Constructions over Finite Fields with Applications to Local Ramanujan Graph and Algebraic Dependence

A thesis submitted

in Partial Fulfillment of the Requirements

for the Degree of

Dual BT-MT

by

Devansh Shringi

17807239

under the guidance of

Nitin Saxena

to the

Department of Computer Science & Engineering

Indian Institute Of Technology Kanpur

May, 2022

Certificate

It is certified that the work contained in the thesis titled **Constructions over Finite Fields with Applications to Local Ramanujan Graph and Algebraic Dependence**, by **Devansh Shringi**, has been carried out under my supervision and that this work has not been submitted elsewhere for a degree.

Prof Nitin Saxena
Department of Computer Science & Engineering
IIT Kanpur

May, 2022

Declaration

This is to certify that the thesis thesis titled **Constructions over Finite Fields with Applications to Local Ramanujan Graph and Algebraic Dependence**, by **Devansh Shringi**, has been authored by me. It presents the research conducted by me under the supervision of **Prof Nitin Saxena**.

To the best of my knowledge, it is an original work, both in terms of research content and narrative, and has not been submitted elsewhere, in part or in full, for a degree. Further, due credit has been attributed to the relevant state-of-the-art and collaborations (if any) with appropriate citations and acknowledgements, in line with established norms and practices.

Devansh

Signature
Devansh Shringi
Dual BT-MT
Computer Science and Engineering
Indian Institute of Technology Kanpur
Kanpur 208016

May, 2022

Abstract

Expanders have been well studied objects in Computer Science that have found usefulness in various fields like decreasing used random bits, designing error-correcting codes, building computer networks, psuedo-random generators, and complexity theory. Ramanujan graphs posses the best expansion properties, finding deep connection to number theory and have important applications in extremal graph theory and computational complexity theory. Existence and construction of Ramanujan graphs has been of great interest in Computer Science and studied extensively. A constant locality function is one in which each output bit depends on just a constant number of input bits, and hence can be computed using small circuits. 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.

Given input polynomials, $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$, they are *Algebraically dependent* if there exists a polynomial A in $\mathbb{F}[y_1, \ldots, y_m]$ such that $A(f_1, \ldots, f_m) = 0$. Testing this efficiently for finite fields has been an open question, and much work has been done on solving it. The concept of algebraic independence finds applications in several areas of mathematics and computer science, including field theory, commutative algebra, algebraic geometry, invariant theory, theory of algebraic matroids, proving lower bounds, creating extractors, and getting hitting sets for Polynomial Identity Testing.

In this thesis, we construct the first *explicit local Ramanujan* graph (bipartite) of degree $q+1$, where $q > 2$ is any prime power. The only known explicit construction of Ramanujan graphs exists for degree $q + 1$, where q is a prime-power. 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).

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 using constructions in Alon and Capalbo (2002).

We will also explore an approach to efficiently test Algebraic dependence of polynomials of small degree with upper bound with coefficients in a field with small characteristic.

Acknowledgements

I have been really fortunate to have received a lot of support from many people during my journey of 5 years completing my degree. First and foremost, I would like to express my gratitude to my advisor, Prof. Nitin Saxena for guiding me the past 5 years. Working with him was an amazing learning experience, where I got to explore the depths of Sylvester-Gallai Configuration, to Ramanujan Graphs and recently Algebraic Independence. I am extremely thankful for the long discussions, introducing new techniques and allowing me to pursue such a wide variety of projects. Almost everything I know in Theoretical computer Science I learned from him, working on this thesis, UG projects and the 4 courses I did under him. I hope to have a similar enthusiasm and passion as he has towards his research, in the coming years of my PhD.

I also owe my gratitude to my parents and sister for being supporting my interests unconditionally. Also, for providing a great environment at home so that I was able to work on the project even in the middle of the pandemic.

I would also like to thank the various Professors whose courses taught me during my 5 years stay. Furthermore, I would like to thank my collaborators in the projects, Diptajit Roy and Rishabh Batra for working with me and patiently listening to my continuous stream of weird ideas. I would also like to thank my labmates Sayak, Sanyam and Sagnik for creating a joyous environment in the lab.

A final thanks to all the friends who helped me cross the 5-year journey, my wing mates, Batchmates, Seniors and Juniors.

Contents

List of Publications

[BSS22] **Explicit Construction Of $Q + 1$ Regular Local Ramanujan Graphs, For All Prime-Powers Q**

Devansh Shringi, Nitin Saxena, and Rishabh Batra

Computational Complexity(Accepted), 2022.

Chapter 4 focus on main results from [BSS22].

Chapter 1

Introduction

Expanders are sparse graphs with strong connectivity properties, due to which they find numerous applications in several areas of computer science — decreasing random bits, designing error correcting codes, pseudo-random generators, extractors, hardness amplification, one-way permutations, and proving complexity results, see the survey [HLW06]. Ramanujan graphs are expanders whose spectral gap is as large as possible. 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.

A lot of these applications require that the neighbors of a given node be computed efficiently, and this has been studied in [BGW99; GV04; ASW09; DV06] 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.

In the first part of this thesis, we will focus on the construction of such local expanders and Ramanujan Graphs, by constructing a special field extension that satisfies the properties required for the graphs constructed from those groups to be

Ramanujan and have constant locality.

Given polynomials $f_1, \dots, f_m$ as input with each $f_i \in \mathbb{F}[x_1, \dots, x_n]$, they are *Algebraically independent* if there doesn't exist a polynomial A such that A in $\mathbb{F}[y_1, \dots, y_m]$ and $A(f_1, \dots, f_m) = 0$. Algebraic independence finds applications in several regions of mathematics and computer science, including field theory, commutative algebra, algebraic geometry, invariant theory, theory of algebraic matroids. In [Lvo84] to analyze program invariants of arithmetic straight line programs, algebraic dependence was used. In [Kal85] transcendence degree was used to give a lower bound on the size of the formula computing a determinant. In [Dvi12], polynomial maps of algebraically independent polynomials over finite $\mathbb{F}$ were used to give explicit construction of deterministic randomness extractors for sources.

In [Agr+16] and [BMS13], several special cases of Polynomial Identity Testing(PIT) were solved by developing smaller deterministic Hitting sets using transcendence degree. In [Cur13] proved hardness of parameterized counting problems using algebraic independence of polynomials.

We will explore an inductive approach to give an efficient Algebraic Dependence testing for polynomials from a small Finite field.

The thesis consists of 7 chapters, where are all chapters except $Chapter 4, 6$ give exposition to the problems through background and related work. Chapter 4 contains the construction of local Ramanujan Graphs for degree $q + 1$, where q is a prime power > 2, from [BSS22] which is the main contribution of this thesis. Chapter 6 contains an Algorithm to test Algebraic independence $f_1, \dots, f_m \in \mathbb{F}_2[x_1, \dots, x_n]$ for $m \leq 4$.

Chapter 2 describes the basic notation followed through out the thesis, and some preliminaries to understand tools required to construct Ramanujan graphs and test for Algebraic Dependence.

Chapter 3 contains a brief description of the work done related to construction of local Expanders, mainly the ideas and tools used. It also includes the construction of local Ramanujan graphs of deg $= 3$.

Chapter 4 contains the construction of local Ramanujan Graphs for degree $q+1$, where q is a prime power, by constructing the required field extensions. This chapter is the main contribution of this thesis.

Chapter 5, contains a literature review of the work done till now on the problem of Algebraic Testing. It describes the current best results known for the various subcases.

Chapter 6, contains an inductive approach to test Algebraic independence $f_1, \ldots, f_m \in \mathbb{F}_2[x_1, \ldots, x_n]$ for $m \leq 4$ and possible attempt to generalize it for the case $m = n$.

Chapter 7 provide a succinct conclusion of the results and describes a few potential next steps.

Chapter 2

Preliminaries

We firstly describe the notation that we will be using all across the report. Then, we will look at some basic ideas and results required to understand the details of the thesis.

