Explicit construction of $q+1$ regular local Ramanujan graphs, for almost all prime-powers q

Rishabh Batra
Indian Institute of Technology,Kanpur,India

Nitin Saxena
Indian Institute of Technology,Kanpur,India

Devansh Shringi
Indian Institute of Technology,Kanpur,India

Abstract

A constant locality function is one in which each output bit depends on just a constant number of input bits. Viola and Wigderson (2018) gave an explicit construction of bipartite degree-3 Ramanujan graphs such that each neighbor of a vertex can be computed using a constant locality function. In this work, we construct the first *explicit local Ramanujan* graph (bipartite) of degree $q+1$, where q is a power of 9 or a power of prime $p \geq 5$.

Alon and Capalbo (2002) used 8-regular and 44-regular Ramanujan graphs to construct unique-neighbor expanders that were 4-regular resp. 6-regular and 'bipartite'. Viola and Wigderson (2018) had asked if a local construction of such unique-neighbor expanders exists. Our construction gives local 8-regular and 44-regular Ramanujan graphs, which also solves the corresponding open problem of the construction of *local* unique-neighbor expanders.

The only known explicit construction of Ramanujan graphs exists for degree $q+1$, where q is a prime-power. In this paper, we essentially *localize* the explicit Ramanujan graphs for $q =$ power-of-9 or power-of-prime $p \geq 5$ (i.e, almost *all* q for which explicit Ramanujan graphs are known). Our results use the explicit Ramanujan graphs by Morgenstern (1994) and the ideas used in Viola and Wigderson (2018). We devise a general way to construct appropriate field extensions of $\mathbb{F}_q$.

2012 ACM Subject Classification Theory of computation → Computational complexity and cryptography; Mathematics of computing → Discrete mathematics; Mathematics of computing → Stochastic processes; Computing methodologies → Symbolic and algebraic manipulation

Keywords and phrases Expanders, Ramanujan graphs, constant locality, NC^0, unique-neighbor expanders, finite fields, residuosity, linear groups, Cayley, Schreier

Digital Object Identifier 10.4230/LIPIcs.BSS.2021.

Acknowledgements N.S. thanks the funding support from SERB (CRG/2020/000045) and N. Rama Rao Chair.

Contents

1 Introduction

Expanders are sparse graphs with strong connectivity properties, due to which they find numerous applications in computer science — decreasing random bits, designing error correcting codes, extractors, pseudo-random generators, hardness amplification, one-way permutations, and proving complexity results; for details, see the survey [13]. Expanders have a lot of practical applications, such as building optimal and cost-efficient computer networks, see [6], which is useful for various network service providers. An important application of expanders is that they help in reducing the number of random bits required for a randomized algorithm. Expanders relate to the construction of error-correcting codes, see [25, 26, 11, 5]. They have been instrumental in proving some important results in complexity theory, such as the PCP theorem [8], and $SL = L$ [24].

Ramanujan graphs are expanders whose spectral gap is as large as possible, see [23]. So they possess the best possible expansion properties; they also tend to have a deep connection to number theory. They have important applications in extremal graph theory and computational complexity theory. Ramanujan graphs are also important in cryptography and can be used to construct low density parity check codes; for more details, see the survey [15].

A lot of these applications require that the neighbors of a given node be computed efficiently; and this has been studied in [4, 12, 3, 7] under various constraints on resources.

We view a d-regular graph as a set of d transition functions $f_i(v) : \{0,1\}^n \to \{0,1\}^n$ where $f_i(v)$ is the i^{th} neighbor of v. A function has *locality* t if each bit of the output depends on only t bits of the input. A graph is t-*local* if all the functions computing its neighbors have locality $\leq t$. The class of functions with constant locality is NC^0. If t is a constant independent of the size of the graph (in an infinite family of graphs), we say the graph has constant locality.

The attention to expanders, where these transition functions have constant locality, was brought in [3]; and in [27] they gave a construction of expander graphs that have locality 1. They also gave construction of degree 3 Ramanujan graphs, which have constant locality.

We answer the question left open in [27, 1] about the construction of local unique-neighbor expanders by providing the first construction of constant locality bipartite Ramanujan graphs to degrees beyond 3.

We construct the first local Ramanujan graphs of degree $q+1$, where q is a power of 9 or a power of prime $p \geq 5$. In particular, making constructions of [1] local required constant locality Ramanujan graphs of degrees 8 and 44, that was left open in [27]; this construction problem we solve in this paper.

1.1 Previous results

The connectivity of a graph is captured by its spectral gap, which is the difference between the moduli of the two largest eigenvalues of the normalized adjacency matrix of the graph. Larger spectral gap implies better connectivity (or *expansion*).

As proved in [23], all sufficiently large d-regular graphs satisfy $\lambda_G \geq 2\sqrt{d-1} - o(1)$, where λ_G is the second-largest eigenvalue in absolute value (while $|\lambda_1| = d$). This gives an upper bound on the spectral gap of expanders. Ramanujan graphs are d-regular graphs with $\lambda_G = 2\sqrt{d-1} - o(1)$, i.e., they are asymptotically the best possible expanders.

Existence and construction of Ramanujan graphs has been of great interest in Computer Science and studied extensively. In [19, 18] it was proved that Ramanujan graphs of all degrees and sizes exist. Explicit construction of Ramanujan graphs of prime+1 degree was given by [17], which were extended to degree =(prime power)+1 in [21]. In [21], they give two constructions, one that works where degree is of the form $2^k + 1$, while the other for degree =(odd prime power)+1. Construction for arbitrary degree is a longstanding open problem [19, 18].

The area of study of small locality is of major interest in theoretical computer science. It was introduced and studied in [3] for AC^0 graphs. In the field of pseudorandomness, [10, 22, 2] gave cryptographic generators of constant locality, where [2] used only logarithmic space.

In [27], an explicit construction of expanders, which were 1-local, was provided. Along with it, they also gave a construction algorithm that made the Ramanujan graph from [21] for degree 3 to be a Ramanujan graph of constant locality.

1.2 Our results

We in this paper give the first construction of bipartite Ramanujan graphs of degree $q+1$, where q is power of any prime $p \geq 5$ or power of 9. We denote the bipartite graph as, $V \times \{0,1\}$ where any vertex (v,a) has a neighbor $(w, 1-a)$. V will be of size $q^n - 1$, where n is of the form $4 \cdot 3^t$, $t \in \mathbb{Z}_{\geq 0}$.

▶ **Theorem 1** (p^k+1 regular). *For any fixed $q = p^k, k \in \mathbb{N}$, prime $p \geq 5$, and variable $n = 4 \cdot 3^t$, there exist $q+1$ explicit $O(\log q)$-local functions $f_1, \ldots, f_{q+1}$ such that the bipartite graph on $2(q^n - 1)$ vertices $(\mathbb{F}_q^n \setminus \{\mathbf{0}\}) \times \{0,1\}$, with $(v,0)$ having neighbors $\{(f_1(v),1), \ldots, (f_{q+1}(v),1)\}$, is a degree $q+1$ Ramanujan graph.*

By explicit, we mean that these functions can be computed in $\text{poly}(n, q)$ time. Also, the graph has a simple description and does not depend on representation theory. Computing the neighbors in this graph is very efficient. Each neighbor of a node can be calculated using $O(n)$ multiplications and additions (in $\mathbb{F}_q$), i.e. in $O(n \cdot \log q \cdot \log\log q)$ time.

