EXPLICIT CONSTRUCTION OF $Q + 1$ REGULAR LOCAL RAMANUJAN GRAPHS, FOR ALL PRIME-POWERS Q

Rishabh Batra, Nitin Saxena, and Devansh Shringi

June 3, 2022

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 $q > 2$ is any prime power.

Alon and Capalbo (2002) used 4-regular, 8-regular and 44-regular Ramanujan graphs to construct unique-neighbor expanders that were 3-regular, 4-regular, 6-regular and 'bipartite' (respectively). Viola and Wigderson (2018) had asked if a local construction of such unique-neighbor expanders exists. Our construction gives local 4-regular, 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 *all* these degrees. Our results use the explicit Ramanujan graphs by Morgenstern (1994) and a significant generalization of the ideas used in Viola and Wigderson (2018).

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

Subject classification. Theory of computation– Algebraic complexity theory, Fixed parameter tractability, Pseudorandomness and derandomization; Computing methodologies– Algebraic algorithms; Mathematics of computing– Combinatoric problems.

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 Hoory *et al.* (2006). Expanders have a lot of practical applications, such as building optimal and cost-efficient computer networks, see Cheung *et al.* (2011), 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 Barg & Zémor (2002); Guruswami (2004); Sipser & Spielman (1996); Spielman (1999). They have been instrumental in proving some important results in complexity theory, such as the PCP theorem Dinur (2007), and $SL = L$ Reingold (2008).

Ramanujan graphs are expanders whose spectral gap is as large as possible, see Nilli (1991). 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 Li (1993).

A lot of these applications require that the neighbors of a given node be computed efficiently; and this has been studied in Arora *et al.* (2009); Bar-Yossef *et al.* (1999); Diehl & Van Melkebeek (2006); Gutfreund & Viola (2004) under various constraints on resources.

We view a d-regular graph as a set of d transition functions $f_i : \mathcal{V} \to \mathcal{V}$ where $f_i(v)$ is the i^{th} neighbor of the vertex $v \in \mathcal{V}$. 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 Arora *et al.* (2009); and in Viola & Wigderson (2018) 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 Alon & Capalbo (2002); Viola & Wigderson (2018) 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 $q > 2$ is any prime power.

In particular, making constructions of Alon & Capalbo (2002) local required constant locality Ramanujan graphs of degrees $4, 8$ *and* 44, *that was left open in Viola & Wigderson (2018); 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 Nilli (1991), 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 Marcus *et al.* (2013, 2018) it was proved that bipartite Ramanujan graphs of all degrees and sizes exist. Explicit construction of Ramanujan graphs of prime+1 degree was given by Lubotzky *et al.* (1988), which were extended to degree =(prime power)+1 in Morgenstern (1994). In Morgenstern (1994), 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 Marcus *et al.* (2013, 2018).

The area of study of small locality is of major interest in theoretical computer science. It was introduced and studied in Arora *et al.* (2009) for AC^0 graphs. In the field of pseudorandomness, Applebaum *et al.* (2006); Goldreich (2000); Mossel *et al.* (2003) gave cryptographic generators of constant locality, where Applebaum *et al.* (2006) used only logarithmic space.

In Viola & Wigderson (2018), an explicit construction of expanders, which were 1-local, was provided. Along with it, the authors also gave a construction algorithm that made the Ramanujan graph from Morgenstern (1994) for degree 3 to be a Ramanujan graph of constant locality.

1.2. Our results. In this paper, we give the first construction of local bipartite Ramanujan graphs of degree $q+1$, where q is power of any prime p. We denote the bipartite graph as, $\mathcal{V} \times \{0,1\}$ where any vertex (v,a) has a neighbor $(w, 1-a)$. The vertex set $\mathcal{V}$ will be of size $q^n - 1$. The parameter n takes values depending on the prime power q.

Theorem 1.1. *[$p=2$] For any $q = 2^k$, 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. Here n is an increasing parameter of form $4 \cdot 3^t$, for every $t \geq 0$, which gives us an infinite family of local, $q+1$-degree Ramanujan graphs.*

In the case of odd p, we need to slightly modify $\mathcal{V}$: by 'clubbing together' the distinct values v and $-v$, in an unordered way.

Theorem 1.2 (Odd p). *For any $q = p^k$ where p is arbitrary odd prime, there exist $q+1$ explicit $O(\log q)$-local functions $f_1, \ldots, f_{q+1}$ such that the bipartite graph on $(q^n - 1)$ vertices $\mathcal{V} \times \{0,1\}$, where $\mathcal{V} := \{\{v,-v\} | v \in (\mathbb{F}_q^n \setminus \{\mathbf{0}\})\}$ where $\{v,-v\}$ denotes an unordered set, with $(\{v,-v\},0)$ having neighbors $\{(f_1(\{v,-v\}),1), \ldots, (f_{q+1}(\{v,-v\}),1)\}$, is a degree $q+1$ Ramanujan graph. Here n is an increasing parameter whose allowed values depend on q (infinitely* *many for each q), which gives us an infinite family of local, $q+1$-degree Ramanujan graphs.*

The unordered set $\{v, -v\}$ is input to the transition functions bit-by-bit. By explicit, we mean that these functions can be computed in poly(n, q) time. Also, the graph has a simple description and we do not require additional results from 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.

This gives the first construction of constant locality Ramanujan graphs that are $q+1$-regular for all prime powers $q > 2$, greatly extending the work started in Viola & Wigderson (2018).

1.3. Proof ideas.

Our construction differs in the cases of prime $p = 2, 3$ and ≥ 5. We discuss the main ideas now.

1.3.1. For q = even prime power.

The case of $q = 2$ was already solved in Viola & Wigderson (2018). We will be localizing the construction given in Theorem 5.13 of Morgenstern (1994).

The original construction of Morgenstern (1994) is a Cayley graph with specific generators Γ of the linear groups $PSL(2, \mathbb{F}_{q^{n/2}})$ (for definitions, see Section 2.3). The extension $\mathbb{F}_{q^{n/2}}$ was defined using an irreducible polynomial of even degree $n/2$. The computation in calculating neighbors had mainly 2 non-local components, the elements of the generators (depends on $L \in \mathbb{F}_{q^{n/2}}$, solution of $L^2 + L + \epsilon$, $\epsilon \in \mathbb{F}_q$ such that $x^2 + x + \epsilon$ is irreducible), which get multiplied, can have high sparsity ($O(n)$) and the multiplication with the normalizing factor (so determinant is 1).

