Reed-Solomon Codes (§17.1, 17.2, 17.3)

These are not hard to write down as cyclic codes, once we have primitive roots in $\mathbb{F}_q$.

THEOREM (Reed-Solomon codes 1960)

Let β in $\mathbb{F}_q$ be a primitive root, and pick $t \leq q-1$.
Then the cyclic code $\mathcal{C} \subset (\mathbb{F}_q)^n$ with blocklength $n = q-1$ having generator polynomial

$$g(x) = (x-\beta)(x-\beta^2)\cdots(x-\beta^{t-2})(x-\beta^{t-1}) \in \mathbb{F}_q[x]$$

is an $[\underset{q-1}{n}, \underset{q-t}{k}, \underset{t}{d}]$ $\mathbb{F}_q$-linear code.

Furthermore, $\tilde{g}(x) = \mathrm{GCD}(g(x), x^{q-1}-1) = g(x)$

$$h(x) = \frac{x^{q-1}-1}{\tilde{g}(x)} = (x-\beta^{t})(x-\beta^{t+1})\cdots(x-\beta^{q-2})(x-\beta^{q-1})$$

$$\mathrm{rate}(\mathcal{C}) = \frac{q-t}{q-1} = 1 - \frac{t-1}{q-1}$$

and $\mathcal{C}$ is MDS, i.e. tight for Singleton's bound:

$$\underbrace{k}_{q-t} = \underbrace{n-(d-1)}_{q-1-(t-1)}$$

EXAMPLE Suppose we want $\mathcal{C}$ to correct up to 4 errors. We need $t = d(\mathcal{C}) = 2\cdot 4+1 = 9$, so want to pick q in $\mathbb{F}_q$ with $t = 9 \le q-1$.

E.g. $q = 11$ works, and is smallest (but could try others such as $q = 13$ or $16 = 2^4$ or $27 = 3^3$, etc.)

Look for a primitive β in $\mathbb{F}_{11}$ $(= \mathbb{Z}/11)$:

e.g. let's test $\beta = 2$

Since $q-1 = 10 = 2^1 \cdot 5^1$, need to check $\beta^{\frac{10}{5}} = 2^{10/5} = 2^2 = 4 \neq 1$

and $\beta^{\frac{10}{2}} = 2^{\frac{10}{2}} = 2^5 = 32 \neq 1$

So we can pick $t = 9$, $t-1 = 8$

$$g(x) = (x-2)(x-2^2)(x-2^3)\cdots(x-2^8)$$
$$= 9+5x+8x^2+3x^3+4x^4+6x^5+10x^6+7x^7+x^8$$

$$h(x) = (x-2^9)(x-2^{10})$$
$$= 6+4x+x^2$$

$$\mathcal{C} = \text{Rowspace}(G) \text{ for } G = \begin{array}{c} \begin{array}{cccccccccc} 1 & x & x^2 & x^3 & & & & & & x^9 \end{array} \\ \begin{bmatrix} 9 & 5 & 8 & 3 & 4 & 6 & 10 & 7 & 1 & 0 \\ 0 & 9 & 5 & 8 & 3 & 4 & 6 & 10 & 7 & 1 \\ & & & \ddots & & & & & & \end{bmatrix} \end{array}$$

$$\mathcal{C}^{\perp} = \text{Rowspace}(H) \text{ for } H = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 4 & 6 \\ 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 4 \\ 4 & 6 & \ddots & & & & & & & \ddots \end{bmatrix}$$

and $\mathcal{C}$ is $[\overset{n}{\underset{q-1}{\underset{\parallel}{10}}}, \overset{k}{\underset{q-t}{\underset{\parallel}{2}}}, \overset{d}{\underset{t}{\underset{\vee}{9}}}]$ with $\text{rate}_q(\mathcal{C}) = 1 - \frac{t-1}{q-1} = 1 - \frac{8}{10} = 1 - \frac{4}{5} = \frac{1}{5}$

EXAMPLE

According to Wikipedia, QR codes use Reed-Solomon codes with $q = 2^8 = 256$ working in $\mathbb{F}_{256} = \mathbb{F}_2[x]/(\underbrace{x^8 + x^4 + x^3 + x^2 + 1}_{f(x)})$

where $\alpha = \bar{x}$ is a primitive root,

that is, $f(x)$ is a primitive irreducible polynomial in $\mathbb{F}_2[x]$.

So they would all have blocklength $n = q-1 = 255$.

However, they vary the choice of t so as to get different levels of error correction.

