=: Explicit constructions of Codes-I :=

[Goal: Constructing asymptotically good q-ary code family]

1. Hamming Code: $\forall\ k \in \mathbb{Z}_{>0}$,

a. $C_{H,k}$: $[2^k-1,\ 2^k-k-1,\ 3]_2$ code over $\mathbb{F}_2$.

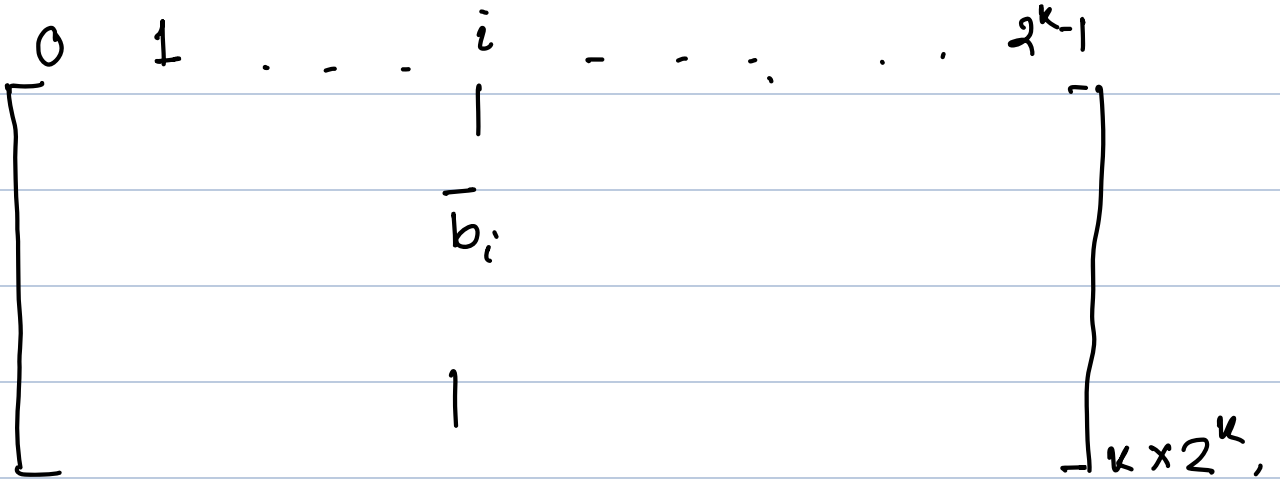
Describe with respect to parity matrix.

for block length n, dimension $n-\log n-1$,

b. $C_{H,k}^{\perp}$: $[2^k-1,\ k,\ 2^{k-1}]_2$ code.

3. Hadamard Code: $\forall\ k \in \mathbb{Z}_{>0}$,

$C_{Had,k}$: Generator matrix is the same as the generator matrix of $C_{H,k}^{\perp}$ with an added column of all zeroes.

