Cyclic codes (§14.2)

Some of the more commonly used codes have this form, including Reed-Solomon codes
($\neq$ Reed-Muller codes!)

DEFINITION:
An $\mathbb{F}_q$-linear code $\mathcal{C} \subseteq (\mathbb{F}_q)^n$ is cyclic if it is RowSpace(G) for a circulant matrix G, that is, one of the form

$$G = \begin{bmatrix} c_0 & c_1 & c_2 & \cdots & & c_{n-1} \\ c_{n-1} & c_0 & c_1 & c_2 & \cdots & c_{n-2} \\ c_{n-2} & c_{n-1} & c_0 & c_1 & \cdots & c_{n-3} \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ c_2 & c_3 & & & c_0 & c_1 \\ c_1 & c_2 & c_3 & \cdots & c_{n-1} & c_0 \end{bmatrix}.$$

Note: G is $n \times n$, not $k \times n$ with $k = \dim \mathcal{C}$
not in standard form,
not of rank n.

In fact, we'll need to figure out how to compute $k = \dim_{\mathbb{F}_q}(\mathcal{C}) = \operatorname{rank} G$.

The key will be this object:

DEF'N: The generator polynomial for G and $\mathcal{C}$ is $g(x) = c_0 + c_1 x + c_2 x^2 + \dots + c_{n-1} x^{n-1} \in \mathbb{F}_q[x]$

EXAMPLE The cyclic code $\mathcal{C} \subset (\mathbb{F}_3)^6$ having generator polynomial

$$g(x) = 1 + 2x + 2x^2 + 2x^3 + x^4 \in \mathbb{F}_3[x]$$
$$= 1 + 2x + 2x^2 + 2x^3 + 1 \cdot x^4 + 0 \cdot x^5$$

is the rowspace of

$$G = \begin{bmatrix} 1 & 2 & 2 & 2 & 1 & 0 \\ 0 & 1 & 2 & 2 & 2 & 1 \\ 1 & 0 & 1 & 2 & 2 & 2 \\ 2 & 1 & 0 & 1 & 2 & 2 \\ 2 & 2 & 1 & 0 & 1 & 2 \\ 2 & 2 & 2 & 1 & 0 & 1 \end{bmatrix}$$

It turns out that G has rank $4 = k = \dim_{\mathbb{F}_3}(\mathcal{C})$, so $\mathcal{C}$ is an $[\underset{\underset{6}{\shortparallel}}{n}, \underset{\underset{4}{\shortparallel}}{k}, d]$ $\mathbb{F}_3$-linear code,

but this is not clear how to compute (yet).

The key is for us to think about the rows of G as coefficient sequences for polynomials in a new ring $\mathbb{F}_q[x]/(x^n-1) :=$ polynomials reduced modulo x^n-1

which has a vector space basis $\{1, x, x^2, \ldots, x^{n-1}\}$:

$1+2x+2x^2+2x^3+x^4$

$\|$

$\mathbb{F}_3$-basis for $\mathbb{F}_3[x]/(x^6-1)$

$$
\begin{array}{lc}
 & \begin{array}{cccccc} 1 & x & x^2 & x^3 & x^4 & x^5 \end{array} \\
\begin{array}{l}
\text{row 1 of } G \leftrightarrow g(x) \\
\text{row 2 of } G \leftrightarrow x\,g(x) \\
\text{row 3 of } G \leftrightarrow x^2 g(x) \\
\text{row 4 of } G \leftrightarrow x^3 g(x) \\
\text{row 5 of } G \leftrightarrow x^4 g(x) \\
\text{row 6 of } G \leftrightarrow x^5 g(x)
\end{array} &
\begin{bmatrix}
1 & 2 & 2 & 2 & 1 & 0 \\
0 & 1 & 2 & 2 & 2 & 1 \\
1 & 0 & 1 & 2 & 2 & 2 \\
2 & 1 & 0 & 1 & 2 & 2 \\
2 & 2 & 1 & 0 & 1 & 2 \\
2 & 2 & 2 & 1 & 0 & 1
\end{bmatrix}
\end{array}
$$

coefficients of remainder here

$$
\begin{array}{r l}
 & \quad x + 2 \\
x^6-1 \,\big) & x^7+2x^6+2x^5+2x^4+x^3 = x^3 g(x) \\
 & x^7 - x \\
\hline
 & \quad 2x^6+2x^5+2x^4+x^3+x \\
 & \quad 2x^6 - 2 \\
\hline
 & \quad 2x^5+2x^4+x^3+x+2
\end{array}
$$

What is this new ring, and how do we work with it?

