Subspace Designs and Error-Correcting Codes

Sayak Chakrabarti

Subspace Designs

Definition (Subspace Designs [GK16, GX13])

Subspace designs are defined as collections of subspaces $\{H_1, H_2, \ldots, H_M\}$, where $H_i \subseteq \mathbb{F}_q^m \; \forall i \in [M]$, with the property that any "low dimensional" subspace W will have less number of intersecting points with H_i's

Error-Correcting Codes

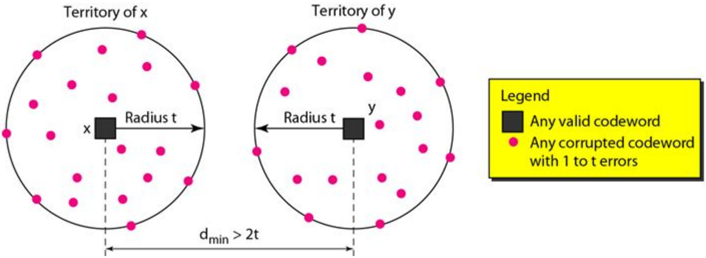
Definition (Error-Correcting Codes)

An error-correcting code, for a distance $\delta \in [0, 1]$, is a function $E : \{0, 1\}^n \mapsto \{0, 1\}^m$ such that $\forall x \neq y$, $x, y \in \{0, 1\}^n$, $\Delta(E(x), E(y)) \geq \delta$.

Error-Correcting Codes

Definition (Error-Correcting Codes)

An error-correcting code, for a distance $\delta \in [0,1]$, is a function $E : \{0,1\}^n \mapsto \{0,1\}^m$ such that $\forall x \neq y$, $x, y \in \{0,1\}^n$, $\Delta(E(x), E(y)) \geq \delta$.



Relation to Computational Complexity Theory

- Subspace designs relate to error-correcting codes [GK16, GX13].

Relation to Computational Complexity Theory

- Subspace designs relate to error-correcting codes [GK16, GX13].
- Error-Correcting codes: Hardness of Approximations (Reducing Hardness) [AB09].

Relation to Computational Complexity Theory

- Subspace designs relate to error-correcting codes [GK16, GX13].
- Error-Correcting codes: Hardness of Approximations (Reducing Hardness) [AB09].
- Hardness of Approximations: Pseudorandomness [NW94]

Relation to Computational Complexity Theory

- Subspace designs relate to error-correcting codes [GK16, GX13].
- Error-Correcting codes: Hardness of Approximations (Reducing Hardness) [AB09].
- Hardness of Approximations: Pseudorandomness [NW94]

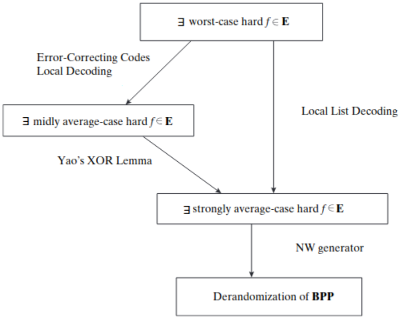


Figure 1: Relation between Hardness and Derandomization using ECC [AB09]

Error-Correcting Codes: Reed-Solomon Codes

Definition (Reed-Solomon Codes [WB99])

For a finite field $\mathbb{F}$, and integers $k \leq n \leq |\mathbb{F}|$, Reed-Solomon code is defined as a function $RS : \mathbb{F}^k \to \mathbb{F}^n$, such that on input $\overline{a} = (a_0, a_1, \ldots, a_{k-1}) \in \mathbb{F}^k$, it outputs $RS(\overline{a}) = (z_0, z_1, \ldots, z_{n-1})$, where $z_j = \sum_{i=0}^{k-1} a_i f_j^i$, for distinct $f_j \in \mathbb{F}$.

Error-Correcting Codes: Reed-Solomon Codes

Definition (Reed-Solomon Codes [WB99])

For a finite field $\mathbb{F}$, and integers $k \leq n \leq |\mathbb{F}|$, Reed-Solomon code is defined as a function $RS : \mathbb{F}^k \to \mathbb{F}^n$, such that on input $\bar{a} = (a_0, a_1, \ldots, a_{k-1}) \in \mathbb{F}^k$, it outputs $RS(\bar{a}) = (z_0, z_1, \ldots, z_{n-1})$, where $z_j = \sum_{i=0}^{k-1} a_i f_j^i$, for distinct $f_j \in \mathbb{F}$.

a_0	a_1	a_2	$\cdots$	a_{n-1}

Error-Correcting Codes: Reed-Solomon Codes

Definition (Reed-Solomon Codes [WB99])

For a finite field $\mathbb{F}$, and integers $k \leq n \leq |\mathbb{F}|$, Reed-Solomon code is defined as a function $RS : \mathbb{F}^k \to \mathbb{F}^n$, such that on input $\bar{a} = (a_0, a_1, \ldots, a_{k-1}) \in \mathbb{F}^k$, it outputs $RS(\bar{a}) = (z_0, z_1, \ldots, z_{n-1})$, where $z_j = \sum_{i=0}^{k-1} a_i f_j^i$, for distinct $f_j \in \mathbb{F}$.