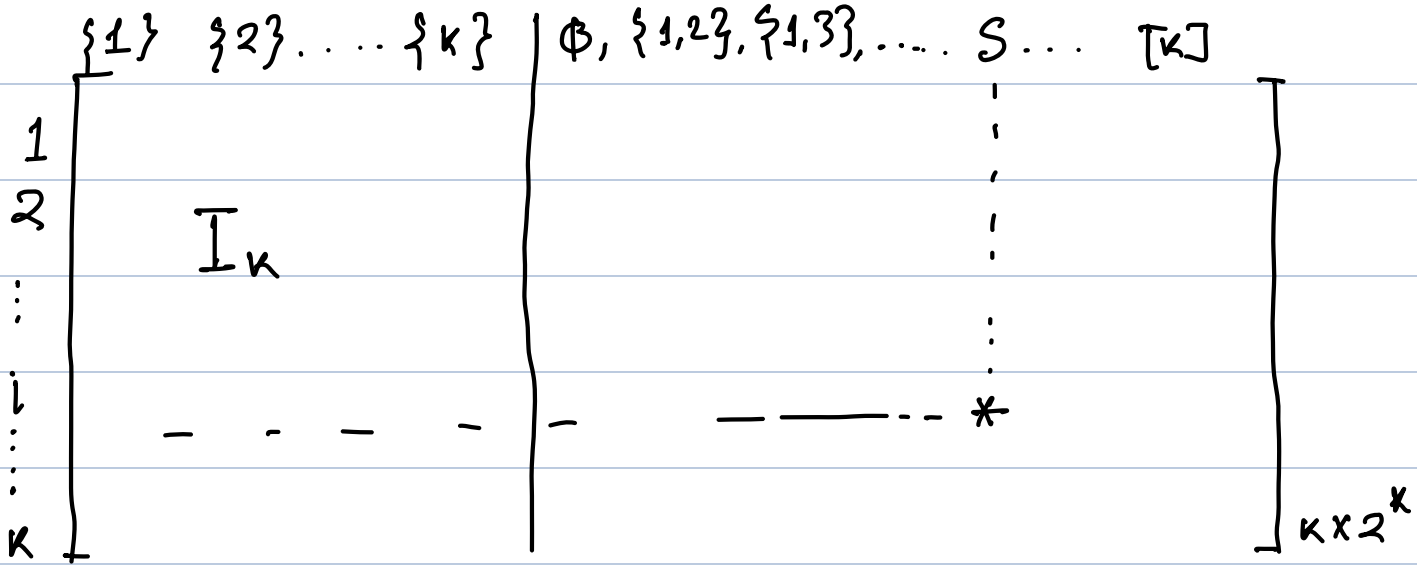


where $\bar{b}_i$ is the k-bit binary representation of the integer i.

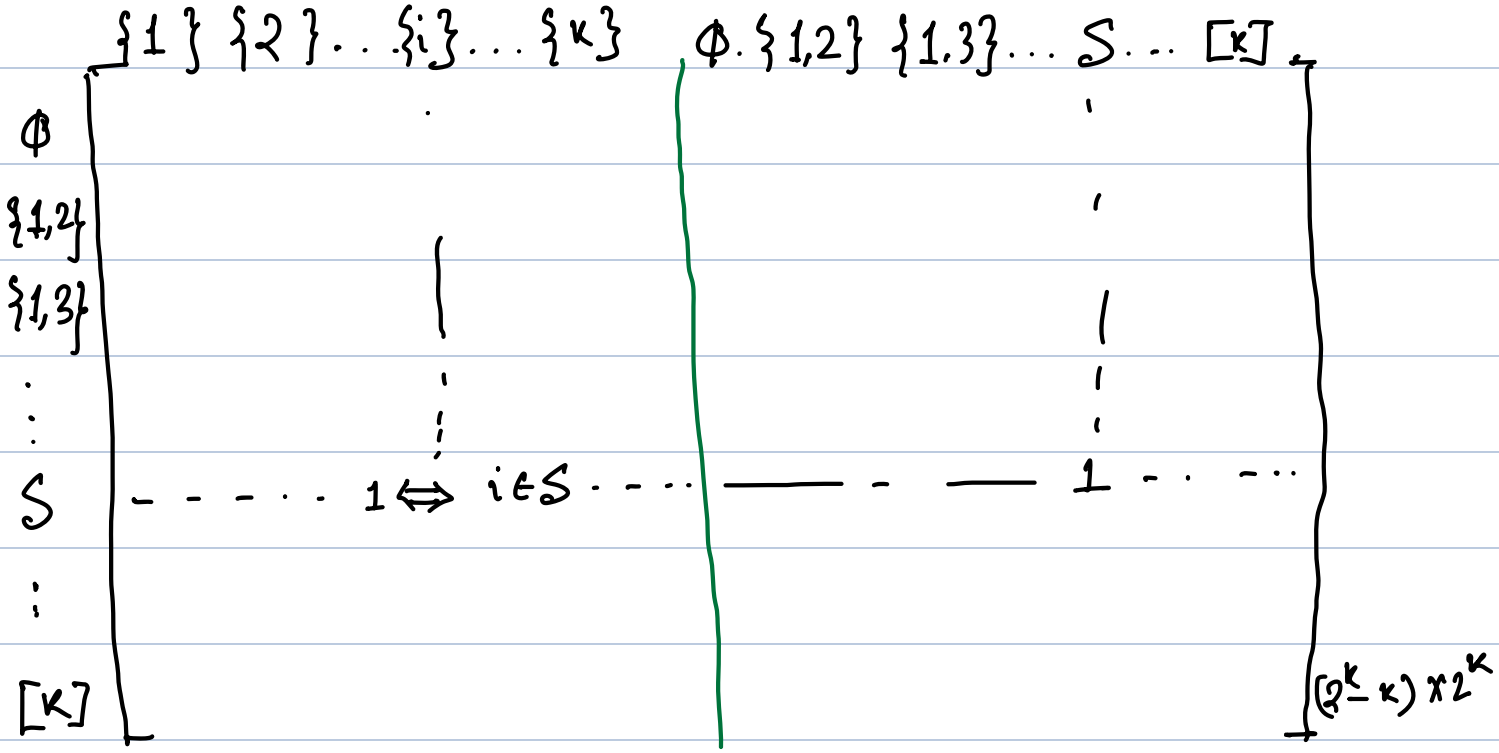
$C_{Had,k}$: $[2^k, k, 2^{k-1}]_2$ code :