PROPOSITION For any $f(x) \in \mathbb{F}[x]$ with $\mathbb{F}$ any field, there is a quotient ring

$$\mathbb{F}[x]/(f(x)) =: \text{"}\mathbb{F}[x] \text{ modulo } f(x)\text{"}$$

where $+, \times$ are done in $\mathbb{F}[x]$, then followed by taking remainder upon division by $f(x)$.

So $\overline{p_1(x)} = \overline{p_2(x)}$ in the ring $\mathbb{F}[x]/(f(x))$

$\iff p_1(x), p_2(x)$ have same remainder on division by $f(x)$

$\iff f(x) \mid p_1(x) - p_2(x)$

Furthermore, $\mathbb{F}[x]/(f(x))$ is not just a ring, but also an $\mathbb{F}$-vectorspace of dimension $d := \deg(f(x))$, with basis $\{\bar{1}, \bar{x}, \bar{x}^2, \ldots, \bar{x}^{d-1}\}$.

EXAMPLES

(1) $\mathbb{F}_q[x]/(x^n-1)$, for example,

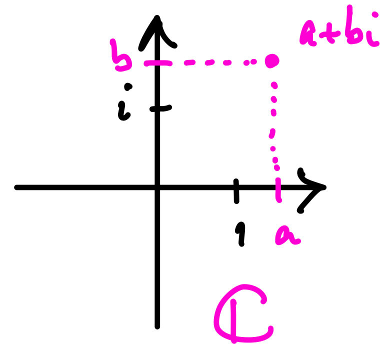
$\mathbb{F}_3[x]/(x^6-1)$ has $\mathbb{F}_3$-basis $\{\bar{1}, \bar{x}, \bar{x}^2, \bar{x}^3, \bar{x}^4, \bar{x}^5\}$

and our cyclic code $\mathcal{C}$ was a subspace inside it spanned by $\{g(x), xg(x), x^2g(x), x^3g(x), x^4g(x), x^5g(x)\}$

(2) $\mathbb{R}[x]/(\underbrace{x^2+1}_{f(x)})$ has $\mathbb{R}$-basis $\{\bar{1}, \bar{x}\}$

and is really a disguised form of

$\mathbb{C} = \{a+bi : a, b \in \mathbb{R}\}$



(an $\mathbb{R}$-vector space with $\mathbb{R}$-basis $\{1, i\}$)

since in $\mathbb{R}[x]/(x^2+1)$, one has

$$\underbrace{(a+b\bar{x})}_{\updownarrow \; a+bi}\underbrace{(c+d\bar{x})}_{\updownarrow \; c+di} = ac + (bc+ad)\bar{x} + bd\bar{x}^2$$

$$= ac + (bc+ad)\bar{x} - bd$$

$$= ac - bd + (bc+ad)\bar{x}$$

$$\updownarrow$$

$$ac-bd + (bc+ad)i$$

Proof of PROPOSITION:

Operations $+, \times$ from $\mathbb{F}[x]$ still make sense in $\mathbb{F}[x]/(f(x))$, and don't depend on choosing representatives $a(x), b(x)$ for $\overline{a(x)}, \overline{b(x)}$

when computing $\bar{a}(x)+\overline{b(x)} = \overline{a(x)+b(x)}$

$$\overline{a(x)} \cdot \overline{b(x)} = \overline{a(x)b(x)}.$$

This is proven exactly as we did it for $+, \times$ in $\mathbb{Z}$ giving $+, \times$ in $\mathbb{Z}/m\mathbb{Z}$.

Checking this makes $\mathbb{F}[x]/(f(x))$ into an $\mathbb{F}$-vector space is also easy.

Why do $\{\bar{1}, \bar{x}, \bar{x}^2, \ldots, \bar{x}^{d-1}\}$ span $\mathbb{F}[x]/(f(x))$?

