

Rank-Metric Decoding

What We Know, What We Don't, and Where to Look Next

Violetta Weger

joint work with:

Hugo Beelloo-Sauerbier Couvée, Antonia Wachter-Zeh

AM-PQC 2026 Workshop on Algebraic Methods in Post-Quantum Cryptography

August, 2026

Why Should We Care About Rank Metric?



Why Should We Care About Rank Metric?



All sizes for NIST security level 1

Code-based KEMs

|pk|

|ct|

HQC (Hamming quasi-cyclic)

2.2 KB

4.4 KB

✓ standardized

Why Should We Care About Rank Metric?



All sizes for NIST security level 1

Code-based KEMs

	$ \text{pk} $	$ \text{ct} $	
HQC (Hamming quasi-cyclic)	2.2 KB	4.4 KB	✓ standardized
RQC (Rank quasi-cyclic)	1.8 KB ↓ 18%	3.6 KB ↓ 18%	× Round 2

Why Should We Care About Rank Metric?

All sizes for NIST security level 1

Code-based KEMs

$|\text{pk}|$

$|\text{ct}|$

HQC (Hamming quasi-cyclic)

2.2 KB

4.4 KB

✓ standardized

RQC (Rank quasi-cyclic)

1.8 KB

3.6 KB

× Round 2

↓ 18%

↓ 18%

Code-based signatures

$|\text{sig}|_{\text{short}}$

$|\text{sig}|_{\text{fast}}$

SDitH (Hamming MPCitH)

3.7 KB

4.4 KB

✓ Round 3

Why Should We Care About Rank Metric?

All sizes for NIST security level 1

Code-based KEMs

	$ \text{pk} $	$ \text{ct} $	
HQC (Hamming quasi-cyclic)	2.2 KB	4.4 KB	✓ standardized
RQC (Rank quasi-cyclic)	1.8 KB ↓ 18%	3.6 KB ↓ 18%	× Round 2

Code-based signatures

	$ \text{sig} _{\text{short}}$	$ \text{sig} _{\text{fast}}$	
SDitH (Hamming MPCitH)	3.7 KB	4.4 KB	✓ Round 3
RYDE (Rank MPCitH)	3.1 KB ↓ 16%	3.5 KB ↓ 20%	

Why Should We Care About Rank Metric?

All sizes for NIST security level 1

Code-based KEMs		$ \text{pk} $	$ \text{ct} $	
HQC	(Hamming quasi-cyclic)	2.2 KB	4.4 KB	✓ standardized
RQC	(Rank quasi-cyclic)	1.8 KB ↓ 18%	3.6 KB ↓ 18%	× Round 2
Code-based signatures		$ \text{sig} _{\text{short}}$	$ \text{sig} _{\text{fast}}$	
SDitH	(Hamming MPCitH)	3.7 KB	4.4 KB	✓ Round 3
RYDE	(Rank MPCitH)	3.1 KB ↓ 16%	3.5 KB ↓ 20%	× Round 2

Why Should We Care About Rank Metric?

All sizes for NIST security level 1

Code-based KEMs

	$ \text{pk} $	$ \text{ct} $	
HQC (Hamming quasi-cyclic)	2.2 KB	4.4 KB	✓ standardized
RQC (Rank quasi-cyclic)	1.8 KB ↓ 18%	3.6 KB ↓ 18%	× Round 2

Code-based signatures

	$ \text{sig} _{\text{short}}$	$ \text{sig} _{\text{fast}}$	
SDitH (Hamming MPCitH)	3.7 KB	4.4 KB	✓ Round 3
RYDE (Rank MPCitH)	3.1 KB ↓ 16%	3.5 KB ↓ 20%	× Round 2

→ Why so compact?

→ Why not selected?

Why Should We Care About Rank Metric?

All sizes for NIST security level 1

Code-based KEMs		$ \text{pk} $	$ \text{ct} $	
HQC	(Hamming quasi-cyclic)	2.2 KB	4.4 KB	✓ standardized
RQC	(Rank quasi-cyclic)	1.8 KB ↓ 18%	3.6 KB ↓ 18%	× Round 2
Code-based signatures		$ \text{sig} _{\text{short}}$	$ \text{sig} _{\text{fast}}$	
SDitH	(Hamming MPCitH)	3.7 KB	4.4 KB	✓ Round 3
RYDE	(Rank MPCitH)	3.1 KB ↓ 16%	3.5 KB ↓ 20%	× Round 2

→ Why so compact?

Harder to decode?

or

Weaker algorithms?

→ Why not selected?

Why Should We Care About Rank Metric?

All sizes for NIST security level 1

Code-based KEMs		$ \text{pk} $	$ \text{ct} $	
HQC	(Hamming quasi-cyclic)	2.2 KB	4.4 KB	✓ standardized
RQC	(Rank quasi-cyclic)	1.8 KB ↓ 18%	3.6 KB ↓ 18%	× Round 2
Code-based signatures		$ \text{sig} _{\text{short}}$	$ \text{sig} _{\text{fast}}$	
SDitH	(Hamming MPCitH)	3.7 KB	4.4 KB	✓ Round 3
RYDE	(Rank MPCitH)	3.1 KB ↓ 16%	3.5 KB ↓ 20%	× Round 2

→ Why so compact?

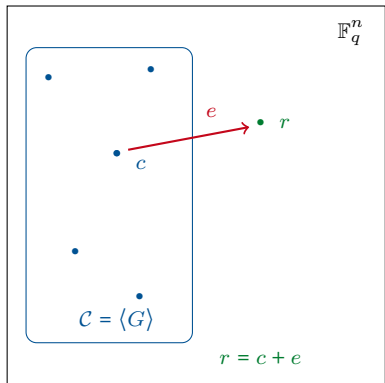
Harder to decode?

or

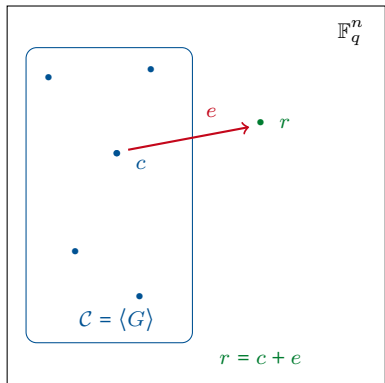
Weaker algorithms?

→ Why not selected?

Little confidence in the hardness?



- linear code: $\mathcal{C} \subseteq \mathbb{F}_q^n$ with $\dim(\mathcal{C}) = k$
- generator matrix: $G \in \mathbb{F}_q^{k \times n}$ $\mathcal{C} = \{mG \mid m \in \mathbb{F}_q^k\} = \langle G \rangle$
- codewords: $c = mG \in \mathcal{C}$
- Hamming distance: $d_H(c, r) = |\{i \mid c_i \neq r_i\}|$
- Hamming weight: $\text{wt}_H(e) = |\{i \mid e_i \neq 0\}|$
- minimum distance: $d_H(\mathcal{C}) = \min\{\text{wt}_H(c) \mid c \in \mathcal{C}, c \neq 0\}$

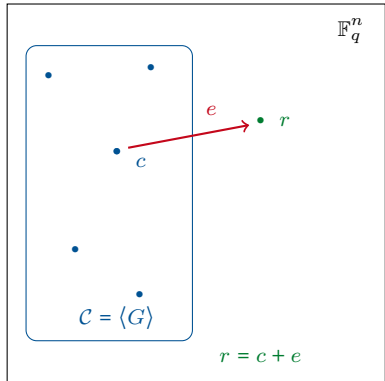


- linear code: $\mathcal{C} \subseteq \mathbb{F}_q^n$ with $\dim(\mathcal{C}) = k$
- generator matrix: $G \in \mathbb{F}_q^{k \times n}$ $\mathcal{C} = \{mG \mid m \in \mathbb{F}_q^k\} = \langle G \rangle$
- codewords: $c = mG \in \mathcal{C}$
- Hamming distance: $d_H(c, r) = |\{i \mid c_i \neq r_i\}|$
- Hamming weight: $\text{wt}_H(e) = |\{i \mid e_i \neq 0\}|$
- minimum distance: $d_H(\mathcal{C}) = \min\{\text{wt}_H(c) \mid c \in \mathcal{C}, c \neq 0\}$

Decoding Problem (DP): Given G , r , and t , find $e \in \mathbb{F}_q^n$ such that

$$r - e \in \langle G \rangle \quad \text{and} \quad \text{wt}_H(e) = t$$

Some Coding – Again



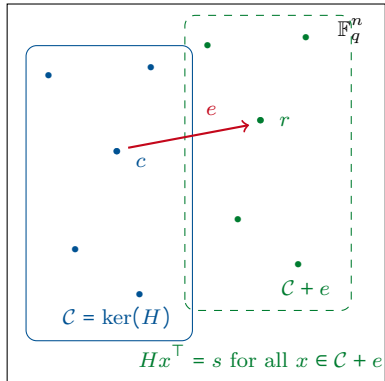
- linear code: $C \subseteq \mathbb{F}_q^n$ with $\dim(C) = k$
- generator matrix: $G \in \mathbb{F}_q^{k \times n}$ $C = \{mG \mid m \in \mathbb{F}_q^k\} = \langle G \rangle$
- codewords: $c = mG \in C$
- Hamming distance: $d_H(c, r) = |\{i \mid c_i \neq r_i\}|$
- Hamming weight: $\text{wt}_H(e) = |\{i \mid e_i \neq 0\}|$
- minimum distance: $d_H(C) = \min\{\text{wt}_H(c) \mid c \in C, c \neq 0\}$

Decoding Problem (DP): Given G , r , and t , find $e \in \mathbb{F}_q^n$ such that

$$r - e \in \langle G \rangle \quad \text{and} \quad \text{wt}_H(e) = t$$

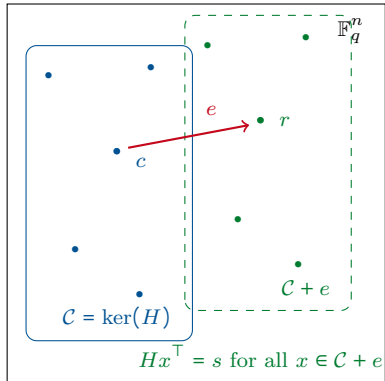
NP-hard

From Decoding to Syndrome Decoding



- linear code: $C \subseteq \mathbb{F}_q^n$ with $\dim(C) = k$
- parity-check matrix: $H \in \mathbb{F}_q^{(n-k) \times n}$
 $C = \ker(H) = \{x \in \mathbb{F}_q^n \mid Hx^\top = 0\}$
- syndrome: $s = Hr^\top = H(c + e)^\top = He^\top$
- Hamming distance: $d_H(c, r) = |\{i \mid c_i \neq r_i\}|$
- Hamming weight: $\text{wt}_H(e) = |\{i \mid e_i \neq 0\}|$
- minimum distance: $d_H(C) = \min\{\text{wt}_H(c) \mid c \in C, c \neq 0\}$

From Decoding to Syndrome Decoding

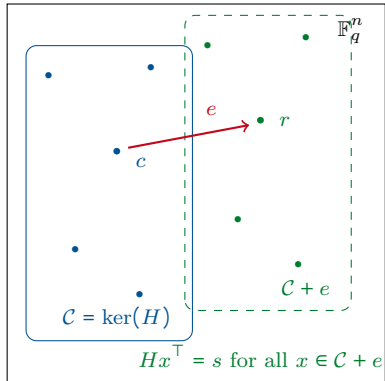


- linear code: $\mathcal{C} \subseteq \mathbb{F}_q^n$ with $\dim(\mathcal{C}) = k$
- parity-check matrix: $H \in \mathbb{F}_q^{(n-k) \times n}$
 $\mathcal{C} = \ker(H) = \{x \in \mathbb{F}_q^n \mid Hx^\top = 0\}$
- syndrome: $s = Hr^\top = H(c + e)^\top = He^\top$
- Hamming distance: $d_H(c, r) = |\{i \mid c_i \neq r_i\}|$
- Hamming weight: $\text{wt}_H(e) = |\{i \mid e_i \neq 0\}|$
- minimum distance: $d_H(\mathcal{C}) = \min\{\text{wt}_H(c) \mid c \in \mathcal{C}, c \neq 0\}$

