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

Devansh Shringi
Advisor: Prof. Nitin Saxena

May 30, 2022

Introduction

Expanders

- Expanders are sparse graphs with strong connectivity properties.
- Connectivity quantified by Vertex, Edge or Spectral expansion.
- (n, d, λ)-expander d regular graph on n-vertices with second-largest eigenvalue$\leq \lambda$.

Expanders

- Decreasing random bits
- Designing error correcting codes, extractors, pseudo-random generators
- Proving complexity results
- optimal and cost-efficient computer networks

Ramanujan Graphs

- In [Nil91], gave a lower bound on the second-largest eigenvalue of the adjacency matrix of a d-regular graph of $2\sqrt{d-1}$
- (n, d, λ)-expander is a Ramanujan graph if $\lambda \leq 2\sqrt{d-1} + o(1)$

Locality

- d-regular G, $|V| = n$, with functions $f_1, \ldots, f_d$, $f_i : V \to V$ with $f_i(v)$-being the i-th neighbor of v in G
- If each output a bit of f depends on at most t input bits,f is a t-local function.
- Constant locality $\implies \mathrm{NC}^0$ circuit for f_i.

Algebraic Dependence

- For polynomials $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$, exists a polynomial $A \in \mathbb{F}[x_1, \ldots, x_m]$
$$A(f_1, \ldots, f_m) = 0$$
- Open for small characteristic finite fields and $\mathbf{f}$ having large inseparable degree.

Preliminaries

Cayley and Schreier Graphs

Definition

(Cayley graph, [VW18]) Let H be a group. Given a multiset S of elements from H, we form the Cayley graph $\mathrm{Cay}(H, S)$ whose vertices are H and where a vertex $h \in H$ has neighbors sh, for every element $s \in S$.

Cayley and Schreier Graphs

Definition

(Schreier graph, [VW18]) Suppose that H is a group acting on a set V, namely there is a homomorphism from H to the group of permutations of V. Then we define the Schreier graph $\mathrm{Sch}(H, S, V)$, whose vertices are V and where the vertex $v \in V$ has neighbors sv, for every element $s \in S$.

Linear Groups

Definition

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

Linear Groups

Definition

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

Definition

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

Jacobian

Definition (Jacobian)

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

Inseparability

- If a polynomial $f \in \mathbb{F}[x]$ has no multiple roots in its splitting field, then it is separable.
- Irreducible polynomial will be separable if the derivative is zero.
- For char=0, irreducible are always separable.
- 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.

Inseparability

- If a polynomial $f \in \mathbb{F}[x]$ has no multiple roots in its splitting field, then it is separable.
- Irreducible polynomial will be separable if the derivative is zero.
- For char=0, irreducible are always separable.
- 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.

Inseparable degree

- We will mainly work with the extension $\mathbb{F}(\mathbf{x})/\mathbb{F}(\mathbf{f})$.
- 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 $\mathbb{F}(f_1, \ldots, f_m)$.

Related Work

Existence and Construction of Ramanujan Graphs

- In [LPS88], Construction of Ramanujan Graphs for degree $p+1$ for all prime p
- In [Mor94], Extended the construction to degree $q+1$, q is any prime power
- In [MSS18], showed the Existence for any degree and size bipartite Ramanujan Graphs

One-Local Expanders

- Existence and Construction of Local expanders was answered in [VW18].
- For every n and large enough d, Gave explicit construction of One-local Expanders over vertices $\{0,1\}^n$ with second eigenvalue $\leq d^{-\Omega(1)}$

Local Ramanujan Graphs of deg=3

- In [VW18], they also gave construction of constant locality 3-regular bipartite Ramanujan Graphs on vertex set $\{0,1\}^n \times \{0,1\}$ for $n = 4 \cdot 3^t$
- Localized Construction from [Mor94] for degree 3.

