

Symmetric Models for Syndrome Decoding

Simone Trebiani

Joint work with Elisa Gorla

Workshop on Algebraic Methods in Post-Quantum Cryptography
Ohrid, 14 August 2026



Syndrome Decoding Problem

- ▶ a parity check matrix $\mathbf{H} \in \mathbb{F}_q^{(n-k) \times n}$ of an $[n, k]$ -linear code $\mathcal{C} \leq \mathbb{F}_q^n$;
- ▶ a syndrome $s \in \mathbb{F}_q^{n-k}$;
- ▶ a target weight $t \in \{0, \dots, n\}$;
 - Hamming weight: $\text{wt}(x) := \#\{i \in \{1, \dots, n\} \mid x_i \neq 0\}$.

(B)SDP: (Bounded) Syndrome Decoding Problem

Find a vector $x \in \mathbb{F}_q^n$ such that $\mathbf{H} \cdot x^\top = s^\top$ and $\text{wt}(x) \leq t$.

ESDP: Exact weight Syndrome Decoding Problem

Find a vector $x \in \mathbb{F}_q^n$ such that $\mathbf{H} \cdot x^\top = s^\top$ and $\text{wt}(x) = t$.

Syndrome Decoding Problem

- ▶ a parity check matrix $\mathbf{H} \in \mathbb{F}_q^{(n-k) \times n}$ of an $[n, k]$ -linear code $\mathcal{C} \leq \mathbb{F}_q^n$;
- ▶ a syndrome $s \in \mathbb{F}_q^{n-k}$;
- ▶ a target weight $t \in \{0, \dots, n\}$;
 - Hamming weight: $\text{wt}(x) := \#\{i \in \{1, \dots, n\} \mid x_i \neq 0\}$.

(B)SDP: (Bounded) Syndrome Decoding Problem

Find a vector $x \in \mathbb{F}_q^n$ such that $\mathbf{H} \cdot x^\top = s^\top$ and $\text{wt}(x) \leq t$.

ESDP: Exact weight Syndrome Decoding Problem

Find a vector $x \in \mathbb{F}_q^n$ such that $\mathbf{H} \cdot x^\top = s^\top$ and $\text{wt}(x) = t$.

NP-complete! $\leadsto$ McEliece cryptosystem, Niederreiter scheme, ...

Previous algebraic approaches

- ▶ Best way: Information Set Decoding (Prange, 1962) & variants.

Previous algebraic approaches

- ▶ Best way: Information Set Decoding (Prange, 1962) & variants.
- ▶ Meneghetti, Pellegrini and Sala (2023):
 - polynomial-time reduction from the SDP to the POlynomial System SOLving problem.

Previous algebraic approaches

- ▶ Best way: Information Set Decoding (Prange, 1962) & variants.
- ▶ Meneghetti, Pellegrini and Sala (2023):
 - polynomial-time reduction from the SDP to the POlynomial System SOLving problem.
- ▶ Caminata, Cartor, Meneghetti, Mora and Pellegrini (2025):
 - improvement: model with **quadratic** polynomials;

Previous algebraic approaches

- ▶ Best way: Information Set Decoding (Prange, 1962) & variants.
- ▶ Meneghetti, Pellegrini and Sala (2023):
 - polynomial-time reduction from the SDP to the POLynomial System SOLving problem.
- ▶ Caminata, Cartor, Meneghetti, Mora and Pellegrini (2025):
 - improvement: model with **quadratic** polynomials;
 - complexity of solving the polynomial system:

$$d_{\text{sol}}(S_{\text{QM}}) \leq \left\lceil \frac{n-1}{2} \right\rceil + \lfloor \log_2 t \rfloor \left\lceil \frac{n-2}{2} \right\rceil + 2$$

where d_{sol} is the *solving degree* of the system ($\leadsto$ the computational cost for computing a Gröbner basis of S is exponential in $d_{\text{sol}}(S)$).