We also construct local Ramanujan graphs for degree $3^{2k} + 1$ with some changes in parameters.

▶ **Theorem 2** ($9^k + 1$ regular). *For any fixed $q = 9^k$ and variable $n = 4 \cdot 5^t$, there exist $q+1$ explicit $O(\log q)$-local functions $f_1, \ldots, f_{q+1}$ such that the bipartite graph of $2(q^n - 1)$ vertices $(\mathbb{F}_q^n \setminus \{\mathbf{0}\}) \times \{0,1\}$, with $(v,0)$ having neighbors $\{(f_1(v),1), \ldots, (f_{q+1}(v),1)\}$, is a degree $q+1$ Ramanujan graph.*

1.3 Proof ideas

We build on the construction in [21] of Ramanujan graphs for odd prime powers and make the computation local. For technical reasons, our design fails for $q = 2$-power or 3^{2k+1}; but works for all other prime-powers. In the following discussion, we will design a finite field extension $\mathbb{F}_{q^{n/2}}$; keeping in mind that $4|n$.

For odd prime-power q, the construction in [21] is a Cayley graph with specific generators Γ of the linear groups $PSL(2, \mathbb{F}_{q^{n/2}})$ and $PGL(2, \mathbb{F}_{q^{n/2}})$ (for definitions, see Section 2.3). We

use Schreier graphs, as used in [27], to change the set of vertices to $(\mathbb{F}_q)^n \setminus \{0^n\}$ which are easier to handle as compared to vertices of Cayley graph of $SL(2, \mathbb{F}_{q^{n/2}})$. Each vertex v, in one part of the bipartite, is essentially a 2×1 vector on elements of $\mathbb{F}_{q^{n/2}}$. The calculation of the neighbors of this, boils down to the multiplication of the vertex vector v with the generator matrices in Γ. Constant locality in this means that the number of $\mathbb{F}_q$-additions needed to compute the product vector should be *constant*; as we can view $\mathbb{F}_q$-multiplication as trivially dependent on $\log q$ (independent of n) input bits. We will be using the $PSL(2, \mathbb{F}_{q^{n/2}})$ graph and change it to $SL(2, \mathbb{F}_{q^{n/2}})$ by adding a normalization term; which will be division by the determinant of the generator matrices.

The elements of the generator matrices are heavily dependent on the degree $d := n/2$ polynomial $g(x)$ which is chosen to represent the extension $\mathbb{F}_{q^{n/2}} = \mathbb{F}_{q^d}$. Therefore, it is needed that the terms be chosen in such a way that each generator in Γ has a constant sparsity representation. The polynomial $g(x)$ also has to be of even degree and irreducible in $\mathbb{F}_q[x]$. Moreover, it is required that the normalization factor $1/\sqrt{x}$ lives in $\mathbb{F}_q[x]/\langle g(x)\rangle$. Finally, the degree of $g(x)$ controls the size of the graph; so we want a family of polynomials $\{g_t\}_t$ of increasing degree satisfying *all* of the above conditions.

Case of $q =$ power of prime $p \geq 5$. In contrast to [27], we make a more general choice of $g(x)$, i.e. for a graph of size $2(q^n - 1)$, $n = 2d = 4 \cdot 3^t$, we chose $g(x)$ of degree d as $g_t(x) := (x^{3^t} - b_1)^2 - \alpha \cdot b_2^2$, for an α non-square in $\mathbb{F}_q$, and $b_1, b_2 \in \mathbb{F}_q$. Fixing this α, what is left to show is: $g_t(x)$ is irreducible and $\sqrt{x} \in \mathbb{F}_q[x]/\langle g_t(x)\rangle = \mathbb{F}_{q^d}$. We first reduce the irreducibility property (over all t) to $b_1 + \sqrt{\alpha} \cdot b_2$ being a non-cube in $\mathbb{F}_{q^2}$; and reduce the existence of $\sqrt{x}$ in $\mathbb{F}_q[x]/\langle g_t\rangle$ (for all t) to the base case $t = 0$.

Then using the fact that α is non-square in $\mathbb{F}_q$, we consider $\{1, \sqrt{\alpha}\}$ as a $\mathbb{F}_q$-basis of $\mathbb{F}_{q^2}$, and look at the span using b_1, b_2 as coefficients (unknown as of yet). As $2|(q^2 - 1)$ and $3|(q^2 - 1)$, and that the group $\mathbb{F}_{q^2} \setminus \{0\}$ is cyclic, we have $(q^2 - 1)/2$ squares and $2(q^2 - 1)/3$ non-cubes in the group. Therefore, there will be 'many' elements in $\mathbb{F}_{q^2} \setminus \{0\}$ that are both squares and non-cubes; which gives us the required $b_1, b_2 \in \mathbb{F}_q$. See the details in Section 3.2.

Case of $q =$ power of 9. Here, redefine $g_t(x) := (x^{5^t} - b_1)^2 - \alpha \cdot b_2^2$. The proof works on similar lines as the above case, and uses the fact that for $q = 9^k$, $5|(q^2 - 1)$. This means that there will be elements in $\mathbb{F}_{q^2}$ that are not 5-th powers but are squares. As above, it can be shown that there exist the required $b_1, b_2 \in \mathbb{F}_q$. See the details in Section 3.3.

Once we have designed these special finite fields, we are left with handling the normalization factor, which in our graph comes out to be $1/\sqrt{x}$. To remove this factor, we will use the tools from [27] of double-cover and π-twist of a graph. Our choice of $g(x)$ ensures that $1/\sqrt{x}$ is an element of $\mathbb{F}_{q^d}$. This makes it possible to remove the normalization factor by converting it into a *bipartite* graph and applying the correct twist. See the details in Section 2.2.

1.4 More on the related results

Small or constant locality constructions are an important subject in theoretical computer science, as they make the implementation of the expanders efficient. The first construction of constant locality Ramanujan graphs of degree 3 was given in [27]; making the local construction problem for other degrees a natural open question.

Ramanujan graphs are used for the construction of unique-neighbor expanders, which have widespread applications, see [1]. In [27], the construction of *local* unique-neighbor expanders is left open, as [1] uses 4-regular, 8-regular and 44-regular Cayley Ramanujan graphs. Even though a construction for these Ramanujan graphs was present, constant locality construction was *unknown* till now. In [1, Sec.2], an infinite family of 8-regular

Ramanujan graphs was used to construct 6-regular resp. 4-regular unique-neighbor expanders. Using our construction, constant locality Ramanujan graphs that are 8-regular are possible, which gives the first construction of *local* 6-regular and 4-regular unique-neighbor expanders.