For example, it mentions as examples two that are

$$\begin{array}{ccc} q-1 & q-t & t \\ \end{array}$$
$$[255, 249, 7] \quad \text{correcting up to } 3 \text{ errors}$$

$$\begin{array}{ccc} q-1 & q-t & t \\ \end{array}$$
$$[255, 233, 23] \quad \text{correcting up to } 11 \text{ errors}$$

THEOREM (Reed-Solomon codes 1960)
Let β in $\mathbb{F}_q$ be a primitive root, and pick $t \le q-1$.
Then the cyclic code $\mathcal{C} \subset (\mathbb{F}_q)^n$ with blocklength $n = q-1$ having generator polynomial
$$g(x) = (x-\beta)(x-\beta^2)\cdots(x-\beta^{t-2})(x-\beta^{t-1}) \in \mathbb{F}_q[x]$$
is an $[\underset{q-1}{\underset{\parallel}{n}}, \underset{q-t}{\underset{\parallel}{k}}, \underset{t}{\underset{\parallel}{d}}]$ $\mathbb{F}_q$-linear code.

Furthermore, $\tilde{g}(x) = \mathrm{GCD}(g(x), x^{q-1}-1) = g(x)$
$$h(x) = \frac{x^{q-1}-1}{\tilde{g}(x)} = (x-\beta^t)(x-\beta^{t+1})\cdots(x-\beta^{n-2})(x-\beta^{n-1})$$
$$\text{rate}(\mathcal{C}) = \frac{q-t}{q-1} = 1 - \frac{t-1}{q-1}$$
and $\mathcal{C}$ is MDS, i.e. tight for Singleton's bound
$$\underset{q-t}{\underset{\parallel}{k}} = \underset{q-1-(t-1)}{\underset{\parallel}{n-(d-1)}}$$

---

proof of Reed-Solomon Theorem:

Most of the assertions come from our discussion of cyclic codes, once we realize that
$$g(x) = (x-\beta)(x-\beta^2)\cdots(x-\beta^{t-2})(x-\beta^{t-1})$$
divides
$$x^{q-1}-1 = \underbrace{(x-\beta)(x-\beta^2)\cdots(x-\beta^{t-1})}_{g(x)} \cdot \underbrace{(x-\beta^t)(x-\beta^{t+1})\cdots(x-\beta^{q-2})(x-\beta^{q-1})}_{h(x)}$$

What is not at all clear is why $d(\mathcal{C}) = t$.

To see this we use another piece of cyclic code theory, called variant check matrices – see §17.2

PROPOSITION: When $\mathcal{C} \subset (\mathbb{F}_q)^n$ is cyclic with generator polynomial $g(x)$ in $\mathbb{F}_q[x]$ having distinct roots so $g(x) = (x-\beta_1)(x-\beta_2)\cdots(x-\beta_m)$ with $\beta_i \neq \beta_j \ \forall i \neq j$, then $\mathcal{C}^\perp = \text{RowSpace}(H')$ for the variant check matrix

$$H' = m\left\{ \underbrace{\begin{bmatrix} 1 & \beta_1^1 & \beta_1^2 & \cdots & \beta_1^{n-1} \\ 1 & \beta_2^1 & \beta_2^2 & \cdots & \beta_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \beta_m^1 & \beta_m^2 & \cdots & \beta_m^{n-1} \end{bmatrix}}_{n} \right.$$

proof of PROP:

$c = [c_0\ c_1 \cdots c_{n-1}]$ dots to zero with all rows of H'

$\iff c_0 + c_1\beta_i^1 + c_2\beta_i^2 + \cdots + c_{n-1}\beta_i^{n-1} = 0$ for $i = 1, 2, \ldots, m$

$\iff c(x) := c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1}x^{n-1}$ has $c(\beta_i) = 0$ for $i = 1, 2, \ldots, m$

$\iff (x - \beta_i)$ divides $c(x)$ in $\mathbb{F}_q[x]$ for $i = 1, 2, \ldots, m$

need $\beta_i \neq \beta_j$ here

$\iff g(x) = \prod_{i=1}^{m}(x-\beta_i)$ divides $c(x)$ in $\mathbb{F}_q[x]$

$\iff \overline{c(x)}$ is a multiple $\overline{f(x)} \cdot \overline{g(x)}$ of $\overline{g(x)}$ in $\mathbb{F}_q[x]/(x^n - 1)$

$\iff c$ is a sum of $\overline{g(x)}, \overline{x g(x)}, \ldots, \overline{x^{n-1} g(x)}$ in $\mathbb{F}_q[x]/(x^n-1)$

$\iff c \in \mathcal{C}$.

Hence $\mathcal{C}^\perp = \text{RowSpace}(H')$ ☒

How does this help us?