Elementary symmetric polynomials and Weights over $\mathbb{F}_2$

Elementary symmetric polynomials in $R := \mathbb{F}_2[x_1, \dots, x_n]$

$$e_{n,j} := \sum_{\alpha \subseteq \{1, \dots, n\}, |\alpha|=j} x_\alpha = \sum_{1 \leq \alpha_1 < \dots < \alpha_j \leq n} x_{\alpha_1} \cdots x_{\alpha_j}.$$

$$e_{3,1} = x_1 + x_2 + x_3, \quad e_{3,2} = x_1x_2 + x_1x_3 + x_2x_3, \quad e_{3,3} = x_1x_2x_3.$$

Elementary symmetric polynomials and Weights over $\mathbb{F}_2$

Elementary symmetric polynomials in $R := \mathbb{F}_2[x_1, \dots, x_n]$

$$e_{n,j} := \sum_{\alpha \subseteq \{1, \dots, n\}, |\alpha|=j} x_\alpha = \sum_{1 \leq \alpha_1 < \dots < \alpha_j \leq n} x_{\alpha_1} \cdots x_{\alpha_j}.$$

$$e_{3,1} = x_1 + x_2 + x_3, \quad e_{3,2} = x_1x_2 + x_1x_3 + x_2x_3, \quad e_{3,3} = x_1x_2x_3.$$

$$x = (x_1, \dots, x_n), \quad \text{wt}(x) = w \quad \rightsquigarrow \quad e_{n,j}(x) = ?$$

Elementary symmetric polynomials and Weights over $\mathbb{F}_2$

$$x = (x_1, x_2, x_3), \quad \text{wt}(x) = w \quad \leadsto \quad e_{3,j}(x) = ?$$

$$w = 0 \leadsto \begin{cases} x_1 + x_2 + x_3 = 0 \\ x_1x_2 + x_1x_3 + x_2x_3 = 0 \\ x_1x_2x_3 = 0 \end{cases}$$

Elementary symmetric polynomials and Weights over $\mathbb{F}_2$

$$x = (x_1, x_2, x_3), \quad \text{wt}(x) = w \quad \leadsto \quad e_{3,j}(x) = ?$$

$$w = 0 \leadsto \begin{cases} x_1 + x_2 + x_3 = 0 \\ x_1x_2 + x_1x_3 + x_2x_3 = 0 \\ x_1x_2x_3 = 0 \end{cases} \quad w = 1 \leadsto \begin{cases} x_1 + x_2 + x_3 = \textcolor{red}{1} \\ x_1x_2 + x_1x_3 + x_2x_3 = 0 \\ x_1x_2x_3 = 0 \end{cases}$$

Elementary symmetric polynomials and Weights over $\mathbb{F}_2$

$$x = (x_1, x_2, x_3), \quad \text{wt}(x) = w \quad \leadsto \quad e_{3,j}(x) = ?$$

$$w = 0 \leadsto \begin{cases} x_1 + x_2 + x_3 = 0 \\ x_1x_2 + x_1x_3 + x_2x_3 = 0 \\ x_1x_2x_3 = 0 \end{cases} \quad w = 1 \leadsto \begin{cases} x_1 + x_2 + x_3 = 1 \\ x_1x_2 + x_1x_3 + x_2x_3 = 0 \\ x_1x_2x_3 = 0 \end{cases}$$

$$w = 2 \leadsto \begin{cases} x_1 + x_2 + x_3 = 0 \\ x_1x_2 + x_1x_3 + x_2x_3 = 1 \\ x_1x_2x_3 = 0 \end{cases} \quad w = 3 \leadsto \begin{cases} x_1 + x_2 + x_3 = 1 \\ x_1x_2 + x_1x_3 + x_2x_3 = 1 \\ x_1x_2x_3 = 1 \end{cases}$$

Elementary symmetric polynomials and Weights over $\mathbb{F}_2$

$$x = (x_1, x_2, x_3), \quad \text{wt}(x) = w \quad \leadsto \quad e_{3,j}(x) = ?$$

$$w = 0 \leadsto \begin{cases} x_1 + x_2 + x_3 = 0 \\ x_1x_2 + x_1x_3 + x_2x_3 = 0 \\ x_1x_2x_3 = 0 \end{cases} \quad w = 1 \leadsto \begin{cases} x_1 + x_2 + x_3 = 1 \\ x_1x_2 + x_1x_3 + x_2x_3 = 0 \\ x_1x_2x_3 = 0 \end{cases}$$

$$w = 2 \leadsto \begin{cases} x_1 + x_2 + x_3 = 0 \\ x_1x_2 + x_1x_3 + x_2x_3 = 1 \\ x_1x_2x_3 = 0 \end{cases} \quad w = 3 \leadsto \begin{cases} x_1 + x_2 + x_3 = 1 \\ x_1x_2 + x_1x_3 + x_2x_3 = 1 \\ x_1x_2x_3 = 1 \end{cases}$$

Equivalent conditions

- 1 $\text{wt}(x) = t$;
- 2 $e_{n,j}(x) = \binom{t}{j}$ for all $j = 1, \dots, n$;