In [1, Sec.4], they also present a simple, explicit family of bounded degree bipartite graphs (referred to as 'bipartite unique-neighbor expanders') which requires an infinite family of 44-regular Ramanujan graphs. Using our construction, we get a local infinite family of 44-regular Ramanujan graphs which gives us the first construction of *local* 'bipartite unique-neighbor expanders', see [1].

Our construction of constant locality Ramanujan graphs is efficiently computable, in time *linear* in n, as we can compute the neighbors for the Ramanujan graphs by transition functions that have constant locality. These can be used to implement expanders more efficiently than the generic method of [21]. Our linear-time efficiency is comparable to the constructions in [20, 9, 14], but the latter expanders were only for the fixed degrees $5, 7, 8, 9, 13$ (thus, unable to reach the eigenvalue bounds of Ramanujan graphs in the limit).

2 Preliminaries

We assume that the graphs that we talk about are undirected, regular and connected. They can be represented using an adjacency matrix, which is a square matrix (symmetric in case of undirected graphs) which shows the number of edges between any two vertices.

Expanders (or expander graphs) are sparse graphs that show strong connectivity properties. The connectivity properties of expanders can be quantified using vertex, edge or spectral expansion. We use spectral expansion to define expanders.

▶ **Definition 3.** ***(Expander)*** *Given a graph G, let λ_G be the second-largest eigenvalue (in magnitude) of the adjacency matrix A_G of the graph. G is called an (n, d, λ) expander if G has n-vertices, is d-regular and has $\lambda_G \leq \lambda$.*

Alon and Bopanna [23] gave a lower bound on the second-largest eigenvalue of the adjacency matrix of a d-regular graph. The graphs that come close to meeting this bound are Ramanujan graphs. In other words, Ramanujan graphs are regular graphs with the maximum possible spectral gap, which makes them excellent spectral expanders.

▶ **Definition 4.** ***(Ramanujan graph)*** *An (n, d, λ) expander G is called a Ramanujan graph if $\lambda_G \leq 2\sqrt{d-1}$.*

2.1 Cayley and Schreier graphs

The initial construction based on [21] is a Cayley graph. A major reason why we consider Cayley graphs, is that their connection to group theory makes the analysis of the spectral gap easier. This yielded the first construction of Ramanujan graphs.

▶ **Definition 5.** ***(Cayley graph [27])*** *Let H be a group. Given a multiset S of elements from H, we form the Cayley graph $Cay(H, S)$ whose vertices are H and where a vertex $h \in H$ has neighbors sh, for every element $s \in S$.*

We will also require the Schreier graph to change the set of vertices to a much simpler set.

▶ **Definition 6.** ***(Schreier graph [27])*** *Suppose that H is a group acting on a set V, namely there is a homomorphism from H to the group of permutations of V. Then we define the Schreier graph $Sch(H, S, V)$, whose vertices are V and where the vertex $v \in V$ has neighbors sv, for every element $s \in S$.*

We will require the following lemma, which shows that the conversion from a Cayley graph to a Schreier graph conserves the spectral gap.

▶ **Lemma 7.** *[27, Lem.2.2] Let λ be an eigenvalue of $Sch(H, S, V)$, then λ is also an eigenvalue of $Cay(H, S)$.*

2.2 Operations related to bipartite graphs

To localize a Ramanujan graph, we will need to convert it into a bipartite graph, while preserving its spectral gap. For this, we will use the double cover of a graph.

▶ **Definition 8.** ***(Double cover of a graph [27])*** *Let G be a graph on vertex set V where vertex v has neighbors $f_i(v)$, $\forall i \in I$. The double-cover of G is the bipartite graph $V \times \{0, 1\}$ where a vertex (v, b) has neighbors $(f_i(v), 1 - b)$, $\forall i \in I$.*

▶ **Lemma 9.** *[27, Fact 2.3] Let G_0 be the double cover of a graph G. If G_0 has eigenvalue λ, then G has eigenvalue λ or $-\lambda$. In particular, the double cover of a Ramanujan graph is a bipartite Ramanujan graph.*

The main idea to go into bipartite version is to apply a twist, which enables us to get rid of a 'non-local multiplication' present inside f_i's.

▶ **Definition 10.** ***(π-twist of a graph [27])*** *Let G be a bipartite graph on vertex set $V \times \{0, 1\}$, where vertex (v, b) has neighbors $(f_i(v), 1 - b)$, $\forall i \in I$. The π-twist of G is the bipartite graph G_0 having the same set of vertices with the modification: vertex $(v, 0) \in G_0$ has neighbors $(\pi f_i v, 1)$, and equivalently vertex $(v, 1) \in G_0$ has neighbors $(f_i \pi^{-1} v, 0)$, $\forall i \in I$.*

Applying a twist conserves the spectral gap.

▶ **Lemma 11.** *[27, Lem.4.2] The eigenvalues of the twisted graph are the same as the original graph, i.e., π-twist preserves the spectral gap.*

2.3 Linear groups

We need the definitions of the following groups for our results. Basically, their action defines the neighbors in the Ramanujan graph.

▶ **Definition 12.** ***(General linear group)*** *The general linear group of degree n over R, denoted by $GL(n, R)$, is defined as the set of $n \times n$ invertible matrices with entries from R, with the operation being the matrix multiplication over R.*

▶ **Definition 13.** ***(Special linear group)*** *The special linear group is the subgroup of $GL(n, R)$ with the additional condition that the determinant of the matrices is 1. It is denoted by $SL(n, R)$.*

So the special linear group of degree n over R, denoted by $SL(n, R)$, is defined as the set of $n \times n$ invertible matrices with determinant 1 having entries from R, with the operation being the matrix multiplication over R.

▶ **Definition 14.** ***(Center of a group)*** *The center of a group G is defined as the set of elements that commute with every element of G. It is denoted as $Z(G) := \{z \in G \,|\, \forall g \in G,\, zg = gz\}$.*

▶ **Definition 15.** ***(Projective linear group)*** *The projective linear group, $PGL(V)$ is the quotient group defined as $PGL(V) := GL(V)/Z(V)$, where $GL(V)$ is the general linear group of V and $Z(V)$ is the center of $GL(V)$.*

▶ **Definition 16.** ***(Projective special linear group)*** *The projective special linear group, $PSL(V)$ is the quotient group defined as $PSL(V) := SL(V)/Z(V)$, where $SL(V)$ is the special linear group of V and $Z(V)$ is the center of $SL(V)$.*

So, the projective linear group $PGL(n, R)$ and the projective special linear group $PSL(n, R)$ are the quotients of $GL(n, R)$ and $SL(n, R)$ by their centers, respectively. The center of $GL(n, R)$ is the collection of *scalar* matrices, $\{sI_n \mid s \in R - \{0\}\}$. The center of $SL(n, R)$ is the subgroup of scalar transformations with *unit* determinant.