2.1 Notation

- $\mathbb{F}$ will be used to denote a field. $\bar{\mathbb{F}}$ will denote the algebraic closure of the field.
- We use $\mathbb{F}[x]$ and $\mathbb{F}(x)$ respectively to denote the ring of polynomials with coefficients from $\mathbb{F}$ with indeterminate x, and its field of fractions.
- We will use vector notation to denote extended set of objects. Therefore, $(\mathbf{x})$ will be representing $(x_1, \ldots, x_n)$ and $(\mathbf{f})$ will be representing $(f_1, \ldots, f_m)$.
- $\mathbb{E}/\mathbb{F}$ denotes that $\mathbb{E}$ is an extension of $\mathbb{F}$. We will use $\mathbb{F}_{q^n}$ to denote extension of $\mathbb{F}_q$ with q^n elements.
- $trdeg_{\mathbb{F}}(f_1, \ldots, f_m)$ will denote the transcendence degree of $f_1, \ldots, f_m$.
- We denote a d-regular graph G with functions $f_1, \ldots, f_d$ where $f_i : \mathcal{V} \rightarrow \mathcal{V}$ where $f_i(v)$ is the i^{th} neighbor of the vertex $v \in \mathcal{V}$ in G.

2.2 Expanders

Expanders (or expander graphs) are sparse graphs that have 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. We call a graph G a (n, d, λ) expander, if G is a d-regular graph over n vertices and has $\lambda_G \leq \lambda$.*

Expanders have a lot of practical applications as well, such as building optimal and cost-efficient computer networks, see [CLL11], 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 [SS96; Spi99; Gur04; BZ02]. They have been instrumental in proving some important results in complexity theory, for example see [Din07] for application in PCP theorem [Din07], and [Rei08] for application in $SL = L$.

In [Nil91], a lower bound of $1 - 2\sqrt{d-1}$ was given on the spectral gap of any d-regular graph. The graphs with spectral gap in $O(1)$ vicinity to this bound are called 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 $\lambda_G \leq 2\sqrt{d-1}$.*

They have important applications in communication network theory, number theory, cryptography and algebraic geometry. Ramanujan graphs are also important in cryptography and can be used to construct low density parity check codes; for more details, see the survey [Li93]. They are also used in the construction of unique-neighbor expanders, see [AC02].

2.3 Cayley and Schreier Graphs

The initial construction based on [Mor94] 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, [VW18])*** *Let H be a group. Given a multiset S with elements $\in H$, the Cayley graph Cay$(H, S) = (V, E)$ is an undirected graph with $V = H$ and for any vertex $h \in H$ there is $(h, sh) \in E$, 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, [VW18])*** *Let H be a group acting on a set V, such that there is a homomorphism from H to the group of permutations of V. Then the Schreier graph Sch(H, S, V), whose is an undirected graph with vertices V and where for every vertex v, we have $(v, sv) \in E$, 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. *[VW18, Lem.2.2] The set of eigenvalues of Sch(H, S, V), is a subset of the set of eigenvalues of Cay(H, S). Therefore, $\Lambda_{Sch} \leq \Lambda Cay$.*

2.4 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, [VW18])*** *Let $G = (V, E)$ be a d-regular graph where vertex for $v \in V$ $(v, f_i(v)) \in E$, $\forall i \in I$. The double-cover of G is defined as the bipartite graph with vertex set $V \times \{0, 1\}$ where a vertex (v, b) is connected to $(f_i(v), 1 - b)$, $\forall i \in I$.*

Lemma 2.7. *[VW18, Fact 2.3] Let G_0 be the bipartite double cover of a graph G. If λ is an eigenvalue of G_0, then $-\lambda$ or λ is an eigenvalue of G. 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, [VW18])*** *G is a bipartite graph on the vertex set $V \times \{0,1\}$, with vertex (v,b) connected to $(f_i(v), 1-b)$, $\forall i \in I$ and π be any 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: a vertex $(v,0) \in G_0$ is connected to $(\pi f_i v, 1)$, and similarly vertex $(v,1) \in G_0$ is connected $(f_i \pi^{-1} v, 0)$, $\forall\, i \in I$.*

Applying a twist conserves the spectral gap.

Lemma 2.9. *[VW18, Lem.4.2] The eigenvalues of the twisted graph are the same as the original graph, i.e., π-twist preserves the spectral gap.*

2.5 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. ***(General linear group)*** *$GL(n,R)$, the general linear group of degree n over R, is defined as the set of $n \times n$ matrices with elements from R that are invertible, with matrix multiplication over R being the operation of the group.*

Definition 2.11. ***(Special linear group)*** *$SL(n,R)$, the general linear group of degree n over R, is defined as the set of $n \times n$ matrices with elements from R that have determinant$= 1$, with matrix multiplication over R being the operation of the group.*

Definition 2.12. ***(Center of a group)*** *We define $Z(G)$ the center of a group G as the set of elements of G that commute with every element, that is $Z(G) := \{z \in G \,|\, \forall g \in G,\, zg = gz\}$.*

Definition 2.13. ***(Projective linear group)*** *$PGL(n, R)$ is the quotient group defined as $PGL(n, R) := GL(n, R)/Z(n, R)$, where $Z(n, R)$ is the center of $GL(n, R)$.*

Definition 2.14. ***(Projective special linear group)*** *$PSL(n, R)$ is the quotient group defined as $PSL(n, R) := SL(n, R)/Z(n, R)$, where $Z(n, R)$ is the center of $SL(n, R)$.*

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 $SL(2, R) = \{I_2, -I_2\}$.

2.6 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 $\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$.

Lemma 2.15. *[LN94, Theorem 3.75] Let $w \geq 2$ be an integer and $a \in \mathbb{F}_q^*$. If the following three conditions are satisfied by w, a, p, q, then and only then is the binomial $x^w - a$ irreducible in $\mathbb{F}_q[x]$:*

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

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

Lemma 2.16. *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 2.15, 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 Lemma 2.15. Hence, $x^p - \beta$ is irreducible. □

We lastly prove the following claim,

Claim 2.17. *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 $\mathbb{F}_r$.*

of Claim 2.17. By Lemma 2.16 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 Lemma 2.15 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 $\mathbb{F}_r[x]$. □

2.7 Algebra Preliminaries

We will need definition of some basic elements from Algebra:

Definition 2.18 (Ideal)**.** *The ideal generated by $f_1, \ldots, f_k$ is the set $\{\sum_i h_i \cdot f_i : h_1, \ldots, h_k \in \mathbb{F}[x_1, \ldots, x_n]\}$ and denoted by $\langle f_1, \ldots, f_k \rangle$.*

We will denote the quotient ring of an ideal by $\mathbb{F}[x_1, \ldots, x_n]/I$. We will use I_d to denote the polynomials in I of degree d.

Definition 2.19 (Radical). *The radical of an ideal I is the set $\{g \in \mathbb{F}[x_1, \dots, x_n] : g^e \in I$ for some integer $e \geq 1\}$ and is denoted by $\sqrt{I}$.*

Definition 2.20 (Algebraically Independent elements). *Let S be a subset of the field extension $\mathbb{E}$ of $\mathbb{F}$. The set is said to be Algebraically independent if the elements of S isn't a solution of $f = 0$ for all polynomials f in $\mathbb{F}[x_1, \dots, x_{|S|}]$.*

Definition 2.21 (Transcendence Degree). *The Transcendence Degree of a field extension $\mathbb{E}/\mathbb{F}$ is the number of elements in the largest algebraically independent subset of $\mathbb{E}$.*

We will require some understanding for inseparability of polynomials and extensions for understanding work done on Algebraic Independence testing.

Definition 2.22 (Separable Polynomial). *[PSS16] If a polynomial has no multiple roots in its splitting field, $f \in \mathbb{F}[x]$ then it is said to be a separable polynomial.*

It is easy to see that an irreducible polynomial will be separable if the derivative is zero. Therefore, for $\text{char}(\mathbb{F}) = 0$ fields all irreducible polynomials are irreducible. Also, for $\text{char}(\mathbb{F}) = p$, a polynomial is inseparable if and only if $f \in \mathbb{F}[x^p]$.

There is a notion of separability in case of field extensions as well.