Elementary symmetric polynomials and Weights over $\mathbb{F}_2$

$$x = (x_1, x_2, x_3), \quad \text{wt}(x) = w \quad \leadsto \quad e_{3,j}(x) = ?$$

$$w = 0 \leadsto \begin{cases} x_1 + x_2 + x_3 = 0 \\ x_1x_2 + x_1x_3 + x_2x_3 = 0 \\ x_1x_2x_3 = 0 \end{cases} \quad w = 1 \leadsto \begin{cases} x_1 + x_2 + x_3 = 1 \\ x_1x_2 + x_1x_3 + x_2x_3 = 0 \\ x_1x_2x_3 = 0 \end{cases}$$

$$w = 2 \leadsto \begin{cases} x_1 + x_2 + x_3 = 0 \\ x_1x_2 + x_1x_3 + x_2x_3 = 1 \\ x_1x_2x_3 = 0 \end{cases} \quad w = 3 \leadsto \begin{cases} x_1 + x_2 + x_3 = 1 \\ x_1x_2 + x_1x_3 + x_2x_3 = 1 \\ x_1x_2x_3 = 1 \end{cases}$$

Equivalent conditions

- 1 $\text{wt}(x) = t$;
- 2 $e_{n,j}(x) = \binom{t}{j}$ for all $j = 1, \dots, n$;

Elementary symmetric polynomials and Weights over $\mathbb{F}_2$

$$x = (x_1, x_2, x_3), \quad \text{wt}(x) = w \quad \leadsto \quad e_{3,j}(x) = ?$$

$$w = 0 \leadsto \begin{cases} x_1 + x_2 + x_3 = 0 \\ x_1x_2 + x_1x_3 + x_2x_3 = 0 \\ x_1x_2x_3 = 0 \end{cases} \quad w = 1 \leadsto \begin{cases} x_1 + x_2 + x_3 = 1 \\ x_1x_2 + x_1x_3 + x_2x_3 = 0 \\ x_1x_2x_3 = 0 \end{cases}$$

$$w = 2 \leadsto \begin{cases} x_1 + x_2 + x_3 = 0 \\ x_1x_2 + x_1x_3 + x_2x_3 = 1 \\ x_1x_2x_3 = 0 \end{cases} \quad w = 3 \leadsto \begin{cases} x_1 + x_2 + x_3 = 1 \\ x_1x_2 + x_1x_3 + x_2x_3 = 1 \\ x_1x_2x_3 = 1 \end{cases}$$

Equivalent conditions

- 1 $\text{wt}(x) = t$;
- 2 $e_{n,j}(x) = \binom{t}{j}$ for all $j = 1, \dots, n$;

Even better: if $r := \lfloor \log_2 n \rfloor$ and $t = t_0 + t_1 2 + \dots + t_r 2^r$,

- 3 $e_{n,2^i}(x) = t_i$ for all $i = 0, \dots, r$.

New model for the ESDP over $\mathbb{F}_2$

- Parity check encoding: $H \cdot x^\top = s^\top \implies$

$$S_1 := \left\{ \sum_{j=1}^n h_{i,j} x_j + s_i \mid i = 1, \dots, n-k \right\};$$

- finite field equations: $x \in \mathbb{F}_2^n \implies$

$$S_2 := \{x_j^2 + x_j \mid j = 1, \dots, n\};$$

- weight constraint encoding: $\text{wt}(x) = t \implies$

$$S_3 := \{e_{n,2^i}(x) + t_i \mid i = 0, \dots, r\}, \quad r = \lfloor \log_2 n \rfloor.$$

$$S := S_1 \cup S_2 \cup S_3$$

$\leadsto$ the solutions of $S = 0$ are exactly the solutions of the ESDP.

Complexity of the new model – Degree of regularity

How hard is it to solve this polynomial system? $\leadsto d_{\text{sol}}(S)$

Complexity of the new model – Degree of regularity

How hard is it to solve this polynomial system? $\leadsto d_{\text{sol}}(S)$

Theorem (Salizzoni, 2023)

Let $F = \{f_1, \dots, f_j\}$ be a family of polynomials in R , then

$$d_{\text{sol}}(F) \leq \max\{d_{\text{reg}}(F) + 1, \deg(f_1), \dots, \deg(f_j)\}.$$

Complexity of the new model – Degree of regularity

How hard is it to solve this polynomial system? $\leadsto d_{\text{sol}}(S)$

Theorem (Salizzoni, 2023)

Let $F = \{f_1, \dots, f_j\}$ be a family of polynomials in R , then

$$d_{\text{sol}}(F) \leq \max\{d_{\text{reg}}(F) + 1, \deg(f_1), \dots, \deg(f_j)\}.$$