2.4 Irreducibility of binomials over finite fields

We will be needing the following lemma for showing irreducibility of polynomial for our field extension. Define $\text{ord}_q(a)$ to be the *multiplicative order* of a in the group $\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$.

▶ **Lemma 17.** *[16, Theorem 3.75] Let $w \geq 2$ be an integer and $a \in \mathbb{F}_q^*$. Then the binomial $x^w - a$ is irreducible in $\mathbb{F}_q[x]$ if and only if the following three conditions are satisfied:*

1. *Every prime divisor p of w divides $\text{ord}_q(a)$*
2. $\gcd\left(w, \frac{q-1}{\text{ord}_q(a)}\right) = 1$
3. *If 4 divides w, then $q = 1 \bmod 4$*

We use the above lemma to get the following result as well.

▶ **Lemma 18.** *If β is non-p-power ($p > 2$ is prime) in $\mathbb{F}_r$, then $x^p - \beta$ is irreducible in $\mathbb{F}_r$.*

Proof. We will be using Lemma 17, with $w = p$, $a = \beta$ and $q = r$. Since β is not p-th power in $\mathbb{F}_r$, we have $p|(r-1)$ (otherwise all elements of $\mathbb{F}_r$ are p-th power) and $\beta^{\frac{r-1}{p}} \neq 1$. Also, $\text{ord}_r(\beta)|(r-1)$. Note that condition 3 is not relevant as p is prime > 2.

For sake of contradiction, assume condition 1 did not hold, and p does not divide $\text{ord}_r(\beta)$, i.e. p and $\text{ord}_r(\beta)$ are coprime. We consider $\beta^{\frac{r-1}{p}} = (\beta^{\frac{r-1}{p \cdot \text{ord}_r(\beta)}})^{\text{ord}_r(\beta)} = 1^{\frac{r-1}{p \cdot \text{ord}_r(\beta)}}$. Since, $p|(r-1)$, $\text{ord}_r(\beta)|(r-1)$ and $\gcd(p, \text{ord}_r(\beta)) = 1$, we can say $\frac{r-1}{p \cdot \text{ord}_r(\beta)}$ is an integer. Therefore, $\beta^{\frac{r-1}{p}} = 1^{\frac{r-1}{p \cdot ord_r(\beta)}} = 1$ which is a contradiction.

Next, assume condition 1 holds but condition 2 does not. So, we have $\gcd\left(p, \frac{r-1}{\text{ord}_r(\beta)}\right) \neq 1$. As p is prime, this means $p|\frac{r-1}{\text{ord}_r(\beta)}$, which again means $\frac{r-1}{p \cdot \text{ord}_r(\beta)}$ is an integer. Therefore, $\beta^{\frac{r-1}{p}} = 1^{\frac{r-1}{p \cdot ord_r(\beta)}} = 1$ which again is a contradiction.

Therefore, for β non-p-power in $\mathbb{F}_r$, $x^p - \beta$ satisfies all the conditions of Lemma 17. Hence $x^p - \beta$ is irreducible. ◀

3 Main results

We start with the construction of Ramanujan graphs given in [21], for degree $q + 1$, where q is power of an odd prime.

▶ **Theorem 19.** *[21, Theorem 4.13]. Let q be an odd prime and ϵ a non-square $\mathbb{F}_q$. Let $g \in \mathbb{F}_q[x]$ be an irreducible polynomial of even degree d, and $\mathbb{F}_{q^d}$ is represented as $\mathbb{F}_q[x]/\langle g(x)\rangle$. Let $L \in \mathbb{F}_{q^d}$ be s.t. $L^2 = \epsilon$ and Γ be the set of matrices,*

$$\Gamma_i = \begin{pmatrix} 1 & \gamma_i - \delta_i L \\ (\gamma_i + \delta_i L)(x-1) & 1 \end{pmatrix} \qquad \forall i \in \{1, \ldots, q+1\}$$

where $\gamma_i, \delta_i \in \mathbb{F}_q$ are all the $q + 1$ solutions in $\mathbb{F}_q$ of $\delta_i^2 \epsilon - \gamma_i^2 = 1$. Then we have:

- *If x is a square* mod $g(x)$*, then the Cayley graph of $PSL(2,\mathbb{F}_{q^d})$ with respect to above generators is a $q+1$ regular Ramanujan graph.*
- *If x is not a square* mod $g(x)$*, then the Cayley graph of $PGL(2,\mathbb{F}_{q^d})$ with respect to above generators is a $q+1$ regular Ramanujan graph.*

We will use $g(x)$ such that $\sqrt{x}$ is in $\mathbb{F}_p[x]/\langle g(x)\rangle$, giving $\mathrm{Cay}(PSL(2,\mathbb{F}_{q^d}),\Gamma)$ as the Ramanujan graph. To make the construction local, we will need $g(x)$ such that $L^2=\epsilon$ has a solution with constant sparsity so that multiplication with the matrix to get neighbors is local.

3.1 Identifying suitable parameters for the Ramanujan graph

This section is dedicated to identifying the following objects, and constructing them efficiently.

▶ **Lemma 20** (Parameters). *Let $q=9^k$ or p^k, prime $p\geq 5$. There exists an explicit polynomial family $g(x)\in\mathbb{F}_q[x]$ with the following properties:*

1. *g is a family of irreducible polynomials in $F_q[x]$ having even degree (which defines the field $\mathbb{F}_{q^d}$).*
2. *$\sqrt{x}\in F_q[x]/\langle g\rangle$ (as we want to use PSL, for which x should be a square).*
3. *$L\notin F_q$ but $L^2\in F_q$ (as we want $L^2=\epsilon$ where ϵ is a non-square in F_q).*
4. *L has constant sparsity (as the computation of a neighbor requires multiplication with the generator matrices and thus all the elements of the matrix should be constant sparsity).*

With an eye on the case of $q=p^k$, prime $p\geq 5$: Let us fix α to be a non-square in $\mathbb{F}_q$, and for (yet to be fixed) $b_1,b_2\in\mathbb{F}_q$ we define a family for $g(x)$ as:

$$g_t(x) \;:=\; (x^{3^t}-b_1)^2-\alpha\cdot b_2^2\,, \qquad \forall t\in\mathbb{Z}_{\geq 0}\,.$$

As $\alpha\cdot b_2^2$ is non-square in $\mathbb{F}_q$, we deduce that $g_0(x)$ is irreducible. For $t\geq 1$, the following lemma reduces the irreducibility of $g_t(x)$ to the existence of the cube root of $b_1+\sqrt{\alpha}\cdot b_2$ in $\mathbb{F}_{q^2}$. (Note: The conjugate $b_1-\sqrt{\alpha}\cdot b_2$ has identical properties due to the automorphism of $\mathbb{F}_{q^2}$.)

