\epsilon|S|$ vertices in Y that are adjacent in Γ to exactly one vertex in S, where α and ϵ are as in Theorem 2.1. We then prove that Γ has maximum degree 25. Then Theorem 3.1 stated below will follow.

Let ν be an arbitrary vertex in V. Then let X_ν be the set of $\gamma \in X$ such that γ is incident to ν in Λ. Let Y_ν denote the set of 21 vertices $\langle \nu, \iota \rangle \in Y$, where $\iota \in \{0, 1, ..., 20\}$. So the Y_ν's partition Y, while each $\gamma \in X$ is contained in precisely two X_ν's; namely, if ν and ν' are the two endpoints of γ, then γ is in both X_ν and $X_{\nu'}$. Also, for each vertex $\nu \in \Lambda$, **(A)** each edge in Γ incident to a vertex in Y_ν is also incident to a vertex in X_ν. Furthermore, **(B)** $\Gamma[X_\nu \cup Y_\nu]$ is isomorphic to H; X_ν maps to W, and Y_ν maps to T.

Now let S be any subset of X. Then $|S \cap X_\nu|$ is the number of edges of S that are incident to ν, for each $\nu \in V$. So now suppose that $|S| \leq \alpha|X|$. Thus, there is a set Q of at least $\epsilon|S|$ vertices $\nu \in \Lambda$ such that $1 \leq |S \cap X_\nu| \leq 7$, because Λ satisfies **(*)** by Theorem 2.1. Then from

(B) it follows that there is, for each $\nu \in Q$, at least one vertex $v \in Y_\nu$ that is adjacent in Γ to exactly one vertex in $S \cap X_\nu$, because H satisfies **(**)** by Proposition 2.3. Then from **(A)**, v is adjacent in Γ to exactly one vertex in S. Therefore, there must be at least $|Q| \geq \epsilon|S|$ vertices in Y that are adjacent in Γ to exactly one vertex in S because the Y_ν's are disjoint.

We now bound the maximum degree of Γ, and then Theorem 3.1 will follow. From **(A)** and **(B)**, each vertex in X has degree no more than $2 \times 5 = 10$, since each $\gamma_e \in X$ is in exactly two X_ν, and vertex in W has degree at most 5 in H. Similar lines of reasoning can be used to show that each vertex in Y has degree at most 25 in Γ, and that there are no more than $7|V(\Gamma)|/2 \leq 7|X|$ edges in Γ.

We have proved the following theorem.

Theorem 3.1 *$\Gamma = (X, Y, E(\Gamma))$ is an (α, ϵ)-unique neighbor expander with input set X and output set Y, where α and ϵ are as in Theorem 2.1.* ■

In fact, we can give an algebraic construction of the $\Gamma \in \mathcal{F}$ as $\mathcal{H}$ is constructed in [6]. First, let l be any integer that is greater than 3. Let us write the group $\mathrm{PSL}_2(\mathbf{Z}/17^l\mathbf{Z})$ as $\hat{V}$, and the group $\mathrm{PGL}_2(\mathbf{Z}/17^l\mathbf{Z})$ as V. Next, let Σ be the set of 44 elements of $\mathbf{Z}^4$ where, an element s of $\mathbf{Z}^4$ is in Σ if and only if the 4 coordinates of s, written as a_1, a_2, a_3, a_4, are such that (1) $a_1^2 + a_2^2 + a_3^2 + a_4^2 = 43$; (2) a_2, a_3, and a_4 are odd and a_2 is positive. Then let ε be a square root of -1 in the ring $\mathbf{Z}/17^l\mathbf{Z}$ (we can find such a ε in $O(l^2)$ time). Next let Σ' be the set of 44 matrices in V such that π is in Σ' if and only if there exists an s in Σ such that

$$\pi = \begin{pmatrix} 7a_1 + 7\varepsilon a_2 & 7a_3 + 7\varepsilon a_4 \\ -a_3 + \varepsilon a_4 & a_1 - \varepsilon a_2 \end{pmatrix}, \tag{6}$$

where a_1, a_2, a_3, and a_4 are the 4 coordinates of s.