- ▶ $f = x^3 + xyz + y^2 + z + 1 \implies f^{\text{top}} := x^3 + xyz \cancel{+ y^2} \cancel{+ z} \cancel{+ 1}$;
- ▶ $(F^{\text{top}}) = (f_1^{\text{top}}, \dots, f_j^{\text{top}})$;
- ▶ R_d is the set of homogeneous polynomials of degree d of R ;
- ▶ $(F^{\text{top}})_d := (F^{\text{top}}) \cap R_d$.

$$d_{\text{reg}}(F) := \min\{d \in \mathbb{N} \mid (F^{\text{top}})_d = R_d\}.$$

Complexity of the new model – Degree of regularity

How hard is it to solve this polynomial system? $\leadsto d_{\text{sol}}(S)$

Theorem (Salizzoni, 2023)

Let $F = \{f_1, \dots, f_j\}$ be a family of polynomials in R , then

$$d_{\text{sol}}(F) \leq \max\{d_{\text{reg}}(F) + 1, \deg(f_1), \dots, \deg(f_j)\}.$$

- ▶ $f = x^3 + xyz + y^2 + z + 1 \implies f^{\text{top}} := x^3 + xyz \cancel{+ y^2} \cancel{+ z} \cancel{+ 1}$;
- ▶ $(F^{\text{top}}) = (f_1^{\text{top}}, \dots, f_j^{\text{top}})$;
- ▶ R_d is the set of homogeneous polynomials of degree d of R ;
- ▶ $(F^{\text{top}})_d := (F^{\text{top}}) \cap R_d$.

$$d_{\text{reg}}(F) := \min\{d \in \mathbb{N} \mid (F^{\text{top}})_d = R_d\}.$$

$$(F^{\text{top}}) = (F^{\text{top}})_0 \oplus (F^{\text{top}})_1 \oplus \dots \oplus (F^{\text{top}})_{d-1} \oplus (F^{\text{top}})_d \oplus (F^{\text{top}})_{d+1} \oplus \dots$$

Complexity of the new model – Degree of regularity

How hard is it to solve this polynomial system? $\leadsto d_{\text{sol}}(S)$

Theorem (Salizzoni, 2023)

Let $F = \{f_1, \dots, f_j\}$ be a family of polynomials in R , then

$$d_{\text{sol}}(F) \leq \max\{d_{\text{reg}}(F) + 1, \deg(f_1), \dots, \deg(f_j)\}.$$

- ▶ $f = x^3 + xyz + y^2 + z + 1 \implies f^{\text{top}} := x^3 + xyz \cancel{+ y^2} \cancel{+ z} \cancel{+ 1}$;
- ▶ $(F^{\text{top}}) = (f_1^{\text{top}}, \dots, f_j^{\text{top}})$;
- ▶ R_d is the set of homogeneous polynomials of degree d of R ;
- ▶ $(F^{\text{top}})_d := (F^{\text{top}}) \cap R_d$.

$$d_{\text{reg}}(F) := \min\{d \in \mathbb{N} \mid (F^{\text{top}})_d = R_d\}.$$

$$(F^{\text{top}}) = (F^{\text{top}})_0 \oplus (F^{\text{top}})_1 \oplus \dots \oplus (F^{\text{top}})_{d-1} \oplus R_d \oplus R_{d+1} \oplus \dots$$

Complexity of the new model – $d_{\text{reg}}(I)$

$$(S^{\text{top}}) = \left(\sum_{j=1}^n h_{1,j} x_j, \dots, \sum_{j=1}^n h_{n-k,j} x_j, x_1^2, \dots, x_n^2, e_{n,1}(x), \dots, e_{n,2^r}(x) \right).$$

Complexity of the new model – $d_{\text{reg}}(I)$

$$(S^{\text{top}}) = \left(\sum_{j=1}^n h_{1,j} x_j, \dots, \sum_{j=1}^n h_{n-k,j} x_j, x_1^2, \dots, x_n^2, e_{n,1}(x), \dots, e_{n,2^r}(x) \right).$$

$$I := (x_1^2, \dots, x_n^2, e_{n,1}(x), \dots, e_{n,2^r}(x)) \implies d_{\text{reg}}(S) \leq d_{\text{reg}}(I).$$

