Lossless Dimension Expanders via Linearized Polynomials and Subspace Designs

Venkat Guruswami, Nicolas Resch and Chaoping Xing

Algebraic Pseudorandomness

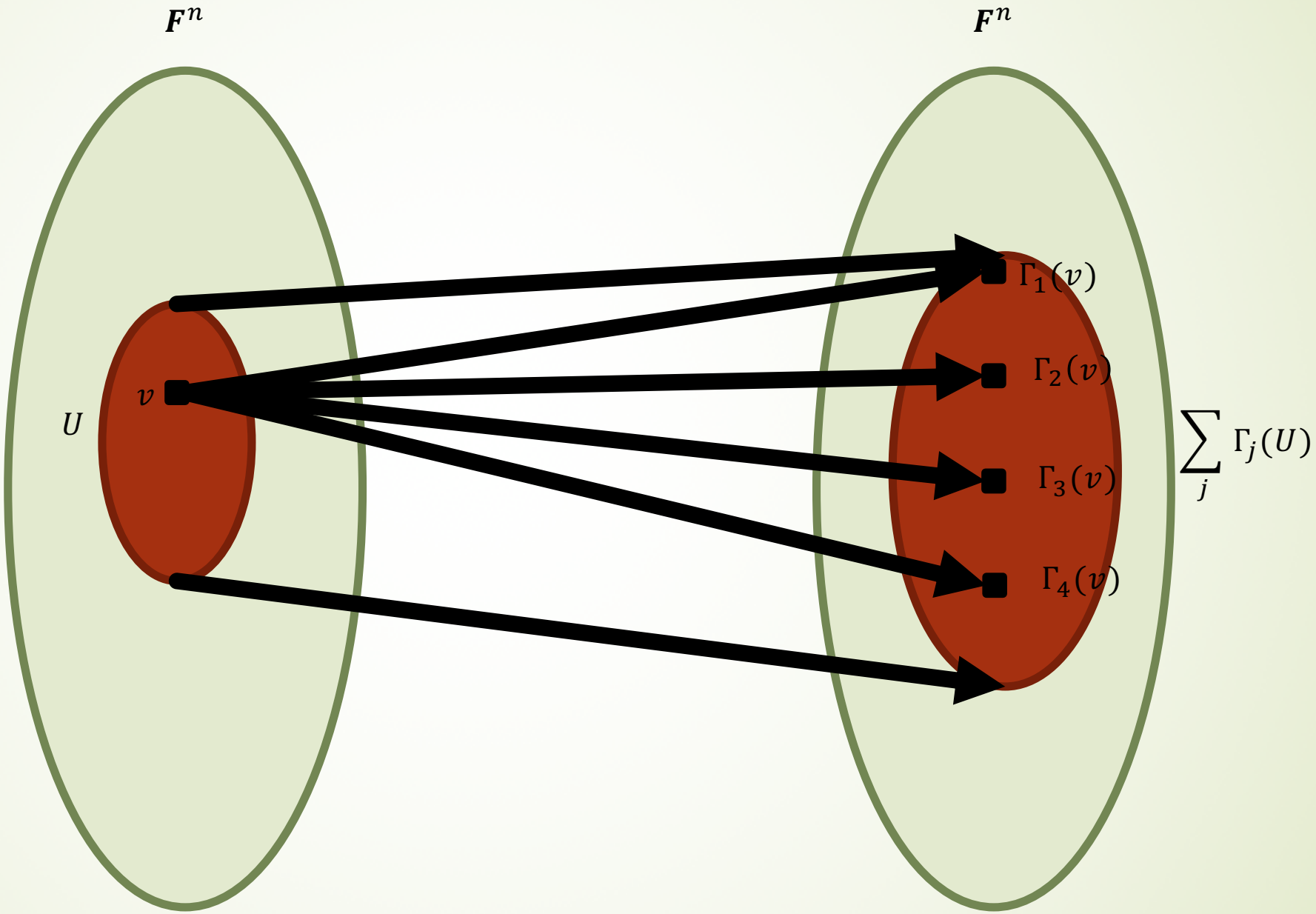
- Traditional pseudorandom objects (e.g., expander graphs, randomness extractors, pseudorandom generators, list-decodable codes etc.) are largely combinatorial objects.
- *Algebraic* pseudorandom objects have recently been studied. Here, dimension of subspaces corresponds to subset size.
- Examples include **dimension expanders**, **subspace designs**, subspace-evasive sets, rank-preserving condensers, list-decodable rank-metric codes.
- Applications include constructions of Ramsey graphs [PR'04], list-decodable codes [GX'12, GX'13, GW'14], affine extractors [Gab'11], polynomial identity testing [KS'11, FS'12].