Because every $a(x) \in \mathbb{F}[x]$ can be written

$$a(x) = f(x)\cdot q(x) + \underbrace{r(x)}_{r_0+r_1x+\ldots+r_{d-1}x^{d-1}} \text{ with } 0 \leq \deg(r) < d$$

$$\Rightarrow \overline{a(x)} = r_0 + r_1\bar{x} + \ldots + r_{d-1}\bar{x}^{d-1} \in \operatorname{span}_{\mathbb{F}}\{\bar{1}, \bar{x}, \ldots, \bar{x}^{d-1}\}$$

Why are $\{\bar{1}, \bar{x}, \bar{x}^2, \ldots, \bar{x}^{d-1}\}$ lin. indep. in $\mathbb{F}[x]/(f(x))$?

$$c_0\cdot\bar{1} + c_1\cdot\bar{x} + c_2\cdot\bar{x}^2 + \ldots + c_{d-1}\bar{x}^{d-1} = \bar{0} \text{ in } \mathbb{F}[x]/(f(x))$$

$\overline{c(x)}$ where $c(x) := c_0 + c_1x + c_2x^2 + \ldots + c_{d-1}x^{d-1}$

$$\Leftrightarrow \overline{c(x)} = \bar{0} \text{ in } \mathbb{F}[x]/f(x)$$

$$\Leftrightarrow \underbrace{f(x)}_{\deg\, d} \mid \underbrace{c(x)}_{\deg \leq d-1} \Leftrightarrow c(x) = 0$$

$$\Leftrightarrow c_0 = c_1 = \ldots = c_{d-1} = 0 \quad \blacksquare$$

How will thinking of our cyclic code $\mathcal{C}$ inside $\mathbb{F}_q[x]/(x^n-1)$ help us?

DEFINITION:

Given n and our generator polynomial

$$g(x) = c_0 + c_1 x + \dots + c_{n-1}x^{n-1} \text{ in } \mathbb{F}_q[x]$$

for our cyclic code $\mathcal{C} \subseteq (\mathbb{F}_q)^n$

let $\tilde{g}(x) := \mathrm{GCD}(g(x), x^n - 1)$

$$h(x) := \frac{x^n - 1}{\tilde{g}(x)} = h_0 + h_1 x + \dots + h_{n-1}x^{n-1}$$

EXAMPLE: Above we had

$$g(x) = 1 + 2x + 2x^2 + 2x^3 + x^4 \text{ in } \mathbb{F}_3[x] \text{ with } n = 6$$

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

$= \mathrm{GCD}(1 + 2x + 2x^2 + 2x^3 + x^4,\ x^6 - 1)$

$= 1 + 2x + x^2$

Euclid's algorithm steps suppressed!

and $h(x) = \dfrac{x^n - 1}{\tilde{g}(x)} = \dfrac{x^6 - 1}{1 + 2x + x^2} = x^4 + x^3 + 2x + 2$

division suppressed!

THEOREM Given $g(x)$ a generator in $\mathbb{F}_q[x]$ for a cyclic code $\mathcal{C}$ of length n, with

$$\left.\begin{array}{l}\tilde{g}(x) = \mathrm{GCD}(g(x), x^n - 1) \\ h(x) = \dfrac{x^n - 1}{\tilde{g}(x)}\end{array}\right\} \text{ as above, then:}$$

(i) $\tilde{g}(x)$ generates the same cyclic code $\mathcal{C}$ as $g(x)$.

(ii) $\mathcal{C}^\perp = \mathrm{RowSpace}(H)$ where

note coefficients of h in decreasing order!

$$H = \begin{bmatrix} h_{n-1} & h_{n-2} & \cdots & h_2 & h_1 & h_0 \\ h_0 & h_{n-1} & \cdots & & h_2 & h_1 \\ \vdots & \vdots & & & & \\ h_{n-2} & h_{n-3} & & & & h_{n-1} \end{bmatrix}$$

another $n \times n$ circulant matrix (so $\mathcal{C}^\perp$ is also cyclic)

(iii) $k = \dim_{\mathbb{F}_q}(\mathcal{C}) = \deg(h(x)) = n - \deg(\tilde{g}(x))$

EXAMPLE Above we have with $n=6$, over $\mathbb{F}_3$

$$G = \begin{bmatrix} 1 & 2 & 2 & 2 & 1 & 0 \\ 0 & 1 & 2 & 2 & 2 & 1 \\ 1 & 0 & 1 & 2 & 2 & 2 \\ 2 & 1 & 0 & 1 & 2 & 2 \\ 2 & 2 & 1 & 0 & 1 & 2 \\ 2 & 2 & 2 & 1 & 0 & 1 \end{bmatrix} \leftrightarrow g(x) = 1 + 2x + 2x^2 + 2x^3 + 1\cdot x^4 + 0\cdot x^5$$

generates $\mathcal{C}$

$$k = \operatorname{rank} G = \dim \mathcal{C} = 4$$
$$= n - \deg(\tilde{g}(x))$$