Local Ramanujan Graphs

- Construction for deg>3 was left open in [VW18].
- Construction in [AC02] of unique-neighbor expanders require Ramanujan graphs of degree $4, 8, 44$.
- Giving local construction of these Ramanujan graphs allows construction of local unique-neighbor expanders

Deg $p^k + 1, p \geq 5$

Original Construction

- Consider ϵ non-square in $\mathbb{F}_q$, $g \in \mathbb{F}_q[x]$ even degree d irreducible.
- $\mathbb{F}_{q^d} = \mathbb{F}_q[x]/\langle g(x) \rangle$, $L \in \mathbb{F}_{q^d}$ $L^2 = \epsilon$.
- $\gamma_i, \delta_i \in \mathbb{F}_q$ are all the $q+1$ solutions in $\mathbb{F}_q$ of $\delta_i^2 \epsilon - \gamma_i^2 = 1$

Original Construction

- Consider ϵ non-square in $\mathbb{F}_q$, $g \in \mathbb{F}_q[x]$ even degree d irreducible.
- $\mathbb{F}_{q^d} = \mathbb{F}_q[x]/\langle g(x) \rangle$, $L \in \mathbb{F}_{q^d}$ $L^2 = \epsilon$.
- $\gamma_i, \delta_i \in \mathbb{F}_q$ are all the $q+1$ solutions in $\mathbb{F}_q$ of $\delta_i^2 \epsilon - \gamma_i^2 = 1$

Original Construction

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

If x is a square $\mod g(x)$, then $\mathrm{Cay}(\mathrm{PSL}(2, \mathbb{F}_{q^d}), \Gamma)$ is a $q+1$ regular Ramanujan graph.

Required Properties

For the extension $\mathbb{F}_{q^d}$ to work, we want $g(x)$ such that

- g is a family of irreducible polynomials, even degree
- $\sqrt{x} \in \mathbb{F}_q[x]/\langle g \rangle$ PSL
- $L \notin \mathbb{F}_q$ but $L^2 \in \mathbb{F}_q$ (as we want $L^2 = \epsilon$ where ϵ is a non-square in $\mathbb{F}_q$).
- L has constant sparsity (multiplication with Γ_i)

The Polynomial Family

Fix α to be a non-square in $\mathbb{F}_q$, and for some $b_1, b_2 \in \mathbb{F}_q$

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

- $L = x^{3^t} - b_1$ for $\epsilon = \alpha \cdot b_2^2$
- $g_t(x)$ is irreducible in $\mathbb{F}_q[x]$ iff $b_1 + \sqrt{\alpha} \cdot b_2$ is non-cube in $\mathbb{F}_{q^2}$
- $\sqrt{x} \in \mathbb{F}_q[x]/\langle g_0 \rangle \rightarrow \sqrt{x} \in \mathbb{F}_q[x]/\langle g_t \rangle, \forall t \geq 1$
- So $\exists b_1, b_2$ s.t. $b_1 + \sqrt{\alpha} \cdot b_2$ is a square but not a cube.
- There are at least $(q^2 - 1)/6$ such pairs of (b_1, b_2)

The Polynomial Family

Fix α to be a non-square in $\mathbb{F}_q$, and for some $b_1, b_2 \in \mathbb{F}_q$

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

- $L = x^{3^t} - b_1$ for $\epsilon = \alpha \cdot b_2^2$
- $g_t(x)$ is irreducible in $\mathbb{F}_q[x]$ iff $b_1 + \sqrt{\alpha} \cdot b_2$ is non-cube in $\mathbb{F}_{q^2}$
- $\sqrt{x} \in \mathbb{F}_q[x]/\langle g_0 \rangle \to \sqrt{x} \in \mathbb{F}_q[x]/\langle g_t \rangle, \forall t \geq 1$
- So $\exists b_1, b_2$ s.t. $b_1 + \sqrt{\alpha} \cdot b_2$ is a square but not a cube.
- There are at least $(q^2-1)/6$ such pairs of (b_1, b_2)