Dimension Expander

- An (η, β)-***dimension expander*** is a collection of linear maps $\Gamma_1, \ldots, \Gamma_d : \boldsymbol{F}^n \to \boldsymbol{F}^n$ such that, for any $U \subseteq \boldsymbol{F}^n$ of dimension at most ηn, we have

$$\dim\left(\sum_{j=1}^{d} \Gamma_j(U)\right) \geq \beta \dim U \ .$$

- The ***degree*** is d.
- For $\eta\beta < 1$ and $d = O(1)$, a random collection of maps will be a dimension expander with good probability; goal is to obtain an explicit construction.


F^n
F^n
U
v
$\Gamma_1(v)$
$\Gamma_2(v)$
$\Gamma_3(v)$
$\Gamma_4(v)$
$\sum_j \Gamma_j(U)$

History

- Wigderson defined problem in 2004.

Authors	Parameters	Field Restriction
Lubotzky–Zelmanov, Harrow, Ben-Aroya–Ta-Shma '08	$\left(\frac{1}{2}, 1+\Omega(1)\right)$	$\boldsymbol{R}, \boldsymbol{C}$
Bourgain–Yehudayoff '13	$\left(\frac{1}{2}, 1+\Omega(1)\right)$	None
Forbes–Guruswami '15	$\left(\frac{1}{\Omega(\sqrt{d})}, \Omega(\sqrt{d})\right)$	$\lvert\boldsymbol{F}\rvert \geq \Omega(n^2)$

Our results

$d = O\left(\frac{1}{\epsilon^3}\right)$, whereas random gets $d = O\left(\frac{1}{\epsilon^2}\right)$.

Theorem. For any $\epsilon > 0$, there exists $d = d(\epsilon)$ such that there is an explicit $\left(\frac{1-\epsilon}{d}, (1-\epsilon)d\right)$-dimension expander of degree d over $\boldsymbol{F}_q^n$ when $q \geq \Omega(n)$.

Also, $\eta = \frac{1-\epsilon}{d}$ is optimal.

Since $\dim(\sum_{j=1}^{d} \Gamma_j(U)) \leq d \dim U$, $\beta = (1-\epsilon)d$ is optimal. We call the expander ***lossless.***

Our results

Theorem. For any $\epsilon > 0$, there exists $d = d(\epsilon)$ such that there is an explicit $\left(\frac{1-\epsilon}{d}, (1-\epsilon)d\right)$-dimension expander of degree d over $\boldsymbol{F}_q^n$ when $q \geq \Omega(n)$.

Theorem. For any $\delta > 0$, there exists $d = d(\delta)$ such that there is an explicit $\left(\frac{1}{\Omega(\delta d)}, \Omega(\delta d)\right)$-dimension expander of degree d over $\boldsymbol{F}_q^n$ when $q \geq \Omega\left(n^{\delta}\right)$.

Linearized Polynomials

- A ***linearized polynomial*** is a polynomial in $\boldsymbol{F}_{q^n}[X]$ of the form

$$f(X) = \sum_{i=0}^{k-1} f_i X^{q^i}$$

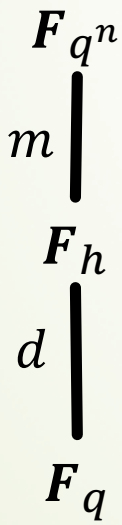
- Max i such that $f_i \neq 0$ is the q-***degree*** of $f(X)$.
- Denote set of all linearized polynomials of q-degree $< k$ by $\boldsymbol{F}_{q^n}[X; (\cdot)^q]^{<k}$.
- If $\alpha, \beta \in \boldsymbol{F}_{q^n}$ and $a, b \in \boldsymbol{F}_q$, then $f(a\alpha + b\beta) = af(\alpha) + bf(\beta)$. That is, as a map $\boldsymbol{F}_{q^n} \to \boldsymbol{F}_{q^n}$, f is $\boldsymbol{F}_q$-linear.

Fact. If $f \in \boldsymbol{F}_{q^n}[X; (\cdot)^q]^{<k} \setminus \{0\}$, then $\dim_{\boldsymbol{F}_q}(\ker f) \leq k - 1$.