Syndrome Decoding Problem (SDP): Given H , s , and t , find $e \in \mathbb{F}_q^n$ such that

$$He^\top = s \quad \text{and} \quad \text{wt}_H(e) = t$$

From Decoding to Syndrome Decoding



- linear code: $C \subseteq \mathbb{F}_q^n$ with $\dim(C) = k$
- parity-check matrix: $H \in \mathbb{F}_q^{(n-k) \times n}$
 $C = \ker(H) = \{x \in \mathbb{F}_q^n \mid Hx^\top = 0\}$
- syndrome: $s = Hr^\top = H(c + e)^\top = He^\top$
- Hamming distance: $d_H(c, r) = |\{i \mid c_i \neq r_i\}|$
- Hamming weight: $\text{wt}_H(e) = |\{i \mid e_i \neq 0\}|$
- minimum distance: $d_H(C) = \min\{\text{wt}_H(c) \mid c \in C, c \neq 0\}$

Syndrome Decoding Problem (SDP): Given H , s , and t , find $e \in \mathbb{F}_q^n$ such that

$$He^\top = s \quad \text{and} \quad \text{wt}_H(e) = t$$

NP-hard

$$x, y \in \mathbb{F}_q^n$$

$$x$$

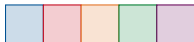

- rank weight $\text{wt}_R(x) = \dim_{\mathbb{F}_q}(\langle x_1, \dots, x_n \rangle_{\mathbb{F}_q})$

$$x, y \in \mathbb{F}_q^{n \times m}$$

Γ ordered basis of $\mathbb{F}_q^m / \mathbb{F}_q$

$$\Gamma(x) \in \mathbb{F}_q^{m \times n}$$

x



expand



$\Gamma(x)$



◦ rank weight $\text{wt}_R(x) = \dim_{\mathbb{F}_q}(\langle x_1, \dots, x_n \rangle_{\mathbb{F}_q})$

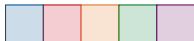
◦ rank weight $\text{wt}_R(x) = \text{rk}(\Gamma(x))$

$$x, y \in \mathbb{F}_q^n$$

Γ ordered basis of $\mathbb{F}_q^m / \mathbb{F}_q$

$$\Gamma(x) \in \mathbb{F}_q^{m \times n}$$

x



expand



$\Gamma(x)$



- rank weight $\text{wt}_R(x) = \dim_{\mathbb{F}_q}(\langle x_1, \dots, x_n \rangle_{\mathbb{F}_q})$
- rank distance $d_R(x, y) = \text{wt}_R(x - y)$
- rank support $\text{supp}_R(x) = \langle x_1, \dots, x_n \rangle_{\mathbb{F}_q} \subseteq \mathbb{F}_q^m$
- min. distance $d_R(\mathcal{C}) = \min\{\text{wt}_R(c) \mid c \in \mathcal{C}, c \neq 0\}$

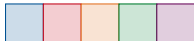
- rank weight $\text{wt}_R(x) = \text{rk}(\Gamma(x))$

$$x, y \in \mathbb{F}_q^n$$

Γ ordered basis of $\mathbb{F}_q^m / \mathbb{F}_q$

$$\Gamma(x) \in \mathbb{F}_q^{m \times n}$$

x



expand



$\Gamma(x)$



- rank weight $\text{wt}_R(x) = \dim_{\mathbb{F}_q}(\langle x_1, \dots, x_n \rangle_{\mathbb{F}_q})$
- rank distance $d_R(x, y) = \text{wt}_R(x - y)$
- rank support $\text{supp}_R(x) = \langle x_1, \dots, x_n \rangle_{\mathbb{F}_q} \subseteq \mathbb{F}_q^m$
- min. distance $d_R(\mathcal{C}) = \min\{\text{wt}_R(c) \mid c \in \mathcal{C}, c \neq 0\}$

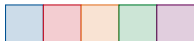
- rank weight $\text{wt}_R(x) = \text{rk}(\Gamma(x))$
- rank distance $d_R(x, y) = \text{rk}(\Gamma(x) - \Gamma(y))$
- rank support next slide

$$x, y \in \mathbb{F}_{q^m}^n$$

Γ ordered basis of $\mathbb{F}_{q^m} / \mathbb{F}_q$

$$\Gamma(x) \in \mathbb{F}_q^{m \times n}$$

x



expand



$\Gamma(x)$



- rank weight $\text{wt}_R(x) = \dim_{\mathbb{F}_q}(\langle x_1, \dots, x_n \rangle_{\mathbb{F}_q})$
- rank distance $d_R(x, y) = \text{wt}_R(x - y)$
- rank support $\text{supp}_R(x) = \langle x_1, \dots, x_n \rangle_{\mathbb{F}_q} \subseteq \mathbb{F}_{q^m}$
- min. distance $d_R(\mathcal{C}) = \min\{\text{wt}_R(c) \mid c \in \mathcal{C}, c \neq 0\}$

- rank weight $\text{wt}_R(x) = \text{rk}(\Gamma(x))$
- rank distance $d_R(x, y) = \text{rk}(\Gamma(x) - \Gamma(y))$
- rank support next slide

Example: $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$ with $\alpha^3 = \alpha + 1$

$$\Gamma = (1, \alpha, \alpha^2)$$

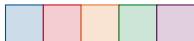
$$x = (\alpha, \alpha + 1, 0, 1, \alpha)$$

$$x, y \in \mathbb{F}_q^m$$

Γ ordered basis of $\mathbb{F}_q^m / \mathbb{F}_q$

$$\Gamma(x) \in \mathbb{F}_q^{m \times n}$$

x



expand



$\Gamma(x)$



- rank weight $\text{wt}_R(x) = \dim_{\mathbb{F}_q}(\langle x_1, \dots, x_n \rangle_{\mathbb{F}_q})$
- rank distance $d_R(x, y) = \text{wt}_R(x - y)$
- rank support $\text{supp}_R(x) = \langle x_1, \dots, x_n \rangle_{\mathbb{F}_q} \subseteq \mathbb{F}_q^m$
- min. distance $d_R(\mathcal{C}) = \min\{\text{wt}_R(c) \mid c \in \mathcal{C}, c \neq 0\}$

- rank weight $\text{wt}_R(x) = \text{rk}(\Gamma(x))$
- rank distance $d_R(x, y) = \text{rk}(\Gamma(x) - \Gamma(y))$
- rank support next slide

Example: $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$ with $\alpha^3 = \alpha + 1$

$$x = (\alpha, \alpha + 1, 0, 1, \alpha)$$

$$\text{wt}_R(x) = 2$$

$$\text{supp}_R(x) = \langle 1, \alpha \rangle_{\mathbb{F}_2} = \{0, 1, \alpha, \alpha + 1\}$$

$$\Gamma = (1, \alpha, \alpha^2)$$

$$\Gamma(x) = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\text{rk} = 2$$

More Supports!

- $x \in \mathbb{F}_q^n$ with $\text{wt}_R(x) = t \quad \rightarrow \quad \exists a \in \mathbb{F}_q^m$ with $\text{wt}_R(a) = t$ and $R \in \mathbb{F}_q^{t \times n}$ with $\text{rk}(R) = t$ s.t.

$$\boxed{x} = \boxed{a} \boxed{R}$$

Column support

$$\text{supp}_{\text{col}}(x) = \text{colsp}_{\mathbb{F}_q}(\Gamma(a)) = \text{colsp}_{\mathbb{F}_q}(\Gamma(x)) \subseteq \mathbb{F}_q^m$$

Row support

$$\text{supp}_{\text{row}}(x) = \text{rowsp}_{\mathbb{F}_q}(R) = \text{rowsp}_{\mathbb{F}_q}(\Gamma(x)) \subseteq \mathbb{F}_q^n$$

- $x \in \mathbb{F}_q^m$ with $\text{wt}_R(x) = t \quad \rightarrow \quad \exists a \in \mathbb{F}_q^t$ with $\text{wt}_R(a) = t$ and $R \in \mathbb{F}_q^{t \times n}$ with $\text{rk}(R) = t$ s.t.

$$\boxed{x} = \boxed{a} \quad \boxed{R}$$

Column support

$$\text{supp}_{\text{col}}(x) = \text{colsp}_{\mathbb{F}_q}(\Gamma(a)) = \text{colsp}_{\mathbb{F}_q}(\Gamma(x)) \subseteq \mathbb{F}_q^m$$

Row support

$$\text{supp}_{\text{row}}(x) = \text{rowsp}_{\mathbb{F}_q}(R) = \text{rowsp}_{\mathbb{F}_q}(\Gamma(x)) \subseteq \mathbb{F}_q^n$$

Example: $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$, $\alpha^3 = \alpha + 1$, $\Gamma = (1, \alpha, \alpha^2)$

$$x = (\alpha, \alpha + 1, 0, 1, \alpha) = (1, \alpha) \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$$\text{supp}_{\text{col}}(x) = \langle (1, 0, 0), (0, 1, 0) \rangle_{\mathbb{F}_2}$$

$$\text{supp}_{\text{row}}(x) = \langle (0, 1, 0, 1, 0), (1, 1, 0, 0, 1) \rangle_{\mathbb{F}_2}$$

Hamming metric

- $\text{supp}_H(x) \subseteq [n]$ subset
- $\text{wt}_H(x) = |\text{supp}_H(x)|$ size
- t -element subsets: $\binom{n}{t}$ binomial

$$x = \begin{array}{|c|c|c|c|c|c|} \hline \text{ } & \text{ } & 0 & \text{ } & 0 & 0 \\ \hline \end{array}$$

$\text{supp}_H(x)$

Rank metric

- $\text{supp}_{\text{row}}(x) \subseteq \mathbb{F}_q^n$ subspace
- $\text{wt}_R(x) = \dim_{\mathbb{F}_q}(\text{supp}_{\text{row}}(x))$ dimension
- t -dimensional subspaces: $\begin{bmatrix} n \\ t \end{bmatrix}_q$ Gaussian

$$\mathcal{X} = \text{supp}_{\text{row}}(x) \subseteq \mathbb{F}_q^n$$

q -analogs

Hamming metric



Rank metric

- $\text{supp}_H(x) \subseteq [n]$ subset
- $\text{wt}_H(x) = |\text{supp}_H(x)|$ size
- t -element subsets: $\binom{n}{t}$ binomial

$$x = \begin{array}{|c|c|c|c|c|c|} \hline & & 0 & & 0 & 0 \\ \hline \end{array}$$

$\text{supp}_H(x)$

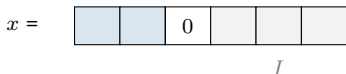
- $\text{supp}_{\text{row}}(x) \subseteq \mathbb{F}_q^n$ subspace
- $\text{wt}_R(x) = \dim_{\mathbb{F}_q}(\text{supp}_{\text{row}}(x))$ dimension
- t -dimensional subspaces: $\begin{bmatrix} n \\ t \end{bmatrix}_q$ Gaussian

$$\mathcal{X} = \text{supp}_{\text{row}}(x) \subseteq \mathbb{F}_q^n$$

q -analogs

Hamming metric

- $\text{supp}_H(x) \subseteq [n]$ subset
- $\text{wt}_H(x) = |\text{supp}_H(x)|$ size
- t -element subsets: $\binom{n}{t}$ binomial



- Puncturing:

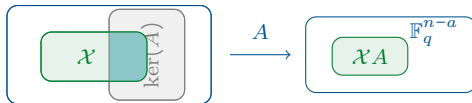
Choose $I \subseteq [n]$, $|I| = a$

$$\pi_I(\mathcal{C}) = \{(c_j)_{j \notin I} \mid c \in \mathcal{C}\} \subseteq \mathbb{F}_q^{n-a}$$

read: delete a coordinates

Rank metric

- $\text{supp}_{\text{row}}(x) \subseteq \mathbb{F}_q^n$ subspace
- $\text{wt}_R(x) = \dim_{\mathbb{F}_q}(\text{supp}_{\text{row}}(x))$ dimension
- t -dimensional subspaces: $\begin{bmatrix} n \\ t \end{bmatrix}_q$ Gaussian



- Puncturing:

Choose $A \in \mathbb{F}_q^{n \times (n-a)}$, $\text{rk}(A) = n - a$

$$\mathcal{C}A = \{xA \mid x \in \mathcal{C}\} = \langle GA \rangle \subseteq \mathbb{F}_q^{n-a}$$

read: quotient by $\ker(A)$

vector codes

- $\mathcal{C} \subseteq \mathbb{F}_q^n$, $\dim_{\mathbb{F}_q}(\mathcal{C}) = k$
- generated by $g_1, \dots, g_k \in \mathbb{F}_q^n$
- $c = \sum_{i=1}^k m_i g_i$, $m_i \in \mathbb{F}_q$

vector codes

$$\Gamma = (\gamma_1, \dots, \gamma_m)$$

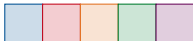


matrix codes

- $\mathcal{C} \subseteq \mathbb{F}_q^n$, $\dim_{\mathbb{F}_q}(\mathcal{C}) = k$ $|\Gamma(\mathcal{C})| = |\mathcal{C}| = q^{mk}$
- generated by $g_1, \dots, g_k \in \mathbb{F}_q^m$
- $c = \sum_{i=1}^k m_i g_i$, $m_i \in \mathbb{F}_q$

- $\Gamma(\mathcal{C}) \subseteq \mathbb{F}_q^{m \times n}$, $\dim_{\mathbb{F}_q}(\Gamma(\mathcal{C})) = km$
- generated by $G_{i,j} = \Gamma(\gamma_j g_i)$ $1 \leq i \leq k$, $1 \leq j \leq m$
- $C = \sum_{i=1}^k \sum_{j=1}^m \lambda_{i,j} G_{i,j}$, $\lambda_{i,j} \in \mathbb{F}_q$

c



$\Gamma(c)$



vector codes $\xrightarrow{\Gamma = (\gamma_1, \dots, \gamma_m)}$

- $\mathcal{C} \subseteq \mathbb{F}_q^n$, $\dim_{\mathbb{F}_q}(\mathcal{C}) = k$ $|\Gamma(\mathcal{C})| = |\mathcal{C}| = q^{mk}$
- generated by $g_1, \dots, g_k \in \mathbb{F}_q^n$
- $c = \sum_{i=1}^k m_i g_i$, $m_i \in \mathbb{F}_q$

matrix codes

- $\Gamma(\mathcal{C}) \subseteq \mathbb{F}_q^{m \times n}$, $\dim_{\mathbb{F}_q}(\Gamma(\mathcal{C})) = km$
- generated by $G_{i,j} = \Gamma(\gamma_j g_i)$ $1 \leq i \leq k$, $1 \leq j \leq m$
- $C = \sum_{i=1}^k \sum_{j=1}^m \lambda_{i,j} G_{i,j}$, $\lambda_{i,j} \in \mathbb{F}_q$

Example: $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, $\alpha^2 = \alpha + 1$, $\Gamma = (1, \alpha)$

$$\mathcal{C} = \langle (1, 0, \alpha), (0, 1, \alpha) \rangle_{\mathbb{F}_4}$$

$$\Gamma(1, 0, \alpha) \quad \Gamma(\alpha(1, 0, \alpha)) \quad \Gamma(0, 1, \alpha) \quad \Gamma(\alpha(0, 1, \alpha))$$

$$\Gamma(\mathcal{C}) = \left\langle \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \right\rangle_{\mathbb{F}_2}$$

vector codes $\xrightarrow{\Gamma = (\gamma_1, \dots, \gamma_m)}$

- $\mathcal{C} \subseteq \mathbb{F}_q^n$, $\dim_{\mathbb{F}_q}(\mathcal{C}) = k$ $|\Gamma(\mathcal{C})| = |\mathcal{C}| = q^{mk}$
- generated by $g_1, \dots, g_k \in \mathbb{F}_q^n$
- $c = \sum_{i=1}^k m_i g_i$, $m_i \in \mathbb{F}_q$

matrix codes

- $\Gamma(\mathcal{C}) \subseteq \mathbb{F}_q^{m \times n}$, $\dim_{\mathbb{F}_q}(\Gamma(\mathcal{C})) = km$
- generated by $G_{i,j} = \Gamma(\gamma_j g_i)$ $1 \leq i \leq k$, $1 \leq j \leq m$
- $C = \sum_{i=1}^k \sum_{j=1}^m \lambda_{i,j} G_{i,j}$, $\lambda_{i,j} \in \mathbb{F}_q$

Example: $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, $\alpha^2 = \alpha + 1$, $\Gamma = (1, \alpha)$

$$\mathcal{C} = \langle (1, 0, \alpha), (0, 1, \alpha) \rangle_{\mathbb{F}_4}$$

$$\Gamma(1, 0, \alpha) \quad \Gamma(\alpha(1, 0, \alpha)) \quad \Gamma(0, 1, \alpha) \quad \Gamma(\alpha(0, 1, \alpha))$$

$$\Gamma(\mathcal{C}) = \left\langle \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \right\rangle_{\mathbb{F}_2}$$

$\mathbb{F}_q$ -linear

$\mathbb{F}_q^m$ -linear

$\mathbb{F}_q^m$ -linear



$\mathbb{F}_q$ -linear

Rank Decoding Problem (RDP)

Given $G \in \mathbb{F}_{q^m}^{k \times n}$, $r \in \mathbb{F}_{q^m}^n$, and t

find $e \in \mathbb{F}_{q^m}^n$ such that

$$r - e \in \langle G \rangle, \quad \text{wt}_R(e) = t$$

Rank Decoding Problem (RDP) $\xrightarrow{\text{expand via } \Gamma}$ $\mathbb{F}_q^m$ -linear MinRank

Given $G \in \mathbb{F}_{q^m}^{k \times n}$, $r \in \mathbb{F}_{q^m}^n$, and t

find $e \in \mathbb{F}_{q^m}^n$ such that

$$r - e \in \langle G \rangle, \quad \text{wt}_R(e) = t$$

Given $G_1, \dots, G_K, R \in \mathbb{F}_q^{m \times n}$ and t

find $E \in \mathbb{F}_q^{m \times n}$ such that

$$R - E \in \langle G_1, \dots, G_K \rangle, \quad \text{rk}(E) = t$$

Rank Decoding Problem (RDP) $\xrightarrow{\text{expand via } \Gamma}$ $\mathbb{F}_{q^m}$ -linear MinRank

Given $G \in \mathbb{F}_{q^m}^{k \times n}$, $r \in \mathbb{F}_{q^m}^n$, and t
find $e \in \mathbb{F}_{q^m}^n$ such that

$$r - e \in \langle G \rangle, \quad \text{wt}_R(e) = t$$

Given $G_1, \dots, G_K, R \in \mathbb{F}_q^{m \times n}$ and t
find $E \in \mathbb{F}_q^{m \times n}$ such that

$$R - E \in \langle G_1, \dots, G_K \rangle, \quad \text{rk}(E) = t$$

$\mathbb{F}_{q^m}$ -linear RDP $\longrightarrow$ $\mathbb{F}_{q^m}$ -linear MinRank $\subseteq$ $\mathbb{F}_q$ -linear MinRank

Rank Decoding Problem (RDP) $\xrightarrow{\text{expand via } \Gamma}$ $\mathbb{F}_q^m$ -linear MinRank

Given $G \in \mathbb{F}_q^{k \times n}$, $r \in \mathbb{F}_q^n$, and t
find $e \in \mathbb{F}_q^n$ such that

$$r - e \in \langle G \rangle, \quad \text{wt}_R(e) = t$$

Given $G_1, \dots, G_K, R \in \mathbb{F}_q^{m \times n}$ and t
find $E \in \mathbb{F}_q^{m \times n}$ such that

$$R - E \in \langle G_1, \dots, G_K \rangle, \quad \text{rk}(E) = t$$

$\mathbb{F}_q^m$ -linear RDP $\longrightarrow$ $\mathbb{F}_q^m$ -linear MinRank $\subseteq$ $\mathbb{F}_q$ -linear MinRank

NP-hard

Open problem: Is rank decoding NP-hard?

e.g. Hamming DP $\rightarrow$ rank DP

Why Might Rank Decoding be Hard?

Randomized reduction idea

$$x \in \mathbb{F}_q^m \text{ with } \text{wt}_R(x) = n$$



$$e \in \mathbb{F}_q^n \text{ with } \text{wt}_H(e) = t, n \leq m$$

$$x_1, \dots, x_n \text{ are } \mathbb{F}_q\text{-independent}$$

$$\begin{array}{ccc}
 e = \begin{array}{|c|c|c|c|c|c|} \hline 0 & & & 0 & & 0 \\ \hline \end{array} & \xrightarrow{\varphi_x : e \mapsto e * x} & e * x = \begin{array}{|c|c|c|c|c|c|} \hline 0 & e_2x_2 & e_3x_3 & 0 & e_5x_5 & 0 \\ \hline \end{array} \in \mathbb{F}_q^m \\
 \text{wt}_H(e) = t & & \text{wt}_R(e * x) = t
 \end{array}$$

Example

$$\mathbb{F}_8 = \mathbb{F}_2(\alpha) \text{ with } \alpha^3 = \alpha + 1 \quad x = (1, \alpha, \alpha^2)$$

$$e = (0, 1, 1) \quad \text{wt}_H(e) = 2 \quad \longrightarrow \quad e * x = (0, \alpha, \alpha^2) \quad \text{wt}_R(e * x) = 2$$

Why Might Rank Decoding be Hard?

Randomized reduction idea

$$x \in \mathbb{F}_q^{n \times m} \text{ with } \text{wt}_R(x) = n$$

 $\iff$

$$e \in \mathbb{F}_q^n \text{ with } \text{wt}_H(e) = t, n \leq m$$

$$x_1, \dots, x_n \text{ are } \mathbb{F}_q\text{-independent}$$

$$\begin{array}{ccc}
 e = \begin{array}{|c|c|c|c|c|c|} \hline 0 & & & 0 & & 0 \\ \hline \end{array} & \xrightarrow{\varphi_x : e \mapsto e * x} & e * x = \begin{array}{|c|c|c|c|c|c|} \hline 0 & e_2x_2 & e_3x_3 & 0 & e_5x_5 & 0 \\ \hline \end{array} \in \mathbb{F}_q^{n \times m} \\
 \text{wt}_H(e) = t & & \text{wt}_R(e * x) = t
 \end{array}$$

Transform the code

$$\mathcal{C} \subseteq \mathbb{F}_q^n \longrightarrow \tilde{\mathcal{C}} = \langle \{c * x \mid c \in \mathcal{C}\} \rangle_{\mathbb{F}_q^m} \subseteq \mathbb{F}_q^{n \times m}$$

$$r = c + e \longrightarrow r * x = c * x + e * x$$

Why Might Rank Decoding be Hard?

