V7a Reed-Solomon Codes

- Invented by Irving Reed and Gustave Solomon in 1960.

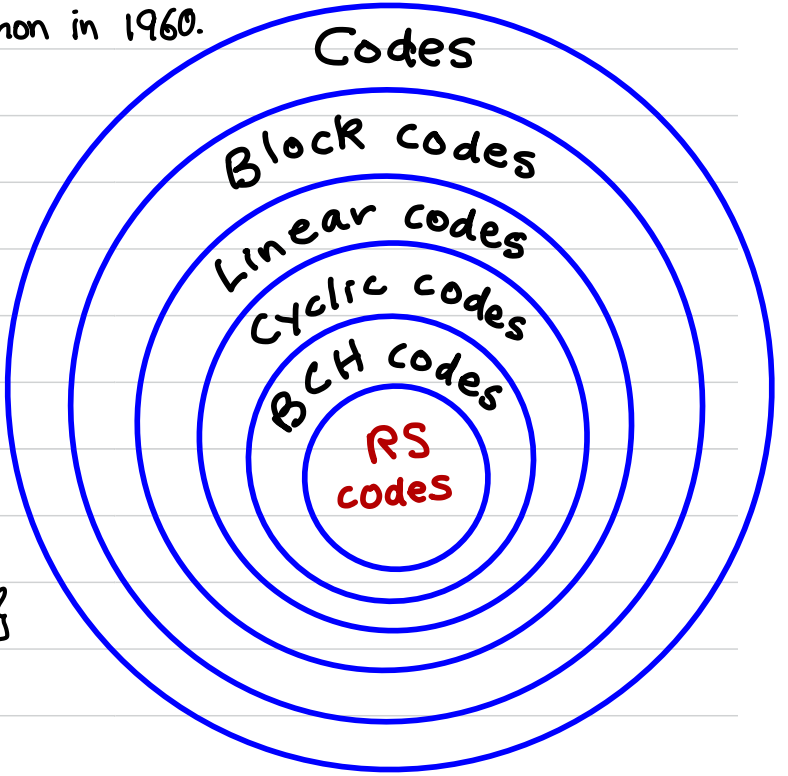
DEFINITION A Reed-Solomon (RS) code is a BCH code of length n over $GF(q)$ where $n \mid (q-1)$.

- **NOTE** Since $q^1 \equiv 1 \pmod{n}$, we have $m=1$.
- **EXAMPLE** Let $q=2^4$ and consider $GF(2^4) = \mathbb{Z}_2[\alpha]/(\alpha^4+\alpha+1)$. Recall that α is a generator of $GF(2^4)^*$. Let $\beta=\alpha^3$. Then $\text{ord}(\beta)=5$, so $q=16$, $n=5$, $m=1$.

Let $g(x) = \text{lcm}\{m_\beta(x), m_{\beta^2}(x), m_{\beta^3}(x)\}$

$= (x-\beta)(x-\beta^2)(x-\beta^3)$

$= x^3 + \alpha^{11}x^2 + \alpha^2 x + \alpha^3.$



EXAMPLE (cont'd)

- Then $g(x)$ is the canonical generator for a $(5,2)$-RS code C over $GF(2^4)$ with $\delta=4$. Since $w(g(x))=4$, we have $d(C)=4$.

- A GM for C is $G = \begin{bmatrix} \alpha^3 & \alpha^2 & \alpha^{11} & 1 & 0 \\ 0 & \alpha^3 & \alpha^2 & \alpha^{11} & 1 \end{bmatrix}_{2\times 5}$.

- Consider the code C' obtained from C by replacing each symbol in codewords in C by its binary representation.

  eg. $(\alpha^3, \alpha^2, \alpha^{11}, 1, 0) \leftrightarrow (0001\ 0010\ 0111\ 1000\ 0000)$.

- It is not difficult to see that C' is closed under addition and scalar multiplication over $\mathbb{Z}_2$. So, C' is a $(20,8)$-binary code.

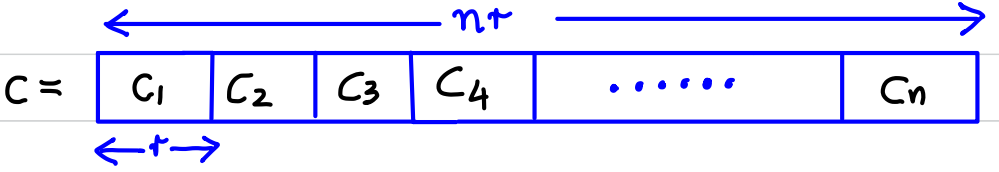
MORE GENERALLY....