a_0	a_1	a_2	$\cdots$	a_{n-1}

- Efficient Decoding [WB86]: Error locator polynomial $Q(x) = \prod_{j=1}^{t}(x - e_{i_j})$

Error-Correcting Codes: Reed-Solomon Codes

Definition (Reed-Solomon Codes [WB99])

For a finite field $\mathbb{F}$, and integers $k \leq n \leq |\mathbb{F}|$, Reed-Solomon code is defined as a function $RS : \mathbb{F}^k \to \mathbb{F}^n$, such that on input $\overline{a} = (a_0, a_1, \ldots, a_{k-1}) \in \mathbb{F}^k$, it outputs $RS(\overline{a}) = (z_0, z_1, \ldots, z_{n-1})$, where $z_j = \sum_{i=0}^{k-1} a_i f_j^i$, for distinct $f_j \in \mathbb{F}$.

a_0	a_1	a_2	$\cdots$	a_{n-1}

- Efficient Decoding [WB86]: Error locator polynomial $Q(x) = \prod_{j=1}^{t}(x - e_{i_j})$
- $P(e_j)Q(e_j) = c_j' Q(e_j)$

Error-Correcting Codes: Reed-Solomon Codes

Definition (Reed-Solomon Codes [WB99])

For a finite field $\mathbb{F}$, and integers $k \leq n \leq |\mathbb{F}|$, Reed-Solomon code is defined as a function $RS : \mathbb{F}^k \to \mathbb{F}^n$, such that on input $\bar{a} = (a_0, a_1, \ldots, a_{k-1}) \in \mathbb{F}^k$, it outputs $RS(\bar{a}) = (z_0, z_1, \ldots, z_{n-1})$, where $z_j = \sum_{i=0}^{k-1} a_i f_j^i$, for distinct $f_j \in \mathbb{F}$.

a_0	a_1	a_2	$\cdots$	a_{n-1}

- Efficient Decoding [WB86]: Error locator polynomial $Q(x) = \prod_{j=1}^{t}(x - e_{i_j})$
- $P(e_j)Q(e_j) = c_j' Q(e_j)$
- Error: $< 50\%$

Error-Correcting Codes: List Decoding

- **List Decoding:** Crossing the 50% barrier [Sud97].

Error-Correcting Codes: List Decoding

- **List Decoding:** Crossing the 50% barrier [Sud97].
- Bivariate error locator polynomial $Q(x, y)$ such that $Q(e_j, c'_j) = 0$ $\forall 0 \leq j \leq n - 1$.
- Linear equation solving such that $R(x) = Q(x, P(x)) = 0$ [Sud96].

Definition (AG Codes [Gop82, Chu04])

Given a non-singular projective curve $\mathbf{X}$ over $\mathbb{F}_q^m$, let $\mathcal{P} = \{P_1, P_2, \dots, P_n\} \subset \mathbf{X}(\mathbb{F}_q)$ be a collection of points. Let a divisor D be such that $\mathcal{P} \cap \mathrm{supp}(D) = \phi$.

Error-Correcting Codes: Algebraic Geometric Codes

Definition (AG Codes [Gop82, Chu04])

Given a non-singular projective curve $\mathbf{X}$ over $\mathbb{F}_q^m$, let $\mathcal{P} = \{P_1, P_2, \ldots, P_n\} \subset \mathbf{X}(\mathbb{F}_q)$ be a collection of points.
Let a divisor D be such that $\mathcal{P} \cap \mathrm{supp}(D) = \phi$. Riemann-Roch Theorem gives a unique vector space $L(D)$.

Error-Correcting Codes: Algebraic Geometric Codes

Definition (AG Codes [Gop82, Chu04])

Given a non-singular projective curve $\mathbf{X}$ over $\mathbb{F}_q^m$, let $\mathcal{P} = \{P_1, P_2, \ldots, P_n\} \subset \mathbf{X}(\mathbb{F}_q)$ be a collection of points.
Let a divisor D be such that $\mathcal{P} \cap \mathrm{supp}(D) = \phi$. Riemann-Roch Theorem gives a unique vector space $L(D)$.

$$C(X, \mathcal{P}, D) = \{(f(P_1), f(P_2), \ldots, f(P_n)) | f \in L(D)\} \subset \mathbb{F}_q^n.$$

Subspace Designs

- Collection of subspaces $\mathcal{H} = \{H_1, H_2, \ldots, H_M\} \subset \mathbb{F}_q^m$.

Subspace Designs

- Collection of subspaces $\mathcal{H} = \{H_1, H_2, \ldots, H_M\} \subset \mathbb{F}_q^m$.
- (s, A)-subspace: Every s-dimensional subspace $W \subset \mathbb{F}_q^m$ intersects with at most A-many H_i's non-trivially.

Subspace Designs

- Collection of subspaces $\mathcal{H} = \{H_1, H_2, \ldots, H_M\} \subset \mathbb{F}_q^m$.
- (s, A)-subspace: Every s-dimensional subspace $W \subset \mathbb{F}_q^m$ intersects with at most A-many H_i's non-trivially.
- "Well Spread-out property" [GK16]: random collection of good subspaces $\rightarrow$ good subspaces.

Subspace Designs: Motivation

- Output size in list-decoding algorithms of RS and AG codes.