We will next define, for each $\iota' \in \mathbf{N}_{44}$, a subset $\chi_{\iota'}$ of $\mathbf{N}_{21}$. On one hand, for each $\iota' \in \mathbf{N}_{25}$, let $\chi_{\iota'}$ be the set of integers $\iota \in \mathbf{N}_{21}$ where either $\iota = 20$, or $\lfloor \frac{\iota'}{5} \rfloor \lfloor \frac{\iota}{5} \rfloor \equiv \iota' - \iota \pmod 5$. On the other hand, for each $\iota' \in \mathbf{N}_{44} \setminus \mathbf{N}_{25}$, let $\chi_{\iota'}$ be the set containing exactly the integer $\iota' - 25$.

Next, let X be a set of $44 \times |\hat{V}|$ vertices, and let Y be a set of $21 \times |V| = 21|X|/22$ vertices. For each $x \in X$, let ν_x be an element of $\hat{V}$, and π_x an element of Σ' such that if x and x' are two distinct vertices in X, then either $\pi_x \neq \pi_{x'}$, or $\nu_x \neq \nu_{x'}$. Similarly, for each vertex $y \in Y$, let ν_y be an element of Y, and ι_y an integer in $\mathbf{N}_{21}$ such that if y and y' are two distinct vertices in Y, then either $\nu_y \neq \nu_{y'}$, or $\iota_y \neq \iota_{y'}$. Finally, let τ be an arbitrary bijection from Σ' to $\mathbf{N}_{44}$.

Then set Γ to be the bipartite graph with parts X and Y, where $x \in X$ and $y \in Y$ are adjacent in Γ if both (1) $\iota_y \in \chi_{\tau(\pi_x)}$, and (2) ν_y equals either ν_x or $\pi_x\nu_x$. ■

In fact, in a similar fashion we can algebraically construct a larger family $\tilde{\mathcal{F}}$ of unique-neighbor expanders, such that, for each N' sufficently large, a graph $\Gamma \in \tilde{\mathcal{F}}$ such that the input set of Γ is no larger than $22N'/21$, and no smaller than N'. Fix a q that is any other prime of the form $q = 4a + 1$, where a is a positive integer (such as, say, $q = 5$), and then let l_1 and l_2 be nonnegative integers such that l_2 is at least 4. Next Σ be as before. Then, let ε be a square root of -1 in the ring $\mathbf{Z}/17^{l_1}q^{l_2}\mathbf{Z}$, which we write as R (we can find ε in time $O((l_1 + l_2)^2)$ if q is $O(1)$). Then set $\hat{V} = \mathrm{PSL}_2(R)$, and $V = \mathrm{PGL}_2(R)$. Next, if 43 is a square in R, then let Σ' be as before. Otherwise, let Σ' be the set of 44 matrices π, where

$$\pi = \begin{pmatrix} a_1 + \varepsilon a_2 & a_3 + \varepsilon a_4 \\ -a_3 + \varepsilon a_4 & a_1 - \varepsilon a_2 \end{pmatrix}. \tag{7}$$

Then we construct a unique-neighbor expander $\tilde{\Gamma}$ from $\mathrm{PGL}_2(R)$ and $\mathrm{PSL}_2(R)$ in the same fashion as we constructed $\Gamma \in \mathcal{F}$ from $\mathrm{PGL}_2(\mathbf{Z}/17^l\mathbf{Z})$ and $\mathrm{PSL}_2(\mathbf{Z}/17^l\mathbf{Z})$. ■

4 VALENCE 3 EXPANDERS

In this section, we present an explicit infinite family $\mathcal{F}'$ of unique-neighbor expanders of maximum degree 3. We do this in the following fashion. Let $\Gamma = (X, Y, E(\Gamma))$ be an arbitrary graph in $\mathcal{F}$ with parts X and Y, and for each vertex $v \in V(\Gamma)$, let τ_v be an arbitrary bijection from the set of positive odd integers less than $2\delta_\Gamma(v)$, to $\mathcal{N}_\Gamma(v)$. We construct from Γ and $\{\tau_v\}$ a bipartite graph $\Gamma' = (X', Y', E(\Gamma')) \in \mathcal{F}'$ with parts X' and Y', where $|X'| = 2|E(\Gamma)| - |Y|$, and $|Y'| = 2|E(\Gamma)| - |X|$. We then show that Γ' is unique-neighbor expander by proving Theorem 4.1.