$$\tilde{G} = \begin{bmatrix} 1 & 2 & 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 2 & 1 \\ 1 & 0 & 0 & 0 & 1 & 2 \\ 2 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \leftrightarrow \tilde{g}(x) = \operatorname{GCD}(g(x), x^6 - 1)$$
$$= 1 + 2x + x^2$$
$$= 1 + 2x + 1\cdot x^2 + 0\cdot x^3 + 0\cdot x^4 + 0\cdot x^5$$

also generates $\mathcal{C}$

$$H = \begin{bmatrix} 0 & 1 & 1 & 0 & 2 & 2 \\ 2 & 0 & 1 & 1 & 0 & 2 \\ 2 & 2 & 0 & 1 & 1 & 0 \\ 0 & 2 & 2 & 0 & 1 & 1 \\ 1 & 0 & 2 & 2 & 0 & 1 \\ 1 & 1 & 0 & 2 & 2 & 0 \end{bmatrix} \xleftrightarrow{\text{(reverse coeffs)}} h(x) = \frac{x^6 - 1}{\tilde{g}(x)}$$
$$= x^4 + x^3 + 2x + 2$$
$$= 0\cdot x^5 + 1\cdot x^4 + 1\cdot x^3 + 0\cdot x^2 + 2x + 2$$

generates $\mathcal{C}^\perp$

$$n - k = \operatorname{rank} H = \dim \mathcal{C}^\perp = 2$$
$$= \deg(\tilde{g}(x))$$

THEOREM Given $g(x)$ a generator in $\mathbb{F}_q[x]$ for a cyclic code $\mathcal{C}$ of length n, with

$$\left.\begin{array}{l}\tilde{g}(x) = GCD(g(x), x^n - 1) \\ h(x) = \dfrac{x^n-1}{\tilde{g}(x)}\end{array}\right\} \text{ as above, then:}$$

(i) $\tilde{g}(x)$ generates the same cyclic code $\mathcal{C}$ as $g(x)$.

(ii) $\mathcal{C}^\perp = \text{RowSpace}(H)$ where

$$H = \begin{bmatrix} h_{n-1} & h_{n-2} & \cdots & h_2 & h_1 & h_0 \\ h_0 & h_{n-1} & \cdots & & h_2 & h_1 \\ \vdots & \vdots & & & & \\ h_{n-2} & h_{n-3} & & & & h_{n-1} \end{bmatrix}$$

note coefficients of h in decreasing order!

another $n \times n$ circulant matrix (so $\mathcal{C}^\perp$ is also cyclic)

(iii) $k = \dim_{\mathbb{F}_q}(\mathcal{C}) = \deg(h(x)) = n - \deg(\tilde{g}(x))$

---

proof of THEOREM:

<u>(i)</u>: We claim that inside the ring $\mathbb{F}_q[x]/(x^n-1)$,

$$\left\{\text{multiples } \overline{f(x)}\,\overline{g(x)} \text{ of } \overline{g(x)}\right\} = \left\{\text{multiples } \overline{f(x)}\,\overline{\tilde{g}(x)} \text{ of } \overline{\tilde{g}(x)}\right\}$$

This is because $\overline{g(x)}$ and $\overline{\tilde{g}(x)}$ are multiples of each other in $\mathbb{F}_q[x]/(x^n-1)$:

- $g(x)$ is already a multiple of $\tilde{g}(x) = GCD(g(x), x^n-1)$ in $\mathbb{F}_q[x]$, so also in $\mathbb{F}_q[x]/(x^n-1)$

- $\exists\, a(x), b(x) \in \mathbb{F}_q[x]$ with $\tilde{g}(x) = a(x)g(x) + b(x)(x^n-1)$ since $\tilde{g}(x) = GCD(g(x), x^n-1)$,

so $\overline{\tilde{g}(x)} = \overline{a(x)}\,\overline{g(x)}$ in $\mathbb{F}_q[x]/(x^n-1)$

But we identified $\mathcal{C} = \mathrm{RowSpace}(G)$

as $\mathcal{C} = \mathrm{span}_{\mathbb{F}_q}\{\overline{x}^i\overline{g(x)}\}_{i=0,1,2,\dots,n-1}$ in $\mathbb{F}_q[x]/(x^n-1)$

$$= \left\{ a_0\overline{g}(x) + a_1\overline{x}\,\overline{g(x)} + \dots + a_{n-1}\overline{x}^{n-1}\overline{g(x)} : a_0, a_1, \dots, a_{n-1} \in \mathbb{F}_q \right\}$$

$$\| $$

$$\overline{(a_0 + a_1x + \dots + a_{n-1}x^{n-1})}\,\overline{g}(x) = \overline{f(x)}\,\overline{g(x)}$$

$$= \left\{ \text{multiples of } \overline{g(x)} \;\; \overline{f(x)}\,\overline{g(x)} \right\}$$

Hence $g(x), \tilde{g}(x)$ generate the same cyclic code $\mathcal{C}$.