Subspace Designs: Motivation

- Output size in list-decoding algorithms of RS and AG codes.
- [GX13]: List decoding solutions of RS code f evaluated at $\mathbb{F}_q \mapsto$ pinned to a linear subspace.

Subspace Designs: Motivation

- Output size in list-decoding algorithms of RS and AG codes.
- [GX13]: List decoding solutions of RS code f evaluated at $\mathbb{F}_q \mapsto$ pinned to a linear subspace.
    - Solution polynomials: $f(x) = f_0 + f_1 x + \cdots + f_{k-1} x^{k-1}$
    - $f_i \in W + A_i(f_0, \ldots, f_{i-1})$, $\forall i \in 0, 1, \ldots, k-1$.

Subspace Designs: Motivation

- Output size in list-decoding algorithms of RS and AG codes.
- [GX13]: List decoding solutions of RS code f evaluated at $\mathbb{F}_q \mapsto$ pinned to a linear subspace.
  - Solution polynomials: $f(x) = f_0 + f_1 x + \cdots + f_{k-1} x^{k-1}$
  - $f_i \in W + A_i(f_0, \ldots, f_{i-1})$, $\forall i \in 0, 1, \ldots, k-1$.
  - Radius $\frac{s}{s+1}(n-k)$, $\dim(W) = s - 1$.

Subspace Designs: Motivation

- Output size in list-decoding algorithms of RS and AG codes.
- [GX13]: List decoding solutions of RS code f evaluated at $\mathbb{F}_q \mapsto$ pinned to a linear subspace.
  - Solution polynomials: $f(x) = f_0 + f_1 x + \cdots + f_{k-1}x^{k-1}$
  - $f_i \in W + A_i(f_0, \ldots, f_{i-1})$, $\forall i \in 0, 1, \ldots, k-1$.
  - Radius $\frac{s}{s+1}(n-k)$, $\dim(W) = s - 1$.
- Also gave a family of AG codes whose list decoded solutions are pinned down to a linear subspace.

Subspace Designs: Motivation

- Messages $f_i \in H_i$, H_i's are $\mathbb{F}_q$ subspaces of $\mathbb{F}_{q^m}$.

Subspace Designs: Motivation

- Messages $f_i \in H_i$, H_i's are $\mathbb{F}_q$ subspaces of $\mathbb{F}_{q^m}$.
- Dimensions of solutions to f_i's of given form: $\sum_{i=0}^{k-1} \dim(W \cap H_i)$.

Subspace Designs: Motivation

- Messages $f_i \in H_i$, H_i's are $\mathbb{F}_q$ subspaces of $\mathbb{F}_{q^m}$.
- Dimensions of solutions to f_i's of given form: $\sum_{i=0}^{k-1} \dim(W \cap H_i)$.

Theorem ([GK16])

For every $R \in (0,1)$, we can construct a family of ECCs of rate R on an alphabet set of size $(1/\epsilon)^{\mathcal{O}(1/\epsilon^2)}$. This can be list decoded in $n^{\mathcal{O}(1)}$ time with $(1 - R - \epsilon)$ errors, which outputs a list of size at most $exp_{1/\epsilon}(exp_{1/\epsilon}(exp(\mathcal{O}(\log^* n))))$.

Subspace Designs

Definition (Weak Subspace Designs [GK16])

A collection of subspaces $\mathcal{H} \subset \mathbb{F}_q^m$ is called an (s, A)-weak subspace design if, for every linear subspace $W \subset \mathbb{F}_q^m$ of dimension s, we have

$$|\{i \in [M] | \dim_{\mathbb{F}_q}(W \cap H_i) > 0\}| \leq A \tag{1}$$

Subspace Designs

Definition (Weak Subspace Designs [GK16])

A collection of subspaces $\mathcal{H} \subset \mathbb{F}_q^m$ is called an (s, A)-weak subspace design if, for every linear subspace $W \subset \mathbb{F}_q^m$ of dimension s, we have

$$|\{i \in [M] | \dim_{\mathbb{F}_q}(W \cap H_i) > 0\}| \leq A \tag{1}$$

Definition (Strong Subspace Desins [GK16])

Similarly, a collection of subspaces $\mathcal{H}$ is called an (s, A)-weak subspace design if, for every linear subspace $W \subseteq \mathbb{F}_q^m$ of dimension s, we have

$$\sum_{i=1}^{M} \dim_{\mathbb{F}_q}(W \cap H_i) \leq A \tag{2}$$

- (s, A)-strong subspace $\rightarrow$ (s, A)-weak subspace.

Subspace Designs

Definition (Weak Subspace Designs [GK16])

A collection of subspaces $\mathcal{H} \subset \mathbb{F}_q^m$ is called an (s, A)-weak subspace design if, for every linear subspace $W \subset \mathbb{F}_q^m$ of dimension s, we have

$$|\{i \in [M] | \dim_{\mathbb{F}_q}(W \cap H_i) > 0\}| \leq A \tag{1}$$

Definition (Strong Subspace Desins [GK16])

Similarly, a collection of subspaces $\mathcal{H}$ is called an (s, A)-weak subspace design if, for every linear subspace $W \subseteq \mathbb{F}_q^m$ of dimension s, we have

$$\sum_{i=1}^{M} \dim_{\mathbb{F}_q}(W \cap H_i) \leq A \tag{2}$$

- (s, A)-strong subspace $\rightarrow$ (s, A)-weak subspace.
- (s, A)-weak subspace $\rightarrow$ (s, sA)-strong subspace.