- Suppose $n \mid (q-1)$, and let $\beta \in GF(q)$ be an element of order n. Then $m_{\beta^i}(x) = x - \beta^i$ for all i.
- A RS code C of length n over $GF(q)$ with designed distance δ is a BCH code of length n over $GF(q)$ with canonical generator
$$g(x) = (x-\beta^a)(x-\beta^{a+1})(x-\beta^{a+2}) \cdots (x-\beta^{a+\delta-2}) \text{ for some } a.$$
- Since $\deg(g) = \delta - 1$, we have $\omega(g) \leq \delta$, and so $d(C) \leq \delta$. By the BCH bound, $d(C) \geq \delta$. Hence, $\boxed{d(C) = \delta.}$

- Since $\dim(C) = k = n - \deg(g) = n - \delta + 1$, we have $k = n - d + 1$, so $\boxed{d = n - k + 1.}$ Now, $d \leq n - k + 1$ for any (n, k, d)-code. Thus, RS codes are optimal in the sense that, for any fixed n, k, q with $n \mid (q-1)$, they achieve maximum distance among all (n, k)-codes over $GF(q)$.

RS CODES HAVE GOOD (CYCLIC) BURST ERROR CORRECTING CAPABILITY

- Let C be a RS code of length n over $GF(2^r)$ and designed distance δ.
- Consider $c = (c_1, c_2, \ldots, c_n) \in C$, and note that $c_i \in GF(2^r)$.
  Let $e = \lfloor (d-1)/2 \rfloor = \lfloor (n-k)/2 \rfloor$.
- By writing each c_i as a binary vector of length r, we can view c as a binary vector of length nr.



- Now, if c is transmitted and a cyclic burst of length $\leq 1 + (e-1)r$ bits is introduced, then at most e $GF(2^r)$ symbols of c are received incorrectly. Thus, the received word can be decoded correctly.

THEOREM Let C be an (n,k)-RS code over $GF(2^r)$. Then C', the code obtained by replacing each symbol in codewords in C by its r-bit binary representation, is an (nr, kr)-binary code with cyclic burst error correcting capability $t = 1 + \left(\left\lfloor \frac{n-k}{2} \right\rfloor - 1\right) r$.

EXAMPLE Consider $GF(2^8) = \mathbb{Z}_2[\alpha]/(\alpha^8+\alpha^4+\alpha^3+\alpha^2+1)$, so $q=256$. Then $\beta=\alpha$ has order $n=255$. Let $g(x) = \prod_{i=1}^{24} (x-\beta^i)$. Then $g(x)$ is the canonical generator for a $(255, 231, 25)$-RS code C over $GF(2^8)$ with error correcting capability $e=12$. The related code C' is a $(2040, 1848)$-binary code with cyclic burst error correcting capability $t=89$. The code C, and others derived from it, have been widely deployed in practice, including in CDs, DVDs, Blu-rays, and QR codes.

V7b Alternative View of Narrow-Sense RS Codes

- Let $F = GF(q)$, let α be a generator of $GF(q)^*$, and let $2 \le \delta < q$. Let $g(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^3)\cdots(x-\alpha^{\delta-1})$.
  Then $g(x)$ is the canonical generator for a BCH-code C over $GF(q)$ of length $n = q-1$, dimension $k = n-\delta+1$, and distance $d = \delta = n-k+1$.
- C is a narrow-sense RS code.

DEFINITION Let $f \in F[x]$. Then $c(f) = (f(1), f(\alpha), f(\alpha^2), \ldots, f(\alpha^{q-2})) \in V_n(F)$.

DEFINITION Let $D = \{c(f) : f \in F[x], \deg(f) \le k-1\} \subseteq V_n(F)$.

THEOREM (alternative view of RS codes) $C = D$.

PROOF 1) D is a vector space over F. [exercise]

2) **CLAIM** $\dim(D) = k$.