In Viola & Wigderson (2018), for construction of degree 3 graphs, the authors move to an easier to represent vertex set of $\mathbb{F}_2^n$ by consider action of $SL(2, \mathbb{F}_{2^{n/2}})$(isomorphic to $PSL(2, \mathbb{F}_{2^{n/2}})$) on $(\mathbb{F}_2^{n/2})^2 \setminus \{\mathbf{0}\}$. The extension is defined using the polynomial $g(x) = x^n + x^{n/2} + 1$ for $n = 2 \cdot 3^t$ as $\mathbb{F}_2[x]/\langle g(x) \rangle$, which makes $L = x^{n/2}$ sparse. Multiplication with the normalizing factor $\frac{1}{\sqrt{x+1}}$ is handled by taking double cover of the graph and applying twist equivalent to multiplication with the factor.

This approach fails for $q = 2^k$ as the family is no longer irreducible for all t and hence cannot be used to make the extension.

For odd q's, the construction in Morgenstern (1994) has small differences that put more constraints on the extension and g. We give more general (g) explicit families for all prime power q's, that satisfying the required properties, thus localizing the known constructions.

For $q = 2^k$, in construction of Morgenstern (1994), we have an ϵ such that $x^2 + x + \epsilon$ is irreducible in $\mathbb{F}_q$. The idea is that as $3|q^2 - 1$, we have elements that are not cubes in $\mathbb{F}_{q^2}$. We choose $g_t(x) := (b_2 \cdot x^{3^t} - b_1)^2 + (b_2 \cdot x^{3^t} - b_1) + \epsilon$. Let $\alpha \in \mathbb{F}_{q^2}$ be the root of $x^2 + x + \epsilon$, which means $x^2 + x + \epsilon$ factors as $(x + \alpha)(x + \alpha + 1)$ in $\mathbb{F}_{q^2}$. This means, after substitution, $g_t(x)$ is irreducible iff there exist $b_1, b_2 \in \mathbb{F}_q$ such that $\frac{\alpha+b_1}{b_2}$ and $\frac{\alpha+b_1+1}{b_2}$ are not cubes in $\mathbb{F}_{q^2}$. Then we show the existence of required $b_1, b_2 \in \mathbb{F}_q$ for any such α by using the bound on the number of cubes in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. The construction for even characteristic requires L as solution of $L^2 + L + \epsilon$ in $\mathbb{F}_{q^d}$, which we get in our construction $L = b_2 \cdot x^{3^t} - b_1$, which is of constant locality.

So we get the required design of finite field for all even characteristics. Now, we use the fact that $PSL(2, \mathbb{F}_{q^{n/2}})$ is isomorphic to $SL(2, \mathbb{F}_{q^{n/2}})$ if q is power of 2. This means $\mathrm{Cay}(SL(2, \mathbb{F}_{q^{n/2}}), \Gamma)$ is a Ramanujan graph from Morgenstern (1994), which we convert to $\mathrm{Sch}(SL(2, \mathbb{F}_{q^{n/2}}), \Gamma, V = \mathbb{F}_q^n \setminus \{\mathbf{0}\})$ preserving spectral gap, with neighbor of $(v, 0)$ being $(\Gamma v, 1)$. Once again, we are left with handling the normalization factor, which for even characteristics construction from Morgenstern (1994) comes out to be $1/\sqrt{1 + x}$ (same as Viola & Wigderson (2018)). To remove this factor, we see that since $\mathbb{F}_q[x]/\langle g_t(x)\rangle$ is a field extension of power of 2, all elements are squares in $\mathbb{F}_q$. In particular, $1 + x$ is a square in $\mathbb{F}_q[x]/\langle g_t(x)\rangle$ which ensures that $1/\sqrt{1 + x}$ is an element of $\mathbb{F}_q[x]/\langle g_t(x)\rangle$. So to remove the normalization factor, we just need to convert the graph into a bipartite graph and then apply the correct twist. See the details in Section 3.1.

1.3.2. For q = odd prime power. We build on the construction in Morgenstern (1994) of Ramanujan graphs for odd prime powers and make the computation local. 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 Morgenstern (1994) is a Cayley graph with specific generators Γ of the linear groups $PSL(2, \mathbb{F}_{q^{n/2}})$ (for definitions, see Section 2.3). The non-locality comes from elements of Γ depending on $L \in \mathbb{F}_{q^{n/2}}$, which is a solution of $L^2 = \epsilon$, ϵ non-square in $\mathbb{F}_q$ and normalization factor $\frac{1}{\sqrt{x}}$. We use Schreier graphs, as used in Viola & Wigderson (2018), to change the set of vertices to $\mathcal{V} := \{\{v, -v\} | v \in (\mathbb{F}_q^n \setminus \{\mathbf{0}\})\}$ which are easier to handle as compared to vertices of Cayley graph of $PSL(2, \mathbb{F}_{q^{n/2}})$. Vector $v \in (\mathbb{F}_q^n \setminus \{\mathbf{0}\})$ is considered as a 2×1 vector with elements in $\mathbb{F}_q^{n/2}$. Therefore, each vertex, in one part of the bipartite, is essentially an *unordered* set containing two 2×1 vectors on elements of $\mathbb{F}_{q^{n/2}}$. The calculation of the neighbors of this set, boils down to the multiplication of the vertex vectors v and $-v$ with the generator matrices in Γ, i.e. $(\{v, -v\}, 0)$ has i-th neighbor $(\{\Gamma_i v, -\Gamma_i v\}, 1)$. This ensured that the action of Γ_i and $-\Gamma_i$ is the same, which means the $PSL(2, \mathbb{F}_{q^{n/2}})$ action is well-defined on the set $\mathcal{V}$ and hence we can convert to Schreier graph (note: The center of $SL(2, \mathbb{F}_{q^{n/2}})$ is ± 1; see Section 2.3). Constant locality in this means that the number of $\mathbb{F}_q$-additions needed to compute the product vectors 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 along with adding a normalization term to generator matrices when converting to Schreier graph; 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 Viola & Wigderson (2018), 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 3.4.

Illustrative example. Considering an example of $q=5$, we see that the possible values for α are 2 and 3. For $\alpha := 2$, we see that $b_1 := 1 =: b_2$ gives a polynomial family $(x^{3^t}-1)^2-2$ satisfying the required conditions: which can be seen by checking irreducibility of $(x^3-1)^2-2$ in $\mathbb{F}_5[x]$ and the existence of $\sqrt{x}=x+2$ in $\mathbb{F}_5[x]/\langle (x-1)^2-2\rangle$, which translates to the existence of the same for larger t. Similarly, for $\alpha := 3$, we set $b_1 := 1, b_2 := 3$, giving the same family $(x^{3^t}-1)^2-2$. We show that the density of b_1, b_2 for any α is high, i.e. a random choice works with high probability. Checking if b_1, b_2 satisfy the condition requires computing in $\mathbb{F}_{q^2}$: $(b_1+\alpha\cdot b_2)^{(q^2-1)/2}$ and $(b_1+\alpha\cdot b_2)^{(q^2-1)/3}$, which can easily be done in poly$(\log q)$ time.