Subspace Designs

Example

- $\alpha_1, \alpha_2, \ldots, \alpha_M \in \mathbb{F}_q$
- $v_{\alpha_i} = (1, \alpha_i, \alpha_i^2, \ldots, \alpha_i^{m-1}) \in \mathbb{F}_q^m$
- $H_i = \{x \in \mathbb{F}_q^m | \langle x, v_{\alpha_i} \rangle = 0\}$

Subspace Designs

Example

- $\alpha_1, \alpha_2, \dots, \alpha_M \in \mathbb{F}_q$
- $v_{\alpha_i} = (1, \alpha_i, \alpha_i^2, \dots, \alpha_i^{m-1}) \in \mathbb{F}_q^m$
- $H_i = \{x \in \mathbb{F}_q^m | \langle x, v_{\alpha_i} \rangle = 0\}$
- (s, m)-strong subspace.

Subspace Designs

Goal: Explicit construction of subspaces using folded RS codes and multiplicity codes [KRZSW18].

Subspace Designs

Goal: Explicit construction of subspaces using folded RS codes and multiplicity codes [KRZSW18].

Definition (Folded Reed-Solomon Codes)

Folded Reed-Solomon codes are a variant of Reed-Solomon Codes. The polynomial f is formed as before, and the ECC outputs

$$f(x) \mapsto (f(1), f(\gamma), f(\gamma^2), \ldots, f(\gamma^{n-1})),$$

a generator γ of $\mathbb{F}_q^*$.

Subspace Designs

Goal: Explicit construction of subspaces using folded RS codes and multiplicity codes [KRZSW18].

Definition (Folded Reed-Solomon Codes)

Folded Reed-Solomon codes are a variant of Reed-Solomon Codes. The polynomial f is formed as before, and the ECC outputs

$$f(x) \mapsto (f(1), f(\gamma), f(\gamma^2), \dots, f(\gamma^{n-1})),$$

a generator γ of $\mathbb{F}_q^*$.

Definition (Multiplicity Codes [KSY14])

It is an ECC similar to Reed-Muller codes where the output is $(f(\bar{a}), \frac{\partial f(\bar{a})}{\partial x}, \frac{\partial f(\bar{a})}{\partial y})$, for $\bar{a} \in \mathbb{F}_q^2$.

Wronskian: A nice algebraic tool

Definition (Classical Wronskian)

Given polynomials $f_1(x), f_2(x), \ldots, f_s(x) \in \mathbb{F}[x]$, the Wronskian $W(f_1, f_2, \ldots, f_s)$ is defined as:

$$\begin{bmatrix} f_1(x) & \ldots & f_s(x) \\ f_1^{(1)}(x) & \ldots & f_s^{(1)}(x) \\ \vdots & & \vdots \\ f_1^{(s-1)}(x) & \ldots & f_s^{(s-1)}(x) \end{bmatrix}.$$

Wronskian: A nice algebraic tool

Definition (Classical Wronskian)

Given polynomials $f_1(x), f_2(x), \dots, f_s(x) \in \mathbb{F}[x]$, the Wronskian $W(f_1, f_2, \dots, f_s)$ is defined as:

$$\begin{bmatrix} f_1(x) & \dots & f_s(x) \\ f_1^{(1)}(x) & \dots & f_s^{(1)}(x) \\ \vdots & & \vdots \\ f_1^{(s-1)}(x) & \dots & f_s^{(s-1)}(x) \end{bmatrix}.$$

$f_1, \dots f_s$ are linearly independent over $\mathbb{F} \iff \det(W(f_1, \dots, f_s)) \neq 0$.

Wronskian: A nice algebraic tool

Definition (Folded Wronskian)

Given polynomials $f_1(x), f_2(x), \ldots, f_s(x) \in \mathbb{F}[x]$ and $\gamma \in \mathbb{F}^*$, the folded Wronskian $W_\gamma(f_1, f_2, \ldots, f_s)$ is defined as:

$$\begin{bmatrix} f_1(x) & \ldots & f_s(x) \\ f_1(\gamma x) & \ldots & f_s(\gamma x) \\ \vdots & & \vdots \\ f_1(\gamma^{s-1} x) & \ldots & f_s(\gamma^{s-1} x) \end{bmatrix}.$$

Wronskian: A nice algebraic tool

Definition (Folded Wronskian)

Given polynomials $f_1(x), f_2(x), \ldots, f_s(x) \in \mathbb{F}[x]$ and $\gamma \in \mathbb{F}^*$, the folded Wronskian $W_\gamma(f_1, f_2, \ldots, f_s)$ is defined as:

$$\begin{bmatrix} f_1(x) & \ldots & f_s(x) \\ f_1(\gamma x) & \ldots & f_s(\gamma x) \\ \vdots & & \vdots \\ f_1(\gamma^{s-1} x) & \ldots & f_s(\gamma^{s-1} x) \end{bmatrix}.$$

$f_1, \ldots f_s$ are linearly independent over $\mathbb{F}$ $\iff$ $\det(W_\gamma(f_1, \ldots, f_s)) \neq 0$.