Complexity of the new model – $d_{\text{reg}}(I)$

$$(S^{\text{top}}) = \left(\sum_{j=1}^n h_{1,j} x_j, \dots, \sum_{j=1}^n h_{n-k,j} x_j, x_1^2, \dots, x_n^2, e_{n,1}(x), \dots, e_{n,2^r}(x) \right).$$

$$I := (x_1^2, \dots, x_n^2, e_{n,1}(x), \dots, e_{n,2^r}(x)) \implies d_{\text{reg}}(S) \leq d_{\text{reg}}(I).$$

A lot of elementary symmetric polynomials belong to I :

Step 0	$e_{n,1}$	$e_{n,2}$	$e_{n,3}$	$\dots$	$e_{n,n-2}$	$e_{n,n-1}$	$e_{n,n}$	$\in I$
Step 1	/	$e_{n-1,2}$	$e_{n-1,3}$	$\dots$	$e_{n-1,n-2}$	$e_{n-1,n-1}$	/	$\in I$
Step 2	/	/	$e_{n-2,3}$	$\dots$	$e_{n-2,n-2}$	/	/	$\in I$
$\vdots$	/	/	/	$\vdots$	/	/	/	$\in I$

Complexity of the new model – $d_{\text{reg}}(S)$

- Final step: $e_{\lfloor \frac{n}{2} \rfloor + 1, \lfloor \frac{n}{2} \rfloor + 1} = x_1 \cdots x_{\lfloor \frac{n}{2} \rfloor + 1} \in I$.

Complexity of the new model – $d_{\text{reg}}(S)$

- ▶ Final step: $e_{\lfloor \frac{n}{2} \rfloor + 1, \lfloor \frac{n}{2} \rfloor + 1} = x_1 \cdots x_{\lfloor \frac{n}{2} \rfloor + 1} \in I$.
- ▶ By symmetry, all the monomials of degree $\lfloor \frac{n}{2} \rfloor + 1$ belong to I .

Complexity of the new model – $d_{\text{reg}}(S)$

- ▶ Final step: $e_{\lfloor \frac{n}{2} \rfloor + 1, \lfloor \frac{n}{2} \rfloor + 1} = x_1 \cdots x_{\lfloor \frac{n}{2} \rfloor + 1} \in I$.
- ▶ By symmetry, all the monomials of degree $\lfloor \frac{n}{2} \rfloor + 1$ belong to I .

$$d_{\text{reg}}(I) \leq \left\lfloor \frac{n}{2} \right\rfloor + 1 \implies d_{\text{reg}}(S) \leq \left\lfloor \frac{n}{2} \right\rfloor + 1.$$

Complexity of the new model – $d_{\text{reg}}(S)$

- ▶ Final step: $e_{\lfloor \frac{n}{2} \rfloor + 1, \lfloor \frac{n}{2} \rfloor + 1} = x_1 \cdots x_{\lfloor \frac{n}{2} \rfloor + 1} \in I$.
- ▶ By symmetry, all the monomials of degree $\lfloor \frac{n}{2} \rfloor + 1$ belong to I .

$$d_{\text{reg}}(I) = \left\lfloor \frac{n}{2} \right\rfloor + 1 \implies d_{\text{reg}}(S) \leq \left\lfloor \frac{n}{2} \right\rfloor + 1.$$

Complexity of the new model – $d_{\text{reg}}(S)$

- ▶ Final step: $e_{\lfloor \frac{n}{2} \rfloor + 1, \lfloor \frac{n}{2} \rfloor + 1} = x_1 \cdots x_{\lfloor \frac{n}{2} \rfloor + 1} \in I$.
- ▶ By symmetry, all the monomials of degree $\lfloor \frac{n}{2} \rfloor + 1$ belong to I .

$$d_{\text{reg}}(I) = \left\lfloor \frac{n}{2} \right\rfloor + 1 \implies d_{\text{reg}}(S) \leq \left\lfloor \frac{n}{2} \right\rfloor + 1.$$

But the degrees are high: $d_{\text{sol}}(S) \leq \max \left\{ d_{\text{reg}}(S) + 1, \max_{f \in S} \deg(f) \right\}$

$$\implies d_{\text{sol}}(S) \leq \begin{cases} 2^r + 1 & \text{if } n = 2^{r+1} - 2 \text{ or } n = 2^{r+1} - 1 \\ 2^r & \text{if } r \geq 2 \text{ and } 2^r \leq n \leq 2^{r+1} - 3, \end{cases}$$

where $r = \lfloor \log_2 n \rfloor$.