[Proof is the same as $C^{\perp}_{H,k}$]

Parity Matrix for $C_{Had,k}$:



$*_i = 1$ iff $i \in S$.



relative distance $= \frac{2^{k-1}}{2^k} = 1/2$, but rate $= \frac{k}{2^k}$

In terms of codeword length.

rel. dist $= \frac{n/2}{n} = 1/2$, but rate $= \frac{\log n}{n} \to 0$ as $n \to \infty$

Reed-Solomon Codes: $\mathbb{F}_q$ is a finite field.

choose $n, k \in \mathbb{Z}_{\geq 0}$ s.t. $k \leq n \leq q$.

$\alpha_1, \alpha_2, \ldots, \alpha_n$: n-distinct elements from $\mathbb{F}_q$.

Encoding function: RS: $\mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n$ as follows.

message $m \in \mathbb{F}_q^k$ can be seen as $(m_0, \ldots, m_{k-1})$ with $m_i \in \mathbb{F}_q$.

then $m \longmapsto$ degree $(k-1)$ poly $f_m(X)$ over $\mathbb{F}_q$ as

$$f_m(X) = m_0 + m_1 X + m_2 X^2 + \cdots + m_{k-1} X^{k-1} \quad \cdots\cdots \text{(Eq. 2)}$$

$$RS(m) = \left(f_m(\alpha_1), f_m(\alpha_2), \ldots, f_m(\alpha_n)\right).$$

A special case of RS code is when $n = q-1$ with the set of evaluation points are $\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$.

Example: $[3, 2]_3$ RS Codes.

$(0,0,0)$ $(1,1,1)$ $(2\ 2\ 2)$ $(0,1,2)$, $(1,2,0)$ $(2,0,1)$

$\downarrow$ 0 $\quad$ $\downarrow$ 1 $\quad$ $\downarrow$ 2 $\quad$ $\downarrow$ x $\quad$ $\downarrow$ $x+1$ $\quad$ $\downarrow$ $x+2$

$(0,2,1) \to 2x \qquad (1,0,2) \to 2x+1 \qquad (2,1,0) \to 2x+2$

Claim 1: RS codes are linear codes.

Proof Idea:

- All polynomials of degree $< k$ form a vector space.

$\Rightarrow \quad \forall\ m_1, m_2 \in \mathbb{F}_q^k$

$$m_i \xrightarrow[\text{Eq. 2}]{} f_{m_i}(x) \text{ for } i = 1, 2 \text{ s.t. } \deg(f_{m_i}(x)) < k$$

$$f_{m_1}(x) + f_{m_2}(x) = f_{m_1 + m_2}(x)$$

$$a f_{m_1}(x) = f_{a m_1}(x) \quad \forall\ a \in \mathbb{F}_q$$

$\Rightarrow \quad \forall\ m_1, m_2 \in \mathbb{F}_q^k$ & $a \in \mathbb{F}_q$

$$RS(m_1) + RS(m_2) = RS(m_1 + m_2)$$

$$a \cdot RS(m_1) = RS(a \cdot m_1)$$

$\Rightarrow$ RS is an $[n, k]_q$ code.

Claim 2: RS is an $[n, k, n-k+1]$ code

Remark: RS-code achieves Singleton bound.

Proof Idea: Need to prove that $\forall\, m \in \mathbb{F}_q^k \setminus \{0\}$,

$$wt(RS(m)) \geq n-k+1$$

$\forall\, m \in \mathbb{F}_q^k \setminus \{0\}$.

$$m \xrightarrow{\text{RS-Encoding}} (f_m(\alpha_1), f_m(\alpha_2), \ldots, f_m(\alpha_n))$$

$\&$ $f_m(X)$ is non-zero polynomial

Proposition 1: For any non-zero polynomial $f(X)$, over a field F, of degree $\leq t$ has atmost t roots.