Definition 2.23 (Separable Extension). *[PSS16] An algebraic extension $\mathbb{E}/\mathbb{F}$ is separable if the minimal polynomial of every element $\alpha \in \mathbb{E}$ over $\mathbb{F}$ is separable.*

In relation to Algebraic independence of polynomials $\mathbf{f}$ where each $f_i \in \mathbb{F}[\mathbf{x}]$, we work with the extension $\mathbb{F}(\mathbf{x})/\mathbb{F}(\mathbf{f})$. The extension $\mathbb{F}(\mathbf{x})/\mathbb{F}(\mathbf{f})$ is algebraic if and only if we have $trdeg(\mathbf{f}) = n$. Therefore, the extension $\mathbb{F}(\mathbf{x})/\mathbb{F}(\mathbf{f})$ is separable if and only if the minimal polynomial of x_i for all $i \in [n]$, over $\mathbb{F}(\mathbf{f})$ is separable. This by definition of minimal polynomial holds true for $\text{char}(\mathbb{F}) = 0$. For $\text{char}(\mathbb{F}) = p$, if $\exists i \in [n]$, such that the min. poly. of x_i lies in $\mathbb{F}[x^p]$, then the extension is inseparable.

Definition 2.24 (Inseparable Degree)**.** *[PSS16] The inseparable degree of the extension $\mathbb{F}(x_1, \ldots, x_n)/\mathbb{F}(f_1, \ldots, f_m)$ is defined as p^m for the minimum m such that for all $i \in [n]$, the minimal polynomial of $x_i^{p^m}$ is separable over $\mathbb{F}(f_1, \ldots, f_m)$.*

The inseparable degree of a system will be a factor of the degree of extension, $\mathbb{F}(x_1, \ldots, x_n)/\mathbb{F}(f_1, \ldots, f_m)$ and therefore is upper bounded by the product of the degree of the polynomials.

Chapter 3

Local Expanders

The connectivity of a graph is captured by its spectral gap, which is the difference between the moduli of the largest and second largest eigenvalue, i.e. $1 - \lambda_G$, of the normalized adjacency matrix of the graph. The Larger spectral gap is, the better connectivity (or *expansion*) is.

As proved in [Nil91], all d-regular graphs of large enough size satisfy $\lambda_G \geq 2\sqrt{d-1} - o(1)$, where λ_G is denoting the second-largest eigenvalue after the moduli (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 [MSS18; MSS13] 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 [LPS88], which were extended to degree =(prime power)+1 in [Mor94]. In [Mor94], 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 [MSS18; MSS13].

The area of study of small locality is of major interest in theoretical computer science. It was introduced and studied in [ASW09] for AC^0 graphs. In the field of pseudorandomness, [Gol00; MST03; AIK06] gave cryptographic generators of constant locality, where [AIK06] used only logarithmic space.

The attention to expanders, where these transition functions have constant locality, was brought in [ASW09]; and in [VW18] they gave a construction of expander graphs that have locality 1. They also gave construction of degree 3 Ramanujan graphs, which have constant locality.

In [VW18], 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 [Mor94] for degree 3 to be a Ramanujan graph of constant locality. We will look into these in a greater detail in this Chapter.

3.1 One Local Expanders

First, we will look at the construction of One-local Expanders given in [VW18]. The main theorem we will prove in this part is the following:

Theorem 3.1. *[VW18, Theorem 1] For every n and large enough d, there exist explicit locality one maps $f_1, \ldots, f_d$, $f_i : \{0,1\}^n \to \{0,1\}^n$, such that a graph on the vertices $\{0,1\}^n$ where vertex $v \in \{0,1\}^n$ is connected to $\{f_1(v), \ldots, f_d(v)\}$, is a d-regular one local expander with spectral gap atleast $1 - d^{\Omega(1)}$.*

We are only required to give construction for $d = O(1)$ with second eigenvalue bound $1-\Omega(1)$ as we take composition of one-local graph with another, the resulting graph is also one-local, hence allowing us to take power of this graph. So a graph of degree d^t will have a second eigenvalue bound of $d^{-\Omega(1)}$ which is equal to $(1-\Omega(1))^t$.

The main idea is to use a Cayley graph of permutation group S_n with a set of generators given in [Kas07]. We cannot directly use the Schreier of this graph directly as it won't be connected. So we use a semi-direct product of it with $(\mathbb{F}_2)^n$ and non-constant size generator, which form a Cayley graph, output an $O(1)$ sized generator graph whose action is connected on $\{0,1\}^n$ and hence the Schreier graph is also an expander.

We will use a reinterpretation of zig-zag product in group theoretic terms which allows us to combine 2 Cayley graphs. It was shown in [ALW01] that semi-direct product of 2 groups H_1 and H_2 functions as such. Wlog, assume H_2 acts on H_1.

Semi-Direct Product:The semi-direct product of the groups H_3 is a group with elements from the set $H_1 \times H_2$, and the operation of multiplication defined as follows

$$(x, y) \cdot (p, q) = (xy^{-1}(p), yq)$$

where $x, p \in H_1$ and $y, q \in H_2$. $y(p)$ is the image of p under the action of y.

Let S_1, S_2 be a set of generators for H_1 and H_2 respectively. We consider S_1 as a union that is disjoint, of a orbits, i.e. $\cup_{i=1}^{a} H_2(x)$, where $H_2(x)$ is the orbit under H_2 of $x \in H_1$. S_3 which is the set of generators wrt to S_1, S_2 for H_3 is given by:

$$S_3 = \{(1_{H_1}, y) \cdot (x_i, 1) \cdot (1_{H_1}, q) : (y, q) \in S_2, i \in [a]\}$$

The main benefit of having the semi-direct product is that the size of the set of generators S_3 is $a|S_2|^2$, even if S_1 has non-constant number of elements. This allows us to control the degree of the new expander irrespective of the $|S_1|$. The following theorem, shows that

Theorem 3.2. *[ALW01] If Cay(A, S) and Cay(B, T) are expanders, then Cay(C, U) as defined above is also an expander.*

For graph Cay(A, S), we choose the group $(\mathbb{F}_2)^n$ with the operation of addition, which can be done by simply doing bit-wise XOR. The set of generators is $S = \{perm(0^n), perm(10^{n-1}), perm(1^{\lceil n/2 \rceil}0^{n-\lceil n/2 \rceil})\}$, where $perm(a)$ is the set containing the image of action of all permutations on a.

Lemma 3.3. *[VW18] The Cayley graph Cay(A, S), with $A = ((\mathbb{F}_2)^n, +)$ and $S = \{0^n, 10^{n-1}, 1^{\lceil n/2 \rceil}0^{n-\lceil n/2 \rceil}\}$, is an expander graph.*

Proof. As eigenvalues of the adjacency matrix of the Cayley graph are the distribution on generators' Fourier coefficients, all we need to show is that the probability

$\langle a, x\rangle = 1$, for every non-zero $a \in (\mathbb{F}_2)^n$ and x chosen uniformly randomly from 1 is far from 0 and 1. $\langle a, x\rangle$ represents inner product of a and x modulo 2. The probability $\langle a, x\rangle = 0$ is $\Omega(1)$ due to $perm(0^n)$ in S. Consider an a with number of 1's larger than $n/3$, then the probability that $\langle a, x\rangle = 1$ is $\Omega(1)$ due to 10^{n-1}, as at least 1/3rd of the permutations will give 1, giving probability at least 1/9. Now consider when number of 1's is less than $n/3$. Let $k = \lceil n/2 \rceil$. Instead of looking at $perm(1^k 0^{n-k})$, we will look at the inner product of $perm(a)$ for a fixed vector a with number of 1's is less than $n/3$ and $1^k 0^{n-k}$. If we consider all but 1 entries that are 1, of a permuted, it will have changed $\leq n/3$ coordinates wrt $1^k 0^{n-k}$. So the last entry that is 1 in a has constant probability of being mapped to 0 and 1 in $1^k 0^{n-k}$, thus giving the $\Omega(1)$ bound. □

Naturally, the group whose action we will consider will be the group of permutation S_n over n elements.

Lemma 3.4. *[Kas07] $\exists$ an explicit set T, with $T = O(1)$, of generators $\subset S_n$ such that the Cayley graph Cay(S_n, T) is an expander.*

Now, we consider the semi-direct group H of S_n acting on $(\mathbb{F}_2)^n$ by permuting the elements. By definition and Lemma 3.4, the generator set S_3 has size $O(1)$. The action of it on an element (a, b) of $\{0, 1\}^n$ is given by xor on a and permuting the elements in b. It is easy to see that $\mathrm{Sch}(H, S_3, \{0, 1\}^n)$ is connected and hence an expander. Since the operation of permutation and xor have locality 1, the graph is a one-local expander.