Explicit Subspace Designs: Folded Reed-Solomon Codes

Weak Subspace Construction [GK16]

For a generator γ of $\mathbb{F}_q^*$ and some t such that $s \leq t \leq m < q$, define the set $\mathcal{F} = \{\gamma^{jt} | j \in \{0, 1, \ldots, q/t\}\}$. Now, $\forall \alpha \in \mathcal{F}$, define the subspaces

$$\mathcal{H}_\alpha = \{P(x) \in \mathbb{F}_q[x]_{<m} | P(\alpha\gamma^i) = 0, \forall i \in \{0, 1, \ldots, t-1\}\}$$

Explicit Subspace Designs: Folded Reed-Solomon Codes

Weak Subspace Construction [GK16]

For a generator γ of $\mathbb{F}_q^*$ and some t such that $s \leq t \leq m < q$, define the set $\mathcal{F} = \{\gamma^{jt} | j \in \{0, 1, \dots, q/t\}\}$. Now, $\forall \alpha \in \mathcal{F}$, define the subspaces

$$\mathcal{H}_\alpha = \{P(x) \in \mathbb{F}_q[x]_{<m} | P(\alpha\gamma^i) = 0, \forall i \in \{0, 1, \dots, t-1\}\}$$

Codimension of $\mathcal{H}_\alpha$ is t.

Explicit Subspace Designs: Folded Reed-Solomon Codes

Weak Subspace Construction [GK16]

For a generator γ of $\mathbb{F}_q^*$ and some t such that $s \leq t \leq m < q$, define the set $\mathcal{F} = \{\gamma^{jt} | j \in \{0, 1, \ldots, q/t\}\}$. Now, $\forall \alpha \in \mathcal{F}$, define the subspaces

$$\mathcal{H}_\alpha = \{P(x) \in \mathbb{F}_q[x]_{<m} | P(\alpha\gamma^i) = 0, \forall i \in \{0, 1, \ldots, t-1\}\}$$

Codimension of $\mathcal{H}_\alpha$ is t.

Theorem ([GK16])

The collection of subspaces given by $\{\mathcal{H}_\alpha | \alpha \in \mathcal{F}\}$ is an $\left(s, \frac{(m-1)s}{t-s+1}\right)$-weak subspace design.

Explicit Subspace Designs: Folded Reed-Solomon Codes

Proof Idea:

- Consider folded Wronskian of basis of W as a polynomial $L(x)$.

Explicit Subspace Designs: Folded Reed-Solomon Codes

Proof Idea:

- Consider folded Wronskian of basis of W as a polynomial $L(x)$.
- $\dim_{\mathbb{F}_q}(W \cap \mathcal{H}_\alpha) > 0 \implies L(\alpha.\gamma^i) = 0$, $0 \leq i \leq t - s$.

Explicit Subspace Designs: Folded Reed-Solomon Codes

Proof Idea:

- Consider folded Wronskian of basis of W as a polynomial $L(x)$.
- $\dim_{\mathbb{F}_q}(W \cap \mathcal{H}_\alpha) > 0 \implies L(\alpha.\gamma^i) = 0$, $0 \le i \le t - s$.
- $\deg(L) = (m-1)s$, $(t - s + 1)$-many roots.

Explicit Subspace Designs: Folded Reed-Solomon Codes

Improving the Construction

s, t, r, q, m are parameters such that $s \leq t \leq m < q$. Given a generator γ of $\mathbb{F}_q^*$ and an $\alpha \in \mathbb{F}_{q^r}$, define

$$S_\alpha = \{\alpha^{q^j}\gamma^i | 0 \leq j < r, 0 \leq i < t\} \subseteq \mathbb{F}_{q^r},$$

and

$$S'_\alpha = \{\alpha^{q^j}\gamma^i | 0 \leq j < r, 0 \leq i < t - s + 1\}.$$

Explicit Subspace Designs: Folded Reed-Solomon Codes

Improving the Construction

s, t, r, q, m are parameters such that $s \leq t \leq m < q$. Given a generator γ of $\mathbb{F}_q^*$ and an $\alpha \in \mathbb{F}_{q^r}$, define

$$S_\alpha = \{\alpha^{q^j}\gamma^i | 0 \leq j < r, 0 \leq i < t\} \subseteq \mathbb{F}_{q^r},$$

and

$$S'_\alpha = \{\alpha^{q^j}\gamma^i | 0 \leq j < r, 0 \leq i < t - s + 1\}.$$

Define $\mathcal{F}$ such that

- $\mathcal{F} = \{\alpha \in \mathbb{F}_{q^r} | \mathbb{F}_q[\alpha] = \mathbb{F}_q\} \subset \mathbb{F}_{q^r}$,
- $\alpha, \beta \in \mathcal{F}, \alpha \neq \beta \implies S_\alpha \cap S_\beta = \phi$,
- $|S_\alpha| = rt$.