Case of $q=3^k, k>1$. In this case, we define r to be the smallest *odd* prime factor of q^2-1. We define $g_t(x) := (x^{r^t}-b_1)^2-\alpha\cdot b_2^2$ in this case. The proof works on similar lines as the above case, using $r|(q^2-1)$ and $2|(q^2-1)$, we have that there will be elements in $\mathbb{F}_{q^2}$ that are not r-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 3.5.

Case of $q=3$. In this case, we see that $q^2-1=8$, which is a power of 2. So the previous techniques do not work here, as all elements have r^{th}-root for any prime $r>2$. So, in this case, we go to the extension $\mathbb{F}_{3^4}$. It has size 80 and so it has elements that are not 5^{th}

powers. In $\mathbb{F}_3$, we see that 2 is the only non-square. So $\sqrt{2}$ helps in generating $\mathbb{F}_{3^2}$. Similarly, $1+\sqrt{2}$ is not a square in $\mathbb{F}_{3^2}$ and hence $\sqrt{1+\sqrt{2}}$ will generate $\mathbb{F}_{3^4}$. We also compute that $(1+\sqrt{1+\sqrt{2}})$ is not 5^{th} power in $\mathbb{F}_{3^4}$, hence becoming the base of the generating polynomial family. We set as $g_0 := x^4+x^3-x+1 = (x+1)^4+x$ which completely factors in $\mathbb{F}_{3^4}$ with roots $(1\pm\sqrt{1\pm\sqrt{2}})^2$ which we know are not 5^{th} powers and are by definition a square in $\mathbb{F}_{3^4}$. This allows us to create the irreducible family as $g_t(x) = (x^{5^t}+1)^4+x^{5^t}$ with x as a square as x^{5^t} is a square.

The equation $L^2 = 2$ has a solution in the extension $\mathbb{F}_{3^4} = \mathbb{F}_q[x]/\langle g_0\rangle$ as $L = x^3+x^2+x+1$ works. For higher t, this becomes $L = x^{3\cdot 5^t}+x^{2\cdot 5^t}+x^{5^t}+1$, therefore satisfying the constant locality condition as t increases. This gives us the infinite family satisfying the required conditions. See the details in Section 3.6.

These three cases give us the design of the finite fields for all odd-characteristics (q being any odd prime-power). Once we have designed these special finite fields, we are left with handling the normalization factor, which for odd characteristics construction from Morgenstern (1994) comes out to be $1/\sqrt{x}$. To remove this factor, we will use the tools from Viola & Wigderson (2018) 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 Viola & Wigderson (2018); 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 Alon & Capalbo (2002). In Viola & Wigderson (2018), the construction of *local* unique-neighbor expanders is left open, as Alon & Capalbo (2002) 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 (Alon & Capalbo 2002, Sec.2), an infinite family of 4-regular and 8-regular Ramanujan graphs was used to construct 3-regular,4-regular and 6-regular unique-neighbor expanders. Using our construction, constant locality Ramanujan graphs that are 4-regular and 8-regular are possible, which gives the first construction of *local* 3-regular, 4-regular and 6-regular unique-neighbor expanders. In construction of 3-regular unique-neighbor expanders, the vertex set of the unique neighbor expanders is edge set of Ramanujan graph, and 2 edges are connected if they have common vertex and the other vertices are $f_i(v)$ and $f_j(v)$ in the 8-regular Ramanujan graph where $|i-j|$ is 1, 4 or 7. As computation of f_i's can be done locally, the unique-neighbor expanders are also local. The construction for other degree are also similarly local.

In (Alon & Capalbo 2002, 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 Alon & Capalbo (2002).

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 Morgenstern (1994) which required time quadratic in n. Our linear-time efficiency is comparable to the constructions in Gabber & Galil (1981); Jimbo & Maruoka (1985); Margulis (1973), 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 2.1. ***(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 $\lambda_G \leq \lambda$.*

A lower bound on the second-largest eigenvalue of the adjacency matrix of a d-regular graph was given in Nilli (1991). 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 2.2. ***(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 Morgenstern (1994) 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 2.3. ***(Cayley graph, Viola & Wigderson (2018))*** *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 2.4. ***(Schreier graph, Viola & Wigderson (2018))*** *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 2.5. *(Viola & Wigderson 2018, Lem.2.2) If λ is 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 bipartite double cover of a graph.

Definition 2.6. ***(Bipartite double cover of a graph, Viola & Wigderson (2018))*** *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 2.7. *(Viola & Wigderson 2018, Fact 2.3) Let G_0 be the bipartite 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 a bipartite version of a graph is to apply a twist, which enables us to get rid of a 'non-local multiplication' present inside f_i's.

Definition 2.8. ***(π-twist of a graph, Viola & Wigderson (2018))*** *Let G be a bipartite graph on vertex set $V \times \{0,1\}$, where vertex (v,b) has neighbors $(f_i(v), 1-b)$, $\forall i \in I$ and π be a permutation on the vertex set. 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 2.9. *(Viola & Wigderson 2018, 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 2.10. ***(Special linear group)*** *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 2.11. ***(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 2.12. ***(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 special linear group $PSL(n, R)$ is the quotient of $SL(n, R)$ by their centers, respectively. The center of $SL(n, R)$ is the subgroup of scalar transformations with *unit* determinant. Therefore, center of $SL(2, R) = \{I_2, -I_2\}$.

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 $\mathrm{ord}_q(a)$ to be the *multiplicative order* of a in the group $\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$.

Theorem 2.13. *(Lidl & Niederreiter 1994, 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:*

(i) *Every prime divisor p of w divides* $\mathrm{ord}_q(a)$

(ii) $\gcd\left(w, \frac{q-1}{\mathrm{ord}_q(a)}\right) = 1$

(iii) *If 4 divides w, then* $q = 1 \bmod 4$

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

LEMMA 2.14. *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 Theorem 2.13, 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 $\beta^{\frac{r-1}{p}} \neq 1$. β can be written as a^k, where a is a generator of $\mathbb{F}_r^*$, giving $\beta^{(r-1)/p} = a^{k(r-1)/p}$, which if $= 1$, will mean that a's order divides $k(r-1)/p$. But we know $\mathrm{ord}(a) = (r-1)$, which means $p|k$, which means β is a p-th power. Also, $\mathrm{ord}_r(\beta)|(r-1)$. 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 $\mathrm{ord_r}(\beta)$, i.e. p and $\mathrm{ord_r}(\beta)$ are coprime. We consider $\beta^{\frac{r-1}{p}} = (\beta^{\frac{r-1}{p\cdot \mathrm{ord}_r(\beta)}})^{\mathrm{ord}_r(\beta)} = 1^{\frac{r-1}{p\cdot \mathrm{ord}_r(\beta)}}$. Since, $p|(r-1)$, $\mathrm{ord}_r(\beta)|(r-1)$ and $\gcd(p, \mathrm{ord}_r(\beta)) = 1$, we can say $\frac{r-1}{p\cdot \mathrm{ord}_r(\beta)}$ is an integer. Therefore, $\beta^{\frac{r-1}{p}} = 1^{\frac{r-1}{p\cdot \mathrm{ord}_r(\beta)}} = 1$ which is a contradiction.