Randomized reduction idea

$$x \in \mathbb{F}_q^{n \times m} \text{ with } \text{wt}_R(x) = n$$

 $\iff$

$$e \in \mathbb{F}_q^n \text{ with } \text{wt}_H(e) = t, n \leq m$$

$$x_1, \dots, x_n \text{ are } \mathbb{F}_q\text{-independent}$$

$$\begin{array}{ccc}
 e = \begin{array}{|c|c|c|c|c|c|} \hline 0 & & & 0 & & 0 \\ \hline \end{array} & \xrightarrow{\varphi_x : e \mapsto e * x} & e * x = \begin{array}{|c|c|c|c|c|c|} \hline 0 & e_2 x_2 & e_3 x_3 & 0 & e_5 x_5 & 0 \\ \hline \end{array} \in \mathbb{F}_q^{n \times m} \\
 \text{wt}_H(e) = t & & \text{wt}_R(e * x) = t
 \end{array}$$

Transform the code

$$\mathcal{C} \subseteq \mathbb{F}_q^n \longrightarrow \tilde{\mathcal{C}} = \langle \{c * x \mid c \in \mathcal{C}\} \rangle_{\mathbb{F}_q^m} \subseteq \mathbb{F}_q^{n \times m}$$

$$r = c + e \longrightarrow r * x = c * x + e * x$$

Problem: $\tilde{\mathcal{C}}$ may contain additional rank-weight- t solutions $e' \neq e * x$

$\rightarrow$ succeeds only with high probability

Why Is Rank Decoding More Expensive?

Hamming metric brute force

Guess the support of e

$\text{supp}_H(e) \subseteq [n]$ with $|\cdot| = t$

$\binom{n}{t}$ possibilities

$$e = \begin{array}{|c|c|c|c|c|c|} \hline & & 0 & & 0 & 0 \\ \hline \end{array}$$

$\text{supp}_H(e)$

Why Is Rank Decoding More Expensive?

Hamming metric brute force

Guess the support of e

$$\text{supp}_H(e) \subseteq [n] \text{ with } |\cdot| = t$$

$\binom{n}{t}$ possibilities

$$e = \begin{array}{|c|c|c|c|c|c|} \hline \square & \square & 0 & \square & 0 & 0 \\ \hline \end{array}$$

$\text{supp}_H(e)$

Rank metric brute force

Guess the support of e

$$\mathcal{E} = \text{supp}_{\text{row}}(e) \subseteq \mathbb{F}_q^n \text{ with } \dim(\cdot) = t$$

$\begin{bmatrix} n \\ t \end{bmatrix}_q$ possibilities

$$\mathcal{E} = \text{supp}_{\text{row}}(e) \subseteq \mathbb{F}_q^n$$

Why Is Rank Decoding More Expensive?

Hamming metric brute force

Guess the support of e

$$\text{supp}_H(e) \subseteq [n] \text{ with } |\cdot| = t$$

$$\binom{n}{t} \text{ possibilities} \ll$$

$$e = \begin{array}{|c|c|c|c|c|c|} \hline \square & \square & 0 & \square & 0 & 0 \\ \hline \end{array}$$

$\text{supp}_H(e)$

Rank metric brute force

Guess the support of e

$$\mathcal{E} = \text{supp}_{\text{row}}(e) \subseteq \mathbb{F}_q^n \text{ with } \dim(\cdot) = t$$

$$\begin{bmatrix} n \\ t \end{bmatrix}_q \text{ possibilities} \sim q^{t(n-t)}$$

$$\mathcal{E} = \text{supp}_{\text{row}}(e) \subseteq \mathbb{F}_q^n$$

Why Is Rank Decoding More Expensive?

Hamming metric brute force

Guess the support of e

$$\text{supp}_H(e) \subseteq [n] \text{ with } |\cdot| = t$$

$$\binom{n}{t} \text{ possibilities} \ll$$

$$e = \begin{array}{|c|c|c|c|c|c|} \hline \text{ } & \text{ } & 0 & \text{ } & 0 & 0 \\ \hline \end{array}$$

$\text{supp}_H(e)$

Rank metric brute force

Guess the support of e

$$\mathcal{E} = \text{supp}_{\text{row}}(e) \subseteq \mathbb{F}_q^n \text{ with } \dim(\cdot) = t$$

$$\begin{bmatrix} n \\ t \end{bmatrix}_q \text{ possibilities} \sim q^{t(n-t)}$$

$$\mathbb{F}_q^n$$

$\mathcal{E} = \text{supp}_{\text{row}}(e)$

Can we do better than brute force?

Prange

Guess $J \subseteq [n]$ with $|J| = n - k$

$\text{supp}_H(e) \subseteq J$

$$e = \begin{array}{|c|c|c|c|} \hline & & 0 & \\ \hline \end{array} \quad \begin{array}{|c|c|} \hline 0 & 0 \\ \hline \end{array}$$

$J \qquad J^c$

Prange

Guess $J \subseteq [n]$ with $|J| = n - k$

$\text{supp}_H(e) \subseteq J$

$$e = \begin{array}{|c|c|c|c|} \hline \text{ } & \text{ } & 0 & \text{ } \\ \hline \end{array} \quad \begin{array}{|c|c|} \hline 0 & 0 \\ \hline \end{array}$$

$J \qquad J^c$

Then only linear algebra remains

$$He^T = \begin{bmatrix} I_{n-k} & A \end{bmatrix} \begin{pmatrix} e_J \\ 0 \end{pmatrix} = s^T \Rightarrow e_J = s$$

check whether $\text{wt}_H(s) = t$

Rank Analog of Prange

Prange

Guess $J \subseteq [n]$ with $|J| = n - k$

$\text{supp}_H(e) \subseteq J$

$$e = \begin{array}{|c|c|c|c|} \hline \text{ } & \text{ } & 0 & \text{ } \\ \hline \end{array} \quad \begin{array}{|c|c|} \hline 0 & 0 \\ \hline \end{array}$$

$J \qquad J^c$

Then only linear algebra remains

$$He^T = \begin{bmatrix} I_{n-k} & A \end{bmatrix} \begin{pmatrix} e_J \\ 0 \end{pmatrix} = s^T \Rightarrow e_J = s$$

check whether $\text{wt}_H(s) = t$

rank-metric Prange (GRS)

Guess $\mathcal{S} = \langle S \rangle \subseteq \mathbb{F}_q^n$ with $\dim(\mathcal{S}) = n - k$

$\text{supp}_{\text{row}}(e) \subseteq \mathcal{S}$

$$\boxed{\mathcal{E} = \text{supp}_{\text{row}}(e)} \quad \mathcal{S}$$

Rank Analog of Prange

Prange

Guess $J \subseteq [n]$ with $|J| = n - k$

$\text{supp}_H(e) \subseteq J$

$$e = \begin{array}{|c|c|c|c|} \hline \text{ } & \text{ } & 0 & \text{ } \\ \hline \end{array} \quad \begin{array}{|c|c|} \hline 0 & 0 \\ \hline \end{array}$$

$J \qquad J^c$

Then only linear algebra remains

$$He^\top = \begin{bmatrix} I_{n-k} & A \end{bmatrix} \begin{pmatrix} e_J \\ 0 \end{pmatrix} = s^\top \Rightarrow e_J = s$$

check whether $\text{wt}_H(s) = t$

rank-metric Prange (GRS)

Guess $\mathcal{S} = \langle S \rangle \subseteq \mathbb{F}_q^n$ with $\dim(\mathcal{S}) = n - k$

$\text{supp}_{\text{row}}(e) \subseteq \mathcal{S}$

$$\mathcal{S} \supseteq \mathcal{E} = \text{supp}_{\text{row}}(e)$$

Then only linear algebra remains

$$e = xS, \quad x \in \mathbb{F}_q^{n-k} \text{ with } HS^\top x^\top = s^\top$$

$m(n - k)$ equations in $m(n - k)$ $\mathbb{F}_q$ -variables

Rank Analog of Prange

Prange

Guess $J \subseteq [n]$ with $|J| = n - k$

$\text{supp}_H(e) \subseteq J$

$$e = \begin{array}{|c|c|c|c|} \hline \text{ } & \text{ } & 0 & \text{ } \\ \hline \end{array} \quad \begin{array}{|c|c|} \hline 0 & 0 \\ \hline \end{array}$$

$J \qquad J^c$

Then only linear algebra remains

$$He^\top = \begin{bmatrix} I_{n-k} & A \end{bmatrix} \begin{pmatrix} e_J \\ 0 \end{pmatrix} = s^\top \Rightarrow e_J = s$$

check whether $\text{wt}_H(s) = t$

$$\Pr[\text{supp}_H(e) \subseteq J] = \binom{n-t}{n-k-t} \binom{n}{n-k}^{-1}$$

rank-metric Prange (GRS)

Guess $\mathcal{S} = \langle S \rangle \subseteq \mathbb{F}_q^n$ with $\dim(\mathcal{S}) = n - k$

$\text{supp}_{\text{row}}(e) \subseteq \mathcal{S}$

$$\mathcal{S} \supseteq \mathcal{E} = \text{supp}_{\text{row}}(e)$$

Then only linear algebra remains

$$e = xS, \quad x \in \mathbb{F}_q^{n-k} \text{ with } HS^\top x^\top = s^\top$$

$m(n-k)$ equations in $m(n-k)$ $\mathbb{F}_q$ -variables

Rank Analog of Prange

Prange

Guess $J \subseteq [n]$ with $|J| = n - k$

$\text{supp}_H(e) \subseteq J$

$$e = \begin{array}{|c|c|c|c|} \hline & & 0 & \\ \hline \end{array} \quad \begin{array}{|c|c|} \hline 0 & 0 \\ \hline \end{array}$$

$J \qquad J^c$

Then only linear algebra remains

$$He^\top = \begin{bmatrix} I_{n-k} & A \end{bmatrix} \begin{pmatrix} e_J \\ 0 \end{pmatrix} = s^\top \Rightarrow e_J = s$$

check whether $\text{wt}_H(s) = t$

$$\Pr[\text{supp}_H(e) \subseteq J] = \binom{n-t}{n-k-t} \binom{n}{n-k}^{-1}$$

rank-metric Prange (GRS)

Guess $\mathcal{S} = \langle S \rangle \subseteq \mathbb{F}_q^n$ with $\dim(\mathcal{S}) = n - k$

$\text{supp}_{\text{row}}(e) \subseteq \mathcal{S}$

$$\mathcal{E} = \text{supp}_{\text{row}}(e) \subseteq \mathcal{S}$$

Then only linear algebra remains

$$e = xS, \quad x \in \mathbb{F}_q^{n-k} \text{ with } HS^\top x^\top = s^\top$$

$m(n-k)$ equations in $m(n-k)$ $\mathbb{F}_q$ -variables

$$\Pr[\mathcal{E} \subseteq \mathcal{S}] = \left[\begin{matrix} n-t \\ n-k-t \end{matrix} \right]_q \left[\begin{matrix} n \\ n-k \end{matrix} \right]_q^{-1}$$

Rank Analog of Prange

Prange

Guess $J \subseteq [n]$ with $|J| = n - k$

$\text{supp}_H(e) \subseteq J$

$$e = \begin{array}{|c|c|c|c|} \hline & & 0 & \\ \hline \end{array} \quad \begin{array}{|c|c|} \hline 0 & 0 \\ \hline \end{array}$$

$J \qquad J^c$

Then only linear algebra remains

$$He^\top = \begin{bmatrix} I_{n-k} & A \end{bmatrix} \begin{pmatrix} e_J \\ 0 \end{pmatrix} = s^\top \Rightarrow e_J = s$$

check whether $\text{wt}_H(s) = t$

$$\text{cost} = \binom{n}{n-k} \binom{n-t}{n-k-t}^{-1}$$

$\ll$

rank-metric Prange (GRS)

Guess $\mathcal{S} = \langle S \rangle \subseteq \mathbb{F}_q^n$ with $\dim(\mathcal{S}) = n - k$

$\text{supp}_{\text{row}}(e) \subseteq \mathcal{S}$

$$\boxed{\mathcal{E} = \text{supp}_{\text{row}}(e)} \quad \mathcal{S}$$

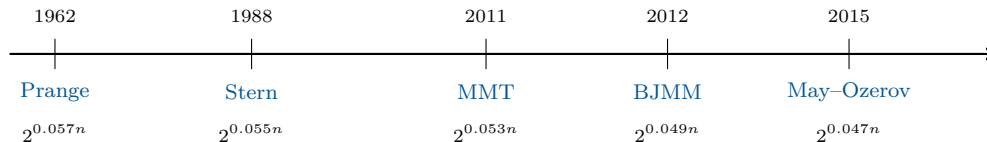
Then only linear algebra remains

$$e = xS, \quad x \in \mathbb{F}_q^{n-k} \text{ with } HS^\top x^\top = s^\top$$

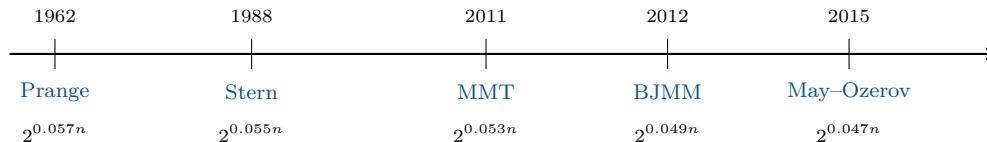
$m(n-k)$ equations in $m(n-k)$ $\mathbb{F}_q$ -variables

$$\text{cost} = \begin{bmatrix} n \\ n-k \end{bmatrix}_q \begin{bmatrix} n-t \\ n-k-t \end{bmatrix}_q^{-1} \sim q^{kt}$$

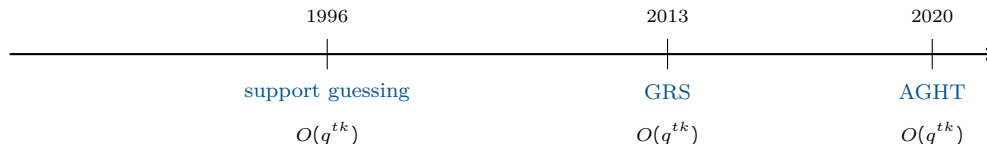
Hamming metric



Hamming metric



Rank metric



→ No improvements

Why Does Hamming ISD Improve?