(ii): We can assume $g(x) = \tilde{g}(x)$ by (i).

Let $b = [b_{n-1} b_{n-2} \cdots b_1 b_0] \in (\mathbb{F}_q)^n$ and we'll try to check that $b \in \mathcal{C}^\perp \iff b \in \mathrm{RowSpace}(H)$.

We have $b \in \mathcal{C}^\perp \iff b \cdot r = 0 \;\; \forall$ rows r of G

$$\iff [b_0 b_1 \cdots b_{n-1}] \cdot v = 0 \;\; \forall \text{ columns } v \text{ of } G$$

circulant matrices have their rows the reverses of their columns

$$\iff [b_0\, b_1 \cdots b_{n-1}] \cdot G = \underline{0}$$

$$\iff b_0(\text{row 1 of } G) + \dots + b_{n-1}(\text{row } n-1 \text{ of } G) = \underline{0}$$

$$\Leftrightarrow \overline{b_0 g(x) + b_1 x g(x) + \dots + b_{n-1} x^{n-1} g(x)} = \bar{0} \quad \text{in } \mathbb{F}_q[x]/(x^n-1)$$

$$\Leftrightarrow x^n - 1 \,\Big|\, (b_0 + b_1 x + \dots + b_{n-1} x^{n-1})\,\tilde{g}(x) \quad \text{in } \mathbb{F}_q[x]$$

divide by $\tilde{g}(x)$

$$\Leftrightarrow h(x) = \frac{x^n - 1}{\tilde{g}(x)} \,\Big|\, \underbrace{b_0 + b_1 x + \dots + b_{n-1} x^{n-1}}_{\text{call this } b(x)} \quad \text{in } \mathbb{F}_q[x]$$

$$\Leftrightarrow b(x) = a_0 h(x) + a_1 x h(x) + \dots + a_{n-1} x^{n-1} h(x)$$

for some $a_i \in \mathbb{F}_q$

$$\Leftrightarrow \overline{b(x)} = \overline{a_0 h(x) + a_1 x h(x) + \dots + a_{n-1} x^{n-1} h(x)} \quad \text{in } \mathbb{F}_q[x]/(x^n-1)$$

$$\Leftrightarrow [b_0 \, b_1 \cdots b_{n-1}] \in \text{RowSpace} \begin{bmatrix} h_0 & h_1 & \cdots & h_{n-1} \\ h_{n-1} & h_0 & h_1 \cdots & h_{n-2} \\ \vdots & & \ddots & \\ h_1 & & & h_0 \end{bmatrix}$$

$$\Leftrightarrow b = [b_{n-1} \cdots b_1 \, b_0] \in \text{RowSpace} \begin{bmatrix} h_{n-1} & \cdots & h_1 & h_0 \\ h_{n-2} & \cdots\; h_1 & h_0 & h_{n-1} \\ \vdots & & \iddots & \vdots \\ h_0 & \cdots & & h_1 \end{bmatrix}$$

that is, $b \in \text{RowSpace}(H)$.

(iii): rank $G \leq \deg(h(x))$ because the coefficients of h give a dependence among the last $\deg(h)+1$ columns of G, and hence since G is circulant, this lets one express any column of G in terms of the last $\deg(h)$ columns.

Swapping roles for G, H and using part (i) and

$$\begin{array}{ccccc} \deg(\tilde{g}) & + & \deg(h) & = & n \\ \rotatebox{90}{$\geq$} & & \rotatebox{90}{$\geq$} & & \\ \operatorname{rank}(H) & + & \operatorname{rank}(G) & = & n \end{array}$$

(since $h = \frac{x^n - 1}{\tilde{g}(x)}$)

(since G, H generate $\mathcal{C}, \mathcal{C}^\perp$)

one deduces that one must have equalities everywhere, and in particular here

$$\begin{array}{ccc} \deg(h) & = & \operatorname{rank}(G) \\ \| & & \| \\ n - \deg(\tilde{g}) & & \dim(\mathcal{C}) =: k \end{array}$$

$\blacksquare$