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

Therefore, for β non-p-power in $\mathbb{F}_r$, $x^p - \beta$ satisfies all the conditions of Theorem 2.13. Hence, $x^p - \beta$ is irreducible. □

We lastly prove the following claim,

CLAIM 2.15. *For any prime power $p \geq 3$, if β is non-p-power in finite field $\mathbb{F}_r$, then $B(x) := x^{p^t} - \beta$ is irreducible over $\mathbb{F}_r$.*

PROOF (of Claim 2.15). By Lemma 2.14 we have, β is a non-p-power in $\mathbb{F}_r$ implies $x^p - \beta$ is irreducible in $\mathbb{F}_r$. As seen in its proof, we have $p|\mathrm{ord}_r(\beta)$ and $\gcd\left(p, \frac{r-1}{\mathrm{ord}_r(\beta)}\right) = 1$.

For irreducibility of $x^{p^t} - \beta$, condition 1 of Theorem 2.13 is satisfied, as p^t has only one prime factor p and $p|\mathrm{ord}_r(\beta)$. For the same reason, $\gcd\left(p, \frac{r-1}{\mathrm{ord}_r(\beta)}\right) = 1$ implies $\gcd\left(p^t, \frac{r-1}{\mathrm{ord}_r(\beta)}\right) = 1$, and hence condition 2 is satisfied. Condition 3 is irrelevant, as $4 \nmid p^t$, for p prime > 2. Therefore, we get $x^{p^t} - \beta$ irreducible in $\mathbb{F}_r[x]$. □

3. Main Results

3.1. Local Ramanujan graph of deg $2^k+1, k>1$: Proof of Theorem 1.1. First, we look at the construction of Ramanujan Graphs in Morgenstern (1994) for q power of 2.

Theorem 3.1. *(Morgenstern 1994, Theorem 5.13) Let q be a power of 2 and $f(x)=x^2+x+\epsilon$ irreducible in $\mathbb{F}_q[x]$. Let $g(x)\in\mathbb{F}_q[x]$ be irreducible 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 a root of $f(x)$, and*

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

where $\gamma_i,\delta_i\in\mathbb{F}_q$ are all the $q+1$ solutions in $\mathbb{F}_q$ of $\gamma_i^2+\gamma_i\delta_i+\delta_i^2\epsilon=1$. Then the Cayley graph of $PSL(2,\mathbb{F}_{q^d})$ with Γ as generators is a $q+1$ regular Ramanujan graph.

For any ϵ such that $x^2+x+\epsilon$ is irreducible over $\mathbb{F}_q$, we choose $g_t(x)$ as

$$g_t(x) := (b_2\cdot x^{3^t}-b_1)^2+(b_2\cdot x^{3^t}-b_1)+\epsilon$$

We show that there exist $b_1\in\mathbb{F}_q$ and $b_2\in\mathbb{F}_q^*$ such that g_t is irreducible, and the extension using it gives local Ramanujan graphs.

Lemma 3.2. *Consider the extension of $\mathbb{F}_q$ to $\mathbb{F}_{q^2}$, and let $\alpha\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q$ be a root of $x^2+x+\epsilon$. g_t is irreducible iff $\frac{\alpha+b_1}{b_2}$ and $\frac{\alpha+b_1+1}{b_2}$ are not cubes in $\mathbb{F}_{q^2}$.*

Proof. As α is a root of $f=x^2+x+\epsilon$ in $\mathbb{F}_{q^2}$, the factorization of f in $\mathbb{F}_{q^2}$ will be $(x+\alpha+1)(x+\alpha)$. So g_t factorizes as $(b_2\cdot x^{3^t}-b_1+\alpha)(b_2\cdot x^{3^t}-b_1+\alpha+1)$ in $\mathbb{F}_{q^2}$. By Claim 2.15, we have if $\frac{\alpha+b_1}{b_2}$ and $\frac{\alpha+b_1+1}{b_2}$ are not cubes in $\mathbb{F}_{q^2}$, then $u:=(b_2\cdot x^{3^t}-b_1+\alpha)$ and $v:=(b_2\cdot x^{3^t}-b_1+\alpha+1)$ are irreducible in $\mathbb{F}_{q^2}$. Any factor of g_t, say $h\in\mathbb{F}_q[x]$, has to either divide one of u,v; or one of h's factor in $\mathbb{F}_{q^2}$ will have to divide u,v. But then the irreducibility of u,v, implies h is trivial and g_t is irreducible (over $\mathbb{F}_q$). □

Lemma 3.3. *For $q = 2^k$, $k \geq 2$, and for any $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, there exist $b_1, b_2 \in \mathbb{F}_q$, $b_2 \neq 0$, such that both $\frac{\alpha+b_1}{b_2}$ and $\frac{\alpha+b_1+1}{b_2}$ are not cubes in $\mathbb{F}_{q^2}$.*

Proof. Let $b_3 \in \mathbb{F}_q^*$ be the multiplicative inverse of b_2. So we need to show $b_3\alpha + b_1b_3$ and $b_3\alpha + b_1b_3 + b_3$ are not both cubes. We know that the number of cubes in $\mathbb{F}_{q^2}^*$ is $\frac{q^2-1}{3}$, and the number of non-cubes is $\frac{2(q^2-1)}{3}$. Also, the number of cubes in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ is $\leq \frac{q^2-1}{3}$ and number of non-cubes is $\geq \frac{2(q^2-1)}{3} - q$. As $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, $\{1, \sqrt{\alpha}\}$ is a $\mathbb{F}_q$-basis of $\mathbb{F}_{q^2}$. So $b_3\alpha + b_1b_3$ will attain values in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ (as $b_3 \neq 0$).