3.2 Local Ramanujan Graphs of Degree 3

In this section, we will present the construction of deg 3 Ramanujan Graphs in [VW18]. The main result to be proven in this section is

Theorem 3.5 (3 regular)**.** *For variable $n = 4 \cdot 3^t$, there exist 3 explicit $O(1)$-local functions $f_1, \ldots, f_3$ s.t. bipartite graph of $2(2^n - 1)$ vertices with vertex set*

$V = (\mathbb{F}_2^n \setminus \{\mathbf{0}\}) \times \{0,1\}$, with $(v,0)$ having neighbors $\{(f_1(v),1),\ldots,(f_{q+1}(v),\ 1)\}$, is a degree $q+1$ Ramanujan graph.

The author used a simplified version for $q = 2$ of the [Mor94] construction for even characteristic from Theorem 4.3 as follows:

Theorem 3.6. *[VW18, Theorem 12] Let $g(x) \in \mathbb{F}_q[x]$ be irreducible of even degree n, and $\mathbb{F}_{q^n}$ is represented as $\mathbb{F}_q[x]/\langle g(x)\rangle$. Let $L \in \mathbb{F}_{q^n}$ be a such that $L^2+L = 1$, and define $z = \frac{1}{\sqrt{1+x}}$. Then Cay$(SL(2,\mathbb{F}_{q^n}),\Gamma)$ with $\Gamma = \{zM_1, zM_2, zM_3\}$ as generators is a 3-regular Ramanujan graph, where*

$$M_1 = \begin{pmatrix} 1 & L \\ (L+1)x & 1 \end{pmatrix}, \qquad M_2 = \begin{pmatrix} 1 & 1 \\ x & 1 \end{pmatrix} \qquad M_3 = \begin{pmatrix} 1 & L+1 \\ Lx & 1 \end{pmatrix}$$

This simplification occurs as $PSL(2,\mathbb{F}_{2^n})$ is isomorphic to $SL(2,\mathbb{F}_{2^n})$, and ϵ from Theorem 4.3 having only one possible value(1) and therefore simplified values of γ_i and δ_i. For n of the form $n = 2 \cdot 3^t$, the authors use

$$g(x) = x^n + x^{n/2} + 1$$

This was shown to be irreducible in $\mathbb{F}_2$ in [Van12]. Further, the value of L for this system is $L = x^{n/2}$ and therefore is sparse.

Having constructed the extension, and hence the Ramanujan graph as the Cay$(SL(2,\mathbb{F}_2^n),\Gamma)$ using Theorem 3.6. Now with $V = (\mathbb{F}_2^n)^2 - \{0,0\}$ as the vertex set, and action of $M \in SL(2,\mathbb{F}_2^n)$ on $v \in V$ defined as vM, we construct the Schreier graph Sch$(SL(2,\mathbb{F}_2^n),\Gamma,V)$. This graph is connected and hence a Schreier graph by Lemma 2.5.

In computation, the task now left is to remove the factor of multiplication with z. For this we look at the dual cover of the Schreier graph as described in Definition 2.6. Now, we have a bipartite graph with $2(2 \cdot 3^t - 1)$ vertices where $(v,0)$ is connected to $(zvM_i,1)$. As $x+1$ is an element of a field with char 2, it's square root also exists in the field, and so does its multiplicative inverse. Therefore, multiplication by z is equivalent to multiplication by a field element, which is just a permutation of the group. Using the appropriate permutation twist from Definition 2.8, we can remove multiplication by z from the neighbor functions. Due to Lemma 2.7 and Lemma 2.9, both these operations preserve the fact that the graph is still a Ramanujan graph. Thus, in the new graph, the neighbors of $(v, 0)$ for $v \in (\mathbb{F}_2^n)^2 - \{0, 0\}$ are $(vM_i, 0)$ for $i \in [3]$.

Proof of Theorem 3.5. We get from Theorem 3.6 that $\mathrm{Cay}(SL\ (2, \mathbb{F}_{q^n}), \Gamma)$ is a 3 regular graph. By Lemma 2.5 we know that $\mathrm{Sch}(\ SL(2, \mathbb{F}_{q^n}),\ \Gamma,\ \mathbb{F}_2^n \setminus \{\mathbf{0}\}\ )$ 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 M_i.

Looking at the transition function M_i in detail, we see that the only steps that can be non-local are multiplication by L and x (multiplication by $\mathbb{F}_q$ elements is independent of n). Multiplication by x can be done by a simple cycle shift and a bitwise XOR. Recall, $L = x^{n/2}$ and $g(x) = x^n + x^{n/2} + 1 = L^2 + L + 1$. When L multiplies, the multiplication by constants is trivial (has $O(1)$-locality, which is constant with respect to n). So, only multiplication by $x^{n/2}$ needs careful analysis. We see that, in $\mathbb{F}_q[x]/\langle g(x)\rangle$, we can write $x^n =: x^{n/2} + 1$,

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 $n/2$ coefficients of powers of x. Write multiplication by $x^{n/2}$ as:

$$\begin{aligned} x^{n/2} \cdot y &= \sum_{j<n} c_j \cdot x^{j+n/2} = \sum_{0 \le j < n/2} c_j \cdot x^{j+n/2} + \sum_{0 \le j < n/2} c_{j+n/2} \cdot x^{j+n} \\ &= x^{n/2} \cdot \sum_{0 \le j < d/2} c_j x^j \ + \ (x^{n/2} + 1) \cdot \sum_{0 \le j < d/2} c_{j+n/2} \cdot x^j \\ &= (y_2 + y_1, y_1) \end{aligned}$$

Since this computation can be done using simple XOR it is efficient. Combining all the additions, the locality can be easily shown to be 4. This shows that all the operations in the transition functions are local. □

One can show that dual cover and twist are necessary operations, as $z = \frac{1}{\sqrt{x+1}}$ can be written as $z = 1 + x + x^2 + \ldots + x^{b-1}$ where $b = (3n+2)/4$. Multiplication by z therefore is not local and even parity on $\Omega(n)$ bits is reducible to multiplication with z.

Chapter 4

Construction of Local Ramanujan Graphs

In this chapter, we give the novel construction of local Ramanujan graphs (bipartite) of degree $q+1$, where q is power of any prime p.

This uses the construction of Ramanujan graphs developed by M. Morgenstern in [Mor94] for degrees $q+1$. The proof of this construction being Ramanujan graphs in itself is very technical and we don't state or prove the correctness of the construction, we just use it as a blackbox.

The results of this chapter are from paper [BSS22]. We will first preset the main results, describe the motivation behind solving the problem, provide the basic Proof ideas and then present the proofs.

4.1 Main Results

We denote the graph as, $\mathcal{V} \times \{0,1\}$ with any $(v,a) \in \mathcal{V} \times \{0,1\}$ 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 4.1. *[$p = 2$] For any $q = 2^k$, there exist $q+1$ explicit $O(\log q)$-local functions $f_1, \ldots, f_{q+1}$ s.t. the graph on $(q^n - 1)$ vertex set $V = (\mathbb{F}_q^n \setminus \{\mathbf{0}\}) \times \{0,1\}$, 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 $4 \cdot 3^t$, 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 4.2 (Odd p)**.** *For any $q = p^k$ where p is arbitrary odd prime, there exist $q+1$ explicit $O(\log q)$-local functions $f_1, \ldots, f_{q+1}$ s.t. the 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, 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 [VW18].

We answer the question left open in [VW18; AC02] about the construction of local unique-neighbor expanders by providing the first construction of constant locality bipartite Ramanujan graphs to degrees beyond 3.

4.2 Relevance and Motivation

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

[VW18]; making the local construction problem for other degrees a natural open question.

Ramanujan graphs are used for the construction of unique-neighbor expanders, see [AC02], which also explains their applications in computer science. In [VW18], the construction of *local* unique-neighbor expanders is left open, as [AC02] 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 [AC02, 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 [AC02, 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 [AC02].

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 [Mor94]. Our linear-time efficiency is comparable to the constructions in [Mar73; GG81; JM85], 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).

4.3 Proof Ideas

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

For $q =$ even prime power

The case of $q = 2$ was already solved in [VW18]. We will be localizing the construction given in Theorem 5.13 of [Mor94]. For $q = 2^k$, we have an ϵ such that $x^2+x+\epsilon$ is irreducible in $\mathbb{F}_q$ from the construction. 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 $PSL(2, \mathbb{F}_q)$ is isomorphic to $SL(2, \mathbb{F}_q)$ if q is power of 2. This means $\mathrm{Cay}(SL(2, \mathbb{F}_q), \Gamma)$ is a Ramanujan graph from [Mor94], which we convert to $\mathrm{Sch}(SL(2, \mathbb{F}_q), \Gamma, V = \mathbb{F}_q^n \setminus \{\mathbf{0}\})$ 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 [Mor94] comes out to be $1/\sqrt{1+x}$ (same as [VW18]). 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 subsection 4.4.1.