Support Splitting

$$e \in \mathbb{F}_q^n \text{ with } \text{wt}_H(e) = t$$

$$e = \begin{array}{|c|c|c|c|c|c|c|c|} \hline 0 & & & 0 & & 0 & & 0 \\ \hline \end{array}$$

$$\text{wt}_H(e) = t$$

Why Does Hamming ISD Improve?

Support Splitting

$$e \in \mathbb{F}_q^n \text{ with } \text{wt}_H(e) = t$$

$$e = \begin{array}{|c|c|c|c|c|c|c|c|} \hline 0 & & & 0 & & 0 & & 0 \\ \hline \end{array}$$

$$\text{wt}_H(e) = t$$

Split the coordinate set $[n] = X \sqcup Y$

$$e = \begin{array}{|c|c|c|c|} \hline 0 & & & 0 \\ \hline \end{array} \quad \begin{array}{|c|c|c|c|} \hline & 0 & & 0 \\ \hline \end{array}$$

$X \qquad Y$

Why Does Hamming ISD Improve?

Support Splitting

$$e \in \mathbb{F}_q^n \text{ with } \text{wt}_H(e) = t$$

$$e = \begin{array}{|c|c|c|c|c|c|c|c|} \hline 0 & & & 0 & & 0 & & 0 \\ \hline \end{array}$$

$$\text{wt}_H(e) = t$$

Split the coordinate set $[n] = X \sqcup Y$

$$e = \begin{array}{|c|c|c|c|} \hline 0 & & & 0 \\ \hline \end{array} \quad \begin{array}{|c|c|c|c|} \hline & 0 & & 0 \\ \hline \end{array}$$

$X \qquad Y$

$$\text{supp}_H(e) = (\text{supp}_H(e) \cap X) \sqcup (\text{supp}_H(e) \cap Y)$$

$$t = \text{wt}_H(e_X) + \text{wt}_H(e_Y)$$

Why Does Hamming ISD Improve?

Support Splitting

$$e \in \mathbb{F}_q^n \text{ with } \text{wt}_H(e) = t$$

$$e = \begin{array}{|c|c|c|c|c|c|c|c|} \hline 0 & & & 0 & & 0 & & 0 \\ \hline \end{array}$$

$$\text{wt}_H(e) = t$$

Split the coordinate set $[n] = X \sqcup Y$

$$\text{supp}_H(e) = (\text{supp}_H(e) \cap X) \sqcup (\text{supp}_H(e) \cap Y)$$

$$e = \begin{array}{|c|c|c|c|} \hline 0 & & & 0 \\ \hline \end{array} \quad \begin{array}{|c|c|c|c|} \hline & 0 & & 0 \\ \hline \end{array}$$

$X \qquad Y$

$$t = \text{wt}_H(e_X) + \text{wt}_H(e_Y)$$

If we guess $\text{wt}_H(e_Y) = b$

then we solve a smaller instance with $\text{wt}_H(e_X) = t - b$

$$(q, n, t) \longrightarrow (q, n - |Y|, t - b)$$

Can We Split Rank Support?

Support splitting

$e \in \mathbb{F}_q^{n_m}$ with $\text{wt}_R(e) = t$ and $\mathcal{E} = \text{supp}_{\text{row}}(e) \subseteq \mathbb{F}_q^n$

Recall Hamming metric:

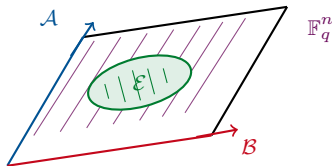
$$\text{supp}_H(e) \subseteq [n] = X \sqcup Y$$

Can We Split Rank Support?

Support splitting

$e \in \mathbb{F}_q^{n_m}$ with $\text{wt}_R(e) = t$ and $\mathcal{E} = \text{supp}_{\text{row}}(e) \subseteq \mathbb{F}_q^n$

split the ambient support space $\mathbb{F}_q^n = \mathcal{A} \oplus \mathcal{B}$



Recall Hamming metric:

$$\text{supp}_H(e) \subseteq [n] = X \sqcup Y$$

$\mathcal{E} \cap \mathcal{A}$ and $\mathcal{E} \cap \mathcal{B}$ may both be small

$$\dim(\mathcal{E}) \neq \dim(\mathcal{E} \cap A) + \dim(\mathcal{E} \cap B)$$

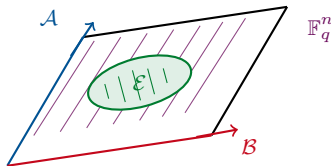
$$|\text{supp}_H(e)| = |\text{supp}_H(e) \cap X| + |\text{supp}_H(e) \cap Y|$$

Can We Split Rank Support?

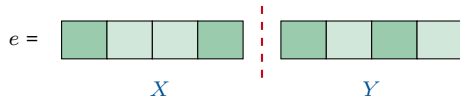
Support splitting

$e \in \mathbb{F}_q^{n \times m}$ with $\text{wt}_R(e) = t$ and $\mathcal{E} = \text{supp}_{\text{row}}(e) \subseteq \mathbb{F}_q^n$

split the ambient support space $\mathbb{F}_q^n = \mathcal{A} \oplus \mathcal{B}$



Projection on coordinates



Recall Hamming metric:

$$\text{supp}_H(e) \subseteq [n] = X \sqcup Y$$

$\mathcal{E} \cap \mathcal{A}$ and $\mathcal{E} \cap \mathcal{B}$ may both be small

$$\dim(\mathcal{E}) \neq \dim(\mathcal{E} \cap \mathcal{A}) + \dim(\mathcal{E} \cap \mathcal{B})$$

$$|\text{supp}_H(e)| = |\text{supp}_H(e) \cap X| + |\text{supp}_H(e) \cap Y|$$

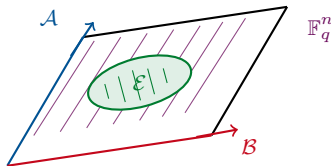
$\text{wt}_R(e_X) = t$ w.h.p. $\rightarrow$ cost still $O(q^{kt})$

Can We Split Rank Support?

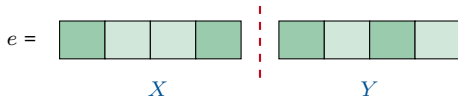
Support splitting

$e \in \mathbb{F}_q^{n \times m}$ with $\text{wt}_R(e) = t$ and $\mathcal{E} = \text{supp}_{\text{row}}(e) \subseteq \mathbb{F}_q^n$

split the ambient support space $\mathbb{F}_q^n = \mathcal{A} \oplus \mathcal{B}$



Projection on coordinates



Recall Hamming metric:

$$\text{supp}_H(e) \subseteq [n] = X \sqcup Y$$

$\mathcal{E} \cap \mathcal{A}$ and $\mathcal{E} \cap \mathcal{B}$ may both be small

$$\dim(\mathcal{E}) \neq \dim(\mathcal{E} \cap \mathcal{A}) + \dim(\mathcal{E} \cap \mathcal{B})$$

$$|\text{supp}_H(e)| = |\text{supp}_H(e) \cap X| + |\text{supp}_H(e) \cap Y|$$

$$\text{wt}_R(e_X) = t \text{ w.h.p.} \rightarrow \text{cost still } O(q^{kt})$$

Open problem: How to do support splitting?



M. Bardet et al. “Improvements of Algebraic Attacks for Solving the Rank Decoding and MinRank”, 2020

from DP to codeword finding: add $r = mG + e$ as row $\rightarrow \widetilde{G} = \begin{pmatrix} G \\ r \end{pmatrix}$

$\rightarrow e \in \langle \widetilde{G} \rangle$ and $k' = k + 1$ $\rightarrow$ new equation: $\widetilde{H}(\lambda e)^\top = 0$



M. Bardet et al. “Improvements of Algebraic Attacks for Solving the Rank Decoding and MinRank”, 2020

new equation: $He^{\top} = 0$

Recall $e = aR$ for $\text{wt}_R(a) = t$ $R \in \mathbb{F}_q^{t \times n}$

Decoding equations: $aRH^{\top} = 0$

Since $a \neq 0$

→

$RH^{\top}$ is rank deficient

$$t \left\{ \underbrace{RH^{\top}}_{n-k^l} \right.$$

$$\text{rk}(RH^{\top}) < t$$

→

all $t \times t$ minors vanish



M. Bardet et al. “Improvements of Algebraic Attacks for Solving the Rank Decoding and MinRank”, 2020

new equation: $He^{\top} = 0$

Recall $e = aR$ for $\text{wt}_R(a) = t$ $R \in \mathbb{F}_q^{t \times n}$

Decoding equations: $aRH^{\top} = 0$

Since $a \neq 0$

$\rightarrow$

$RH^{\top}$ is rank deficient

$$t \left\{ \underbrace{\boxed{RH^{\top}}}_{n-k^l} \right.$$

$\text{rk}(RH^{\top}) < t$

$\rightarrow$

all $t \times t$ minors vanish

Cauchy–Binet: $\det((RH^{\top})_{*,J}) = \sum_{|T|=t} \det(R_{*,T}) \det((H^{\top})_{T,J}) = 0$

$J \subseteq [n - k^l]$ cols of $RH^{\top}$
 $T \subseteq [n]$ cols of R /rows of $H^{\top}$



M. Bardet et al. “Improvements of Algebraic Attacks for Solving the Rank Decoding and MinRank”, 2020

new equation: $He^{\top} = 0$

Recall $e = aR$ for $\text{wt}_R(a) = t$ $R \in \mathbb{F}_q^{t \times n}$

Decoding equations: $aRH^{\top} = 0$

Since $a \neq 0$

$\rightarrow$

$RH^{\top}$ is rank deficient

$$t \left\{ \underbrace{\boxed{RH^{\top}}}_{n-k'} \right.$$

$\text{rk}(RH^{\top}) < t$

$\rightarrow$

all $t \times t$ minors vanish

Cauchy–Binet: $\det((RH^{\top})_{*,J}) = \sum_{|T|=t} r_T \det((H^{\top})_{T,J}) = 0$

$J \subseteq [n - k']$ cols of $RH^{\top}$
 $T \subseteq [n]$ cols of R /rows of $H^{\top}$