A further improvement – Model variant

We can do better, we did not even use $\mathbf{H}$...

$$\mathbf{H} = (\mathbf{L} \mid \mathbf{I}_{n-k}) = \left(\begin{array}{ccc|ccc} & & & x_{k+1} & \cdots & x_n \\ \cdots \ell_1 \cdots & 1 & \cdots & 0 \\ & \vdots & \ddots & \vdots \\ \cdots \ell_{n-k} \cdots & 0 & \cdots & 1 \end{array} \right)$$

A further improvement – Model variant

We can do better, we did not even use $\mathbf{H}$...

$$\mathbf{H} = (\mathbf{L} \mid \mathbf{I}_{n-k}) = \left(\begin{array}{ccc|ccc} & & & x_{k+1} & \cdots & x_n \\ \cdots \ell_1 \cdots & 1 & \cdots & 0 \\ & \vdots & \ddots & \vdots \\ \cdots \ell_{n-k} \cdots & 0 & \cdots & 1 \end{array} \right)$$

The substitution is still useless if we do not lower the degrees ☹

A further improvement – Model variant

We can do better, we did not even use H ...

$$H = (L \mid I_{n-k}) = \left(\begin{array}{ccc|ccc} & & & x_{k+1} & \cdots & x_n \\ \cdots \ell_1 \cdots & 1 & \cdots & 0 \\ & \vdots & \ddots & \vdots \\ \cdots \ell_{n-k} \cdots & 0 & \cdots & 1 \end{array} \right)$$

The substitution is still useless if we do not lower the degrees ☹

But we can **remove** the highest degree equation!

$$S'_3 := \{e_{n,2^i}(x) + t_i \mid i = 0, \dots, r-1\}.$$

We lose control on the last bit of $\text{wt}(x)$, but for many choices of t it is determined $\leadsto$ the model variant S' works!

Complexity of the model variant $S' = 0$

$$J := (x_1^2, \dots, x_n^2, e_{n,1}(x), \dots, e_{n,2^{r-1}}(x)) .$$

Complexity of the model variant $S' = 0$

$$J := (x_1^2, \dots, x_n^2, e_{n,1}(x), \dots, e_{n,2^r-1}(x)).$$

Before applying the substitution, we have that, modulo $x_1^2, \dots, x_n^2$,

$$J = (e_{k,j}(x_1, \dots, x_k) + e_{n-k,j}(x_{k+1}, \dots, x_n) \mid j = 1, \dots, 2^r - 1).$$

Complexity of the model variant $S' = 0$

$$J := (x_1^2, \dots, x_n^2, e_{n,1}(x), \dots, e_{n,2^r-1}(x)).$$

Before applying the substitution, we have that, modulo $x_1^2, \dots, x_n^2$,

$$J = (e_{k,j}(x_1, \dots, x_k) + e_{n-k,j}(x_{k+1}, \dots, x_n) \mid j = 1, \dots, 2^r - 1).$$

Applying the substitution from $\mathbf{H} = (\mathbf{L} \mid \mathbf{I}_{n-k})$

$$x_{k+1} = \ell_1(x_1, \dots, x_k), \dots, x_n = \ell_{n-k}(x_1, \dots, x_k),$$

we get

$$J = (e_{k,j}(x_1, \dots, x_k) + e_{n-k,j}(\ell_1, \dots, \ell_{n-k}) \mid j = 1, \dots, 2^r - 1)$$

modulo $x_1^2, \dots, x_k^2$.

The substitution kicks in

The coefficient of any squarefree monomial of $e_{n-k,j}(\ell_1, \dots, \ell_{n-k})$ is the sum of certain minors of $\mathbf{L}$ of order j .

The substitution kicks in

The coefficient of any squarefree monomial of $e_{n-k,j}(\ell_1, \dots, \ell_{n-k})$ is the sum of certain **minors of L of order j** .

$$j > \text{rk}(L) \implies e_{n-k,j}(\ell) \equiv 0 \pmod{x_1^2, \dots, x_k^2}.$$

The substitution kicks in

The coefficient of any squarefree monomial of $e_{n-k,j}(\ell_1, \dots, \ell_{n-k})$ is the sum of certain minors of $\mathbf{L}$ of order j .

$$j > \text{rk}(\mathbf{L}) \implies e_{n-k,j}(\ell) \equiv 0 \pmod{x_1^2, \dots, x_k^2}.$$

Therefore, modulo $x_1^2, \dots, x_k^2$,

$$J = (e_{k,j}(x) + e_{n-k,j}(\ell) \mid 1 \leq j \leq \text{rk}(\mathbf{L})) + (e_{k,j}(x) \mid \text{rk}(\mathbf{L}) < j \leq 2^r - 1)$$

$\leadsto$ now we have some "isolated" consecutive $e_{k,j}(x)$!