Explicit Subspace Designs: Folded Reed-Solomon Codes

Improving the Construction

s, t, r, q, m are parameters such that $s \leq t \leq m < q$. Given a generator γ of $\mathbb{F}_q^*$ and an $\alpha \in \mathbb{F}_{q^r}$, define

$$S_\alpha = \{\alpha^{q^j}\gamma^i | 0 \leq j < r, 0 \leq i < t\} \subseteq \mathbb{F}_{q^r},$$

and

$$S'_\alpha = \{\alpha^{q^j}\gamma^i | 0 \leq j < r, 0 \leq i < t - s + 1\}.$$

Define $\mathcal{F}$ such that

- $\mathcal{F} = \{\alpha \in \mathbb{F}_{q^r} | \mathbb{F}_q[\alpha] = \mathbb{F}_q\} \subset \mathbb{F}_{q^r}$,
- $\alpha, \beta \in \mathcal{F}, \alpha \neq \beta \implies S_\alpha \cap S_\beta = \phi$,
- $|S_\alpha| = rt$.

We take $|\mathcal{F}| = \Omega(\frac{q^r}{rt})$. Also, $|S_\alpha| = r(t - s + 1)$

Explicit Subspace Designs: Folded Reed-Solomon Codes

Strong Subspace Construction [GK16]

For every $\alpha \in \mathcal{F}$, define the subspaces

$$\mathcal{H}_\alpha = \{P(x) | P(\alpha.\gamma^j) \equiv 0 \ \forall j \in \{0, 1, \ldots, t-1\}\}.$$

Explicit Subspace Designs: Folded Reed-Solomon Codes

Strong Subspace Construction [GK16]

For every $\alpha \in \mathcal{F}$, define the subspaces

$$\mathcal{H}_\alpha = \{P(x) | P(\alpha.\gamma^j) \equiv 0 \ \forall j \in \{0, 1, \ldots, t-1\}\}.$$

$\mathcal{H}_\alpha$ has codimension rt.

Explicit Subspace Designs: Folded Reed-Solomon Codes

Strong Subspace Construction [GK16]

For every $\alpha \in \mathcal{F}$, define the subspaces

$$\mathcal{H}_\alpha = \{P(x) | P(\alpha.\gamma^j) \equiv 0 \;\forall j \in \{0, 1, \ldots, t-1\}\}.$$

$\mathcal{H}_\alpha$ has codimension rt.

Theorem ([GK16])

The collection $(\mathcal{H}_\alpha)_{\alpha \in \mathcal{F}}$ is an $\left(s, \frac{(m-1)s}{r(t-s+1)}\right)$-strong subspace.

Explicit Subspace Designs: Folded Reed-Solomon Codes

Proof Idea:

- Given basis $P_1, \ldots, P_s$ of W, form its folded Wronskian $M(x)$.

Explicit Subspace Designs: Folded Reed-Solomon Codes

Proof Idea:

- Given basis $P_1, \ldots, P_s$ of W, form its folded Wronskian $M(x)$.
- The matrix $M(\alpha) \in \mathbb{F}_{q^r}^{t \times s}$ satisfies $\mathrm{rank}(M(\alpha)) \leq s - \dim_{\mathbb{F}_q}(W \cap \mathcal{H}_\alpha)$.

Explicit Subspace Designs: Folded Reed-Solomon Codes

Proof Idea:

- Given basis $P_1, \ldots, P_s$ of W, form its folded Wronskian $M(x)$.
- The matrix $M(\alpha) \in \mathbb{F}_{q^r}^{t \times s}$ satisfies $\mathrm{rank}(M(\alpha)) \leq s - \dim_{\mathbb{F}_q}(W \cap \mathcal{H}_\alpha)$.
- For each $\beta \in S'_\alpha$, we have $\dim(W \cap H_\alpha) \leq \mathrm{mult}(L, \beta) \leq s(m-1)$

Explicit Subspace Designs: Folded Reed-Solomon Codes

Proof Idea:

- Given basis $P_1, \ldots, P_s$ of W, form its folded Wronskian $M(x)$.
- The matrix $M(\alpha) \in \mathbb{F}_{q^r}^{t \times s}$ satisfies
  $\text{rank}(M(\alpha)) \leq s - \dim_{\mathbb{F}_q}(W \cap \mathcal{H}_\alpha)$.
- For each $\beta \in S'_\alpha$, we have $\dim(W \cap H_\alpha) \leq \text{mult}(L, \beta) \leq s(m-1)$
- Sum over all α and β.

Explicit Subspace Designs: Multiplicity Codes

Strong Subspace Construction [GK16]

For each $\alpha \in \mathbb{F}_q$, consider the subspaces

$$\mathcal{H}_\alpha = \{P(x) \in \mathbb{F}_q[x]^{<m} | \mathrm{mult}(P, \alpha) \geq t\}$$

Explicit Subspace Designs: Multiplicity Codes

Strong Subspace Construction [GK16]

For each $\alpha \in \mathbb{F}_q$, consider the subspaces

$$\mathcal{H}_\alpha = \{P(x) \in \mathbb{F}_q[x]^{<m} | \mathrm{mult}(P, \alpha) \geq t\}$$

$\mathcal{H}_\alpha$ has codimension t.

Explicit Subspace Designs: Multiplicity Codes

Strong Subspace Construction [GK16]

For each $\alpha \in \mathbb{F}_q$, consider the subspaces

$$\mathcal{H}_\alpha = \{P(x) \in \mathbb{F}_q[x]^{<m} | \mathrm{mult}(P, \alpha) \geq t\}$$

$\mathcal{H}_\alpha$ has codimension t.