The Construction

- Fix $\alpha_1, \ldots, \alpha_d$, a basis for $\boldsymbol{F}_h/\boldsymbol{F}_q$, where $h = q^d$ and d is degree.
- Fix $L \subseteq \boldsymbol{F}_{q^n}[X; (\cdot)^q]^{<k}$ of $\boldsymbol{F}_q$-dimension n.
- For $j = 1, \ldots, d$, define

$$\Gamma_j : L \to \boldsymbol{F}_{q^n} \quad \text{by} \quad f \mapsto f(\alpha_j) \, .$$



Intuitively, we'd like to show that subspaces of dimension s are expanded to subspaces of dimension $(d - k + 1)s$.

Contrapositive Characterization

Proposition. Let $\Gamma_1, \dots, \Gamma_d : \boldsymbol{F}^n \to \boldsymbol{F}^n$. Suppose that $\forall\, V \subseteq \boldsymbol{F}^n$ s.t. $\dim V \leq \eta\beta n$, we have

$$\dim\{u \in \boldsymbol{F}^n : \forall\, j \in [d],\ \Gamma_j(u) \in V\} \leq \left(\frac{1}{\beta}\right) \dim V\ .$$

Then $\{\Gamma_j : j \in [d]\}$ forms a (η, β)-dimension expander.

- Thus, for $V \subseteq \boldsymbol{F}_{q^n}$, we need to understand

$$\{f \in L : \forall j \in [d], f(\alpha_j) \in V\} = \{f \in L : f(\boldsymbol{F}_h) \subseteq V\}\ .$$

- First, let us study

$$\{f \in \boldsymbol{F}_{q^n}[X; (\cdot)^q]^{<k} : f(\boldsymbol{F}_h) \subseteq V\}\ .$$

Aside: Connection to Coding Theory

- The condition we study is like a "rank-metric list-recovery" problem.
- [Guruswami-Wang-Xing '16] recently provided an explicit construction of a rank-metric code list-decodable up to the Singleton bound.
- Our construction is similar, but the parameter regime is sufficiently different that we require novel constructions (particularly, the subspace design).
- This is very much akin to [Guruswami-Umans-Vadhan '08], where an explicit construction of bipartite expander graphs were obtained from Parvaresh-Vardy codes.

Interpolation

- Recall: we want to understand

$$\{f \in \boldsymbol{F}_q[X;(\cdot)^q]^{<k} : f(\boldsymbol{F}_h) \subseteq V\} .$$

- For integers $D, s \leq m$, consider

$$Q(Y_0, Y_1, \dots, Y_{s-1}) = A_0(Y_0) + A_1(Y_1) + \cdots + A_{s-1}(Y_{s-1}) ,$$

each $A_i(Y_i) \in \boldsymbol{F}_{q^n}[Y_i;(\cdot)^q]^{<D}$.

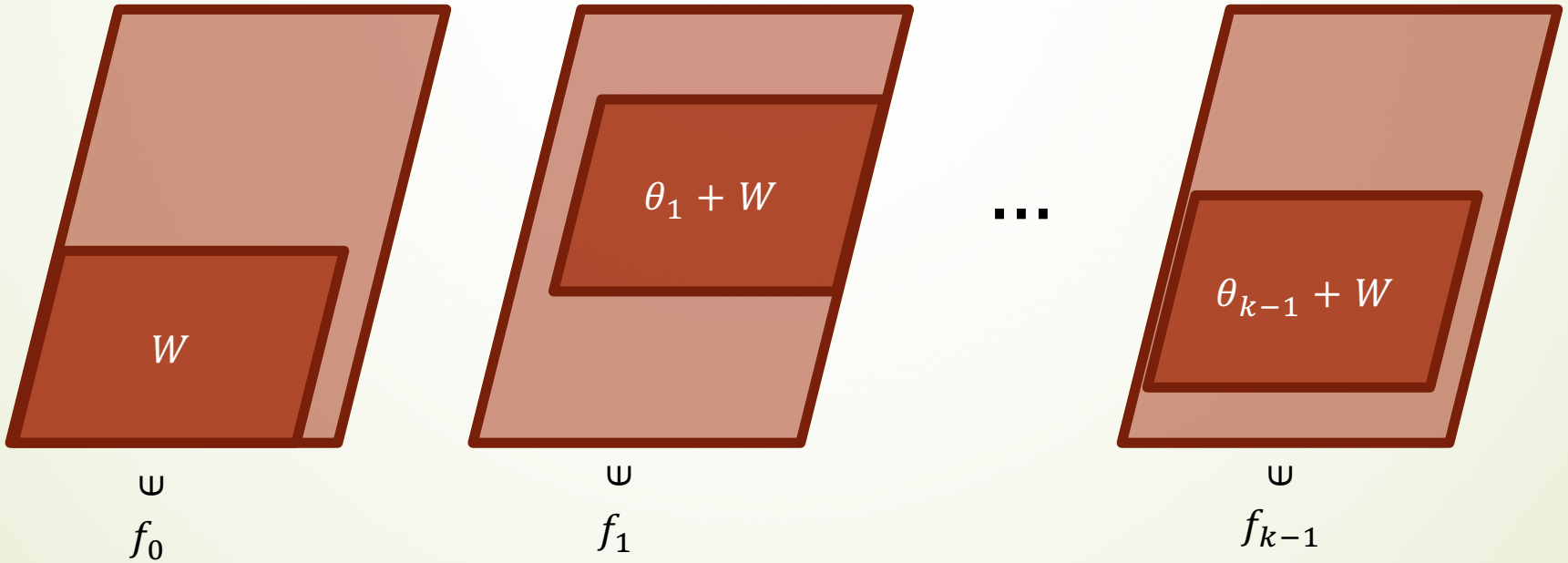
- Let $B \coloneqq \dim_{\boldsymbol{F}_q} V$ and suppose $B < Ds \leq d - k + 1$. Can find $Q \neq 0$ as above such that, if $f(\boldsymbol{F}_h) \subseteq V$,