Proof Idea: Proof by induction on t, starting from $t=0$. [Explain].

1.

Proposition 1 $\Rightarrow \forall\, m \in \mathbb{F}_q^k \setminus \{0\}$, $wt(RS(m)) \geq n-k+1$

Alternate view: $\forall\, m_1, m_2 \in \mathbb{F}_q^k$ with $m_1 \neq m_2$

$$\begin{aligned}
\Delta(RS(m_1), RS(m_2)) &= \#\{ i \in [n] \mid f_{m_1}(\alpha_i) \neq f_{m_2}(\alpha_i) \} \\
&= n - \#\{ i \in [n] \mid f_{m_1}(\alpha_i) = f_{m_2}(\alpha_i) \}. \\
&= n - \#\{ i \in [n] \mid f_{m_1}(\alpha_i) - f_{m_2}(\alpha_i) = 0 \} \\
&= n - \#\{ i \in [n] \mid f_{m_1 - m_2}(\alpha_i) = 0 \}. \\
&\geq n - (k-1). \quad \text{[proposition 1]} \\
&= n-k+1. \qquad \square
\end{aligned}$$

This combined with Singleton bound ⇒

$\text{dist}(\text{RS-codes}) = n-k+1$.

Q1: Can we construct an explicit codewords of $wt = n-k+1$.? [Explain]

Generator matrix: Find $m_1, m_2, \ldots, m_k \in \mathbb{F}_q^k$ s.t. $RS(m_1), RS(m_2), \ldots, RS(m_k)$ forms a basis for RS-codes.

- Nice basis for polynomials over $\mathbb{F}_q$ of degree $< k$,
  $1, x, x^2, \ldots, x^{k-1}$: [Monomial Basis.
- Generator matrix: i^{th} row is the evaluation of x^i at $(\alpha_1, \ldots, \alpha_n)$

⇒

$$
\begin{array}{c}
 \\
1 \\
x \\
x^2 \\
\vdots \\
x^i \\
\vdots \\
x^{k-1}
\end{array}
\begin{array}{c}
\begin{array}{cccccccc} \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_j & \cdots & & \alpha_n \end{array} \\
\left[\begin{array}{cccccccc}
1 & 1 & 1 & \cdots & 1 & \cdots & & 1 \\
\alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_j & \cdots & & \alpha_n \\
\alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \cdots & \alpha_j^2 & \cdots & & \alpha_n^2 \\
\vdots & & & & & & & \\
\alpha_1^i & \alpha_2^i & \alpha_3^i & \cdots & \alpha_j^i & \cdots & & \alpha_n^i \\
\vdots & & & & & & & \\
\alpha_1^{k-1} & \alpha_2^{k-1} & \alpha_3^{k-1} & \cdots & \alpha_j^{k-1} & \cdots & & \alpha_n^{k-1}
\end{array}\right]_{k \times n}
\end{array}
$$

Before discussing Dual of RS-code, we take a slight detour & discuss MDS codes.

Maximum Distance Separable (MDS) code:

Definition: An $(n, k, d)_q$ code is called MDS code if $d = n - k + 1$

Example: Reed-Solomon code is a MDS code.

Notation: $\forall\, S \subseteq [n]$ of $|S| = k$, C_S is the set of all codewords in C projected onto the indices in S.

Proposition 1: Let $C \subseteq \Sigma^n$ be a code of integral dimension k be an MDS code. Then, $\forall\, S \subseteq [n]$ with $|S| = k$

$$|C_S| = q^k$$

[Explain for RS-codes.]

[Explain the general proof].

- Exercise: show that the converse direction of Proposition is also true.]
- Exercise: for any $[n, k]_q$ MDS code C, $C^\perp$ is also an MDS code.
- Exercise: For any generator matrix G of $[n, k]_q$ MDS code, any subset of k-cols of G are linearly independent & vice-versa!

=: Explicit constructions of Codes - II :=

Recap of Last class:

- Definition of Reed-Solomon Codes; $RS(E, k, q)$ for $E \subseteq \mathbb{F}_q$.
- Definition of MDS-Codes; its property as Proposition 1 in the previous lecture.

Today's Lecture:

Proposition 1 in last lecture $\Rightarrow$ Pseudorandom property of MDS Codes!