The Polynomial Family

Fix α to be a non-square in $\mathbb{F}_q$, and for some $b_1, b_2 \in \mathbb{F}_q$

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

- $L = x^{3^t} - b_1$ for $\epsilon = \alpha \cdot b_2^2$
- $g_t(x)$ is irreducible in $\mathbb{F}_q[x]$ iff $b_1 + \sqrt{\alpha} \cdot b_2$ is non-cube in $\mathbb{F}_{q^2}$
- $\sqrt{x} \in \mathbb{F}_q[x]/\langle g_0 \rangle \to \sqrt{x} \in \mathbb{F}_q[x]/\langle g_t \rangle, \forall t \geq 1$
- So $\exists b_1, b_2$ s.t. $b_1 + \sqrt{\alpha} \cdot b_2$ is a square but not a cube.
- There are at least $(q^2 - 1)/6$ such pairs of (b_1, b_2)

The Polynomial Family

Fix α to be a non-square in $\mathbb{F}_q$, and for some $b_1, b_2 \in \mathbb{F}_q$

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

- $L = x^{3^t} - b_1$ for $\epsilon = \alpha \cdot b_2^2$
- $g_t(x)$ is irreducible in $\mathbb{F}_q[x]$ iff $b_1 + \sqrt{\alpha} \cdot b_2$ is non-cube in $\mathbb{F}_{q^2}$
- $\sqrt{x} \in \mathbb{F}_q[x]/\langle g_0 \rangle \rightarrow \sqrt{x} \in \mathbb{F}_q[x]/\langle g_t \rangle, \forall t \geq 1$
- So $\exists b_1, b_2$ s.t. $b_1 + \sqrt{\alpha} \cdot b_2$ is a square but not a cube.
- There are at least $(q^2-1)/6$ such pairs of (b_1, b_2)

The Polynomial Family

Fix α to be a non-square in $\mathbb{F}_q$, and for some $b_1, b_2 \in \mathbb{F}_q$

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

- $L = x^{3^t} - b_1$ for $\epsilon = \alpha \cdot b_2^2$
- $g_t(x)$ is irreducible in $\mathbb{F}_q[x]$ iff $b_1 + \sqrt{\alpha} \cdot b_2$ is non-cube in $\mathbb{F}_{q^2}$
- $\sqrt{x} \in \mathbb{F}_q[x]/\langle g_0 \rangle \to \sqrt{x} \in \mathbb{F}_q[x]/\langle g_t \rangle, \forall t \geq 1$
- So $\exists b_1, b_2$ s.t. $b_1 + \sqrt{\alpha} \cdot b_2$ is a square but not a cube.
- There are at least $(q^2 - 1)/6$ such pairs of (b_1, b_2)

Example

Consider Example of $q = 5$

- $\alpha = 2,\ b_1 = b_2 = 1,\ g_t = (x^{3^t} - 1)^2 - 2$. Check irreducibility of $(x^3 - 1)^2 - 2$ in $\mathbb{F}_5[x]$ and the existence of $\sqrt{x} = x + 2$ in $\mathbb{F}_5[x]/\langle (x-1)^2 - 2 \rangle$.
- For $\alpha = 3,\ b_1 = b_2 = 3,\ g_t = (x^{3^t} - 1)^2 - 2$.
- Can be done in randomized poly$(\log q)$ time.

Simplification

- Need Simpler vertex set
- Center of $SL(2, \mathbb{F}_{q^d})$ is ± 1
- Action of $\mathrm{PSL}(2, \mathbb{F}_{q^d})$ on $\mathcal{V} := \{\{v, -v\} | v \in (\mathbb{F}_{q^d}^2 \setminus \{\mathbf{0}\})\}$ defined for $A \in PSL(2, \mathbb{F}_{q^d})$ as $\{v, -v\} \mapsto \{Av, -Av\}$
- Still need to handle multiplication by $\frac{1}{\sqrt{x}}$

Bipartite Operations

Definition

(Bipartite double cover of a graph, [VW18]) Let G be a graph on vertex set V where vertex v has neighbors $f_i(v)$, $\forall i \in I$. The double-cover of G is the bipartite graph $V \times \{0,1\}$ where a vertex (v,b) has neighbors $(f_i(v), 1-b)$, $\forall i \in I$.