The vertex-set $V(\Gamma')$ of Γ' is $\{\nu_{v,\iota} |\ \ v \in V(\Gamma)$, and $\iota \in [2\delta_\Gamma(v) - 1]\}$. Then $\nu_{v,\iota}$ and $\nu_{\hat{v},\hat{\iota}}$ are adjacent in Γ' if and only if either
(1) $v = \hat{v}$, and $\hat{\iota} \in \{\iota + 1, \iota - 1\}$, or
(2) ι and ι' are both odd, and $\tau_v(\iota) = \hat{v}$, and $\tau_{\hat{v}}(\hat{\iota}) = v$.
The input and output sets of Γ' are X' and Y', respectively, where
$X' = \{\nu_{v,\iota} \in V(\Gamma')|$ either (1) $v \in X$, and ι is odd, or (2) $v \in Y$, and ι is even$\}$, and
$Y' = V(\Gamma') \setminus X'$. ■

In other words, we expand each $v \in V(\Gamma)$ to a path χ_v of $2\delta_\Gamma(v) - 1$ vertices, and add an edge between χ_x and χ_y if and only if x and y are adjacent in Γ, such that exactly every other vertex, starting with the endpoints, of χ_v, for every $v \in V(\Gamma)$, is incident to exactly one of these edges not in χ_v (and the remaining vertices aren't incident to any edges outside of χ_v). The resulting graph is Γ'.

Then X' is the set of vertices that are either (a) in χ_x, for some $x \in X$, and are incident to an edge outside of χ_x, or (b) in χ_y, for some $y \in Y$, and are not incident to an edge outside of χ_y. The other part Y' is the remaining set of vertices. ■

It is easy to check that the maximum degree of Γ' is indeed 3. Also, it is not hard to check that X' and Y' are indeed independent. Also, $|X'| = \sum_{x \in X} \delta_\Gamma(x) + \sum_{y \in Y} \delta_\Gamma(y) - 1 = 2|E(\Gamma)| - |Y|$, while $|Y'| = 2|E(\Gamma)| - |X|$. We've established in the last section that $|E(\Gamma)| \leq 7|X|$, and that $|Y| = 21|X|/22$, so $|X'| \geq 311|Y'|/310$. Thus, we next prove the following theorem by showing that, for every sufficiently small subset S' of X', there are many vertices in Y' adjacent to exactly one vertex in S'.

Theorem 4.1 *Γ' is a $(\alpha/9, \epsilon/2^{17})$-unique neighbor expander, where α and ϵ are as in Theorem 3.1, and has maximum degree 3.*

We prove Theorem 4.1 in Appendix II.

References

[1] N. Alon. Eigenvalues, geometric expanders, sorting in rounds, and Ramsey theory. *Combinatorica, 6 (1986)*, pp. 207–219.

[2] S. Arora, T. Leighton, and B. Maggs. Path selection in a nonblocking network, *SIAM J. Computing 25 (1996)*, pp. 600–625.

[3] M. Capalbo, O. Reingold, S. Vadhan, A. Wigderson. Constant-degree expansion beyond the degree/2 barrier, to appear in STOC 2002.

[4] N. Kahale. On the second eigenvalue and linear expansion, DIMACS Series in Discrete Mathematics and Theoretical Computer Science 10 (1992), J. Friedman, ed., pp. 49–62.

[5] N. Kahale. Eigenvalues and expansion of regular graphs, *J. Assoc. Comput. Mach. 42 (1995)*, pp. 1091–1106.

[6] A. Lubotsky. *Discrete Groups, Expanding Graphs, and Invariant Measures*, Progress in Mathematics (125), Birkhäusser Verlag, Basel 1994.