For $q =$ odd prime power

We build on the construction in [Mor94] 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 [Mor94] is a Cayley graph with specific generators Γ of the linear groups $PSL(2, \mathbb{F}_{q^{n/2}})$ (for definitions, see section 2.5). We use Schreier graphs, as used in [VW18], 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 2.5). 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 [VW18], 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 subsection 4.4.4.

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 subsection 4.4.5.

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 subsection 4.4.6.

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 [Mor94] comes out to be $1/\sqrt{x}$. To remove this factor, we will use the tools from [VW18] 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 2.4.

4.4 Proofs of Main Results

4.4.1 Local Ramanujan Graph of Degree $2^k + 1, k > 1$: Proof of Theorem 4.1

First, we look at the construction of Ramanujan Graphs in [Mor94] for q power of 2.

Theorem 4.3. *[Mor94, 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 Cay($PSL(2, \mathbb{F}_{q^d}), \Gamma$) 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 4.4. *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 2.17, 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 4.5. *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 $b_3\alpha + b_1 b_3$ is $\geq \frac{2(q^2-1)}{3} - q$, which would mean that the number of cube values attained by $b_3\alpha + b_1 b_3 + b_3$ 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 4.3 we get that Cay$(PSL(2, \mathbb{F}_{q^d}), \Gamma)$ is a Ramanujan graph. We consider 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 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 4.6 ($2^k + 1$ 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 graph of $2(q^n - 1)$ with vertex set $(\mathbb{F}_q^n \setminus \{\mathbf{0}\}) \times \{0, 1\}$, 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 4.6. We get from Theorem 4.3 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 steps that can be non-local 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 4.1. Combining Theorem 4.6 and the result from [VW18], 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 4.1. □

4.4.2 Ramanujan Graphs of Degree $p^k + 1$, $p \neq 2$

We start with the construction of Ramanujan graphs given in [Mor94], for degree $q + 1$, where q is power of an odd prime.

Theorem 4.7. *[Mor94, 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 $\mathrm{mod}\, g(x)$*, then the Cayley graph of $PSL(2, \mathbb{F}_{q^d})$ with respect to above generators is a $q+1$ regular Ramanujan graph.*

We will use $g(x)$ such that $\sqrt{x}$ is in $\mathbb{F}_p[x]/\langle g(x)\rangle$, giving 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. $q = 3$.

4.4.3 First case: Identifying suitable parameters for the Ramanujan Graph

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

Lemma 4.8 (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:*

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

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

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

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 4.9. *$g_t(x)$ 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 2.17 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 4.10. *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 $\bmod g_0$, 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 4.9-Lemma 4.10, 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 4.11. *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 4.9 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 4.8 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 4.11 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. □

4.4.4 Local Ramanujan Graph of Degree $p^k + 1$, $p \geq 5$

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 mod $g(x)$, from Theorem 4.7, 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 4.9) and the existence of $\sqrt{x} \in \mathbb{F}_q[x]/\langle g_0 \rangle$ (Lemma 4.10). Using Lemma 4.11, 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 2.5). 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 4.7.

Lemma 4.12 (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 4.7 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 steps that can be non-local 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 can be done locally as it is just a combination of a cyclic shift and possibly one addition. 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 4.13 ($p^k + 1$ 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 $f_1, \ldots, f_{q+1}$ s.t. the graph on $(q^n - 1)$ vertex set $\mathcal{V} \times \{0, 1\}$, 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 4.13. From Lemma 4.12 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 [VW18], 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 4.13. □

4.4.5 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 4.14 (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 4.9, $(x^{r^t} - b_1)^2 - \alpha \cdot b_2^2$ 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 2.17, 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 4.10 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 4.15 ($3^k + 1$ 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 $f_1, \ldots, f_{q+1}$ s.t. the graph on $(q^n - 1)$ vertex set $\mathcal{V} \times \{0, 1\}$, 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 4.15. Following the proof of Lemma 4.12, 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 4.13, 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 4.15. □

4.4.6 Local Ramanujan Graphs of Degree 4: Wrap-up Theorem 4.2

For $q = 3$, the only non-square in $\mathbb{F}_q$ is 2. We need g satisfying the conditions of Lemma 4.8, 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 4.16. *For $q = 3$ and $\epsilon = 2$, $g_t(x) = (x^{5^t}+1)^4+x^{5^t}$ satisfies all the properties of Lemma 4.8.*

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 2.17, 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 4.10 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 4.8. □

Using Theorem 4.7 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 4.17. *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 performed with constant locality operations 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 4.18 (4 regular). *For $q = 3$, and variable $n = 8 \cdot 5^t$, there exist $q + 1$ explicit constant locality functions $f_1, \ldots, f_{q+1}$ s.t. the graph of such that the bipartite graph on $(q^n - 1)$ vertex set $\mathcal{V} \times \{0, 1\}$, 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 4.18. We get from Theorem 4.7 that Cay$(PSL\ (2, \mathbb{F}_{q^d}), z\Gamma)$ is a $q+1$ regular graph. By Lemma 2.5 we know that Sch($PSL(2, \mathbb{F}_{q^d})$, $z\Gamma$, $V = \mathbb{F}_q^n \setminus \{\mathbf{0}\}$) 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 4.17, 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 4.2. Combining Theorem 4.13, Theorem 4.15 and Theorem 4.18, we get the construction for $q+1$-regular bipartite local Ramanujan graph, for *all* odd prime powers q. This completes the proof of Theorem 4.2. □

Chapter 5

Algebraic Dependence Testing

In this chapter, we will work on the problem of testing if input polynomials are Algebraically dependent or not.

Definition 5.1 (Algebraically Dependent Polynomials). *Polynomials* $\mathbf{f} \in \mathbb{F}[\mathbf{x}]$ *are* Algebraically independent *if* $\exists A$ *in* $\mathbb{F}[\mathbf{y}]$ *such that* $A(\mathbf{f}) = 0$

Analog to linear rank, we have Transcendence Degree for polynomials.

Definition 5.2 (Transcendence Degree of Polynomials). *The Transcendence Degree of a set of Polynomials* $S = f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$ *is the cardinality in the largest algebraically independent subset of* S*.* S *is algebraically independent iff* $trdeg(S) = |S|$*.*

If the polynomials are not algebraically independent and $\exists A$ such that $A(f_1, \ldots, f_m) = 0$, we call it the **Annihilator** of $f_1, \ldots, f_m$.

Now, we show the following lemma which allows us to replace $\mathbb{F}$ with $\bar{\mathbb{F}}$.

Lemma 5.3. *If* $f_1, \ldots, f_m \in \mathbb{F}[x_1,]$ *are dependent in* $\mathbb{E}/\mathbb{F}$*, then they are also dependent in* $\mathbb{F}$*.*

Proof. Assume $\mathbf{f}$ is dependent in $\mathbb{E}/\mathbb{F}$ with corresponding Annihilator A. We can replace $\mathbb{E}$ with an extension which has coordinates of A, and hence $\mathbb{E}$ is a finite extension. By primitive element theorem, it has a generator α, which generates all the elements in $\mathbb{E}$. Let D be the degree of $\mathbb{E}$, we write A as $A = \sum_{i=0}^{D} \alpha^i A_i(y_1, \ldots, y_m)$

with A_i having coefficients in $\mathbb{F}$. As $A(f_1(\mathbf{x}, \ldots, f_m(\mathbf{x})$ evaluates to 0 on all points in $\mathbb{F}^n$, and as all values cannot contain α, each A_i also evaluates to 0, giving an annihilator with coefficients in $\mathbb{F}$. We should note that $deg(A) \geq deg(A_i)$, so going to an extension doesn't give an advantage of smaller degree annihilators. □

The problem of testing Algebraic dependence was first shown to be in PSPACE by Perron in [Per32] by giving the following bound on degree of Annihilator.