PROOF OF CLAIM Let $f, g \in F[x]$, $\deg(f) \leq k-1$, $\deg(g) \leq k-1$. Suppose $c(f) = c(g)$. Then $f(\alpha^i) = g(\alpha^i)$ for $0 \leq i \leq q-2$, so $(f-g)(\alpha^i) = 0$ for $0 \leq i \leq q-2$. Thus, $f-g$ is a polynomial of degree $\leq k-1$ with $\geq q-1$ roots. But $k < q$ (recall: $k+d = q$). So, we most have $f-g = 0$, so $f = g$.
It follows that $|D| = q^k$, so $\dim(D) = k$. □

PROOF (cont'd)

3) Let's prove that $D \subseteq C$. Let $c(f) \in D$, where $f(x) = \sum_{j=0}^{k-1} f_j x^j$.
Then $c(f) = (f(1), f(\alpha), \ldots, f(\alpha^{q-2})) \Leftrightarrow C_f(x) = \sum_{i=0}^{n-1} f(\alpha^i) x^i$.

Now, for each t, $1 \le t \le \delta - 1$, we have

$$C_f(\alpha^t) = \sum_{i=0}^{n-1} \left(\sum_{j=0}^{k-1} f_j \alpha^{ij} \right) \alpha^{it} = \sum_{j=0}^{k-1} f_j \left(\sum_{i=0}^{n-1} \alpha^{(j+t)i} \right) = \sum_{j=0}^{k-1} f_j \left(\frac{\alpha^{(j+t)n} - 1}{\alpha^{j+t} - 1} \right).$$

Note that $\alpha^{j+t} \neq 1$, since $1 \le j+t \le k-1+\delta-1 = n-1$, so $C_f(\alpha^t) = 0$.
Thus $g(x) \mid C_f(x)$, so $c(f) \in C$. Hence $D \subseteq C$.

4) Since $\dim(C) = \dim(D) = k$, we have $C = D$. □

- Encoding $m = (m_0, m_1, \ldots, m_{k-1}) \in F^k$: Let $f(x) = \sum_{j=0}^{k-1} m_j x^j$. Then $m \mapsto c = c(f)$.

V7C BERLEKAMP-WELCH DECODING ALGORITHM

RECALL $C = \{c(f) = (f(1), f(\alpha), \ldots, f(\alpha^{n-1})) : f \in F[x], \deg(f) \le k-1\}$.

$n = q-1$, $d = n-k+1$, $e = \lfloor (n-k)/2 \rfloor$.

- Suppose $c = c(f)$ is transmitted and r is received. Suppose that $d(r,c) = t \le e$. The objective is to determine c from r.

DEFINITION Let $\tilde{E}(x) = \left[\prod_{\substack{0 \le i \le n-1 \\ c_i \ne r_i}} (x - \alpha^i) \right] x^{e-t}$.

NOTE: $\tilde{E}$ is monic and $\deg(\tilde{E}) = e$.

Let $\tilde{Q}(x) = \tilde{E}(x) f(x)$.

NOTE: $\deg(\tilde{Q}) \le e+k-1$.

THEOREM For all $0 \le i \le n-1$, $r_i \tilde{E}(\alpha^i) = \tilde{Q}(\alpha^i)$.

PROOF If $c_i \ne r_i$, then $\tilde{E}(\alpha^i) = 0$, so $r_i \tilde{E}(\alpha^i) = 0 = \tilde{Q}(\alpha^i)$.

If $c_i = r_i$, then $r_i = f(\alpha^i)$, so $r_i \tilde{E}(\alpha^i) = f(\alpha^i) \tilde{E}(\alpha^i) = \tilde{Q}(\alpha^i)$. □

THEOREM Let $E(x), Q(x) \in F[x]$ with:

(i) E monic, $\deg(E) = e$,

(ii) $\deg(Q) \leq e+k-1$, and

(iii) $r_i E(\alpha^i) = Q(\alpha^i)$ for all $0 \leq i \leq n-1$.

Then $Q(x)/E(x) = \tilde{Q}(x)/\tilde{E}(x) = f(x)$.

PROOF Let $R(x) = \tilde{Q}(x)E(x) - Q(x)\tilde{E}(x)$. Then $\deg(R) \leq 2e+k-1$.

For all $0 \leq i \leq n-1$,

$$R(\alpha^i) = \tilde{Q}(\alpha^i)E(\alpha^i) - Q(\alpha^i)\tilde{E}(\alpha^i) = r_i\tilde{E}(\alpha^i)E(\alpha^i) - r_i E(\alpha^i)\tilde{E}(\alpha^i) = 0.$$

Thus, $R(x)$ has n roots, $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$. But $e = \lfloor (n-k)/2 \rfloor < (n-k+1)/2$, so $\deg(R) \leq 2e+k-1 < (n-k+1)+k-1 = n$.