▶ **Lemma 21.** *$g_t(x)$ is irreducible in $\mathbb{F}_q[x]$ if and only if $b_1+\sqrt{\alpha}\cdot b_2$ is non-cube in $\mathbb{F}_{q^2}$.*

Proof. Observe that $g_t=(x^{3^t}-b_1-\sqrt{\alpha}\cdot b_2)\cdot(x^{3^t}-b_1+\sqrt{\alpha}\cdot b_2)$ is the factorization over $\mathbb{F}_{q^2}$. Consider its $\mathbb{F}_q$-automorphism $\sigma:\sqrt{\alpha}\mapsto-\sqrt{\alpha}$. Let us denote $(x^{3^t}-b_1-\sqrt{\alpha}\cdot b_2)$ by f_t. Then $(x^{3^t}-b_1+\sqrt{\alpha}\cdot b_2)=\sigma(f_t)$. Assume $\exists h\in\mathbb{F}_q[x]$ such that h divides $g_t=f_t\cdot\sigma(f_t)$. There are only two cases possible:

- **h divides one of f_t and $\sigma(f_t)$**: In this case, h would divide both the factors because if h divides the first factor, then $\sigma(h)=h$ would divide the second factor. So $h^2|g_t$, which contradicts g_t's square-freeness. The square-freeness easily follows from the coprimality of: $g=(x^{3^t}-b_1)^2-\alpha\cdot b_2^2$ and $\frac{dg}{dx}=2\cdot 3^t\cdot x^{3^t-1}(x^{3^t}-b_1)$. So, this case is not possible for a nontrivial h.
- **$\exists u\in\mathbb{F}_{q^2}[x]$ such that $u|f_t$ and $h=u\cdot\sigma(u)$**: If u is nontrivial then $f_t=(x^{3^t}-b_1-\sqrt{\alpha}\cdot b_2)$ is reducible over $\mathbb{F}_{q^2}$. Since $t\geq 1$ and $\mathbb{F}_{q^2}$ has a cube-root of unity, it follows from the following Claim 22 that, $(b_1+\sqrt{\alpha}\cdot b_2)$ is cube in $\mathbb{F}_{q^2}$. So, this case is possible for a nontrivial h iff $b_1+\sqrt{\alpha}\cdot b_2\in\mathbb{F}_{q^2}$ is cube.

◀

▷ Claim 22. If β is non-cube in finite field $\mathbb{F}_r$, then $B(x):=x^{3^t}-\beta$ is irreducible over $\mathbb{F}_r$.

Proof of Claim 22. By Lemma 18 we have, β is a non-cube in $\mathbb{F}_r$ implies $x^3-\beta$ is irreducible in $\mathbb{F}_r$. As seen in its proof, we have $3|\text{ord}_r(\beta)$ and $\gcd\left(3, \frac{r-1}{\text{ord}_r(\beta)}\right) = 1$.

For irreducibility of $x^{3^t}-\beta$, condition 1 of Lemma 17 is satisfied, as 3^t has only one prime factor 3 and $3|\text{ord}_r(\beta)$. For the same reason, $\gcd\left(3, \frac{r-1}{\text{ord}_r(\beta)}\right) = 1$ implies $\gcd\left(3^t, \frac{r-1}{\text{ord}_r(\beta)}\right) = 1$, and hence condition 2 is satisfied. Condition 3 is irrelevant, as $4 \nmid 3^t$. Therefore, we get $x^{3^t}-\beta$ irreducible in $\mathbb{F}_r[x]$. ◀

The following lemma reduces the problem of existence of $\sqrt{x} \in \mathbb{F}_q[x]/\langle g_t(x)\rangle$ to that of the existence of $\sqrt{x} \in \mathbb{F}_q[x]/\langle g_0(x)\rangle$.

▶ **Lemma 23.** *If $\sqrt{x}$ is in $\mathbb{F}_q[x]/\langle g_0\rangle$, then $\sqrt{x}$ is in $\mathbb{F}_q[x]/\langle g_t\rangle, \forall t \geq 1$.*

Proof. We know that $g_0 = (x-b_1)^2 - \alpha \cdot b_2^2$ for the non-square α. Consider $\beta := b_1 + \sqrt{\alpha}\cdot b_2$ in $\mathbb{F}_{q^2}$. From the hypothesis, if x is a square mod g_0, then β (and its conjugate $b_1 - \sqrt{\alpha}\cdot b_2$) is a square in $\mathbb{F}_{q^2}$. Since the field $\mathbb{F}_{q^d} := \mathbb{F}_q[x]/\langle g_t\rangle$ subsumes $\mathbb{F}_{q^2}$, thus, x^{3^t} is a square in $\mathbb{F}_{q^d}$.

We know that the multiplicative group of $\mathbb{F}_{q^d}$ is cyclic. Let λ be a generator of this group; its order is q^d-1. There exists unique $m \in [q^d-1]$ s.t. $x = \lambda^m$, which means $x^{3^t} = \lambda^{m\cdot 3^t}$. Since x^{3^t} is a square, we deduce: $2|(m\cdot 3^t)$, which means $2|m$. Hence, $x = \lambda^m$ itself is a square in $\mathbb{F}_{q^d} = \mathbb{F}_q[x]/\langle g_t\rangle$. ◀

Based on the above Lemmas 21-23, our problem reduces to finding $b_1, b_2 \in \mathbb{F}_q$ such that $b_1 \pm \sqrt{\alpha}\cdot b_2$ is non-cube, but is a square in $\mathbb{F}_{q^2}$. We solve this in the following lemma.

▶ **Lemma 24.** *Assume $q = p^k$, prime $p \geq 5$. There exist $((q^2-1)/6$ many$)$ $b_1, b_2 \in \mathbb{F}_q$ such that, $g_t(x)$ is irreducible and $\sqrt{x}$ exists in $\mathbb{F}_q[x]/\langle g_t\rangle$.*

Proof. From Lemma 21 we know that $g_t(x)$ is irreducible if and only if $b_1 + \sqrt{\alpha}\cdot b_2$ is non-cube in $\mathbb{F}_{q^2}$.

Considering mod g_0, $x = b_1 \pm \sqrt{\alpha}\cdot b_2$. So, $\sqrt{x}$ in $\mathbb{F}_q[x]/\langle g_0\rangle$ is equivalent to $b_1 + \sqrt{\alpha}\cdot b_2$ being a square in $\mathbb{F}_{q^2}$ (recall: α is non-square in $\mathbb{F}_q$).

Clearly, $\{1, \sqrt{\alpha}\}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^2}$. Since q is odd, we know $\mathbb{F}_{q^2}\setminus\{0\}$ is a cyclic group of even order. Thus, the number of squares in $\mathbb{F}_{q^2}\setminus\{0\}$ is $(q^2-1)/2$. Also, as $3 \nmid q$, we have $3|(q^2-1)$, and thus, the number of non-cubes is $2(q^2-1)/3$. Therefore, there are $\geq (q^2-1)/6$ elements y's in $\mathbb{F}_{q^2}\setminus\{0\}$ which are square but non-cube.