Definition

(π-twist of a graph, [VW18]) Let G be a bipartite graph on vertex set $V \times \{0,1\}$, where vertex (v,b) has neighbors $(f_i(v), 1-b)$, $\forall i \in I$ and π be a permutation on the vertex set. The π-twist of G is the bipartite graph G_0 having the same set of vertices with the modification: vertex $(v,0) \in G_0$ has neighbors $(\pi f_i v, 1)$, and equivalently vertex $(v,1) \in G_0$ has neighbors $(f_i \pi^{-1} v, 0)$, $\forall i \in I$.

Bipartite Operations

Definition

(Bipartite double cover of a graph, [VW18]) Let G be a graph on vertex set V where vertex v has neighbors $f_i(v)$, $\forall i \in I$. The double-cover of G is the bipartite graph $V \times \{0,1\}$ where a vertex (v,b) has neighbors $(f_i(v), 1-b)$, $\forall i \in I$.

Definition

(π-twist of a graph, [VW18]) Let G be a bipartite graph on vertex set $V \times \{0,1\}$, where vertex (v,b) has neighbors $(f_i(v), 1-b)$, $\forall i \in I$ and π be a permutation on the vertex set. The π-twist of G is the bipartite graph G_0 having the same set of vertices with the modification: vertex $(v,0) \in G_0$ has neighbors $(\pi f_i v, 1)$, and equivalently vertex $(v,1) \in G_0$ has neighbors $(f_i \pi^{-1} v, 0)$, $\forall i \in I$.

Final Structure

- Take Double Cover of $\mathrm{Sch}(\mathrm{PSL}(2, \mathbb{F}_{q^d}), \Gamma, V)$
- Apply π-twist, equivalent of multiplication with $\frac{1}{\sqrt{x}}$
- $(\{v, -v\}, 0)$ connected to $(\{\Gamma_i v, -\Gamma_i v\}, 1)$
- Constant sparsity $\implies$ Constant additions $\implies$ $O(\log(q))$ locality

Deg $3^k + 1$

The difference

- $q^2 - 1$ no longer divisible by 3! Therefore, all elements in $\mathbb{F}_{q^2}$ are cubes.
- For $k > 1$, there must be a prime $r > 3$, that divides $q^2 - 1$
- For $q = 3$, we will need to goto $\mathbb{F}_{q^4}$ instead of $\mathbb{F}_{q^2}$

$k > 1$

Let r be the smallest prime > 3 dividing $q^2 - 1$.Fix α to be a non-square in $\mathbb{F}_q$, and for some $b_1, b_2 \in \mathbb{F}_q$

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

- $L = x^{r^t} - b_1$ for $\epsilon = \alpha \cdot b_2^2$
- $g_t(x)$ is irreducible in $\mathbb{F}_q[x]$ iff $b_1 + \sqrt{\alpha} \cdot b_2$ is non-rth root in $\mathbb{F}_{q^2}$.
- So $\exists b_1, b_2$ s.t. $b_1 + \sqrt{\alpha} \cdot b_2$ is a square but not a r-th root.
- There are at least $\frac{(r-2)(q^2-1)}{2r}$ such pairs of (b_1, b_2)

Deg $= 4$

- $\epsilon = 2$ in this case
- We use the family

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

- Factors as product of $(x^{5^t} - (1 \pm \sqrt{1 \pm \sqrt{2}})^2)$
- $(1 \pm \sqrt{1 \pm \sqrt{2}})^2$ isn't a 5-th power and is a square in $\mathbb{F}_{q^4}$
- $L = x^{3 \cdot 5^t} + x^{2 \cdot 5^t} + x^{5^t} + 1$ satisfies $L^2 = 2$ in $\mathbb{F}_{q^d}$