Hence, we must have $R(x) = 0$, so $\dfrac{Q(x)}{E(x)} = \dfrac{\tilde{Q}(x)}{\tilde{E}(x)} = f(x)$. $\square$

BERLEKAMP-WELCH DECODING (1986)

INPUT: $r = (r_0, r_1, r_2, \ldots, r_{n-1})$.

1. Find $E, Q \in F[x]$ with E monic, $\deg(E) = e$, $\deg(Q) \leq e+k-1$, and $r_i E(\alpha^i) = Q(\alpha^i)$ $\forall 0 \leq i \leq n-1$. If no such E, Q exist, then reject r and STOP.
2. Compute $f(x) = Q(x)/E(x)$. (If $E(x) \nmid Q(x)$, then reject r and STOP.)
3. Compute $c = c(f)$.
4. If $d(r, c) \leq e$ then return(c); else reject r.

Q How to find E and Q?

A Linear algebra!

- There are $2e+k$ variables, the coefficients of E and Q.
- Each condition $r_i E(\alpha^i) = Q(\alpha^i)$ yields one linear equation, so there are n equations.

RUNNING TIME: Step 1 + Step 2 + Step 3 + Step 4 = $O(n^3)$.

$O(n^3)$ $O(n^2)$ $O(n^2)$ $O(n)$

The algorithm is efficient, i.e., polynomial time.

EXAMPLE • $q=11$, $n=10$, $\alpha=2$, $k=4$, $d=n-k+1=7$, $e=\lfloor (n-k)/2 \rfloor = 3$.

• α is a generator of $\mathbb{Z}_{11}^*$:

$\alpha^1=2, \alpha^2=4, \alpha^3=8, \alpha^4=5, \alpha^5=10, \alpha^6=9, \alpha^7=7, \alpha^8=3, \alpha^9=6, \alpha^{10}=1.$

• $C=\{c(f) : f\in \mathbb{Z}_{11}[x], \deg(f)\le 3\}$ is a $(10,4,7)$-RS code over $\mathbb{Z}_{11}$.

• **ENCODING** Let $m=(3,0,7,9) \longleftrightarrow f(x)=3+7x^2+9x^3$.

Then $m \mapsto c=c(f)=(8,4,9,10,5,1,3,1,1,10)$.

• **TRANSMISSION** c is sent, $r=(8,4,0,10,6,1,3,7,1,10)$ is received.

• **DECODING** $E(x)=a_0+a_1x+a_2x^2+x^3$, $a_i\in\mathbb{Z}_{11}$.

$Q(x)=b_0+b_1x+b_2x^2+\cdots+b_6x^6$, $b_i\in\mathbb{Z}_{11}$.

The conditions $r_i E(\alpha^i)=Q(\alpha^i)$, $0\le i\le 9$, yield 10 equations:

i: $r_i a_0 + r_i\alpha^i a_1 + r_i\alpha^{2i} a_2 + \underbrace{r_i\alpha^{3i}}_{t} = b_0+\alpha^i b_1+\alpha^{2i}b_2+\cdots+\alpha^{6i}b_6.$

EXAMPLE (cont'd)

i	a_0	a_1	a_2	t	b_0	b_1	b_2	b_3	b_4	b_5	b_6
0	8	8	8	8	1	1	1	1	1	1	1
1	4	8	5	10	1	2	4	8	5	10	9
2	0	0	0	0	1	4	5	9	3	1	4
3	10	3	2	5	1	8	9	6	4	10	3
4	6	8	7	2	1	5	3	4	9	1	5
5	1	10	1	10	1	10	1	10	1	10	1
6	3	5	1	9	1	9	4	3	5	1	9
7	7	5	2	3	1	7	5	2	3	10	4
8	1	3	9	5	1	3	9	5	4	1	3
9	10	5	8	4	1	6	3	7	9	10	5

- Solve to get $a_0=3, a_1=6, a_2=6, b_0=9, b_1=7, b_2=6, b_3=6, b_4=8, b_5=6, b_6=9$.
- $E(x) = x^3+6x^2+6x+3$.
- $Q(x) = 9x^6+6x^5+8x^4+6x^3+6x^2+7x+9$.
- $Q(x)/E(x) = 9x^3+7x^2+3$.
- $c = (8,4,9,10,5,1,3,1,1,10)$, and $d(r,c)=3$.
- Thus, $m=(3,0,7,9)$.