Explanation: A set $T \subseteq \mathbb{F}_q^n$ is said to be a t-wise independent source if given a uniformly random sample $(X_1, \ldots, X_n) \in T$ and any subset of t variables are uniformly independently random over $\mathbb{F}_q$, i.e., $\forall\ S \subseteq [n]$ with $S = \{i_1, \ldots, i_t\}$

$$(X_{i_1}, X_{i_2}, \ldots, X_{i_t}) \in_r \mathbb{F}_q^t.$$

Trivial observation: $T = \mathbb{F}_q^n$ is t-wise independent source $\forall\ 1 \le t \le n$.

Non trivial observation: $[n, k]_q$ MDS code $\Rightarrow$ k-wise independent source of size q^k.

Exercise: Construct a k-wise independent source $T \subseteq \mathbb{F}_2^n$ of $|T| \le (2k)^k$, i.e., using at most $k(\log_2 n + 1)$ random bits. [More details see Exercise 3.13 & 3.14 of Essential Coding Theory]

Dual of RS-Code:

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \end{bmatrix}_{k \times n} = G \text{ (generator matrix)}$$

Already Discussed Approach:

$$\tilde{G} = \begin{bmatrix} G \\ \hat{G} \end{bmatrix} \quad \begin{matrix} \} k \times n \\ \} n-k \times n \end{matrix}$$

$\Rightarrow \tilde{G}$ is full rank.

Consider $\tilde{G}^{-1} = \begin{bmatrix} H_1 & H_2 \end{bmatrix}$

H_1: $n \times k$, H_2: $n \times n-k$

$\because$ we know that $G \cdot H_2 = 0$

$\Rightarrow H_2^T$ is generator matrix for $RS(k,n,q)^{\perp}$

Q1: Can you describe an "easy" & "meaningful" extension: $G \mapsto \tilde{G}$?

Answer:

$$\begin{bmatrix} 1 & 1 & \cdots & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & & \alpha_j & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & & \alpha_j^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & & \vdots & & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & & \alpha_j^{k-1} & \cdots & \alpha_n^{k-1} \\ \alpha_1^k & \alpha_2^k & & \alpha_j^k & \cdots & \alpha_n^k \\ \vdots & \vdots & & \vdots & & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_j^{n-1} & \cdots & \alpha_n^{n-1} \end{bmatrix}_{n \times n} = \tilde{G}$$

Question: Why full rank? Why meaningful?

[Explain via univariate polynomial Evaluation]. [called Vandermonde Matrix].

Question: What is $\tilde{G}^{-1}$? [use the meaningfulness of $\tilde{G}$]

Answer: U is a set of all univariate polynomials over $\mathbb{F}_q$ of degree $< n$.

U is a vector space.

U has two representations

Coefficient vector

$(c_0, c_1, \ldots, c_{n-1})$

$\downarrow$

$c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$

Basis: $\{1, x, \ldots, x^{n-1}\}$

[Monomial basis]

Evaluation vector.

Fix n distinct points: $\alpha_1, \alpha_2, \ldots, \alpha_n$

$(c_0, \ldots, c_{n-1}) \mapsto f(x) \in U$ s.t.

$(c_0, \ldots, c_{n-1}) = (f(\alpha_1), \ldots, f(\alpha_n))$.

Basis: ?

Lagrange Interpolation polynomial:

$$L_1(x) = (x-\alpha_2)(x-\alpha_3)\cdots(x-\alpha_n)$$

$$L_2(x) = (x-\alpha_1)(x-\alpha_3)(x-\alpha_4)\cdots(x-\alpha_n)$$

$$\vdots$$

$$L_i(x) = (x-\alpha_1)\cdots(x-\alpha_{i-1})(x-\alpha_{i+1})\cdots(x-\alpha_n)$$

$$\vdots$$

Observation: $\Rightarrow \deg(L_i(x)) < n$.

2. For any $(c_1, c_2, \ldots, c_n)$,

$$f(x) = \sum_{i=1}^{n} c_i \frac{L_i(x)}{L_i(\alpha_i)}$$ be the polynomial

s.t. $(f(\alpha_1), \ldots, f(\alpha_n)) = (c_1, \ldots, c_n)$.