As $\{1, \sqrt{\alpha}\}$ is a basis of $\mathbb{F}_{q^2}$, each of these y's give us a unique (b_1, b_2) for which $b_1 + \sqrt{\alpha}\cdot b_2$ is a square but non-cube. ◀

Proof (of Lemma 20 for $q = p^k, p \geq 5$). Set $g(x) = g_t(x)$ of even degree $d = 2\cdot 3^t$. Set $\epsilon = \alpha \cdot b_2^2$ which is non-square, as α is a fixed non-square. To get $L^2 = \epsilon \in \mathbb{F}_q$, we simply set $L = (x^{3^t} - b_1)$ in $\mathbb{F}_q[x]/\langle g_t(x)\rangle$; clearly $L \notin \mathbb{F}_q$. So properties 3 and 4 are satisfied by our choice.

Lemma 24 shows that for our α, there exist 'many' $b_1, b_2 \in \mathbb{F}_q$ such that properties 1 and 2 are satisfied as well.

Thus, going over $t \in \mathbb{Z}_{\geq 0}$, we have constructed an infinite family of explicit g as promised. ◀

3.2 Local Ramanujan graph of deg p^k+1, $p \geq 5$: Proof of Theorem 1

From the previous section, we get that there exists b_1, b_2, for any non-square $\alpha \in \mathbb{F}_q$, where $q = p^k$ for prime $p \geq 5$, s.t. $g = g_t(x) = (x^{3^t} - b_1)^2 - \alpha \cdot b_2^2$ is an irreducible polynomial of even degree $d = 2 \cdot 3^t$, modeling the field $\mathbb{F}_{q^d} = \mathbb{F}_q[x]/\langle g_t(x)\rangle$. As mentioned already, $L = (x^{3^t} - b_1) \in \mathbb{F}_{q^d}$, so that $L^2 = \alpha \cdot b_2^2 = \epsilon$. Denote $z := (1/\sqrt{x}) \in \mathbb{F}_{q^d}$ and matrices $z\Gamma$,

$$z \cdot \Gamma_i := \frac{1}{\sqrt{x}} \begin{pmatrix} 1 & \gamma_i - \delta_i L \\ (\gamma_i + \delta_i L)(x-1) & 1 \end{pmatrix} \qquad \forall i \in \{1, \ldots, q+1\}$$

where $\gamma_i, \delta_i \in \mathbb{F}_q$ are all the $q+1$ solutions of: $\delta_i^2 \epsilon - \gamma_i^2 = 1$.

Since x is a square mod $g(x)$, from Theorem 19 (after adjusting for the normalization factor), we get that the Cayley graph of $SL(2, \mathbb{F}_{q^d})$ with respect to the above generators (i.e. $\mathrm{Cay}(SL(2, \mathbb{F}_{q^d}), \Gamma)$) is a $q+1$ regular Ramanujan graph. The required b_1, b_2 can be found out by simply going over all the values in $\mathbb{F}_q$, and checking the irreducibility of g_0 (Lemma 21) and the existence of $\sqrt{x} \in \mathbb{F}_q[x]/\langle g_0\rangle$ (Lemma 23). All this is easily doable in $\mathrm{poly}(q)$ time (or in *randomized poly(*$\log q$*)-time*).

In our case, we have the normalization factor $z = 1/\sqrt{x}$ which makes the determinants (of our generators) 1. But the problem is that multiplication by z may *not* be local. To solve this, we first construct the Schreier graph from the Cayley graph with the vertex set $V = (\mathbb{F}_{q^d})^2 - \{\mathbf{0}\}$. This means that the number of $\mathbb{F}_q$ elements needed to represent each vertex in V will be $n = 2d = 4 \cdot 3^t$. This new graph will remain a Ramanujan graph as a result of Lemma 7.

So, now we have $\mathrm{Sch}(SL(2, \mathbb{F}_{q^d}), z\Gamma, V)$ as our graph. We now convert this into a bipartite graph by taking a double cover of it. Again, this new bipartite graph is a Ramanujan graph by Lemma 9. The problem of multiplication by z remains to be solved. To solve this, we take the twist of the graph, with the multiplication by $\sqrt{x}$ as the permutation chosen for the twist. As $\sqrt{x}$ is an element of $\mathbb{F}_q[x]/\langle g(x)\rangle$, multiplication by it is equivalent to a permutation of the elements, which can be removed using the appropriate twist. Now, as we have multiplied each node by $\sqrt{x}$, we can see that we can remove the normalization factor z from the functions $(z\Gamma_1, z\Gamma_2, z\Gamma_3 \ldots z\Gamma_{q+1})$ to calculate the neighbor. So only multiplication by $(\Gamma_1, \Gamma_2, \Gamma_3 \ldots \Gamma_{q+1})$ needs to be done, which is local (as we will easily show). By Lemma 11, we have this new graph as a Ramanujan graph as well.

Final graph parameters. Let $n = 4 \cdot 3^t, t \in \mathbb{Z}_{\geq 0}$, $d = n/2$, and $\mathbb{F}_{q^d} = \mathbb{F}_q[x]/\langle g_t\rangle$. We define $G = G_t$ to be the graph obtained as: start with $\mathrm{Sch}(\, SL(2, \mathbb{F}_{q^d}),\, z\Gamma,\, V = \mathbb{F}_q^n - \{\mathbf{0}\}\,)$, take its double cover, and apply the twist equivalent of multiplying with $\sqrt{x} \in \mathbb{F}_{q^d}$. Thus, G is a bipartite graph on vertices $(\mathbb{F}_q^n - \{\mathbf{0}\}) \times \{0, 1\}$ with neighbors of $(v, 0)$ being $(\Gamma_i \cdot v,\, 1)$ where matrices Γ_i are as in Theorem 19.

▶ **Lemma 25** (Locality). *G is a $q+1$ regular Ramanujan graph, with the transition functions $f_1, \ldots, f_{q+1}$, where $(f_i(v), 1) := (\Gamma_i \cdot v,\, 1)$ is the i-th neighbor of $(v, 0)$, such that $\forall i \in [q+1]$, f_i has constant locality ($= O(\log q)$).*

Proof. We get from Theorem 19 that $\mathrm{Cay}(SL(2, \mathbb{F}_{q^d}), z\Gamma)$ is a $q+1$ regular graph. By Lemma 7 we know that $\mathrm{Sch}(\, SL(2, \mathbb{F}_{q^d}),\, z\Gamma,\, V = \mathbb{F}_q^n - \{\mathbf{0}\}\,)$ is also a Ramanujan graph. By Lemmas 9-11, we get that after applying double cover and twist, spectral gap remains the same, and z gets removed. Therefore, G is a $q+1$ regular Ramanujan graph. Now we need to show: each f_i has constant locality.