For the sake of contradiction, assume that whenever $b_3\alpha + b_1b_3$ is not a cube, $b_3\alpha + b_1b_3 + b_3$ is a cube (as we vary $b_1 \in \mathbb{F}_q, b_2 \in \mathbb{F}_q^*$). The number of non-cube values attained by $b_3\alpha + b_1b_3$ is $\geq \frac{2(q^2-1)}{3} - q$, which would mean that the number of cube values attained by $b_3\alpha + b_1b_3 + b_3$ is $\geq \frac{2(q^2-1)}{3} - q$. But the number of cubes in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ is $\leq \frac{q^2-1}{3}$; which is a contradiction for all $q \geq 4$. □

Thus, we have for any ϵ s.t. $x^2 + x + \epsilon$ is irreducible in $\mathbb{F}_q$, there exist b_1, b_2 such that $g_t(x)$ is irreducible of even degree $d = 2 \cdot 3^t$, modeling the field $\mathbb{F}_{q^d} := \mathbb{F}_q[x]/\langle g_t(x)\rangle$. The parameter L for our choice of g_t will be $b_2 \cdot x^{3^t} - b_1$, which has constant locality. Using Theorem 3.1 we get that $\mathrm{Cay}(PSL(2, \mathbb{F}_{q^d}), \Gamma)$ is a Ramanujan graph. We consider $\mathrm{Cay}(SL(2, \mathbb{F}_{q^d}), z\Gamma)$, after adding the normalization constant z equal to $\frac{1}{\sqrt{x+1}}$ (as determinant of $\Gamma = x + 1$); as $PSL(2, \mathbb{F}_{q^d})$ is isomorphic to $SL(2, \mathbb{F}_{q^d})$ in characteristic 2.

Using Lemma 2.5, we can as well move to the graph $\mathrm{Sch}(SL(2, \mathbb{F}_{q^d}), z\Gamma, \mathbb{F}_q^n \setminus \{\mathbf{0}\})$, where $n := 2d = 4 \cdot 3^t$. As fields $\mathbb{F}_q$ of characteristic 2 have size 2^λ, and $\mathbb{F}_q^*$ have size $2^\lambda - 1$, all elements of $\mathbb{F}_q$ are squares (as, $\gcd(2, 2^\lambda - 1) = 1$). So, z is an element of $\mathbb{F}_{q^d}$, and multiplication by it can be removed by taking double cover and applying the required twist.

Finally, we also give local construction of Ramanujan graphs for degree $2^k + 1$, $k \geq 2$.

Theorem 3.4 ($2^k + 1$ regular, $k > 1$). *For any fixed $q = 2^k$, 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 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.

Proof (of Theorem 3.4). We get from Theorem 3.1 that Cay$(PSL(2, \mathbb{F}_{q^d}), z\Gamma)$ is a $q+1$ regular graph. By Lemma 2.5 we know that Sch$(\,PSL(2, \mathbb{F}_{q^d}),\ z\Gamma,\ \mathbb{F}_q^n \setminus \{\mathbf{0}\}\,)$ is also a Ramanujan graph. By Lemma 2.7-Lemma 2.9, 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, which is just multiplication by Γ_i.

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). Recall, $L = b_2 \cdot x^{d/2} - b_1$ and $g(x) = (b_2 x^{d/2} - b_1)^2 + (b_2 x^{d/2} - b_1) + \epsilon = L^2 + L + \epsilon$. 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 $p_1 = \frac{1}{b_2}$ and $p_2 = \frac{b_1^2+b_1+\epsilon}{b_2^2}$; 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 1.1). Combining Theorem 3.4 and the result from Viola & Wigderson (2018), we see that we get the construction for $q+1$-regular bipartite local Ramanujan graph, for all 2-powers q. This completes the proof of Theorem 1.1. □

3.2. Ramanujan graphs of deg p^k+1, $p \neq 2$. We start with the construction of Ramanujan graphs given in Morgenstern (1994), for degree $q+1$, where q is power of an odd prime.

THEOREM 3.5. *(Morgenstern 1994, 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 if x is a square $\bmod g(x)$, then the Cayley graph of $PSL(2, \mathbb{F}_{q^d})$ with respect to above generators is a $q+1$ regular Ramanujan graph.

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. We divide the task of localizing into the following three cases (in the order of technical difficulty):

1. $q = p^k$, $p \geq 5$,
2. $q = 3^k$, $k \geq 2$,
3. $q = 3$.

3.3. First case: Identifying suitable parameters for the Ramanujan graph. This section is dedicated to identifying the following objects, and constructing them efficiently.

Lemma 3.6 (Parameters). *Let q be any odd prime power. There exists an explicit polynomial family $g(x) \in \mathbb{F}_q[x]$ with the following properties:*

(i) g is a family of irreducible polynomials in $\mathbb{F}_q[x]$ having even degree (which defines the field $\mathbb{F}_{q^d}$).

(ii) $\sqrt{x} \in \mathbb{F}_q[x]/\langle g \rangle$ (as we want to use PSL, for which x should be a square).

(iii) $L \notin \mathbb{F}_q$ but $L^2 \in \mathbb{F}_q$ (as we want $L^2 = \epsilon$ where ϵ is a non-square in $\mathbb{F}_q$).

(iv) 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 3.7. *$g_t(x)$ 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 2.15 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.

□

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 3.8. *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 Lemma 3.7-Lemma 3.8, 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 3.9. *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 3.7 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 $\bmod g_0$, $x = b_1 \pm \sqrt{\alpha} \cdot b_2$. 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 3.6 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 (iii)-(iv) are satisfied by our choice.

Lemma 3.9 shows that for our α, there exist 'many' $b_1, b_2 \in \mathbb{F}_q$ such that properties (i)-(ii) are satisfied as well.

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

3.4. Local Ramanujan graph of deg $p^k + 1$, $p \geq 5$.

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 $\bmod g(x)$, from Theorem 3.5, we get that the Cayley graph of $PSL(2, \mathbb{F}_{q^d})$ with respect to the above generators (i.e. Cay$(PSL(2, \mathbb{F}_{q^d}), \Gamma)$) 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 3.7) and the existence of $\sqrt{x} \in \mathbb{F}_q[x]/\langle g_0 \rangle$ (Lemma 3.8). Using Lemma 3.9, we get see that a random b_1, b_2 satisfy this with probability $\frac{1}{6}$, which means, All this is easily doable in poly(q) time (or in *randomized poly(*$\log q$*)-time*).

Note that the center of $SL(2, \mathbb{F}_{q^d})$ is ± 1 (see Section 2.3). Inspired by that, we define $\mathcal{V} := \{\{v, -v\} | v \in (\mathbb{F}_{q^d}^2 \setminus \{\mathbf{0}\})\}$ and action of $A \in PSL(2, \mathbb{F}_{q^d})$ as $\{v, -v\} \mapsto \{Av, -Av\}$. As the matrices are invertible, A acts like a permutation on the vertices. Now, we consider the graph $\mathrm{Sch}(PSL(2, \mathbb{F}_{q^d}), z\Gamma, \mathcal{V})$. This means that the number of $\mathbb{F}_q$ elements needed to represent each vertex in $\mathcal{V}$ will be $n = 2d = 4 \cdot 3^t$. This new graph will remain a Ramanujan graph as a result of Lemma 2.5. We add 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.