[Explain & explain why it is a basis].

$$\left\{ \frac{L_1(x)}{L_1(\alpha_1)}, \frac{L_2(x)}{L_2(\alpha_2)}, \ldots, \frac{L_n(x)}{L_n(\alpha_n)} \right\}$$: another basis

for U s.t. given evaluation vector we get corresponding Polynomial; lets call it Lagrange basis.

Meaningfulness of Vandermonde matrix: Try to view it as basis transformation; monomial basis → Lagarange basis.

$$\begin{array}{c} \\ 1 \\ x \\ x^2 \\ \vdots \\ x^{n-1} \end{array} \begin{array}{c} \begin{array}{cccc} \frac{L_1(x)}{L_1(\alpha_1)} & \frac{L_2(x)}{L_2(\alpha_2)} & \cdots & \frac{L_n(x)}{L_n(\alpha_n)} \end{array} \\ \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \cdots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{bmatrix}_{n \times n} \end{array} = \tilde{A}$$, i.e. i^{th} row becomes coefficients when we write x^i as the linear combination of Lagarange basis.

Given coefficient vector $\bar{c} \in \mathbb{F}_q^n$, $\bar{c} \cdot \tilde{A}$ gives the evaluation vector of the corresponding polynomial.

$\Rightarrow \tilde{A}^{-1}$ should do the inverse operation of it, i.e., Given evaluation vector $\bar{c}$ of a polynomial in U, $\bar{c} \cdot \tilde{A}^{-1}$ should produce the coefficient vector.

$\Rightarrow$

$$\begin{array}{c} \\ \frac{L_1(x)}{L_1(\alpha_1)} \\ \frac{L_2(x)}{L_2(\alpha_2)} \\ \vdots \\ \frac{L_i(x)}{L_i(\alpha_i)} \\ \vdots \\ \frac{L_n(x)}{L_n(\alpha_n)} \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & x & \cdots & x^j & \cdots & x^{n-1} \end{array} \\ \left[\begin{array}{cccccc} & & & \vdots & & \\ & & & \vdots & & \\ & & & \vdots & & \\ \cdots & & & \mathrm{Coeff}_{x^j}\left(\frac{L_i(x)}{L_i(\alpha_i)}\right) & & \\ & & & \vdots & & \\ & & & \vdots & & \end{array}\right] \end{array} = \tilde{G}^{-1}$$

$\Rightarrow$ transpose of the submatrix of $\tilde{G}^{-1}$ formed by columns indexed by $x^k, x^{k+1}, \ldots, x^{n-1}$ forms a parity matrix of $RS(E,k,q)$ with $E=\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$.

More Explicit Description:

$$H: \quad \begin{bmatrix} 1 & 1 & & 1 \\ \alpha_1 & \alpha_2 & & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & & \alpha_n^2 \\ \vdots & \vdots & \cdots & \vdots \\ \alpha_1^{n-k-1} & \alpha_2^{n-k-1} & & \alpha_n^{n-k-1} \end{bmatrix}_{n-k\times n} \begin{array}{l} \\ \\ \\ \cdot L_1(\alpha_1) \\ \\ \\ \end{array} \begin{array}{l} \\ \\ \\ \cdot L_2(\alpha_2) \\ \\ \\ \end{array} \quad \cdots \quad \begin{array}{l} \\ \\ \\ \cdot L_n(\alpha_n) \\ \\ \\ \end{array}$$

is a parity matrix for $RS(E,k,q)$ with $E=\{\alpha_1,\ldots,\alpha_n\}$.

i.e.

$$RS(E,k,q)^{\perp} = \{(c_1\cdot L_1(\alpha_1), c_2\cdot L_2(\alpha_2), \ldots, c_n L_n(\alpha_n)) \mid (c_1,\ldots,c_n) \in RS(E,n-k,q)\}.$$

[For Proof, see Problem sheet]

For $E = \mathbb{F}_q$:

$$RS(E, \kappa, q)^{\perp} = RS(E, n-\kappa, q)$$ [Exercise]

For $E = \mathbb{F}_q^* = \{1, \alpha, \alpha^2, \ldots\ldots, \alpha^{q-2}\}$

$$RS(E, \kappa, q)^{\perp} = \left\{ \left(p(1), p(\alpha), p(\alpha^2) \ldots p(\alpha^n)\right) \mid p(x) \in \mathbb{F}_q[x] \right.$$
$$\left. \text{with } \deg(p(x)) \leq n-\kappa \text{ \& } x \mid p(x) \right\}.$$

[Exercise].