Deg $2^k + 1$

Original Construction

- Consider ϵ st $x^2+x+\epsilon$ is irreducible in $\mathbb{F}_q$, $g \in \mathbb{F}_q[x]$ even degree d irreducible.
- $\mathbb{F}_{q^d} = \mathbb{F}_q[x]/\langle g(x) \rangle$, $L \in \mathbb{F}_{q^d}$ $L^2+L+\epsilon = 0$.
- $\gamma_i, \delta_i \in \mathbb{F}_q$ are all the $q+1$ solutions in $\mathbb{F}_q$ of $\gamma_i^2 + \gamma_i\delta_i + \delta_i^2\epsilon = 1$

Original Construction

- Consider ϵ st $x^2+x+\epsilon$ is irreducible in $\mathbb{F}_q$, $g \in \mathbb{F}_q[x]$ even degree d irreducible.
- $\mathbb{F}_{q^d} = \mathbb{F}_q[x]/\langle g(x) \rangle$, $L \in \mathbb{F}_{q^d}$ $L^2+L+\epsilon = 0$.
- $\gamma_i, \delta_i \in \mathbb{F}_q$ are all the $q+1$ solutions in $\mathbb{F}_q$ of $\gamma_i^2 + \gamma_i\delta_i + \delta_i^2\epsilon = 1$

Original Construction

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

$\mathrm{Cay}(\mathrm{PSL}(2, \mathbb{F}_{q^d}), \Gamma)$ is a $q+1$ regular Ramanujan graph.

Polynomial family

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

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

- $L = b_2 \cdot x^{3^t} - b_1$ is constant sparsity.
- Let $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ be a root of $x^2 + x + \epsilon$, then g_t is irreducible iff $\frac{\alpha + b_1}{b_2}$ and $\frac{\alpha + b_1 + 1}{b_2}$ are not cubes in $\mathbb{F}_{q^2}$
- As char$= 2$, everything has a square root

Polynomial family

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

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

- $L = b_2 \cdot x^{3^t} - b_1$ is constant sparsity.
- Let $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ be a root of $x^2+x+\epsilon$, then g_t is irreducible iff $\frac{\alpha+b_1}{b_2}$ and $\frac{\alpha+b_1+1}{b_2}$ are not cubes in $\mathbb{F}_{q^2}$
- As char$=2$, everything has a square root

Final Structure

- $PSL(2, \mathbb{F}_{2^d})$ isomorphic to $SL(2, \mathbb{F}_{2^d})$, so we can use vertex set $\mathbb{F}_q^n \setminus \{\mathbf{0}\}$
- We go to Schreier, then take double cover and twist to remove multiplication with $\frac{1}{\sqrt{1+x}}$

Algebraic Dependence

General Results

- If $f_1, \ldots, f_m \in \mathbb{F}[x_1,]$ are dependent in $\mathbb{E}/\mathbb{F}$, then they are also dependent in $\mathbb{F}$.
- $f_1, \ldots, f_m$ 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 $A(f_1, \ldots, f_m) = 0$.
- In [GSS19], Testing Algebraic Dependence of input polynomials $f_1, \ldots, f_n$ is in $AM \cap coAM$.

Large Fields

- Let $\mathbf{f} \subset \mathbb{F}[\mathbf{x}]$ polynomials of deg$\leq d$, and $trdeg_{\mathbb{F}}(\mathbf{f})$ is bounded r. If $\text{char}(\mathbb{F}) > d^r$ or $\text{char}(\mathbb{F}) = 0$, then $trdeg_{\mathbb{F}}(\mathbf{f})$ is equal to the rank of the Jacobian matrix, i.e. $rank_{\mathbb{F}[x]}\mathcal{J}_{\mathbf{x}}(\mathbf{f})$.
- In [PSS16], it was shown that Jacobian being 0 shows either the polynomials are dependent or independent but inseparable.