Looking at the transition function Γ_i in detail, we see that the only non-trivial steps are multiplication by L and x (multiplication by $\mathbb{F}_q$ elements is independent of n). Multiplication

by x is just a combination of a cyclic shift and possibly one addition, which can be done locally. Recall, $L = x^{d/2} - b_1$ and $g(x) = (x^{d/2} - b_1)^2 - \alpha \cdot b_2^2 = L^2 - \epsilon$. When L multiplies, the multiplication by b_1 is trivial (has $O(\log q)$-locality, which is constant with respect to n). So, only multiplication by $x^{d/2}$ needs careful analysis. We see that, in $\mathbb{F}_q[x]/\langle g(x)\rangle$, we can write $x^d =: p_1 x^{d/2} + p_2$, where $p_1 = 2b_1$ and $p_2 = \alpha \cdot b_2^2 - b_1^2$; so $p_1, p_2 \in \mathbb{F}_q$.

Write any element $y \in \mathbb{F}_q[x]/\langle g(x)\rangle$ as $y =: (y_2, y_1)$, where vector y_2 (resp. y_1) corresponds to the most (resp. least) significant $d/2$ coefficients of powers of x. Write multiplication by $x^{d/2}$ as:

$$\begin{aligned} x^{d/2} \cdot y &= \sum_{j<d} c_j \cdot x^{j+d/2} = \sum_{0\le j<d/2} c_j \cdot x^{j+d/2} + \sum_{0\le j<d/2} c_{j+d/2} \cdot x^{j+d} \\ &= x^{d/2} \cdot \sum_{0\le j<d/2} c_j x^j \;+\; (p_1 x^{d/2} + p_2) \cdot \sum_{0\le j<d/2} c_{j+d/2} \cdot x^j \\ &= x^{d/2} \cdot \sum_{0\le j<d/2} (c_j + p_1 c_{j+d/2}) \cdot x^j \;+\; p_2 \cdot \sum_{0\le j<d/2} c_{j+d/2} \cdot x^j \\ &= (p_1 y_2 + y_1,\, p_2 y_2)\,. \end{aligned}$$

Since, p_1, p_2 are $\mathbb{F}_q$ elements, the locality of multiplication is $O(\log q)$ = constant with respect to the size of the graph (as t, n grow). This shows that all the operations in the transition functions are local. ◀

Proof (of Theorem 1). From Lemma 25 we saw that the graph G is a $q+1$ regular bipartite Ramanujan graph with $2(q^n - 1)$ vertices, and their transition functions having constant locality (i.e. independent of n). Thus, neighbors of $(v, 0)$ can be computed in constant locality. We can obtain the transition functions for all sizes, using poly(q)-time preprocessing to find $\alpha, b_1, b_2 \in \mathbb{F}_q$.

We see that, similar to [27], our construction for Ramanujan graphs is also efficiently computable; as generation of (and multiplication by) x and L can be efficiently done. Calculating f_i's require $O(n)$ $\mathbb{F}_q$-multiplications (while calculating $p_1 y_2, p_2 y_2$) and $O(n)$ additions, as sparsity of terms is constant (in Γ_i). This makes the expander explicit with $O(n \cdot \log q \cdot \log\log q)$-time. This completes the proof of Theorem 1. ◀

3.3 Local Ramanujan graph of degree $3^{2k} + 1$: Proof of Theorem 2

Let q be a 9-power. This case needs a different treatment as $\mathbb{F}_q$ has non-squares, but it does not have a non-cube! Similar to the previous section, we fix α to be a non-square in $\alpha \in \mathbb{F}_q$. For some $b_1, b_2 \in \mathbb{F}_q$ (yet to be fixed) and the variable $t \in \mathbb{Z}_{\ge 0}$, we define a family for polynomial $g(x)$ as:

$$g_t(x) \;:=\; (x^{5^t} - b_1)^2 - \alpha \cdot b_2^2\,.$$

Lemma 21 translates in this case to $b_1 + \sqrt{\alpha} \cdot b_2$ not being 5-th power in $\mathbb{F}_{q^2}$. The proof idea is similar: as $5 \,|\, (q^2 - 1)$ means that $\mathbb{F}_{q^2}$ has a non-5th-power. Moreover, $(x^{5^t} - b_1)^2 - \alpha \cdot b_2^2$ factors into the coprime factors $(x^{5^t} - b_1 - \sqrt{\alpha} \cdot b_2)$ and $(x^{5^t} - b_1 + \sqrt{\alpha} \cdot b_2)$. Any factor dividing one of them will also divide the other under the automorphism $\sigma : \sqrt{\alpha} \mapsto -\sqrt{\alpha}$. Thus, $(x^{5^t} - b_1 - \sqrt{\alpha} \cdot b_2)$ must be irreducible over $\mathbb{F}_{q^2}$ for g_t to be irreducible over $\mathbb{F}_q$. So, $b_1 + \sqrt{\alpha} \cdot b_2$ should be non-5th-power in $\mathbb{F}_{q^2}$.

Lemma 23 remains the same on replacing 3^t by 5^t. Thus, $\sqrt{x} \in \mathbb{F}_q[x]/\langle g_0\rangle$ implies $\sqrt{x} \in \mathbb{F}_q[y]/\langle g_t(y)\rangle$, $\forall t \ge 1$.

Thus, the question boils down to showing the existence of $b_1, b_2 \in \mathbb{F}_q$ such that $b_1 + \sqrt{\alpha} \cdot b_2$ is square in $\mathbb{F}_{q^2}$, but non-5th-power.

▶ **Lemma 26.** *Assume $q = 9^k$. There exist $(3(q^2-1)/10$ many$)$ $b_1, b_2 \in \mathbb{F}_q$ such that, $g_t(x)$ is irreducible and $\sqrt{x}$ exists in $\mathbb{F}_q[x]/\langle g_t \rangle$.*

Proof. From the above discussion, we know that $g_t(x)$ is irreducible if and only if $b_1 + \sqrt{\alpha} \cdot b_2$ is non-5th-power in $\mathbb{F}_{q^2}$.

Considering mod g_0, $x = b_1 \pm \sqrt{\alpha} \cdot b_2$. So, $\sqrt{x}$ in $\mathbb{F}_q[x]/\langle g_0 \rangle$ is equivalent to $b_1 + \sqrt{\alpha} \cdot b_2$ being a square in $\mathbb{F}_{q^2}$ (recall: α is non-square in $\mathbb{F}_q$).

Clearly, $\{1, \sqrt{\alpha}\}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^2}$. Since q is odd, we know $\mathbb{F}_{q^2} \setminus \{0\}$ is a cyclic group of even order. Thus, the number of squares in $\mathbb{F}_{q^2} \setminus \{0\}$ is $(q^2-1)/2$. Also, as $q \equiv (-1)^k \bmod 5$, we have $5|(q^2-1)$, and thus, the number of non-5th-power is $4(q^2-1)/5$. Therefore, there are $\geq 3(q^2-1)/10$ elements y's in $\mathbb{F}_{q^2} \setminus \{0\}$ which are square but non-5th-power.