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

[8] M. Morgenstern. Existence and explicit constructions of $q+1$ regular Ramanujan graphs for every prime power q, *J. Combin. Theory Ser. B, 62 (1994)*, pp. 44–62.

[9] N. Pippenger. Self-routing superconcentrators, *Journal Comp. Syst. Sciences (52) 1996* pp. 53–62.

5 Appendix: Pf of Thm 4.1

Before we prove Theorem 4.1, we introduce notation, and then we make observations. For each $x \in X$, let X'_x denote the set of $\delta_\Gamma(x)$ vertices $\nu_{x,\iota}$, where ι is odd (so X'_x is a subset of X'), and let Y'_x denote the set of $\delta_\Gamma(x) - 1$ vertices $\nu_{x,\iota}$, where ι is even (so Y'_x is a subset of Y'). For each $y \in Y$, let Y'_y denote the set of $\delta_\Gamma(y)$ vertices $\nu_{y,\iota}$, where ι is odd (so Y'_y is a subset of Y'), and let X'_y denote the set of $\delta_\Gamma(y) - 1$ vertices $\nu_{y,\iota}$, where ι is even (so X'_y is a subset of X'). Then the X'_v's, where $v \in V(\Gamma)$, partition X', and the Y'_v's partition Y'. We next make observations.

Observation 1: For any vertex $x \in X$, every vertex adjacent to a vertex in Y'_x is in X'_x.

Observation 2: Let U be any nonempty subset of X'_y, where y is an arbitrary vertex in Y. Then there are at least 2 vertices in Y'_y that are adjacent to exactly one vertex in U.

(Proof: The induced subgraph of $X'_y \cup Y'_y$ is the path χ_y, with endpoints $\nu_{y,1}$ and $\nu_{y,2\delta_\Gamma(y)-1}$, and edges $\{\nu_{y,\iota}, \nu_{y,\iota+1}\}$ for each positive integer ι less than $2\delta_\Gamma(y) - 1$. So X'_y is precisely the set containing every other vertex of χ_y starting with the neighbors of the endpoints. From this the observation follows.)

Observation 3: Let U be any nonempty proper subset of X'_x, where x is an arbitrary vertex in X. Then there is at least 1 vertex in Y'_y that is adjacent to exactly one vertex in U.

The proof of Observation 3 is similar in spirit to that of Observation 2.

Observation 4: Let y and $\bar{y}$ be distinct vertices in Y. Then there are no edges in Γ' between X'_y and $Y'_{\bar{y}}$.

Having presented Observations 1–4, we next introduce some notation. Let S' be an arbitrary subset of X' of cardinality no greater than $\alpha|X'|/9$. Then let Q_0 denote the set of vertices $x \in X$ where $S' \cap X'_x = X'_x$, and let S'_0 denote the set of vertices $x' \in S'$ contained in some X'_x where $x \in Q_0$. Let S'_1 denote the vertices of S' in some X'_x, where $x \in X \setminus Q_0$, and let S'_2 denote the set of vertices in some X'_y, where $y \in Y$. So S'_0, S'_1, and S'_2 partition S'. We prove the following lemma.

Lemma 5.1 *The number l of vertices in Y' adjacent to exactly one vertex in S' is at least* $\max\{\epsilon|S'_0|/10 - 3|S'_1|,\ |S'_1|/9,\ |S'_2|/12 - 3(|S'_0| + |S'_1|)\}$.