Low Inseparable Degree

- $\mathcal{H}(f(\mathbf{x})) = f(\mathbf{x}+\mathbf{a}) - f(\mathbf{a})$, where a is formal variable representing random shift in $\mathbb{F}^n$
- Relating Functional Dependence and Algebraic Dependence, they showed Algebraic dependence being equal to $\mathcal{H}_t(f_n) \equiv 0$ modulo $\langle 1, \mathcal{H}_t(f_1), \ldots, \mathcal{H}_t(f_{n-1})\rangle^t$ (t is inseparable degree)
- Doing the computation in monomial space of n-variate degree $\leq t$, gives $poly(s, \binom{n+t}{n})$ time algorithm

Example

- $f_i := x_i^p - x_{i+1}$ for $i \in [n-1]$ and $f_n := x_n$ in $\mathbb{F}_p[x]$
- Jacobian vanishes, minimal polynomial

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

- Inseparable degree p^n, exponential even in $\mathbb{F}_2$ with Quadratics

Our Approach

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

Small cases

- **Case: $\mathbf{m} = \mathbf{2}$**
  1. Linear parts independent
  2. linear terms l_1 and αl_1, $f2 := f_1 - \alpha f_2$ and $f_2 := \sqrt{f2}$ removing inseparability

Small Cases

- **Case: $\mathbf{m = 3}$**

$$f_1 : x_1x_2$$
$$f_2 : x_2x_3$$
$$f_3 : x_3x_1$$

Becomes $f_1 = x_1 + Q_1$ and $f_2 = x_2 + Q_2$, and $f_3 = x_3^2 + x_1x_2$

Least Monomial Independence

- For a monomial ordering, Independence of Least monomials of $\mathbf{f} \implies$ Independence of $\mathbf{f}$.
- Using $LM(f_1 \cdot f_2) = LM(f_1) \cdot LM(f_2)$ and $LM(f_1 + f_2) = min(LM(f_1), LM(f_2))$.

Small cases

- **Case: $\mathbf{m = 3}$**

$$f_1 : x_1 x_2$$
$$f_2 : x_2 x_3$$
$$f_3 : x_3 x_1$$

  Becomes $f_1 = x_1 + Q_1$ and $f_2 = x_2 + Q_2$, and $f_3 = x_3^2 + x_1 x_2$
- Consider in grevlex ordering, $LM(f_1) = x_1, LM(f_2) = x_2, LM(f_3) = x_3^2$, hence certificate of independence

Small cases

- **Case: $\mathbf{m} = \mathbf{4}, \mathbf{5}$** $f_1 = x_1 + Q_1, f_2 = x_2 + Q_2, f_3 = x_3^2 + Q_3,$ $f_4 = l_4 + x_4^2 + Q_4,\ l_4$ has x_1, x_2, x_3
- We can use Frobenius powering to remove x_3, by $f_4 := f_4^2 + f_3$
- Number of monomials remain same

Worst Case

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

Occurs when $m \geq 6$.

Possible approach

Use a weighted monomial ordering, and get system of inequalities

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

If there is solution $\implies$ Independence. Working on proving that Independence $\implies$ Solution.

Questions?

- We gave an explicit construction of bipartite Ramanujan Graphs of degree $q+1$, for all prime power q, with locality $O(\log q)$.
- We also explored an approach for testing algebraic Dependence of Quadratic polynomials over $\mathbb{F}_2$

References

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

Zeyu Guo, Nitin Saxena, and Amit Sinhababu.
Algebraic dependencies and pspace algorithms in approximative complexity over any field.
Theory of Computing, 15(16):1–30, 2019.

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

Moshe Morgenstern.
Existence and explicit constructions of $q+1$ regular Ramanujan graphs for every prime power q.