As $\{1, \sqrt{\alpha}\}$ is a basis of $\mathbb{F}_{q^2}$, each of these y's give us a unique (b_1, b_2) for which $b_1 + \sqrt{\alpha} \cdot b_2$ is a square but non-5th-power. ◀

Proof (of Theorem 2). Following the proof of Lemma 25, now with $n = 2d = 4 \cdot 5^t$, we deduce that the graph G is a $q+1$ regular bipartite Ramanujan graph with $2(q^n-1)$ vertices, and their transition functions having constant locality (namely, $O(\log q)$, independent of n). Thus, neighbors of $(v, 0)$ can be computed in constant locality. We can obtain the transition functions for all sizes, using poly(q)-time preprocessing to find $\alpha, b_1, b_2 \in \mathbb{F}_q$.

Exactly like in the proof of Theorem 1, our construction for Ramanujan graphs is also efficiently computable. In fact, the expander is explicit in $O(n \cdot \log q \cdot \log\log q)$-time. This completes the proof of Theorem 2. ◀

4 Conclusion

We give the first construction of bipartite Ramanujan graphs of constant locality of degree $q+1$, $q = p^k$, prime $p \geq 5$ of size $2(q^n-1)$, where n is of the form $4 \cdot 3^t$. We also give the first construction of bipartite Ramanujan graphs for $q = 9^k$, of size $2(q^m-1)$, where m is of the form $4 \cdot 5^t$. This solves the construction problem for constant-locality Ramanujan graphs, which was previously known *only* for degree 3.

Our results allow the construction of local 6-regular resp. 4-regular unique-neighbor expanders, and local 'bipartite' unique-neighbor expanders, see [1].

Our work leaves the following questions still open:

1. Construct constant-locality Ramanujan graphs of degree $3^{2m+1}+1$ resp. 2^k+1.
2. Construct Ramanujan graphs of locality 1.
3. Construct *non*-bipartite constant-locality Ramanujan graphs.
4. Construct local 3-regular unique-neighbor expanders. (This is subsumed in point 1 above.)
5. Construct Ramanujan graphs of degree $q+1$, where q is *not* a prime-power.

References

1 Noga Alon and Michael Capalbo. Explicit unique-neighbor expanders. In *The 43rd Annual IEEE Symposium on Foundations of Computer Science, (FOCS 2002). Proceedings*, pages 73–79. IEEE, 2002.

2 Benny Applebaum, Yuval Ishai, and Eyal Kushilevitz. Cryptography in NCˆ0. *SIAM Journal on Computing*, 36(4):845–888, 2006.

3 Sanjeev Arora, David Steurer, and Avi Wigderson. Towards a study of low-complexity graphs. In *International Colloquium on Automata, Languages, and Programming*, pages 119–131. Springer, 2009.

4 Ziv Bar-Yossef, Oded Goldreich, and Avi Wigderson. Deterministic amplification of space-bounded probabilistic algorithms. In *Proceedings. Fourteenth Annual IEEE Conference on Computational Complexity (Formerly: Structure in Complexity Theory Conference)(Cat. No. 99CB36317)*, pages 188–198. IEEE, 1999.

5 Alexander Barg and Gilles Zémor. Error exponents of expander codes. *IEEE Transactions on Information Theory*, 48(6):1725–1729, 2002.

6 Ho Yee Cheung, Lap Chi Lau, and Kai Man Leung. Graph connectivities, network coding, and expander graphs. *IEEE 52nd Annual Symposium on Foundations of Computer Science (FOCS 2011)*, pages 190–199, 2011.

7 Scott Diehl and Dieter Van Melkebeek. Time-space lower bounds for the polynomial-time hierarchy on randomized machines. *SIAM Journal on Computing*, 36(3):563–594, 2006.

8 Irit Dinur. The PCP theorem by gap amplification. *Journal of the ACM*, 54(3):12–es, 2007.

9 Ofer Gabber and Zvi Galil. Explicit constructions of linear-sized superconcentrators. *Journal of Computer and System Sciences*, 22(3):407–420, 1981.

10 Oded Goldreich. Candidate one-way functions based on expander graphs. *IACR Cryptol. ePrint Arch.*, 2000:63, 2000.

11 Venkatesan Guruswami. Guest column: error-correcting codes and expander graphs. *ACM SIGACT News*, 35(3):25–41, 2004.

12 Dan Gutfreund and Emanuele Viola. Fooling parity tests with parity gates. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 381–392. Springer, 2004.

13 Shlomo Hoory, Nathan Linial, and Avi Wigderson. Expander graphs and their applications. *Bulletin of the American Mathematical Society*, 43(4):439–561, 2006.

14 Shuji Jimbo and Akira Maruoka. Expanders obtained from affine transformations. In *Proceedings of the 17th annual ACM Symposium on Theory of Computing (STOC)*, pages 88–97, 1985.

15 Wen-Ching Winnie Li. A survey of Ramanujan graphs. *Arithmetic, Geometry, and Coding Theory, Luminy, France*, pages 127–143, 1993.

16 Rudolf Lidl and Harald Niederreiter. *Introduction to finite fields and their applications*. Cambridge university press, 1994.

17 Alexander Lubotzky, Ralph Phillips, and Peter Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988.

18 Adam Marcus, Daniel A Spielman, and Nikhil Srivastava. Interlacing families I: Bipartite Ramanujan graphs of all degrees. In *IEEE 54th Annual Symposium on Foundations of Computer Science*, pages 529–537. IEEE, 2013.

19 Adam W Marcus, Daniel A Spielman, and Nikhil Srivastava. Interlacing families IV: Bipartite Ramanujan graphs of all sizes. *SIAM Journal on Computing*, 47(6):2488–2509, 2018.

20 Grigorii Aleksandrovich Margulis. Explicit constructions of concentrators. *Problemy Peredachi Informatsii*, 9(4):71–80, 1973.

21 Moshe Morgenstern. Existence and explicit constructions of $q + 1$ regular Ramanujan graphs for every prime power q. *Journal of Combinatorial Theory, Series B*, 62(1):44–62, 1994.

22 Elchanan Mossel, Amir Shpilka, and Luca Trevisan. On epsilon-biased generators in NCˆ0. In *Annual Symposium on Foundations of Computer Science*, volume 44, pages 136–145. Citeseer, 2003.

23 Alon Nilli. On the second eigenvalue of a graph. *Discrete Mathematics*, 91(2):207–210, 1991.

24 Omer Reingold. Undirected connectivity in log-space. *Journal of the ACM (JACM)*, 55(4):1–24, 2008.

25 Michael Sipser and Daniel A Spielman. Expander codes. *IEEE transactions on Information Theory*, 42(6):1710–1722, 1996.

26 Daniel A Spielman. Constructing error-correcting codes from expander graphs. In *Emerging Applications of Number Theory*, pages 591–600. Springer, 1999.

27 Emanuele Viola and Avi Wigderson. Local expanders. *computational complexity*, 27(2):225–244, 2018.