REED-SOLOMON CODES OVER F_q

(q-ary RS codes)

Let α - primitive in F_q

($q = 2^b$, $F_q = \{0,1\}^b$)

Consider LINEAR RS code defined by the check matrix

$$H = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ \vdots & & & & \\ 1 & \alpha^t & \alpha^{2t} & \cdots & \alpha^{t(n-1)} \end{bmatrix}$$

Assume $n < q \Rightarrow \alpha^i \neq \alpha^j$

This RS code has distance $t+2$

$[n, n-t-1, t+2]$ RS codes

$d = r+1$ - OPTIMAL BY SINGLETON B.

These codes require minimal numbers of redundand bits and useful for large q

(e.g. $q = 2^b$, $b = 32$)

For H any $t+1$ columns are linearly independent:

$H = [h_1\ h_2 \ldots\ h_n] \Rightarrow$

$c_1 h_1 \oplus c_2 h_2 \ldots \oplus c_n h_n \neq 0$

FOR ANY $c_1, \ldots, c_n \in F_q$

(At least one $c_i \neq 0$)

EXAMPLE $t=3 \Rightarrow d=4$

$[n, n-3, 4]$ RS codes

Let $q=8$ $(b=3)$ $n=5$

$[5,2,4]$ RS code

$$H=\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 \end{bmatrix}$$

$\alpha = 010$

$P(x) = x^3 \oplus x \oplus 1$

$\alpha^3 = \alpha \oplus 1$

$P(\alpha) = 0$