Bound on the solving degree of the model variant S'

We can now apply the same idea as before ☺ $\leadsto$ bound on $d_{\text{reg}}(J)$.

This bound implies

$$d_{\text{sol}}(S') \leq \begin{cases} 2^r + 2 & \text{if } n = 2^{r+1} - 1, k \geq 2^r, \\ & \text{and } \text{rk}(\mathbf{L}) = n - k, \\ \max \left\{ \left\lfloor \frac{k + \text{rk}(\mathbf{L})}{2} \right\rfloor + 2, 2^{r-1} \right\} & \text{otherwise.} \end{cases}$$

$\implies$ explicit **dependence** on the instance of the ESDP!

The rank of the matrix $\mathbf{L}$

How to choose a good $\mathbf{L}$? Many options for $\mathbf{H} = (\mathbf{L} \mid \mathbf{I}_{n-k}) \dots$

$$\mathbf{H} = \left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{array} \right) \xrightarrow[\begin{smallmatrix} R_1 \leftrightarrow R_1 + R_2 \\ C_1 \leftrightarrow C_4 \end{smallmatrix}]{\quad} \left(\begin{array}{cc|cc} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{array} \right) = \mathbf{H}'$$

$\implies \text{rk}(\mathbf{L})$ is not a code invariant.

The rank of the matrix $\mathbf{L}$

How to choose a good $\mathbf{L}$? Many options for $\mathbf{H} = (\mathbf{L} \mid \mathbf{I}_{n-k}) \dots$

$$\mathbf{H} = \left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{array} \right) \xrightarrow[R_1 \leftrightarrow R_1 + R_2]{C_1 \leftrightarrow C_4} \left(\begin{array}{cc|cc} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{array} \right) = \mathbf{H}'$$

$\implies \text{rk}(\mathbf{L})$ is not a code invariant.

If $d(\mathbf{C}) > k$, then any matrix $\mathbf{L}$ is full rank.

The rank of the matrix $\mathbf{L}$

How to choose a good $\mathbf{L}$? Many options for $\mathbf{H} = (\mathbf{L} \mid \mathbf{I}_{n-k}) \dots$

$$\mathbf{H} = \left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{array} \right) \xrightarrow[R_1 \leftrightarrow R_1 + R_2]{C_1 \leftrightarrow C_4} \left(\begin{array}{cc|cc} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{array} \right) = \mathbf{H}'$$

$\implies \text{rk}(\mathbf{L})$ is not a code invariant.

If $d(\mathbf{C}) > k$, then any matrix $\mathbf{L}$ is full rank.

What if $d(\mathbf{C}) \leq k$?

The rank of the matrix $\mathbf{L}$

How to choose a good $\mathbf{L}$? Many options for $\mathbf{H} = (\mathbf{L} \mid \mathbf{I}_{n-k}) \dots$

$$\mathbf{H} = \left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{array} \right) \xrightarrow[\begin{smallmatrix} R_1 \leftrightarrow R_1 + R_2 \\ C_1 \leftrightarrow C_4 \end{smallmatrix}]{\begin{smallmatrix} C_1 \leftrightarrow C_4 \\ R_1 \leftrightarrow R_1 + R_2 \end{smallmatrix}} \left(\begin{array}{cc|cc} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{array} \right) = \mathbf{H}'$$

$\implies \text{rk}(\mathbf{L})$ is not a code invariant.

If $d(\mathbf{C}) > k$, then any matrix $\mathbf{L}$ is full rank.

What if $d(\mathbf{C}) \leq k$? $\leadsto$ **Generalized Hamming weights:**

- ▶ for a codeword $c \in \mathbf{C}$, $\text{supp}(c) := \{i \in \{1, \dots, n\} \mid c_i \neq 0\}$;
- ▶ for a subcode $\mathbf{D} \leq \mathbf{C}$, $\text{supp}(\mathbf{D}) := \bigcup_{x \in \mathbf{D}} \text{supp}(x)$

$$d_i(\mathbf{C}) := \min\{|\text{supp}(\mathbf{D})| \mid \mathbf{D} \leq \mathbf{C}, \dim(\mathbf{D}) = i\}, \quad 1 \leq i \leq k.$$

Generalized Hamming weights and $\text{rk}(\mathbf{L})$

- ▶ *Minimum distance*: $d_1(\mathbf{C}) = d(\mathbf{C})$;
- ▶ *Monotonicity*: $1 \leq d_1(\mathbf{C}) < d_2(\mathbf{C}) < \dots < d_k(\mathbf{C}) \leq n$.