Theorem ([GK16])

The collection $(\mathcal{H}_\alpha)_{\alpha \in \mathcal{F}}$ is an $\left(s, \frac{(m-1)s}{(t-s+1)}\right)$-strong subspace.

Explicit Subspace Designs: Multiplicity Codes

Proof Idea:

- Given basis $P_1, \ldots, P_s$ of W, form its Wronskian $M(x)$.

Explicit Subspace Designs: Multiplicity Codes

Proof Idea:

- Given basis $P_1, \ldots, P_s$ of W, form its Wronskian $M(x)$.
- $W \cap \mathcal{H}_\alpha$ is nontrivial $\implies$ $M(\alpha)$ is singular matrix.

Explicit Subspace Designs: Multiplicity Codes

Proof Idea:

- Given basis $P_1, \ldots, P_s$ of W, form its Wronskian $M(x)$.
- $W \cap \mathcal{H}_\alpha$ is nontrivial $\implies$ $M(\alpha)$ is singular matrix.
- $\text{rank}(M(\alpha)) = s - \dim(W \cap \mathcal{H}_\alpha)$.

Explicit Subspace Designs: Multiplicity Codes

Proof Idea:

- Given basis $P_1, \ldots, P_s$ of W, form its Wronskian $M(x)$.
- $W \cap \mathcal{H}_\alpha$ is nontrivial $\implies$ $M(\alpha)$ is singular matrix.
- $\text{rank}(M(\alpha)) = s - \dim(W \cap \mathcal{H}_\alpha)$.
- $\text{mult}(L, \alpha) \geq (t - s + 1).\dim(W \cap \mathcal{H}_\alpha)$.

Explicit Subspace Designs: Multiplicity Codes

Improving the Construction

s, t, r, q, m are parameters such that $s \leq t \leq m < \mathrm{char}(\mathbb{F}_q)$.

- Again, we form $\mathcal{F}_0 \subseteq \mathbb{F}_{q^r}$ s.t. $\mathbb{F}_q[\alpha] = \mathbb{F}_{q^r}$.

Explicit Subspace Designs: Multiplicity Codes

Improving the Construction

s, t, r, q, m are parameters such that $s \leq t \leq m < \mathrm{char}(\mathbb{F}_q)$.

- Again, we form $\mathcal{F}_0 \subseteq \mathbb{F}_{q^r}$ s.t. $\mathbb{F}_q[\alpha] = \mathbb{F}_{q^r}$.
- We have $|\mathcal{F}_0| = q^r(1 - o(1))$. Partition $\mathcal{F}_0$ into r sets such that they are mutual conjugates over $\mathbb{F}_q$.

Explicit Subspace Designs: Multiplicity Codes

Improving the Construction

s, t, r, q, m are parameters such that $s \le t \le m < \mathrm{char}(\mathbb{F}_q)$.

- Again, we form $\mathcal{F}_0 \subseteq \mathbb{F}_{q^r}$ s.t. $\mathbb{F}_q[\alpha] = \mathbb{F}_{q^r}$.
- We have $|\mathcal{F}_0| = q^r(1 - o(1))$. Partition $\mathcal{F}_0$ into r sets such that they are mutual conjugates over $\mathbb{F}_q$.
- Choose one element from each of these sets to form $\mathcal{F}$ with $|\mathcal{F}| \approx q^r/r$

Explicit Subspace Designs: Multiplicity Codes

Strong Subspace Construction [GK16]

For each $\alpha \in \mathcal{F}$, consider the subspaces

$$\mathcal{H}_\alpha = \{P(x) \in \mathbb{F}_q[x]^{<m} | \mathrm{mult}(P, \alpha) \geq t\}$$

Explicit Subspace Designs: Multiplicity Codes

Strong Subspace Construction [GK16]

For each $\alpha \in \mathcal{F}$, consider the subspaces

$$\mathcal{H}_\alpha = \{P(x) \in \mathbb{F}_q[x]^{<m} | \mathrm{mult}(P, \alpha) \geq t\}$$

$\mathcal{H}_\alpha$ has codimension t.

Explicit Subspace Designs: Multiplicity Codes

Strong Subspace Construction [GK16]

For each $\alpha \in \mathcal{F}$, consider the subspaces

$$\mathcal{H}_\alpha = \{P(x) \in \mathbb{F}_q[x]^{<m} | \mathrm{mult}(P, \alpha) \geq t\}$$

$\mathcal{H}_\alpha$ has codimension t.

Theorem ([GK16])

The collection $(\mathcal{H}_\alpha)_{\alpha \in \mathcal{F}}$ is an $\left(s, \frac{(m-1)s}{r(t-s+1)}\right)$-strong subspace.

Explicit Subspace Designs: Multiplicity Codes

Proof Idea:

- Given basis $P_1, \ldots, P_s$ of W, form its Wronskian $M(x)$.

Explicit Subspace Designs: Multiplicity Codes

Proof Idea:

- Given basis $P_1, \ldots, P_s$ of W, form its Wronskian $M(x)$.
- $W \cap \mathcal{H}_\alpha$ is nontrivial $\implies$ $M(\alpha)$ is singular matrix.