Variables: $N_{\text{var}} = \binom{n}{t}$

Equations: $N_{\text{eq}} = m \binom{n - k'}{t}$

w.h.p. independent



M. Bardet et al. “Improvements of Algebraic Attacks for Solving the Rank Decoding and MinRank”, 2020

new equation: $He^{\top} = 0$

Recall $e = aR$ for $\text{wt}_R(a) = t$ $R \in \mathbb{F}_q^{t \times n}$

Decoding equations: $aRH^{\top} = 0$

Since $a \neq 0$

$\rightarrow$

$RH^{\top}$ is rank deficient

$$t \left\{ \underbrace{\boxed{RH^{\top}}}_{n-k'} \right.$$

$\text{rk}(RH^{\top}) < t$

$\rightarrow$

all $t \times t$ minors vanish

Cauchy–Binet: $\det((RH^{\top})_{*,J}) = \sum_{|T|=t} r_T \det((H^{\top})_{T,J}) = 0$

$J \subseteq [n - k']$ cols of $RH^{\top}$
 $T \subseteq [n]$ cols of R /rows of $H^{\top}$

Variables: $N_{\text{var}} = \binom{n}{t}$

Equations: $N_{\text{eq}} = m \binom{n - k'}{t}$

w.h.p. independent

Overdetermined: $N_{\text{eq}} \geq N_{\text{var}}$

$\rightarrow$ Cost:

$O(N_{\text{eq}} N_{\text{var}}^{\omega-1})$

ω lin. algebra constant

MaxMinors: $N_{\text{eq}} = m \binom{n - k'}{t}, \quad N_{\text{var}} = \binom{n}{t}$

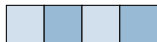
Problem: usually $N_{\text{eq}} < N_{\text{var}}$

MaxMinors: $N_{\text{eq}} = m \binom{n - k'}{t}, \quad N_{\text{var}} = \binom{n}{t}$

Problem: usually $N_{\text{eq}} < N_{\text{var}}$

Hybrid approach: guess that a entries of the error are zero

$e =$



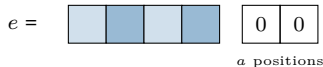
0	0
---	---

a positions

MaxMinors: $N_{\text{eq}} = m \binom{n - k'}{t}, \quad N_{\text{var}} = \binom{n}{t}$

Problem: usually $N_{\text{eq}} < N_{\text{var}}$

Hybrid approach: guess that a entries of the error are zero

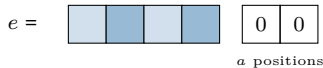


1. Base-field variables a zero columns of $R \rightarrow at$ variables over $\mathbb{F}_q$ fixed to 0 $\Pr \sim q^{-at}$

MaxMinors: $N_{\text{eq}} = m \binom{n - k'}{t}, \quad N_{\text{var}} = \binom{n}{t}$

Problem: usually $N_{\text{eq}} < N_{\text{var}}$

Hybrid approach: guess that a entries of the error are zero



1. Base-field variables a zero columns of $R \rightarrow at$ variables over $\mathbb{F}_q$ fixed to 0 $\Pr \sim q^{-at}$

2. Guess supersupport $\mathcal{A} = \{x \in \mathbb{F}_q^n : x_{i_1} = \dots = x_{i_a} = 0\}$

$$\dim(\mathcal{A}) = n - a$$



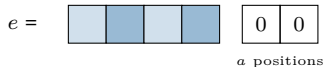
$$\mathcal{E} \subseteq U(\mathcal{A})$$

for some lin. isometry U

MaxMinors: $N_{\text{eq}} = m \binom{n - k'}{t}, \quad N_{\text{var}} = \binom{n}{t}$

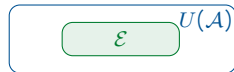
Problem: usually $N_{\text{eq}} < N_{\text{var}}$

Hybrid approach: guess that a entries of the error are zero



1. Base-field variables a zero columns of $R \rightarrow at$ variables over $\mathbb{F}_q$ fixed to 0 $\Pr \sim q^{-at}$

2. Guess supersupport $\mathcal{A} = \{x \in \mathbb{F}_q^n : x_{i_1} = \dots = x_{i_a} = 0\}$
 $\dim(\mathcal{A}) = n - a$



$\mathcal{E} \subseteq U(\mathcal{A})$

for some lin. isometry U

3. Shortening

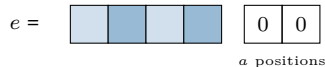
If $\mathcal{E} \subseteq \langle S \rangle = \mathcal{S}$, $\dim(\mathcal{S}) = n - a$, $S \in \mathbb{F}_q^{(n-a) \times n}$

$$eH^\top = s \rightarrow e'H'^\top = s \quad H' = HS^\top, \quad e = e'S, \quad \text{wt}_R(e') = t$$

MaxMinors: $N_{\text{eq}} = m \binom{n - k'}{t}, \quad N_{\text{var}} = \binom{n}{t}$

Problem: usually $N_{\text{eq}} < N_{\text{var}}$

Hybrid approach: guess that a entries of the error are zero



1. Base-field variables a zero columns of $R \rightarrow at$ variables over $\mathbb{F}_q$ fixed to 0 $\Pr \sim q^{-at}$

2. Guess supersupport $\mathcal{A} = \{x \in \mathbb{F}_q^n : x_{i_1} = \dots = x_{i_a} = 0\}$
 $\dim(\mathcal{A}) = n - a$



$\mathcal{E} \subseteq U(\mathcal{A})$

for some lin. isometry U

3. Shortening

If $\mathcal{E} \subseteq \langle S \rangle = \mathcal{S}$, $\dim(\mathcal{S}) = n - a$, $S \in \mathbb{F}_q^{(n-a) \times n}$

$eH^\top = s \rightarrow e'H'^\top = s$

$H' = HS^\top, e = e'S, \text{wt}_R(e') = t$

New instance: $(q, m, n, k, t) \rightarrow (q, m, n - a, k - a, t)$

Condition: $m \binom{n - k}{t} \geq \binom{n - a}{t}$

How Good Is the Hybrid Technique?

Cost: $O\left(m \textcolor{red}{q}^{a_{\min} t} \binom{n - k'}{t} \binom{n - a_{\min}}{t}^{\omega-1}\right)$ ← guessing

Question: How quickly does $a_{\min}$ grow?

How Good Is the Hybrid Technique?

Cost: $O\left(m q^{a_{\min} t} \binom{n - k'}{t} \binom{n - a_{\min}}{t}^{\omega-1}\right)$ ← guessing

Question: How quickly does $a_{\min}$ grow?

◦ If $t(n) = O(\log n)$ cost $O(q^{3t})$ $q^{3t(n) \log_q n + o(t \log n)}$ → smaller than GRS

How Good Is the Hybrid Technique?

Cost: $O\left(m q^{a_{\min} t} \binom{n - k'}{t} \binom{n - a_{\min}}{t}^{\omega - 1}\right)$ ← guessing

Question: How quickly does $a_{\min}$ grow?

- If $t(n) = O(\log n)$ cost $O(q^{3t})$ $q^{3t(n) \log_q n + o(t \log n)}$ → smaller than GRS
- If $t(n) = \omega(\log n)$ cost $O(q^{tk})$ $q^{Rt(n)n + o(tn)}$ → same as GRS

How Good Is the Hybrid Technique?

Cost: $O\left(m q^{a_{\min} t} \binom{n - k'}{t} \binom{n - a_{\min}}{t}^{\omega^{-1}}\right)$ ← guessing

Question: How quickly does $a_{\min}$ grow?

- If $t(n) = O(\log n)$ cost $O(q^{3t})$ $q^{3t(n) \log_q n + o(t \log n)}$ → smaller than GRS
- If $t(n) = \omega(\log n)$ cost $O(q^{tk})$ $q^{Rt(n)n + o(tn)}$ → same as GRS

Random codes: attain rank GV w.h.p.

$$\frac{d}{n} = \frac{m/n + 1}{2} - \sqrt{(mk)/n^2 + \frac{(m/n - 1)^2}{4}} \quad \text{w.h.p.} \quad \rightarrow \quad t = \Theta(n)$$

→ Best known attack for random codes: $O(q^{kt})$

Open problem: Better hybrid approach?



H. Sauerbier Couvée, A. Wachter-Zeh, V. W. “Hybrid Subsupport Guessing: A New Hybrid Technique for the Rank Decoding Problem”, PQCrypto 2026



H. Sauerbier Couvée, A. Wachter-Zeh, V. W. “Hybrid Subsupport Guessing: A New Hybrid Technique for the Rank Decoding Problem”, PQCrypto 2026

Supersupport guessing

$$\mathcal{E} = \text{supp}_{\text{row}}(e) \subseteq \mathcal{S} \quad \dim(\mathcal{S}) = n - a$$



same as shortening

$$H' = HS^{\top} \quad e = e'S \quad \text{wt}_R(e') = t$$

$$(q, m, n, k, t) \longrightarrow (q, m, n - a, k - a, t)$$

$$m \binom{n-k'}{t} \geq \binom{n-a}{t}$$



H. Sauerbier Couvée, A. Wachter-Zeh, V. W. “Hybrid Subsupport Guessing: A New Hybrid Technique for the Rank Decoding Problem”, PQCrypto 2026

Supersupport guessing

$$\mathcal{E} = \text{supp}_{\text{row}}(e) \subseteq \mathcal{S} \quad \dim(\mathcal{S}) = n - a$$



same as shortening

$$H' = HS^{\top} \quad e = e'S \quad \text{wt}_R(e') = t$$

$$(q, m, n, k, t) \longrightarrow (q, m, n - a, k - a, t)$$

$$m \binom{n-k'}{t} \geq \binom{n-a}{t}$$

Subsupport guessing

$$\text{guess } \mathcal{B} = \ker(B) \subseteq \mathcal{E} \quad \dim(\mathcal{B}) = b$$



same as puncturing

$$G' = GB \quad e' = eB \quad \text{wt}_R(e') = t - b$$

$$(q, m, n, k, t) \longrightarrow (q, m, n - b, k, t - b)$$

$$m \binom{n-b-k'}{t-b} \geq \binom{n-b}{t-b}$$



H. Sauerbier Couvée, A. Wachter-Zeh, V. W. “Hybrid Subsupport Guessing: A New Hybrid Technique for the Rank Decoding Problem”, PQCrypto 2026

Supersupport guessing

$$\mathcal{E} = \text{supp}_{\text{row}}(e) \subseteq \mathcal{S} \quad \dim(\mathcal{S}) = n - a$$



same as shortening

$$H' = HS^{\top} \quad e = e'S \quad \text{wt}_R(e') = t$$

$$(q, m, n, k, t) \longrightarrow (q, m, n - a, k - a, t)$$

$$m\binom{n-k'}{t} \geq \binom{n-a}{t}$$

Subsupport guessing

$$\text{guess } \mathcal{B} = \ker(B) \subseteq \mathcal{E} \quad \dim(\mathcal{B}) = b$$



same as puncturing

$$G' = GB \quad e' = eB \quad \text{wt}_R(e') = t - b$$

$$(q, m, n, k, t) \longrightarrow (q, m, n - b, k, t - b)$$

$$m\binom{n-b-k'}{t-b} \geq \binom{n-b}{t-b}$$



H. Sauerbier Couvée, A. Wachter-Zeh, V. W. “Hybrid Subsupport Guessing: A New Hybrid Technique for the Rank Decoding Problem”, PQCrypto 2026

Supersupport guessing

$$\mathcal{E} = \text{supp}_{\text{row}}(e) \subseteq \mathcal{S} \quad \dim(\mathcal{S}) = n - a$$



same as shortening

$$H' = HS^{\top} \quad e = e'S \quad \text{wt}_R(e') = t$$

$$(q, m, n, k, t) \longrightarrow (q, m, n - a, k - a, t)$$

$$m \binom{n-k'}{t} \geq \binom{n-a}{t}$$

Subsupport guessing

$$\text{guess } \mathcal{B} = \ker(B) \subseteq \mathcal{E} \quad \dim(\mathcal{B}) = b$$



same as puncturing

$$G' = GB \quad e' = eB \quad \text{wt}_R(e') = t - b$$

$$(q, m, n, k, t) \longrightarrow (q, m, n - b, k, t - b)$$

$$m \binom{n-b-k'}{t-b} \geq \binom{n-b}{t-b}$$

RYDE-5 v2:

MaxMinors new hybrid 317 → 284

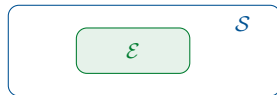
bits of work factor

Where to Look Next: Need Magic!