Proof: We first show that $l \geq \epsilon|S'_0|/10 - 3|S'_1|$. We first claim that (a) the number of vertices in Y' adjacent to exactly one vertex in S'_0 is at least $\epsilon|S'_0|/10$. Indeed, let $x \in X$ and $y \in Y$ be vertices in Γ. There is exactly one edge in Γ' from X'_v to Y'_y if and only if v and y are adjacent, otherwise there are no edges. So if we let Q be the set of vertices in Y that are adjacent in Γ to exactly one vertex in Q_0, then, for each $y \in Q$, there is exactly one edge bewteen Y'_y and $\cup_{x \in Q_0} X'_x = S'_0$. This implies that there is exactly one vertex y' in Y'_y that is adjacent to a vertex in S'_0, and that y' is also adjacent to exactly one vertex in S'_0, for each $y \in Q$. So to show (a), all we need to show is that $|Q| \geq \epsilon|S'_0|/10$. However, by Theorem 3.1, $Q \geq \epsilon|Q_0|$. Indeed, we first claim that that $|Q_0| \leq \alpha|X|$. Since $|S'| \leq \alpha|X'|/9$, it follows that (i) $|S_0| \leq 2\alpha|X|$, since $|X'| = 2|E(\Gamma)| - |Y| \leq 14|X|$, and $S'_0 \subseteq S'$. But (ii) $|Q_0| \leq |S'_0|/2$ since each vertex in X has degree at least 2 in Γ. So by (i) and (ii), $|Q_0| \leq \alpha|X|$. So by Theorem 3.1, (iii) $|Q|$ is indeed at least $\epsilon|Q_0|$. So we now use (iii) to show that $|Q|$ is at least $\epsilon|S'_0|/10$. However, $|S'_0| \leq 10|Q_0|$, because each vertex in X has degree at most 10 in Γ, so $|Q| \geq \epsilon|S'_0|/10$, and so (a) follows.

Since each vertex has degree at most 3, it follows from (a) that $l \geq \epsilon|S'_0|/10 - 3(|S'_1| + |S'_2|)$. We next prove a tighter lower bound; that (b) $l \geq \epsilon|S'_0|/10$ - $3|S'_1|$. However, (b) follows from Observations 2 and 4. Indeed, let y be an arbitrary vertex in Q, where Q is as in the above paragraph. We claim that (b') there is at least one vertex in Y'_y that is adjacent to exactly one vertex in $S'_0 \cup S'_2$. Indeed, we've already established that there is exactly one vertex y' in Y'_y that is adjacent to a vertex in S'_0, for each $y \in Q$, and that y' is adjacent to exactly one vertex in S'_0. So if $S'_2 \cap X'_y$ is empty, then (b') follows from Observation 4. However, suppose $S'_2 \cap Y'_y = U'$ is nonempty. Then by Observation 2, there is at least 2 vertices in Y'_y adjacent to exactly one vertex in U', so there is at least one vertex in Y'_y adjacent to exactly one vertex in $S'_0 \cap U'$. So (b') follows here as well by Observation 4. Since each vertex has degree at most 3, (b) follows from (b).

Similar arguments can be used to show that (c) $l \geq |S'_2|/12 - 3(|S'_1| + |S'_0|)$. Let $|Q_2|$ be the set of vertices $y \in Y$ such that X'_y is nonempty. By Observation 2, there are at least $2|Q_2|$ vertices in Y' adjacent to exactly one vertex in S'_2. Since each vertex in Y has degree no larger than 25 in Γ, $|X'_y| \leq 24$ for each such $y \in Y$, so $24|Q_2| \leq |S'_2|$. So there are at least $|S'_2|/12$ vertices in Y' that are adjacent to exactly one vertex in S'_2. Since each vertex in Γ' has degree at most 3, (c) follows.

Finally, we prove that (d) $l \geq |S'_1|/9$. Let Q_1 be the set of vertices x of X where $S'_1 \cap X'_x$ is nonempty. By Observation 3, for each $x \in Q_1$, there is at least one vertex y' in Y'_x that is adjacent to exactly one vertex in $S' \cap X'_x$, so the number of vertices adjacent to exactly one vertex in S'_1 is at least $|Q_1|$. However, by Observation 1, that vertex y' is also adjacent to exactly one vertex in S'. So there are at least $|Q_1|$ vertices in Y' adjacent to exactly one vertex in S'. However, each vertex in X has degree at most 10 in Γ, so by definition of S'_1, there can be at most 9 vertices in $X'_x \cap S'$ for each $x \in Q_1$, so $|Q_1| \geq |S'_1|/9$. So (d), and thus Lemma 5.1, follows. ■

So from Lemma 5.1, we can conclude that Γ' is a $(\alpha/9, \epsilon/2^{17})$-unique neighbor expander, and Theorem 4.1 follows. ■