Theorem 5.4 (Perron's bound). *Given $f_1, \ldots, f_m$ alg. dependent polynomials, $\exists A \in \mathbb{F}[y_1, \ldots, f_m]$ with $deg(A) \leq \prod_{i=1}^{m} deg(f_i)$ such that $A(f_1, \ldots, f_m) = 0$.*

This bound is known to be tight, as shown in [Kay09]. Computing the exact Annihilator is therefore known to be hard. But the decision problem of algebraic dependence has a simple solution for field of char($\mathbb{F}$) = 0 in [Jac41] and char($\mathbb{F}$) $> d^r$ in [BMS13] due to the following criteria:

Lemma 5.5 (Jacobian Criteria). *[BMS13; Jac41] Let $\mathbf{f} \subset \mathbb{F}[\mathbf{x}]$ polynomials of deg$\leq d$, and trdeg$_{\mathbb{F}}(\mathbf{f})$ is bounded r. If char$(\mathbb{F}) > d^r$ or char$(\mathbb{F}) = 0$, then trdeg$_{\mathbb{F}}(\mathbf{f})$ is equal to the rank of the Jacobian matrix, i.e. rank$_{\mathbb{F}[x]}\mathcal{J}_{\mathbf{x}}(\mathbf{f})$.*

Definition 5.6 (Jacobian). *The Jacobian matrix of polynomials $\mathbf{f} \in \mathbb{F}[\mathbf{x}]$ is defined as the matrix $\mathcal{J}_{\mathbf{x}}(\mathbf{f}) = (\partial_{x_j}(f_i)_{m \times n}$.*

But for smaller characteristic fields, the question of efficiently testing Algebraic Dependence remains open.

Another way to define, Transcendence degree of polynomials provided a geometric way to approach the problem of Algebraic testing in [GSS19]. We observe that $\mathbb{F}[\mathbf{f}]$ is finitely generated with at most m generators, and therefore it is isomorphic to $\mathbb{F}[\mathbf{x}]/\mathcal{I}$ for some ideal $\mathcal{I}$. The isomorphism takes each $y_i \to f_i$. It is easy to see that the ideal $\mathcal{I}$ is the ideal of all Annihilators of $\mathbb{F}$.

The ring $\mathbb{F}[\mathbf{y}]/\mathcal{I}$ corresponds to the affine variety define by the equations in $\mathcal{I}$, which we call it Y. Consider the map on $\mathbf{A}^n$ where i^{th} coordinate goes f_i, which we call $\phi_{\mathbf{f}}$. The closure of the image of this map $\phi_{\mathbf{f}}$ is exactly Y. It is easy to show from this that Y is an irreducible affine variety.

Now, we look at the algebro-geometric definition of transcendence degree as follows

Definition 5.7. *[SR94] The dimension of an irreducible affine variety is the transcendence degree of its function field.*

Applying this to Y, gives us that $f_1, \ldots, f_m$ are algebraically independent iff $dim(Y) = m$. This gap in the dimension for dependent and independent polynomials allows an application of the Goldwasser-Sipser Set Lowerbound protocol, which gives AM and coAM protocols, and hence the following result.

Theorem 5.8. *[GSS19] Testing Algebraic Dependence of input polynomials $f_1, \ldots, f_n$ is in $AM \cap coAM$.*

In [PSS16], gave an algorithm to test Algebraic dependence when the inseparable degree of the extension $\mathbb{F}(\mathbf{x})/\mathbb{F}(\mathbf{f})$ is small. For $\mathbf{f}$ dependent polynomials, we cannot write $f_n = A(f_1, \ldots, f_{n-1})$ in all cases, but in [PSS16] they showed that after a random shift and allowing power series, f_1 can be written as a function of $f_2, \ldots, f_n$. Define $\mathcal{H}(f(\mathbf{x})) = f(\mathbf{x} + \mathbf{a}) - f(\mathbf{a})$, where a is formal variable representing random shift in $\mathbb{F}^n$. Formally, they showed in the paper the following theorem relating functional dependence and algebraic independence:

Theorem 5.9. *[PSS16, Theorem 10] Let $\mathbf{f} \subset \mathbb{F}[\mathbf{x}]$. If $trdeg(\mathbf{f})$ is r, then $\exists \{g_1, \ldots, g_r\} \subset \{f_1, \ldots, f_m\}$ which are algebraically independent, s.t. for random $z \in \mathbb{F}^n$, $\exists p_i \in \mathbb{F}[\mathbf{y}]$ such that alll polynomial f_i's satisfy $f_i(\mathbf{x} + \mathbf{z}) = p_i(g_1(\mathbf{x} + \mathbf{z}), \ldots, g_k(\mathbf{x} + \mathbf{z}))$.*

Truncating this computation to the inseparable degree t results in Algebraic dependence being equal to $\mathcal{H}_t(f_n) \equiv 0$ modulo $\langle 1, \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_{n-1})\rangle^t$. The separable case with $t = 1$ shows that the Jacobian criteria for dependence is equivalent to the linear terms being $\mathbb{F}(\mathbf{a})$ linearly dependent. Therefore, Jacobian being 0 shows either the polynomials are dependent or independent bu inseparable.

Since, the above testing can be done efficiently in the space of n-variate degree t monomials, it gives a $poly(s, \binom{n+t}{n})$ time algorithm, where s is the input size of the circuits computing $\mathbf{f}$.

Consider, The following case

Example 5.10. *Let $\mathbb{F} = \mathbb{F}_p$ for some prime p. Let $f_i := x_i^p - x_{i+1}$ for $i \in [n-1]$ and $f_n := x_n$. We can easily see that the polynomials are independent, and also that Jacobian vanishes. We also see that the minimal polynomial for x_i, $i < n$ is given by*

$$y^{p^{n-i}} = f_n + \sum_{j=1}^{n-i} f_{n-j}^{p^j}$$

Thus, the inseparable degree of system is p^n. Bounded degree polynomial systems can, therefore, also have exponential inseparable degree, which cannot be efficiently solved using the approach in [PSS16].

This inspired us to solve the smallest and simplest case where degree of f_i's is bounded by 2 over the field $\mathbb{F}_2$.

Chapter 6

Algebraic Independence Testing For Quadratics Over $\mathbb{F}_2$

In this chapter, we explore an inductive way to develop certificates testifying Algebraic Independence for the simplest open case currently, that is $\deg(f_i) \leq 2, \forall i \in [m]$, $f_i \in \mathbb{F}_2[x_1, \ldots, x_n]$.

From discussion in the previous chapter, it is clear that giving an algorithm that outputs a certificate for input algebraically independent polynomials in poly-time is sufficient. So, we assume the input polynomials to be independent and develop certificates.

We will be first preprocessing the input polynomials $f_1, \ldots, f_m$, $f_i \in \mathbb{F}_2[x_1, \ldots, x_n], \forall i \in [m]$ have degree ≤ 2 using the following 4 tools :

- Applying the random shift $H(f_i) = f(\mathbf{x} + \mathbf{z}) - f(\mathbf{z})$
- Substitution $x_i \to \sqrt{x_i}$ if there is only x_i^2 in all f_j's
- Substitution $f_i \to \sqrt{f_i}$ if f_i is a square
- Minimal condition No subset $\{f_1, \ldots, f_r\}$ such that the polynomials in it has only $\leq r < n$ variables.

The above ensure that every f_i has a linear part. No variable is such that only x_i^2 exist. No polynomial is a square. Any subset of r polynomials has $\geq r + 1$ variables, and no variable exist in just one polynomial. We observe that none of the operations above decrease the transcendence degree of the system. Wlog, we assume each f_i contains x_i.

Now, we will attempt to obtain certificates of independence for input polynomials $f_1, \ldots, f_m$ for $m = 2, 3, ...$ and then try to generalize our findings to $m = n$.

Case: $\mathbf{m = 2}$

After applying H of $(z_1, \ldots, z_n)$ on f_1 and f_2, if they have independent linear terms in x_i's, then the Jacobian will work. We can use linear maps to take l_1,l_2 to x_1, x_2.

If f_1, f_2 give linear terms l_1 and αl_1, then we have $H(f_1 - \alpha f_2)$ with 0 linear terms, and hence $f_1 - \alpha f_2$ it will be a square, as $H(f_1 - \alpha f_2)$ will have no linear terms, meaning $f_1 - \alpha f_2$ will have no linear terms. So, we use $f2 := f_1 - \alpha f_2$ and $f_2 := \sqrt{f2}$ removing inseparability and taking us to the former part of this case.