Fun fact: subspaces like to avoid each other!

Supersupport guessing: choose a random subspace $\mathcal{S} \subseteq \mathbb{F}_q^n$

and hope that $\mathcal{E} = \text{supp}_{\text{row}}(e) \subseteq \mathcal{S}$ if not: start over



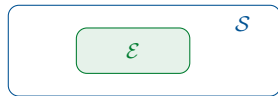
Where to Look Next: Need Magic!

Fun fact: subspaces like to avoid each other!

Supersupport guessing: choose a random subspace $\mathcal{S} \subseteq \mathbb{F}_q^n$

and hope that $\mathcal{E} = \text{supp}_{\text{row}}(e) \subseteq \mathcal{S}$ if not: start over

Magic step given $\mathcal{S}$, can we test if $\mathcal{S} \cap \mathcal{E} \neq \{0\}$?



Where to Look Next: Need Magic!

Fun fact: subspaces like to avoid each other!

Supersupport guessing: choose a random subspace $\mathcal{S} \subseteq \mathbb{F}_q^n$

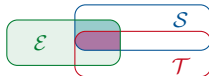
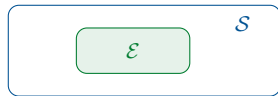
and hope that $\mathcal{E} = \text{supp}_{\text{row}}(e) \subseteq \mathcal{S}$ if not: start over

Magic step given $\mathcal{S}$, can we test if $\mathcal{S} \cap \mathcal{E} \neq \{0\}$?

→ adaptive algorithm: choose $\mathcal{S} \cap \mathcal{T} \neq \{0\}$ and do magic step

→ w.h.p. $\mathcal{S} \cap \mathcal{T} \cap \mathcal{E} \neq \{0\}$ → find one basis of $\mathcal{E}$

→ after $2t$ steps w.h.p. found $\mathcal{E}$ and e



Where to Look Next: Need Magic!

Fun fact: subspaces like to avoid each other!

Supersupport guessing: choose a random subspace $\mathcal{S} \subseteq \mathbb{F}_q^n$

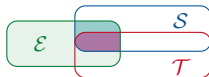
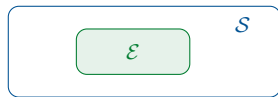
and hope that $\mathcal{E} = \text{supp}_{\text{row}}(e) \subseteq \mathcal{S}$ if not: start over

Magic step given $\mathcal{S}$, can we test if $\mathcal{S} \cap \mathcal{E} \neq \{0\}$?

→ adaptive algorithm: choose $\mathcal{S} \cap \mathcal{T} \neq \{0\}$ and do magic step

→ w.h.p. $\mathcal{S} \cap \mathcal{T} \cap \mathcal{E} \neq \{0\}$ → find one basis of $\mathcal{E}$

→ after $2t$ steps w.h.p. found $\mathcal{E}$ and e



Open problem: how to do magic step?

Associated Hamming code

q -ary simplex code

take one representative of every 1-dimensional subspace of $\mathbb{F}_q^n$

$$S \in \mathbb{F}_q^{n \times N} \quad N = \frac{q^n - 1}{q - 1}$$

→ every nonzero codeword has constant Hamming weight q^{n-1}

Associated Hamming code

q -ary simplex code

take one representative of every 1-dimensional subspace of $\mathbb{F}_q^n$

$$S \in \mathbb{F}_q^{n \times N} \quad N = \frac{q^n - 1}{q - 1}$$

→ every nonzero codeword has constant Hamming weight q^{n-1}

Example: $q = 3, n = 2, N = 4$

$$S = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$$

Where to Look Next: Hamming Metric?

Associated Hamming code

q -ary simplex code

take one representative of every 1-dimensional subspace of $\mathbb{F}_q^n$

$$S \in \mathbb{F}_q^{n \times N} \quad N = \frac{q^n - 1}{q - 1}$$

→ every nonzero codeword has constant Hamming weight q^{n-1}

Example: $q = 3, n = 2, N = 4$

$$S = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$$

$\mathcal{C} = \langle G \rangle \subseteq \mathbb{F}_{q^m}^n \quad G \in \mathbb{F}_{q^m}^{k \times n} \quad \rightarrow \quad \text{associated Hamming code} \quad \mathcal{C}^H = \langle GS \rangle \quad \text{length } N, \text{ dimension } k$

$$\boxed{G} \cdot \boxed{S} = \boxed{GS}$$

Where to Look Next: Hamming Metric?

Associated Hamming code

q -ary simplex code

take one representative of every 1-dimensional subspace of $\mathbb{F}_q^n$

$$S \in \mathbb{F}_q^{n \times N} \quad N = \frac{q^n - 1}{q - 1}$$

→ every nonzero codeword has constant Hamming weight q^{n-1}

Example: $q = 3, n = 2, N = 4$

$$S = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$$

$\mathcal{C} = \langle G \rangle \subseteq \mathbb{F}_{q^m}^n \quad G \in \mathbb{F}_{q^m}^{k \times n} \quad \rightarrow \quad \text{associated Hamming code} \quad \mathcal{C}^H = \langle GS \rangle \quad \text{length } N, \text{ dimension } k$

$$\boxed{G} \cdot \boxed{S} = \boxed{GS}$$

$x \in \mathbb{F}_{q^m}^n$ with

$$\text{wt}_R(x) = t$$

$$\rightarrow \text{wt}_H(xS) = \frac{q^n - q^{n-t}}{q - 1} = t^H$$

Where to Look Next: Hamming Metric?

Associated Hamming code

q -ary simplex code

take one representative of every 1-dimensional subspace of $\mathbb{F}_q^n$

$$S \in \mathbb{F}_q^{n \times N} \quad N = \frac{q^n - 1}{q - 1}$$

→ every nonzero codeword has constant Hamming weight q^{n-1}

Example: $q = 3, n = 2, N = 4$

$$S = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$$

$\mathcal{C} = \langle G \rangle \subseteq \mathbb{F}_{q^m}^n \quad G \in \mathbb{F}_{q^m}^{k \times n} \quad \rightarrow \quad \text{associated Hamming code} \quad \mathcal{C}^H = \langle GS \rangle \quad \text{length } N, \text{ dimension } k$

$$\boxed{G} \cdot \boxed{S} = \boxed{GS}$$

$x \in \mathbb{F}_{q^m}^n$ with

$$\text{wt}_R(x) = t$$

$$\rightarrow \text{wt}_H(xS) = \frac{q^n - q^{n-t}}{q - 1} = t^H$$

$$(G, r, t) \longrightarrow (GS, rS, t^H)$$

Rank Decoding → Hamming Decoding

Can We Use Hamming-Metric ISD?

Problem: $N = \frac{q^n - 1}{q - 1}$ is huge

Do we really have to construct GS ? No!

Can We Use Hamming-Metric ISD?

Problem: $N = \frac{q^n - 1}{q - 1}$ is huge

Do we really have to construct GS ? No!

Prange on $\mathcal{C}^H$ choose an information set $I \subseteq [N]$, $|I| = k$

$$rS = mGS + eS \quad \rightarrow \quad rS_I = mGS_I \quad \text{if } (eS)_I = 0 \quad \rightarrow \text{solve for } m$$

$$k \left\{ \underbrace{S_I^\top}_n \right.$$

only compute

$$GS_I \in \mathbb{F}_q^{k \times k}$$

and invert it

Can We Use Hamming-Metric ISD?

Problem: $N = \frac{q^n - 1}{q - 1}$ is huge

Do we really have to construct GS ? No!

Prange on $\mathcal{C}^H$ choose an information set $I \subseteq [N]$, $|I| = k$

$$rS = mGS + eS \quad \rightarrow \quad rS_I = mGS_I \quad \text{if } (eS)_I = 0 \quad \rightarrow \text{solve for } m$$

$$k \left\{ \underbrace{S_I^\top}_n \right. \quad \text{only compute} \quad GS_I \in \mathbb{F}_q^{k \times k} \quad \text{and invert it}$$

number of error-free positions: $N - t^H = \frac{q^{n-t} - 1}{q - 1}$

$$\Pr[(eS)_I = 0] = \binom{N - t^H}{k} \binom{N}{k}^{-1}$$

Can We Use Hamming-Metric ISD?

Problem: $N = \frac{q^n - 1}{q - 1}$ is huge

Do we really have to construct GS ? No!

Prange on $\mathcal{C}^H$ choose an information set $I \subseteq [N]$, $|I| = k$

$$rS = mGS + eS \quad \rightarrow \quad rS_I = mGS_I \quad \text{if } (eS)_I = 0 \quad \rightarrow \text{solve for } m$$

$$k \left\{ \underbrace{S_I^\top}_n \right. \quad \text{only compute} \quad GS_I \in \mathbb{F}_{q^m}^{k \times k} \quad \text{and invert it}$$

number of error-free positions: $N - t^H = \frac{q^{n-t} - 1}{q - 1}$

$$\Pr[(eS)_I = 0] = \binom{N - t^H}{k} \binom{N}{k}^{-1} \approx q^{-kt} \quad \rightarrow \text{cost } O(q^{kt}) = \text{GRS!}$$

Can We Use Hamming-Metric ISD?

Problem: $N = \frac{q^n - 1}{q - 1}$ is huge

Do we really have to construct GS ? No!

Prange on $\mathcal{C}^H$ choose an information set $I \subseteq [N]$, $|I| = k$

$$rS = mGS + eS \quad \rightarrow \quad rS_I = mGS_I \quad \text{if } (eS)_I = 0 \quad \rightarrow \text{solve for } m$$

$$k \left\{ \underbrace{S_I^\top}_n \right. \quad \text{only compute} \quad GS_I \in \mathbb{F}_{q^m}^{k \times k} \quad \text{and invert it}$$

number of error-free positions: $N - t^H = \frac{q^{n-t} - 1}{q - 1}$

$$\Pr[(eS)_I = 0] = \binom{N - t^H}{k} \binom{N}{k}^{-1} \approx q^{-kt} \quad \rightarrow \text{cost } O(q^{kt}) = \text{GRS!}$$

can we now do Stern / support splitting?

Can We Use Hamming-Metric ISD?

Problem: $N = \frac{q^n - 1}{q - 1}$ is huge

Do we really have to construct GS ? No!

Prange on $\mathcal{C}^H$ choose an information set $I \subseteq [N]$, $|I| = k$

$$rS = mGS + eS \quad \rightarrow \quad rS_I = mGS_I \quad \text{if } (eS)_I = 0 \quad \rightarrow \text{solve for } m$$

$$k \left\{ \underbrace{S_I^\top}_n \right. \quad \text{only compute} \quad GS_I \in \mathbb{F}_{q^m}^{k \times k} \quad \text{and invert it}$$

number of error-free positions: $N - t^H = \frac{q^{n-t} - 1}{q - 1}$

$$\Pr[(eS)_I = 0] = \binom{N - t^H}{k} \binom{N}{k}^{-1} \approx q^{-kt} \quad \rightarrow \text{cost } O(q^{kt}) = \text{GRS!}$$

can we now do Stern / support splitting?

$\rightarrow$ optimizes in Prange

Can We Use Hamming-Metric ISD?

Problem: $N = \frac{q^n - 1}{q - 1}$ is huge

Do we really have to construct GS ? No!