So, now we have $\mathrm{Sch}(PSL(2, \mathbb{F}_{q^d}), z\Gamma, \mathcal{V})$ 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 2.7. 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 2.9, 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 $\mathrm{Sch}(PSL(2, \mathbb{F}_{q^d})$, $z\Gamma$, $\mathcal{V})$, 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 $\mathcal{V} := \{\{v, -v\} | v \in (\mathbb{F}_{q^d}^2 \setminus \{\mathbf{0}\})\}$ with neighbors of $(\{v, -v\}, 0)$ being $(\{\Gamma_i v, -\Gamma_i v\}, 1)$, where matrices Γ_i are as in Theorem 3.5.

LEMMA 3.10 (Locality). *G is a $q+1$ regular Ramanujan graph, with the transition functions $f_1, \ldots, f_{q+1}$, where $(f_i(\{v, -v\}), 1) := (\{\Gamma_i v, -\Gamma_i v\},\ 1)$ is the i-th neighbor of $(\{v, -v\}, 0)$, such that $\forall i \in [q+1]$, f_i has constant locality ($= O(\log q)$).*

PROOF. We get from Theorem 3.5 that $\mathrm{Cay}(PSL(2, \mathbb{F}_{q^d}), z\Gamma)$ is a $q+1$ regular graph. By Lemma 2.5 we know that $\mathrm{Sch}(\, PSL(2, \mathbb{F}_{q^d}),\ z\Gamma,\ \mathcal{V}\,)$ is also a Ramanujan graph. By Lemma 2.7-Lemma 2.9, 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). The multiplication with v and $-v$ has the only effect of doubling the locality. 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. The total number of additions required to calculate $\Gamma_i v$ is 8, hence the total locality will be $16 \log q$. □

This completes the construction of local Ramanujan graphs for degree p^k for prime $p \geq 5$.

Theorem 3.11 ($p^k + 1$ 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 $(q^n - 1)$ vertices $\mathcal{V} \times \{0, 1\}$, where $\mathcal{V} := \{\{v, -v\} | v \in (\mathbb{F}_q^n \setminus \{\mathbf{0}\})\}$ where $\{v, -v\}$ denotes an unordered set, with $(\{v, -v\}, 0)$ having neighbors $\{(f_1(\{v, -v\}), 1), \ldots, (f_{q+1}(\{v, -v\}), 1)\}$, is a degree $q+1$ Ramanujan graph.*

Proof (of Theorem 3.11). From Lemma 3.10 we saw that the graph G is a $q+1$ regular bipartite Ramanujan graph with $(q^n - 1)$ vertices, and their transition functions having constant locality (i.e. independent of n). Thus, neighbors of $(\{v, -v\}, 0)$ 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 Viola & Wigderson (2018), 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 3.11. □

3.5. Local Ramanujan graph of degree $3^k + 1, k \geq 2$:. In this case, we have $q = 3^k$. This case needs a different treatment as $\mathbb{F}_q$ has non-squares, but it does not have a non-cube!

We will look at $q^2 - 1 = (q-1)(q+1)$, $q = 3^k$. We observe that $q^2 - 1$ will have a prime factor $r > 3$: as $q - 1, q + 1$ are not divisible by 3 and they cannot be 2-power simultaneously (as $2(q-1) > (q+1)$). We fix r to be the smallest such prime factor. Eg. for even k, $r = 5$.

We fix α to be a non-square in $\mathbb{F}_q$, for $b_1, b_2 \in \mathbb{F}_q$ (yet to be fixed) we define a family of polynomials $g_t(x)$ for $t \geq 1$ as:

$$g_t(x) := (x^{r^t} - b_1)^2 - \alpha \cdot b_2^2$$

Lemma 3.12 (Non-rth square). *There exist ($\frac{(r-2)(q^2-1)}{2r}$ many) $b_1, b_2 \in \mathbb{F}_q$ such that g_t is irreducible and x is a square in $\mathbb{F}_q[x]/\langle g_t \rangle$.*

Proof. As done in Lemma 3.7, $(x^{r^t} - b_1)^2 - \alpha \cdot b_2^2$ factors into the coprime factors $(x^{r^t} - b_1 - \sqrt{\alpha} \cdot b_2)$ and $(x^{r^t} - b_1 + \sqrt{\alpha} \cdot b_2)$. Any factor dividing one of them will also divide the other under the automorphism $\sigma : \sqrt{\alpha} \mapsto -\sqrt{\alpha}$. Thus, $(x^{r^t} - b_1 - \sqrt{\alpha} \cdot b_2)$ must be irreducible over $\mathbb{F}_{q^2}$ for g_t to be irreducible over $\mathbb{F}_q$. By Claim 2.15, we have $x^{r^t} - b_1 - \sqrt{\alpha} \cdot b_2$ irreducible if $b_1 + \sqrt{\alpha} \cdot b_2$ is not r-th power in $\mathbb{F}_{q^2}$, as r is a prime > 3.

Lemma 3.8 remains the same on replacing 3^t by r^t. Thus, $\sqrt{x} \in \mathbb{F}_q[x]/\langle g_0 \rangle$ implies $\sqrt{x} \in \mathbb{F}_q[x]/\langle g_t(x) \rangle$, $\forall t \geq 1$. Considering mod g_0, $x = b_1 \pm \sqrt{\alpha} \cdot b_2$, therefore $\sqrt{x} \in \mathbb{F}_q[x]/\langle g_0 \rangle$, is equivalent to $b_1 + \sqrt{\alpha} \cdot b_2$ being a square in $\mathbb{F}_{q^2}$.

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-rth-power.

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 $(q^2 - 1)/2$. From our choice of r, we know $r|(q^2 - 1)$, and thus, the number of non-rth-power is $(r-1)(q^2-1)/r$. Therefore, there are $\geq \frac{(r-2)}{2r}$ elements y in $\mathbb{F}_{q^2} \setminus \{0\}$ which are square but not-rth-power.

Clearly, $\{1, \sqrt{\alpha}\}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^2}$. Each of the y's obtained above gives a unique (b_1, b_2) for which $b_1 + \sqrt{\alpha} \cdot b_2$ is square in $\mathbb{F}_{q^2}$, but non-rth-power. □

This give us the construction of local Ramanujan graphs for degree $3^k + 1$ ($k \geq 2$).