Case: $\mathbf{m = 3}$

From previous case, we can say that we have $f_1 = x_1 + Q_1$ and $f_2 = x_2 + Q_2$. Now, if $H(f_3)$ has a linear term with x_3 then, we have separability and Jacobian gives independence.

Now, if $H(f_3)$ has only one of x_1 or x_2, we can obtain it in $x_3 + Q_3$ form using arguments as in case $m = 2$. So the case remains when both x_1, x_2 are present in linear terms of $H(f_3)$. This happens with $x_1 + x_2 + x_3^2$ or $x_1x_2 + x_3^2$. Adding f_1 and f_2 with appropriate scaling will remove the linear terms in f_3. We cannot take $\sqrt{x_3}$, because f_1, f_2 may have x_3. The simplest such case will be the following:

$$f_1 : x_1x_2$$

$$f_2 : x_2x_3$$

$$f_3 : x_3x_1$$

Now we see that the least monomial in f_3 according to grevlex ordering is x_3^2, with respect to variable ordering $x_1 > x_2 > x_3 > \ldots > x_n$. If there is any other monomial x_i^2, then we just swap x_i and x_3. So the least monomials for f_1, f_2, f_3 are x_1, x_2, x_3^2 respectively. Lastly, we see that this acts like a certificate, as an Annihilator for **f**, will also act like an Annihilator for the least monomials as well.

Case: $\mathbf{m = 4}$

From the above, we have that either $f_1 = x_1 + Q_1, f_2 = x_2 + Q_2, f_3 = x_3 + Q_3$ or $f_1 = x_1 + Q_1, f_2 = x_2 + Q_2, f_3 = x_3^2 + Q_3$. If $H(f_4)$ has a linear term with x_4 then, we have the certificate for independence as x_4 will be the least term.

The first case of $f_1 = x_1 + Q_1, f_2 = x_2 + Q_2, f_3 = x_3 + Q_3$ behaves like the case of $m = 3$, which will finally gives polynomial in form $f_1 = x_1 + Q_1, f_2 = x_2 + Q_2, f_3 = x_3 + Q_3, f_4 = x_4^2 + Q_4$.

So the case that remains is of $f_1 = x_1 + Q_1, f_2 = x_2 + Q_2, f_3 = x_3^2 + Q_3$, where x_4 is not in linear term of f_4. SO, $f_4 = l_4 + x_4^2 + Q_4$ x_1, x_2 in linear terms can easily be removed by adding f_1, f_2 with appropriate scaling. But, we cannot remove x_3 from the linear term.

So, now we will add Frobenius powering to our tool set as well. We can set $f := f^p$ if we are working in the field $\mathbb{F}_p$. We can do this because even though the degree might increase, but the number of monomials remain same. One can argue that this is the core reason behind inseparability. Also, it is easy to see that this doesn't change algebraic dependence.

So we set $f_4 = f_4^2 + f_3$. Since, we know x_4 occurs linearly in one of f_1, f_2, f_3, otherwise we can just use $x_4 \rightarrow \sqrt{x_4}$, and obtain x_4 in linear term. linear x_4 cannot be in f_3, otherwise we would have made it as x_3. So the worst case is when f_3 has x_1x_2 and f_1/f_2 have linear x_4. Now if x_4 is in f_1 or f_2, we apply H on f_4 and the linear terms that come are x_1 x_2, removing which will introduce x_4. In the worst case in this case, we will obtain the polynomials as $f_1 = x_1 + Q_1, f_2 = x_2 + Q_2, f_3 = x_3 + Q_3, f_4 = x_4^4 + Q_4$, where Q_4 has degree

≥ 4 and all terms have higher weight than x_4^4. x_4^4 happens only when $f_4 = x_3 + x_4^2$, which is a special case, in others $x_4^2 + Q_4$ is final form of f_4. This also works as a certificate, as the least terms are linearly independent.

Case: m = 5

The above works with $m = 5$ as well, as the maximum path for any Frobenius can be of one step, which will ensure that x_5^2 becomes the least term when we keep using H and remove the linear terms. The worst case will be when $f_4 = x_4^2 + Q_4$ and $f_5 = x_4 + x_5^2$, and when we apply Frobenius on f_5, the worst case will be when x_2x_3 gets introduced in f_5. Using H and addition to remove x_2 or x_3 will get us to linear x_1 or linear x_5. In the former case Q_1 will have to contain linear x_5, and hence using only one Frobenius jump, we can reach x_5. Thus worst case also remains same and we get certificate $f_1 = x_1 + Q_1, f_2 = x_2 + Q_2, f_3 = x_3 + Q_3, f_4 = x_4^2 + Q_4, f_5 = x_5^4 + Q_5$.

Case: m = 6

The above approach fails at $m = 6$, as the path to x_6 from above may enter a monomial which cannot be removed simply by using H and removing linear terms.

Consider the following example:

Example 6.1. *The following case fails because once we use Frobenius and get $f_6 = x_2x_3 + x_6^4$, removing x_2x_3 is not possible as the terms it produces x_2, x_3 when added give terms which have higher weight than x_2x_3.*

$$f_1 : x_1 + x_2^2 + x_4^2$$

$$f_2 : x_2 + x_1^2$$

$$f_3 : x_3 + x_2^2$$

$$f_4 : x_4 + x_3x_6$$

$$f_5 : x_5^2 + x_2x_3$$

$$f_6 : x_5 + x_6^2$$

This doesn't happen in $m = 5$ as after f_4 is taken for causing Frobenius in f_5, i.e. $f_5 = x_4 + x_5^2$ and $f_4 = x_4^2 + x_2x_3$, and if f_2,f_3 give terms higher weight than x_2, x_3, then f_1 will have linear x_5. The initial linear map to make $f_1 = x_1 + Q_1$, will in that case introduce x_5^2 into f_2, f_3 making the case impossible.

A Possible Solution

Since, we cannot remove x_2x_3 directly from f_6, a possible solution is to instead of using grevlex, use weighted ordering for monomials. So each x_i will have weight w_i, and weight of a monomial $x_1^{e_1}x_2^{e_2}\dots x_n^{e_n}$ is $\sum_{i=1}^{n} e_iw_i$. So after the transformations, the above example becomes

$$\begin{aligned}
&f_1 : x_1 + x_2^2 + x_4^2 + x_3^2 + x_6^2\\
&f_2 : x_2 + x_1^2\\
&f_3 : x_3 + x_2^2\\
&f_4 : x_4 + x_3x_6\\
&f_5 : x_5^2 + x_2x_3 + x_1^2 + x_2^2\\
&f_6 : x_6^4 + x_2x_3
\end{aligned}$$

Since we want the first term in each case to be least, it gives us the following system of inequalities

$$\begin{aligned}
w_1 &< 2w_2, w_1 < 2w_4, w_1 < 2w_3, w_1 < 2w_6 \\
w_2 &< 2w_1 \\
w_3 &< 2w_2 \\
w_4 &< w_3 + w_6 \\
2w_5 &< w_2 + w_3, w_5 < w_1, w_5 < w_2 \\
4w_6 &< w_2 + w_3
\end{aligned}$$

Any assignment of w_i's that satisfies the above will act as a certificate of Algebraic Independence. A path forward possible is to show that such a weight assignment will exist for all independent polynomials. Thereofore, a solution of the polytope acts like a certificate for algebraic independence.

A major drawback of this is approach is that it may not be extendable to larger fields as it ignores the coefficient(except 0) which is not a problem in $\mathbb{F}_2$, but will matter in larger fields.

Chapter 7

Conclusions

In this thesis, 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 [AC02].

For Algebraic Independence, we give a distinct solution approach to the problem for Quadratic polynomials over $\mathbb{F}_2$, solving till $m \leq 5$. For larger m, we give a possible solution that could work over $\mathbb{F}_2$.

7.1 Open Problems

Our work on local Ramanujan Graphs 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.

For Algebraic Dependence, the proof that the polytope approach will work for all Quadratics in $\mathbb{F}_2$ is the natural forward step. Generalizing this is to higher fields and degree will be the next open questions to answer.

References

[BSS22] Rishabh Batra, Nitin Saxena, and Devansh Shringi. “Explicit Construction Of $Q + 1$ Regular Local Ramanujan Graphs, For All Prime-Powers Q”. In: *Computational Complexity(Accepted)* (2022).