For $g(x) = (x-\beta)(x-\beta^2)\cdots(x-\beta^{t-1})$ as in Reed-Solomon,

$$H' = \begin{bmatrix} 1 & \beta & \beta^2 & \beta^3 & \cdots & \beta^{n-1} \\ 1 & \beta^2 & (\beta^2)^2 & (\beta^2)^3 & & (\beta^2)^{n-1} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & \beta^{t-1} & (\beta^{t-1})^2 & (\beta^{t-1})^3 & \cdots & (\beta^{t-1})^{n-1} \end{bmatrix}$$

$(\beta^i)^j = (\beta^j)^i$

$$= \begin{bmatrix} 1 & \beta & \beta^2 & \beta^3 & \cdots & \beta^{n-1} \\ 1 & \beta^2 & (\beta^2)^2 & (\beta^3)^2 & & (\beta^{n-1})^2 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & \beta^{t-1} & (\beta^2)^{t-1} & (\beta^3)^{t-1} & \cdots & (\beta^{n-1})^{t-1} \end{bmatrix}$$

any choice of $t-1$ columns from here gives linear independent columns, because it will be a Vandermonde matrix:

$$V := \begin{bmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_{t-1} \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_{t-1}^2 \\ \vdots & & & \\ \alpha_1^{t-1} & \alpha_2^{t-1} & \cdots & \alpha_{t-1}^{t-1} \end{bmatrix}$$

with $\alpha_1, \alpha_2, \ldots, \alpha_{t-1}$ distinct powers of β, hence $\alpha_i \neq \alpha_j \ \forall i \neq j$.

THEOREM (see Appendix A.5 for one standard proof)

If $\alpha_i \neq \alpha_j$ for $i \neq j$, $\det \begin{bmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_{t-1} \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_{t-1}^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{t-1} & \alpha_2^{t-1} & & \alpha_{t-1}^{t-1} \end{bmatrix} = \underbrace{\underbrace{\alpha_1\alpha_2\cdots\alpha_{t-1}}_{\neq 0} \prod_{1\le i<j\le t-1} \underbrace{(\alpha_j-\alpha_i)}_{\neq 0}}_{\neq 0}$

proof: Here's another standard proof, by induction on t using row operations, which don't change the determinant. We'll illustrate the inductive step for $t-1=4$.

First note $\det \begin{bmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \alpha_4^2 \\ \alpha_1^3 & \alpha_2^3 & \alpha_3^3 & \alpha_4^3 \\ \alpha_1^4 & \alpha_2^4 & \alpha_3^4 & \alpha_4^4 \end{bmatrix}$

factoring α_i out of each entry in column i

$= \alpha_1\alpha_2\alpha_3\alpha_4 \det \begin{bmatrix} 1 & 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \alpha_4^2 \\ \alpha_1^3 & \alpha_2^3 & \alpha_3^3 & \alpha_4^3 \end{bmatrix}$

Want this $\det(U_t) = \prod_{1\le i<j\le 4} (\alpha_j-\alpha_i)$

Subtract α_i(row i) from row $i+1$ for $i=1,2,3$ to give

$$\det(U_t) = \det \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & \alpha_2-\alpha_1 & \alpha_3-\alpha_1 & \alpha_4-\alpha_1 \\ 0 & \alpha_2^2-\alpha_1\alpha_2 & \alpha_3^2-\alpha_1\alpha_3 & \alpha_4^2-\alpha_1\alpha_4 \\ 0 & \alpha_2^3-\alpha_1\alpha_2^2 & \alpha_3^3-\alpha_1\alpha_3^2 & \alpha_4^3-\alpha_1\alpha_4^2 \end{bmatrix}$$

$$\det(U_4) = \det \begin{bmatrix} \alpha_2-\alpha_1 & \alpha_3-\alpha_1 & \alpha_4-\alpha_1 \\ (\alpha_2-\alpha_1)\alpha_2 & (\alpha_3-\alpha_1)\alpha_3 & (\alpha_4-\alpha_1)\alpha_4 \\ (\alpha_2-\alpha_1)\alpha_2^2 & (\alpha_3-\alpha_1)\alpha_3^2 & (\alpha_4-\alpha_1)\alpha_4^2 \end{bmatrix}$$

factor out $\alpha_j - \alpha_1$ from column $j-1$

$$= (\alpha_2-\alpha_1)(\alpha_3-\alpha_1)(\alpha_4-\alpha_1) \underbrace{\det \begin{bmatrix} 1 & 1 & 1 \\ \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_2^2 & \alpha_3^2 & \alpha_4^2 \end{bmatrix}}_{= \prod_{2 \le i < j \le 4} (\alpha_j - \alpha_i)}$$

by induction, since this looks like U_3

$$= \prod_{1 \le i < j \le 4} (\alpha_j - \alpha_i) \quad \blacksquare$$

Once we know the variant check matrix H' generating $\mathcal{C}^\perp$ has all $t-1$ subsets of columns independent, we know $d(\mathcal{C}) \ge t$. But then the Singleton bound forces $k \le n-(d(\mathcal{C})-1)$

$$\cancel{n}-t \le \cancel{n}\cancel{-1}-(d(\mathcal{C})-\cancel{1})$$

$\Rightarrow d(\mathcal{C}) \le t$. So $d(\mathcal{C}) = t$ $\blacksquare$