Theorem 3.13 ($3^k + 1$ regular, $k > 1$). *For any fixed $q = 3^k$, r such that r is the smallest prime > 3 dividing $q^2 - 1$, and variable $n = 4 \cdot r^t$, there exist $q + 1$ explicit $O(\log q)$-local functions $f_1, \ldots, f_{q+1}$ such that the bipartite graph on $(q^n - 1)$ vertices $\mathcal{V} \times \{0, 1\}$, where $\mathcal{V} := \{\{v, -v\} | v \in (\mathbb{F}_q^n \setminus \{\mathbf{0}\})\}$ where*

$\{v,-v\}$ *denotes an unordered set, with* $(\{v,-v\},0)$ *having neighbors* $\{(f_1(\{v,-v\}),1),\ldots,(f_{q+1}(\{v,-v\}),1)\}$*, is a degree* $q+1$ *Ramanujan graph.*

Proof (of Theorem 3.13). Following the proof of Lemma 3.10, now with $n=2d=4\cdot r^t$, we deduce that the graph G is a $q+1$ regular bipartite Ramanujan graph with (q^n-1) vertices, and their transition functions having constant locality (namely, $O(\log q)$, independent of n). Thus, neighbors of $(\{v,-v\},0)$ 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 3.11, 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 3.13. □

3.6. Local Ramanujan graphs of degree 4: Wrap-up Theorem 1.2. For $q=3$, the only non-square in $\mathbb{F}_q$ is 2. We need g satisfying the conditions of Lemma 3.6, with ϵ fixed to 2. We use the following family of polynomials for g as $t\geq 1$:

$$g_t(x)=(x^{5^t}+1)^4+x^{5^t}$$

Lemma 3.14. *For* $q=3$ *and* $\epsilon=2$, $g_t(x)=(x^{5^t}+1)^4+x^{5^t}$ *satisfies all the properties of Lemma 3.6.*

Proof. We know as 2 is non-square in $\mathbb{F}_3$, $\sqrt{2}$ generates $\mathbb{F}_{3^2}$. Looking in $\mathbb{F}_{3^2}=\mathbb{F}_3[x]/\langle x^2-2\rangle$, we see that $1\pm\sqrt{2}$ is a non-square and hence $\sqrt{1\pm\sqrt{2}}$ will generate $\mathbb{F}_{3^4}$. Denote the values $(1\pm\sqrt{1\pm\sqrt{2}})^2$ by $\alpha_1,\alpha_2,\alpha_3,\alpha_4$. We consider the polynomial in $\mathbb{F}_3[x]$ with these roots in $\mathbb{F}_{3^4}$, which is $x^4+x^3-x+1=(x+1)^4+x$, i.e. g_0. We know g_0 is irreducible as its roots are in $\mathbb{F}_{3^4}$ but not in lower extensions. Now if we consider g_t, we can see that in $\mathbb{F}_{3^4}$, it factorizes as $\prod_{i=1}^4(x^{5^t}-\alpha_i)$.

Let h be a factor of g_t in $\mathbb{F}_q[x]$. In $\mathbb{F}_{q^4}[x]$, h cannot divide a product of three of the factors $(x^{5^t}-\alpha_i)$: as a composition of the two maps $\sigma_1:\sqrt{2}\mapsto-\sqrt{2}$ or $\sigma_2:\sqrt{1+\sqrt{2}}\mapsto-\sqrt{1+\sqrt{2}}$ will 'cover' any remaining factor. Therefore, h must have 4 factors in $\mathbb{F}_{q^4}$, each of which will divide one of $x^{5^t} - \alpha_i$. So, proving anyone irreducible, means g_t is irreducible. It is easy to see that $\alpha_1^{(q^4-1)/5} = \alpha_1^{16} \neq 1$ in $\mathbb{F}_{q^4}$ and hence α_1 is a non-5-th-power in $\mathbb{F}_{q^4}$. Using Claim 2.15, we get that $x^{5^t} - \alpha_1$ is irreducible over $\mathbb{F}_{q^4}$, and hence g_t is irreducible in $\mathbb{F}_q$.

Lemma 3.8 remains the same on replacing 3^t by 5^t. Thus, $\sqrt{x} \in \mathbb{F}_q[x]/\langle g_0 \rangle$ implies $\sqrt{x} \in \mathbb{F}_q[x]/\langle g_t(x) \rangle$, $\forall t \geq 1$. Considering mod g_0, we have $x = (1 + \sqrt{1+\sqrt{2}})^2$, which is a square of $1 + \sqrt{1+\sqrt{2}}$ which is in $\mathbb{F}_{q^4}$. Precisely, $\sqrt{x} = x^3 + x^2 + 2x + 1$ in $\mathbb{F}_q[x]/\langle g_0 \rangle$.

We observe that $(x^3 + x^2 + x + 1)^2 = 2$ in $\mathbb{F}_q[x]/\langle g_0(x) \rangle$. Therefore, we set $L := x^{3\cdot 5^t} + x^{2\cdot 5^t} + x^{5^t} + 1$, giving us $L^2 = 2 \bmod g_t(x)$. L also has constant sparsity of 4. Thus, $g_t = (x^{5^t} + 1)^4 + x^{5^t}$ satisfies all the four properties of Lemma 3.6. □

Using Theorem 3.5 we get that $\mathrm{Cay}(PSL(2, \mathbb{F}_q[x]/\langle g_t \rangle), \Gamma)$ is a Ramanujan graph. We consider $\mathrm{Cay}(PSL(2, \mathbb{F}_q[x]/\langle g_t \rangle), z\Gamma)$, after adding the normalization constant z equal to $\frac{1}{\sqrt{x}}$. Using Lemma 2.5, we have $\mathrm{Sch}(PSL(2, \mathbb{F}_q[x]/\langle g_t \rangle), z\Gamma, \mathbb{F}_q^n)$, where $n = 2d = 8 \cdot 5^t$. As we already have $\sqrt{x} \in \mathbb{F}_{q^d} := \mathbb{F}_q[x]/\langle g_t \rangle$, z is an element of $\mathbb{F}_{q^d}$, and multiplication by it can be removed by taking double cover and applying the required twist. Thus, we have a bipartite Ramanujan graph G where neighbors of $(\{v, -v\}, 0)$ being $\{(f_1(\{v, -v\}), 1)$.

Lemma 3.15. *Multiplication of* Γ *matrices with a vector in* $\mathbb{F}_{q^d}^2$, $q = 3$, $d = 4 \cdot 5^t$ *and* $g_t(x) := (x^{5^t} + 1)^4 + x^{5^t} = x^d + x^{3d/4} - x^{d/4} + 1$ *has constant locality.*

Proof. Multiplication with Γ involves the main non-trivial steps as multiplication with x and L. Multiplication with x is just a cyclic shift among values of $\mathbb{F}_{q^d}$ and possibly 3 additions, which have $O(\log q)$ locality. Recall $L = x^{3\cdot 5^t} + x^{2\cdot 5^t} + x^{5^t} + 1 = x^{3d/4} + x^{d/2} + x^{d/4} + 1$. So, we need to show multiplication with $x^{3d/4}$, $x^{d/2}$, and $x^{d/4}$ is local as well in $\mathbb{F}_{q^d}$. We also see that modulo g_t, $x^d = -x^{3d/4} + x^{d/4} - 1$.