[HLW06] Shlomo Hoory, Nathan Linial, and Avi Wigderson. “Expander graphs and their applications”. In: *Bulletin of the American Mathematical Society* 43.4 (2006), pp. 439–561.

[BGW99] 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)*. IEEE. 1999, pp. 188–198.

[GV04] Dan Gutfreund and Emanuele Viola. “Fooling parity tests with parity gates”. In: *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques.* Springer, 2004, pp. 381–392.

[ASW09] Sanjeev Arora, David Steurer, and Avi Wigderson. “Towards a study of low-complexity graphs”. In: *International Colloquium on Automata, Languages, and Programming*. Springer. 2009, pp. 119–131.

[DV06] Scott Diehl and Dieter Van Melkebeek. “Time-space lower bounds for the polynomial-time hierarchy on randomized machines”. In: *SIAM Journal on Computing* 36.3 (2006), pp. 563–594.

[Lvo84] MS L’vov. “Calculation of invariants of programs interpreted over an integrality domain”. In: *Cybernetics* 20.4 (1984), pp. 492–499.

[Kal85] KA Kalorkoti. “A lower bound for the formula size of rational functions”. In: *SIAM Journal on Computing* 14.3 (1985), pp. 678–687.

[Dvi12] Zeev Dvir. “Extractors for varieties”. In: *Computational complexity* 21.4 (2012), pp. 515–572.

[Agr+16] Manindra Agrawal et al. “Jacobian hits circuits: Hitting sets, lower bounds for depth-D occur-k formulas and depth-3 transcendence degree-k circuits”. In: *SIAM Journal on Computing* 45.4 (2016), pp. 1533–1562.

[BMS13] Malte Beecken, Johannes Mittmann, and Nitin Saxena. “Algebraic independence and blackbox identity testing”. In: *Information and Computation* 222 (2013), pp. 2–19.

[Cur13] Radu Curticapean. “Counting Matchings of Size k Is \sharp $W[1]-$Hard”. In: *International Colloquium on Automata, Languages, and Programming*. Springer. 2013, pp. 352–363.

[CLL11] Ho Yee Cheung, Lap Chi Lau, and Kai Man Leung. “Graph Connectivities, Network Coding, and Expander Graphs”. In: *IEEE 52nd Annual Symposium on Foundations of Computer Science (FOCS 2011)* (2011), pp. 190–199.

[SS96] Michael Sipser and Daniel A Spielman. “Expander codes”. In: *IEEE transactions on Information Theory* 42.6 (1996), pp. 1710–1722.

[Spi99] Daniel A Spielman. “Constructing error-correcting codes from expander graphs”. In: *Emerging Applications of Number Theory.* Springer, 1999, pp. 591–600.

[Gur04] Venkatesan Guruswami. “Guest column: error-correcting codes and expander graphs”. In: *ACM SIGACT News* 35.3 (2004), pp. 25–41.

[BZ02] Alexander Barg and Gilles Zémor. “Error exponents of expander codes”. In: *IEEE Transactions on Information Theory* 48.6 (2002), pp. 1725–1729.

[Din07] Irit Dinur. “The PCP theorem by gap amplification”. In: *Journal of the ACM* 54.3 (2007), 12–es.

[Rei08] Omer Reingold. “Undirected connectivity in log-space”. In: *Journal of the ACM (JACM)* 55.4 (2008), pp. 1–24.

[Nil91] Alon Nilli. “On the second eigenvalue of a graph”. In: *Discrete Mathematics* 91.2 (1991), pp. 207–210.

[Li93] Wen-Ching Winnie Li. “A survey of Ramanujan graphs”. In: *Arithmetic, Geometry, and Coding Theory, Luminy, France* (1993), pp. 127–143.

[AC02] Noga Alon and Michael Capalbo. “Explicit unique-neighbor expanders”. In: *The 43rd Annual IEEE Symposium on Foundations of Computer Science, (FOCS 2002). Proceedings.* IEEE. 2002, pp. 73–79.

[Mor94] Moshe Morgenstern. “Existence and explicit constructions of $q+1$ regular Ramanujan graphs for every prime power q”. In: *Journal of Combinatorial Theory, Series B* 62.1 (1994), pp. 44–62.

[VW18] Emanuele Viola and Avi Wigderson. “Local expanders”. In: *computational complexity* 27.2 (2018), pp. 225–244.

[LN94] Rudolf Lidl and Harald Niederreiter. *Introduction to Finite Fields and their Applications.* 2nd ed. Cambridge University Press,Cambridge,UK, 1994. DOI: `10.1017/CBO9781139172769`.

[PSS16] Anurag Pandey, Nitin Saxena, and Amit Sinhababu. “Algebraic independence over positive characteristic: New criterion and applications to locally low algebraic rank circuits”. In: *41st International Symposium on Mathematical Foundations of Computer Science (MFCS 2016).* Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik. 2016.

[MSS18] Adam W Marcus, Daniel A Spielman, and Nikhil Srivastava. “Interlacing families IV: Bipartite Ramanujan graphs of all sizes”. In: *SIAM Journal on Computing* 47.6 (2018), pp. 2488–2509.

[MSS13] 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*. IEEE. 2013, pp. 529–537.

[LPS88] Alexander Lubotzky, Ralph Phillips, and Peter Sarnak. "Ramanujan graphs". In: *Combinatorica* 8.3 (1988), pp. 261–277.

[Gol00] Oded Goldreich. "Candidate One-Way Functions Based on Expander Graphs." In: *IACR Cryptol. ePrint Arch.* 2000 (2000), p. 63.

[MST03] Elchanan Mossel, Amir Shpilka, and Luca Trevisan. "On epsilon-Biased Generators in NC^0". In: *Annual Symposium on Foundations of Computer Science*. Vol. 44. Citeseer. 2003, pp. 136–145.

[AIK06] Benny Applebaum, Yuval Ishai, and Eyal Kushilevitz. "Cryptography in NC^0". In: *SIAM Journal on Computing* 36.4 (2006), pp. 845–888.

[Kas07] Martin Kassabov. "Symmetric groups and expander graphs". In: *Inventiones mathematicae* 170.2 (2007), pp. 327–354.

[ALW01] Noga Alon, Alexander Lubotzky, and Avi Wigderson. "Semi-direct product in groups and zig-zag product in graphs: connections and applications". In: *Proceedings 42nd IEEE Symposium on Foundations of Computer Science*. IEEE. 2001, pp. 630–637.

[Van12] Jacobus Hendricus Van Lint. *Introduction to coding theory*. Vol. 86. Springer Science & Business Media,Springer-Verlag Berlin Heidelberg, Germany, 2012. DOI: `https://doi.org/10.1007/978-3-642-58575-3`.

[Mar73] Grigorii Aleksandrovich Margulis. "Explicit constructions of concentrators". In: *Problemy Peredachi Informatsii* 9.4 (1973), pp. 71–80.

[GG81] Ofer Gabber and Zvi Galil. "Explicit constructions of linear-sized superconcentrators". In: *Journal of Computer and System Sciences* 22.3 (1981), pp. 407–420.

[JM85] Shuji Jimbo and Akira Maruoka. "Expanders obtained from affine transformations". In: *Proceedings of the 17th annual ACM Symposium on Theory of Computing (STOC)*. 1985, pp. 88–97.

[Per32] O Perron. "Algebra I (Die Grundlagen) Göschens Lehrbücherei". In: *Berlin und Leipzig* (1932), pp. 184–193.

[Kay09] Neeraj Kayal. "The complexity of the annihilating polynomial". In: *2009 24th Annual IEEE Conference on Computational Complexity*. IEEE. 2009, pp. 184–193.

[Jac41] Carl Gustav Jacob Jacobi. "De Determinantibus functionalibus." In: *Journal für die reine und angewandte Mathematik (Crelles Journal)* 1841.22 (1841), pp. 319–359.

[GSS19] Zeyu Guo, Nitin Saxena, and Amit Sinhababu. "Algebraic Dependencies and PSPACE Algorithms in Approximative Complexity over Any Field". In: *Theory of Computing* 15.16 (2019), pp. 1–30. DOI: `10.4086/toc.2019.v015a016`. URL: `https://theoryofcomputing.org/articles/v015a016`.

[SR94] Igor Rostislavovich Shafarevich and Miles Reid. *Basic algebraic geometry.* Vol. 2. Springer, 1994.