$$Q\left(f, f^{\sigma}, \dots, f^{\sigma^{s-1}}\right)(X) = 0 ,$$

where $f^{\sigma^j} \coloneqq \sum_i f_i^{h^j} X^{q^i}$.

Periodic Subspace Structure

- The space of $f(X) = \sum_i f_i X^{q^i} \in \boldsymbol{F}_{q^n}[X; (\cdot)^q]$ such that $Q\left(f, f^{\sigma}, \ldots, f^{\sigma^{s-1}}\right)(X) = 0$ has the following structure:
  - There is an $\boldsymbol{F}_h$-subspace $W \subseteq \boldsymbol{F}_{q^n}$ of dimension $\leq s-1$, and $f_0 \in W$.
  - There are $\theta_1, \ldots, \theta_{k-1} \in \boldsymbol{F}_{q^n}$ such that $f_i \in \theta_i + W$.
- We call such a subspace of $\left(\boldsymbol{F}_{q^n}\right)^k$ $(s-1, d)$-***periodic subspace***.
- **Morally**: can pretend $(f_0, f_1, \ldots, f_{k-1}) \in W^k$.



Choice of L

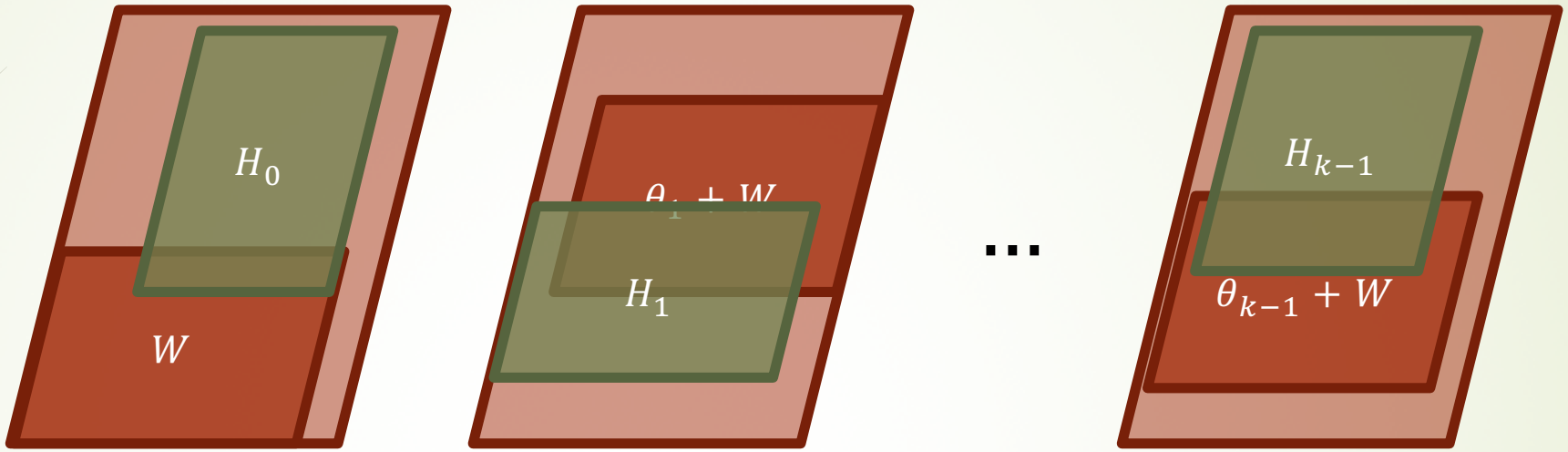
- Thus, we would like to choose L so as to have small intersection with *any* periodic subspace.
- We will define

$$L := \left\{ f(X) = \sum_{i=0}^{k-1} f_i X^{q^i} : f_i \in H_i \ \forall i \right\},$$

where $H_0, H_1, \dots, H_{k-1} \subseteq \boldsymbol{F}_{q^n}$ form a ***subspace design***.