Let the input be $y \in \mathbb{F}_{q^d}$, $y = \sum_{i<d} c_i \cdot x^i$ with which we will consider multiplication with $x^{3d/4}$. We write it as (y_4, y_3, y_2, y_1), where vector y_4 corresponds to the most significant $d/4$ coefficients of power of x, y_3 the next significant $d/4$ coefficients and y_2 the next $d/4$, while y_1 to the $d/4$ least significant coefficients. Multiplication with $x^{d/4}$ is thus,

$$\begin{aligned}
x^{d/4} \cdot y &= \sum_{i<d} c_i \cdot x^{i+3d/4} \\
&= \sum_{i<d/4} c_i \cdot x^{i+d/4} + \sum_{i<d/4} c_{i+d/4} \cdot x^{i+d/2} + \sum_{i<d/4} c_{i+d/2} \cdot x^{i+3d/4} \\
&+ \sum_{i<d/4} c_{i+3d/4} \cdot x^{i+d} \\
&= \sum_{i<d/4} c_i \cdot x^{i+d/4} + \sum_{i<d/4} c_{i+d/4} \cdot x^{i+d/2} + \sum_{i<d/4} c_{i+d/2} \cdot x^{i+3d/4} \\
&+ (-x^{3d/4} + x^{d/4} - 1) \cdot \sum_{i<d/4} c_{i+3d/4} \cdot x^i \\
&= x^{3d/4} \sum_{i<d/4} (c_{i+d/2} - c_{i+3d/4}) \cdot x^i \; + \; x^{d/2} \sum_{i<d/4} c_{i+d/4} \cdot x^i \\
&+ \; x^{d/4} \sum_{i<d/4} (c_i + c_{i+3d/4}) \cdot x^i \; - \; \sum_{i<d/4} c_{i+3d/4} \cdot x^i \\
&= (y_3 - y_4, y_2, y_1 + y_4, -y_4)
\end{aligned}$$

Thus, multiplication with $x^{d/4}$ can easily be done in constant locality. Similarly, it can be shown that $x^{d/2} \cdot y = (y_2 - y_3 + y_4, y_1 + y_4, y_3 + y_4, y_4 - y_3)$ and $x^{3d/4} \cdot y = (y_1 - y_2 + y_3, y_3 + y_4, y_2 + y_3 - y_4, y_3 - y_2 - y_4)$. Therefore, multiplication by L can be done in constant locality and hence multiplication of Γ with an element of $(\mathbb{F}_3)^n$ can be done in constant locality. □

This leads to the following construction of Ramanujan graphs for degree $3+1$.

Theorem 3.16 (4 regular). *For $q = 3$, and variable $n = 8 \cdot 5^t$, there exist $q+1$ explicit constant locality functions $f_1, \ldots, f_{q+1}$*

such that the bipartite graph of such that the bipartite graph on $(q^n - 1)$ *vertices* $\mathcal{V} \times \{0, 1\}$, *where* $\mathcal{V} := \{\{v, -v\} | v \in (\mathbb{F}_q^n \setminus \{\mathbf{0}\})\}$ *where* $\{v, -v\}$ *denotes an unordered set, with* $(\{v, -v\}, 0)$ *having neighbors* $\{(f_1(\{v, -v\}), 1), \ldots, (f_{q+1}(\{v, -v\}), 1)\}$, *is a degree* 4 *Ramanujan graph.*

Proof (of Theorem 3.16). We get from Theorem 3.5 that $\mathrm{Cay}(PSL(2, \mathbb{F}_{q^d}), z\Gamma)$ is a $q + 1$ regular graph. By Lemma 2.5 we know that $\mathrm{Sch}(\,PSL(2, \mathbb{F}_{q^d}), z\Gamma, V = \mathbb{F}_q^n \setminus \{\mathbf{0}\}\,)$ is also a Ramanujan graph. By Lemma 2.7-Lemma 2.9, 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. From Lemma 3.15, we have that the neighbor of $(\{v, -v\}, 0)$ in G can be calculated using constant locality. Thus, G is our 4-regular constant locality bipartite Ramanujan graph. □

Proof (of Theorem 1.2). Combining Theorem 3.11, Theorem 3.13 and Theorem 3.16, we get the construction for $q + 1$-regular bipartite local Ramanujan graph, for *all* odd prime powers q. This completes the proof of Theorem 1.2. □

4. Conclusion

We give the first construction of bipartite Ramanujan graphs of constant locality of degree $q + 1$, for *any* prime power q. 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 3-regular, 4-regular and 6-regular unique-neighbor expanders, and local 'bipartite' unique-neighbor expanders, see Alon & Capalbo (2002).

Our work leaves the following questions still open:

1. Construct Ramanujan graphs of locality 1.

2. Construct *non*-bipartite constant-locality Ramanujan graphs.

3. Construct Ramanujan graphs of degree $q + 1$, where q is *not* a prime-power.

Acknowledgements

We thank the anonymous reviewers for their helpful comments to improve an earlier draft with preliminary results. N.S. thanks the funding support from DST-SERB (CRG/2020/000045) and N.Rama Rao Chair.

References

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

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

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

Ziv Bar-Yossef, Oded Goldreich & Avi Wigderson (1999). 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)*, 188–198. IEEE.

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

Ho Yee Cheung, Lap Chi Lau & Kai Man Leung (2011). Graph Connectivities, Network Coding, and Expander Graphs. *IEEE 52nd Annual Symposium on Foundations of Computer Science (FOCS 2011)* 190–199.

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

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

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

Oded Goldreich (2000). Candidate One-Way Functions Based on Expander Graphs. *IACR Cryptol. ePrint Arch.* **2000**, 63.

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

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

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

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

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

Rudolf Lidl & Harald Niederreiter (1994). *Introduction to finite fields and their applications*. Cambridge university press.

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

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

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

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

MOSHE MORGENSTERN (1994). 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.

ELCHANAN MOSSEL, AMIR SHPILKA & LUCA TREVISAN (2003). On epsilon-Biased Generators in NCˆ0. In *Annual Symposium on Foundations of Computer Science*, volume 44, 136–145. Citeseer.

ALON NILLI (1991). On the second eigenvalue of a graph. *Discrete Mathematics* **91**(2), 207–210.

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

MICHAEL SIPSER & DANIEL A SPIELMAN (1996). Expander codes. *IEEE transactions on Information Theory* **42**(6), 1710–1722.

DANIEL A SPIELMAN (1999). Constructing error-correcting codes from expander graphs. In *Emerging Applications of Number Theory*, 591–600. Springer.

EMANUELE VIOLA & AVI WIGDERSON (2018). Local expanders. *computational complexity* **27**(2), 225–244.

Manuscript received 30 December 2021

RISHABH BATRA
Centre for Quantum Technologies, National University of Singapore
rishabh10batra@gmail.com

NITIN SAXENA
Indian Institute of Technology, Kanpur, India
nitin@cse.iitk.ac.in
https://www.cse.iitk.ac.in/users/nitin/

DEVANSH SHRINGI
Indian Institute of Technology, Kanpur, India
devansh@cse.iitk.ac.in
https://devansh99.github.io/