Explicit Subspace Designs: Multiplicity Codes

Proof Idea:

- Given basis $P_1, \ldots, P_s$ of W, form its Wronskian $M(x)$.
- $W \cap \mathcal{H}_\alpha$ is nontrivial $\implies$ $M(\alpha)$ is singular matrix.
- $\text{rank}(M(\alpha)) \leq s - \dim(W \cap \mathcal{H}_\alpha)$.

Explicit Subspace Designs: Multiplicity Codes

Proof Idea:

- Given basis $P_1, \ldots, P_s$ of W, form its Wronskian $M(x)$.
- $W \cap \mathcal{H}_\alpha$ is nontrivial $\implies M(\alpha)$ is singular matrix.
- $\mathrm{rank}(M(\alpha)) \leq s - \dim(W \cap \mathcal{H}_\alpha)$.
- $\mathrm{mult}(L, \alpha) \geq (t - s + 1).\dim(W \cap \mathcal{H}_\alpha)$.

Explicit Subspace Designs: Multiplicity Codes

Proof Idea:

- Given basis $P_1, \ldots, P_s$ of W, form its Wronskian $M(x)$.
- $W \cap \mathcal{H}_\alpha$ is nontrivial $\implies$ $M(\alpha)$ is singular matrix.
- $\mathrm{rank}(M(\alpha)) \leq s - \dim(W \cap \mathcal{H}_\alpha)$.
- $\mathrm{mult}(L, \alpha) \geq (t - s + 1).\dim(W \cap \mathcal{H}_\alpha)$.
- $(m-1).s \geq \sum_{\alpha \in \mathcal{F}_0} \mathrm{mult}(L, \alpha) = \sum_{\alpha \in \mathcal{F}} r.\mathrm{mult}(L, \alpha) \geq r.(t - s + 1) \sum_{\alpha \in \mathcal{F}} \dim(W \cap H_\alpha)$.

Consequences of List Decoding

- Pick subcodes of codes using subspaces to reduce list size.

Consequences of List Decoding

- Pick subcodes of codes using subspaces to reduce list size.
- In RS, coefficients of polynomials are restricted to subspaces $\mathcal{H}$ that form (s, A)-strong subspace designs.
- Error: $\frac{s}{s+1}(q-k)$; $\dim(H_i) = (1-\epsilon)m$; Rate: $\frac{(1-\epsilon)k}{q}$.

Consequences of List Decoding

- Pick subcodes of codes using subspaces to reduce list size.
- In RS, coefficients of polynomials are restricted to subspaces $\mathcal{H}$ that form (s, A)-strong subspace designs.
- Error: $\frac{s}{s+1}(q-k)$; $\dim(H_i) = (1-\epsilon)m$; Rate: $\frac{(1-\epsilon)k}{q}$.
- Pick $s = \mathcal{O}(1/\epsilon)$, $m = \Omega(s/\epsilon)$.

Consequences of List Decoding

- Pick subcodes of codes using subspaces to reduce list size.
- In RS, coefficients of polynomials are restricted to subspaces $\mathcal{H}$ that form (s, A)-strong subspace designs.
- Error: $\frac{s}{s+1}(q-k)$; $\dim(H_i) = (1-\epsilon)m$; Rate: $\frac{(1-\epsilon)k}{q}$.
- Pick $s = \mathcal{O}(1/\epsilon)$, $m = \Omega(s/\epsilon)$.
- AG codes: Do in blocks [GX13, GK16].

Sanjeev Arora and Boaz Barak.

Computational complexity: a modern approach.

Cambridge University Press, 2009.

Key One Chung.

Goppa codes, December 2004.

Department of Mathematics, Iowa State University.

Venkatesan Guruswami and Swastik Kopparty.

Explicit subspace designs.

Combinatorica, 36(2):161–185, 2016.

Valerii Denisovich Goppa.

Algebraico-geometric codes.

Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya, 46(4):762–781, 1982.

Venkatesan Guruswami and Chaoping Xing.

List decoding reed-solomon, algebraic-geometric, and gabidulin subcodes up to the singleton bound.

In *Proceedings of the forty-fifth annual ACM symposium on Theory of computing*, pages 843–852, 2013.

Swastik Kopparty, Noga Ron-Zewi, Shubhangi Saraf, and Mary Wootters.

Improved decoding of folded reed-solomon and multiplicity codes.

In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 212–223. IEEE, 2018.

Swastik Kopparty, Shubhangi Saraf, and Sergey Yekhanin.

High-rate codes with sublinear-time decoding.

Journal of the ACM (JACM), 61(5):1–20, 2014.

Noam Nisan and Avi Wigderson.

Hardness vs randomness.

Journal of computer and System Sciences, 49(2):149–167, 1994.

Madhu Sudan.

Maximum likelihood decoding of reed solomon codes.

In *Proceedings of 37th Conference on Foundations of Computer Science*, pages 164–172. IEEE, 1996.

Madhu Sudan.

Decoding of reed solomon codes beyond the error-correction bound.

Journal of complexity, 13(1):180–193, 1997.

Lloyd R Welch and Elwyn R Berlekamp.

Error correction for algebraic block codes, December 30 1986.

US Patent 4,633,470.

Stephen B Wicker and Vijay K Bhargava.

Reed-Solomon codes and their applications.

John Wiley & Sons, 1999.

Thank You!