Definition. A collection $H_0, H_1, \dots, H_{k-1} \subseteq \boldsymbol{F}_{q^n}$ of $\boldsymbol{F}_q$-subspaces is called a (s, A, d)-***subspace design*** if, for every $\boldsymbol{F}_{q^d}$-subspace $W \subseteq \boldsymbol{F}_{q^n}$ with $\dim_{\boldsymbol{F}_{q^d}} W = s$,

$$\sum_{i=0}^{k-1} \dim_{\boldsymbol{F}_q}(H_i \cap W) \leq As\,.$$



Theorem. Let $H_0, H_1, \dots, H_{k-1}$ give a (s, A, d)-subspace design for all $s \le \mu n$, where $0 \le \mu < 1/d$, and assume each $\dim_{\boldsymbol{F}_q} H_i = n/k$. Then $\Gamma_1, \dots, \Gamma_d : L \to \boldsymbol{F}_{q^n}$ gives a $\left(\mu A, \frac{d-k+1}{A}\right)$-dimension expander.

Constructions of Subspace Designs

Theorem. [GK'16] Suppose $s \le t \le n < q$. There exists an explicit collection of $M \ge \Omega(q^r/r)$ subspaces $V_1, \ldots, V_M \subseteq \boldsymbol{F}_q^n$, each of codimension rt, which form an $\left(s, \frac{n-1}{r(t-s+1)}, 1\right)$-subspace design.

Construction 1. Let $\delta > 0$. If $q \ge n^\delta$ there exists a $\left(s, \frac{8}{\delta}, d\right)$-subspace design for all $s \le \frac{1-2\delta}{4d} n$. Moreover each subspace has $\boldsymbol{F}_q$-dimension n/k.

Construction 2. Let $\epsilon > 0$. If $q \ge n/d$ there exists a $(s, 1+\epsilon, d)$-subspace design for all $s \le \frac{1-\epsilon}{d} n$. Moreover each subspace has $\boldsymbol{F}_q$-dimension n/k and $k = O\left(\frac{1}{\epsilon^2}\right)$, $d = O\left(\frac{1}{\epsilon^3}\right)$.

"High-degree" Folded Reed-Solomon Construction

- Take $V_1, \dots, V_k \subseteq \boldsymbol{F}_q[X]^{<\epsilon n}$, subspace design from [GK '16] with $\epsilon \approx 1/\sqrt{k}$.
- Let $\tau: \boldsymbol{F}_q(x) \to \boldsymbol{F}_q(x)$ the field automorphism mapping $X \mapsto \zeta X$, where ζ is a generator for $\boldsymbol{F}_q^*$.
- Define the map $\pi: \boldsymbol{F}_q[X]^{<\epsilon n} \to \boldsymbol{F}_{q^d}^m$ by

$$f \mapsto \left(f(P), f(P^\tau), \dots, f\left(P^{\tau^{m-1}}\right)\right).$$

  - P is an irreducible polynomial of degree d such that $P(X), P^\tau = P(\zeta X), \dots, P^{\tau^{m-1}} = P(\zeta^{m-1}X)$ are pairwise coprime,
  - $f\left(P^{\tau^j}\right)$ is the residue of f when evaluated at the place P.
- Define $H_i = \pi(V_i)$ for $i = 1, \dots, k$.

Summary and Open Problems

- Explicit construction of a $\left(\frac{1-\epsilon}{d}, (1-\epsilon)d\right)$-dimension expander when $|\boldsymbol{F}| \geq \Omega(n)$, or $\left(\frac{1}{\Omega(\delta d)}, \Omega(\delta d)\right)$-dimension expander when $|\boldsymbol{F}| \geq n^{\delta}$.
- Main ingredients: linearized polynomials, subspace designs.

- Decrease the field size? Or obtain same result over $\boldsymbol{R}, \boldsymbol{C}$?
- Applications of dimension expanders?

Thank You!