Generalized Hamming weights and $\text{rk}(\mathbf{L})$

- ▶ *Minimum distance*: $d_1(\mathbf{C}) = d(\mathbf{C})$;
- ▶ *Monotonicity*: $1 \leq d_1(\mathbf{C}) < d_2(\mathbf{C}) < \dots < d_k(\mathbf{C}) \leq n$.

If $d(\mathbf{C}) \leq k$, it makes sense to ask which is $\max\{i \mid d_i(\mathbf{C}) \leq k\}$.

Generalized Hamming weights and $\text{rk}(\mathbf{L})$

- ▶ *Minimum distance*: $d_1(\mathbf{C}) = d(\mathbf{C})$;
- ▶ *Monotonicity*: $1 \leq d_1(\mathbf{C}) < d_2(\mathbf{C}) < \dots < d_k(\mathbf{C}) \leq n$.

If $d(\mathbf{C}) \leq k$, it makes sense to ask which is $\max\{i \mid d_i(\mathbf{C}) \leq k\}$.

$$\text{rk}(\mathbf{L}) \geq k - \max\{i \in \{1, \dots, k\} \mid d_i(\mathbf{C}) \leq k\}.$$

$\leadsto$ explicit relationship between $\text{rk}(\mathbf{L})$ and some invariants of $\mathbf{C}$.

Generalized Hamming weights and $\text{rk}(\mathbf{L})$

- ▶ *Minimum distance*: $d_1(\mathbf{C}) = d(\mathbf{C})$;
- ▶ *Monotonicity*: $1 \leq d_1(\mathbf{C}) < d_2(\mathbf{C}) < \dots < d_k(\mathbf{C}) \leq n$.

If $d(\mathbf{C}) \leq k$, it makes sense to ask which is $\max\{i \mid d_i(\mathbf{C}) \leq k\}$.

$$\text{rk}(\mathbf{L}) \geq k - \max\{i \in \{1, \dots, k\} \mid d_i(\mathbf{C}) \leq k\}.$$

$\leadsto$ explicit relationship between $\text{rk}(\mathbf{L})$ and some invariants of $\mathbf{C}$.

Thanks! Gracie!

Other cases - BSDP and $q > 2$

- Bounded Syndrome Decoding Problem:

$$\text{wt}(x) \leq t \iff e_{n,j}(x) = 0 \quad \forall j = t+1, \dots, n$$

$$d_{\text{reg}}(S_B) \leq \left\lfloor \frac{n+t}{2} \right\rfloor + 1.$$

Other cases - BSDP and $q > 2$

- ▶ Bounded Syndrome Decoding Problem:

$$\text{wt}(x) \leq t \iff e_{n,j}(x) = 0 \quad \forall j = t+1, \dots, n$$

$$d_{\text{reg}}(S_B) \leq \left\lfloor \frac{n+t}{2} \right\rfloor + 1.$$

- ▶ Field of larger size ($q > 2$):

- ESDP: variables $\{z_i\}_{i=1}^n$ and equations $\{x_i^{q-1} - z_i \mid i = 1, \dots, n\}$

$$d_{\text{reg}}(S^q) \leq k(q-2) + \left\lfloor \frac{n}{2} \right\rfloor + 1.$$

- BSDP: "almost" as in the binary case

$$d_{\text{reg}}(S_B^q) \leq k(q-1) + 1.$$

► Regular Syndrome Decoding Problem:

$\text{wt}(x) = t \leadsto x = (y_1 \parallel \cdots \parallel y_t)$, where $y_\ell \in \mathbb{F}_q^{\frac{n}{t}}$ and $\text{wt}(y_\ell) = 1$.

In the binary case:

$$d_{\text{reg}}(S_R) \leq \left\lfloor \frac{n}{2} \right\rfloor + 1,$$

and therefore

$$d_{\text{sol}}(S_R) \leq \left\lfloor \frac{n}{2} \right\rfloor + 2.$$

Solutions of $S'_3 = 0$

$$S'_3 := \{e_{n,2^i}(x) + t_i \mid i = 0, \dots, r-1\}$$

The solutions of $S'_3 = 0$ are exactly

$$\left\{ \begin{array}{ll} \text{the vectors of weight } t \text{ or } t + 2^r & \text{if } 0 \leq t \leq n - 2^r \\ \text{the vectors of weight } t & \text{if } n - 2^r + 1 \leq t \leq 2^r - 1 \\ \text{the vectors of weight } t \text{ or } t - 2^r & \text{if } 2^r \leq t \leq n. \end{array} \right.$$