Prange on $\mathcal{C}^H$ choose an information set $I \subseteq [N]$, $|I| = k$

$$rS = mGS + eS \quad \rightarrow \quad rS_I = mGS_I \quad \text{if } (eS)_I = 0 \quad \rightarrow \text{solve for } m$$

$$k \left\{ \underbrace{S_I^\top}_n \right. \quad \text{only compute} \quad GS_I \in \mathbb{F}_{q^m}^{k \times k} \quad \text{and invert it}$$

number of error-free positions: $N - t^H = \frac{q^{n-t} - 1}{q - 1}$

$$\Pr[(eS)_I = 0] = \binom{N - t^H}{k} \binom{N}{k}^{-1} \approx q^{-kt} \quad \rightarrow \text{cost } O(q^{kt}) = \text{GRS!}$$

can we now do Stern / support splitting?

$\rightarrow$ optimizes in Prange

why?

$\rightarrow$ huge length N ?

$\rightarrow$ huge alphabet $\mathbb{F}_{q^m}$?

Where to Look Next: Algebraic q -ary ISD?

Hamming decoding over $\mathbb{F}_{2^m}$

$$He^{\top} = s^{\top}, \quad H \in \mathbb{F}_{2^m}^{(n-k) \times n}, \quad \text{wt}_H(e) = t$$

Where to Look Next: Algebraic q -ary ISD?

Hamming decoding over $\mathbb{F}_{2^m}$

$$He^\top = s^\top, \quad H \in \mathbb{F}_{2^m}^{(n-k) \times n}, \quad \text{wt}_H(e) = t$$

If we knew k additional equations

$$Ae^\top = s'^\top$$

such that

$\begin{pmatrix} H \\ A \end{pmatrix}$ is invertible,

→ easy problem:

$$e^\top = \begin{pmatrix} H \\ A \end{pmatrix}^{-1} \begin{pmatrix} s \\ s' \end{pmatrix}$$

Where to Look Next: Algebraic q -ary ISD?

Hamming decoding over $\mathbb{F}_{2^m}$

$$He^\top = s^\top, \quad H \in \mathbb{F}_{2^m}^{(n-k) \times n}, \quad \text{wt}_H(e) = t$$

If we knew k additional equations

$$Ae^\top = s'^\top$$

such that $\begin{pmatrix} H \\ A \end{pmatrix}$ is invertible,

→ easy problem:

$$e^\top = \begin{pmatrix} H \\ A \end{pmatrix}^{-1} \begin{pmatrix} s \\ s' \end{pmatrix}$$

Expand over $\mathbb{F}_2$

$$\Gamma(H) \Gamma(e)^\top = \Gamma(s)^\top$$

$m(n-k)$ equations in mn variables

$$\Gamma(e) = \underbrace{\Gamma(e_1)}_m \underbrace{\Gamma(e_2)}_m \cdots \underbrace{\Gamma(e_n)}_m$$

Where to Look Next: Algebraic q -ary ISD?

Hamming decoding over $\mathbb{F}_2^m$

$$He^\top = s^\top, \quad H \in \mathbb{F}_2^{(n-k) \times n}, \quad \text{wt}_H(e) = t$$

If we knew k additional equations

$$Ae^\top = s'^\top$$

such that $\begin{pmatrix} H \\ A \end{pmatrix}$ is invertible,

→ easy problem:

$$e^\top = \begin{pmatrix} H \\ A \end{pmatrix}^{-1} \begin{pmatrix} s \\ s' \end{pmatrix}$$

Expand over $\mathbb{F}_2$

$$\Gamma(H) \Gamma(e)^\top = \Gamma(s)^\top$$

$m(n-k)$ equations in mn variables

$$\Gamma(e) = \begin{array}{|c|c|} \hline \Gamma(e_1) & \Gamma(e_2) \\ \hline 0 & x \cdots x \\ \hline \end{array} \cdots \begin{array}{|c|} \hline \Gamma(e_n) \\ \hline 0 \\ \hline \end{array}$$

add n equations supported on one block:

$$\langle (x, \dots, x), \Gamma(e_i) \rangle = 0$$

$$e_i = 0$$

→ always satisfied

$$e_i \neq 0$$

→ with prob $\approx 1/2$

Where to Look Next: Algebraic q -ary ISD?

Hamming decoding over $\mathbb{F}_2^m$

$$He^\top = s^\top, \quad H \in \mathbb{F}_2^{(n-k) \times n}, \quad \text{wt}_H(e) = t$$

If we knew k additional equations

$$Ae^\top = s'^\top$$

such that $\begin{pmatrix} H \\ A \end{pmatrix}$ is invertible,

→ easy problem:

$$e^\top = \begin{pmatrix} H \\ A \end{pmatrix}^{-1} \begin{pmatrix} s \\ s' \end{pmatrix}$$

Expand over $\mathbb{F}_2$

$$\Gamma(H) \Gamma(e)^\top = \Gamma(s)^\top$$

$m(n-k)$ equations in mn variables

$$\Gamma(e) = \begin{array}{|c|c|c|} \hline \Gamma(e_1) & \Gamma(e_2) & \cdots & \Gamma(e_n) \\ \hline 0 & x \cdots x & \cdots & 0 \\ \hline \end{array}$$

add n equations supported on one block:

$$\langle (x, \dots, x), \Gamma(e_i) \rangle = 0$$

$$e_i = 0$$

→ always satisfied

$$e_i \neq 0$$

→ with prob $\approx 1/2$

Open problem: How to get more equations?

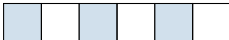
Where to Look Next: Dual Attacks?

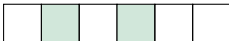
Dual code: $\mathcal{C}^\perp = \{x \in \mathbb{F}_q^n : \langle x, c \rangle = 0, \forall c \in \mathcal{C}\} = \langle H \rangle$

Hamming metric

$$r = mG + e \quad \text{and small } h \in \mathcal{C}^\perp$$

$$\rightarrow \langle r, h \rangle = \langle e, h \rangle$$

$$e =$$


$$h =$$


$$S = \text{supp}_H(h)$$

$$\langle e, h \rangle = \sum_{i \in S} e_i h_i \neq 0 \quad \rightarrow \quad e_S \neq 0$$

information on the support

$\rightarrow$ reduce search space / add equations

Where to Look Next: Dual Attacks?

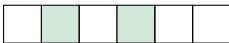
Dual code: $\mathcal{C}^\perp = \{x \in \mathbb{F}_q^n : \langle x, c \rangle = 0, \forall c \in \mathcal{C}\} = \langle H \rangle$

Hamming metric

$$r = mG + e \quad \text{and small } h \in \mathcal{C}^\perp$$

$$\rightarrow \langle r, h \rangle = \langle e, h \rangle$$

$$e =$$


$$h =$$


$$S = \text{supp}_H(h)$$

$$\langle e, h \rangle = \sum_{i \in S} e_i h_i \neq 0 \quad \rightarrow e_S \neq 0$$

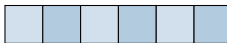
information on the support

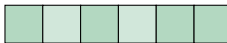
$\rightarrow$ reduce search space / add equations

Rank metric

$$r = mG + e \quad \text{and small } h \in \mathcal{C}^\perp$$

$$\rightarrow \langle r, h \rangle = \langle e, h \rangle$$

$$e =$$


$$h =$$


$$S = \text{supp}_H(h) = n$$

$$\langle e, h \rangle = \sum_{i \in S} e_i h_i \neq 0 \quad \rightarrow \text{no information}$$

Where to Look Next: Dual Attacks?

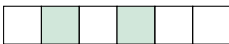
Dual code: $\mathcal{C}^\perp = \{x \in \mathbb{F}_q^n : \langle x, c \rangle = 0, \forall c \in \mathcal{C}\} = \langle H \rangle$

Hamming metric

$$r = mG + e \quad \text{and small } h \in \mathcal{C}^\perp$$

$$\rightarrow \langle r, h \rangle = \langle e, h \rangle$$

$$e =$$


$$h =$$


$$S = \text{supp}_H(h)$$

$$\langle e, h \rangle = \sum_{i \in S} e_i h_i \neq 0 \quad \rightarrow e_S \neq 0$$

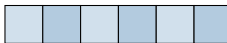
information on the support

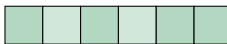
$\rightarrow$ reduce search space / add equations

Rank metric

$$r = mG + e \quad \text{and small } h \in \mathcal{C}^\perp$$

$$\rightarrow \langle r, h \rangle = \langle e, h \rangle$$

$$e =$$


$$h =$$


$$S = \text{supp}_H(h) = n$$

$$\langle e, h \rangle = \sum_{i \in S} e_i h_i \neq 0 \quad \rightarrow \text{no information}$$

can we use instead $\text{Tr}(\langle e, h \rangle)$ or $\langle e, h \rangle^{q^i}$?

why interesting? RYDE uses $\dim(\mathcal{C}^\perp) = 8$

Where to Look Next: Dual Attacks?

Dual code: $\mathcal{C}^\perp = \{x \in \mathbb{F}_q^n : \langle x, c \rangle = 0, \forall c \in \mathcal{C}\} = \langle H \rangle$

Hamming metric

$$r = mG + e \quad \text{and small } h \in \mathcal{C}^\perp$$

$$\rightarrow \langle r, h \rangle = \langle e, h \rangle$$

$$e = \begin{array}{|c|c|c|c|c|c|} \hline \text{blue} & \text{white} & \text{blue} & \text{white} & \text{blue} & \text{white} \\ \hline \end{array}$$

$$h = \begin{array}{|c|c|c|c|c|c|} \hline \text{white} & \text{green} & \text{white} & \text{green} & \text{white} & \text{white} \\ \hline \end{array}$$

$$S = \text{supp}_H(h)$$

$$\langle e, h \rangle = \sum_{i \in S} e_i h_i \neq 0 \quad \rightarrow e_S \neq 0$$

information on the support

$\rightarrow$ reduce search space / add equations

Rank metric

$$r = mG + e \quad \text{and small } h \in \mathcal{C}^\perp$$

$$\rightarrow \langle r, h \rangle = \langle e, h \rangle$$

$$e = \begin{array}{|c|c|c|c|c|c|} \hline \text{blue} & \text{blue} & \text{blue} & \text{blue} & \text{blue} & \text{blue} \\ \hline \end{array}$$

$$h = \begin{array}{|c|c|c|c|c|c|} \hline \text{green} & \text{green} & \text{green} & \text{green} & \text{green} & \text{green} \\ \hline \end{array}$$

$$S = \text{supp}_H(h) = n$$

$$\langle e, h \rangle = \sum_{i \in S} e_i h_i \neq 0 \quad \rightarrow \text{no information}$$

can we use instead $\text{Tr}(\langle e, h \rangle)$ or $\langle e, h \rangle^{q^i}$?

why interesting? RYDE uses $\dim(\mathcal{C}^\perp) = 8$

Open problem: how to do rank-dual attacks?

What have we Seen?



What we know

- Rank DP randomized reduction
- Combinatorial solver: q -analog of Prange
- Algebraic modeling works for $t = O(\log n)$

What we don't know

- ? Is Rank Decoding NP-hard?
- ? How to split supports?
- ? Can algebraic modeling work beyond $t = O(\log n)$?

Where to Look Next?

- Can we detect non-trivial intersections?
- Can we exploit the associated Hamming code?
- Can we improve q -ary ISD?
- Can we translate dual attacks?

Where to Look Next?

- Can we detect non-trivial intersections?
- Can we exploit the associated Hamming code?
- Can we improve q -ary ISD?
- Can we translate dual attacks?

Harder to decode or do we simply not know how?

Where to Look Next?

- Can we detect non-trivial intersections?
- Can we exploit the associated Hamming code?
- Can we improve q -ary ISD?
- Can we translate dual attacks?

Happy to discuss!



slides

Harder to decode or do we simply not know how?

Workshop on the Mathematics of Post-Quantum Cryptography

September 7–11, 2026

Raitenhaslach, Germany



<https://mathpqc26.cry.cit.tum.de/index.html>