Math 127, Mon Apr 25

- Reading for today: 8.4–8.5.
- Reading for Wed Apr 27: 9.2–9.3.
- PS09 outline due today(-ish), completed version due Wed(-ish)
- **EXAM 3** on Mon May 02 or Wed May 04 — take that survey now!

Cyclic codes

Definition

Let $\mathcal{C}$ be a binary linear code of length n. To say that $\mathcal{C}$ is **cyclic** means that it is closed under cyclic permutation of coordinates.

That is, to say that $\mathcal{C}$ is cyclic means that if $\begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{n-1} \end{bmatrix}$ is in $\mathcal{C}$, then

so are $\begin{bmatrix} c_{n-1} \\ c_0 \\ c_1 \\ \vdots \\ c_{n-2} \end{bmatrix}$, $\begin{bmatrix} c_{n-2} \\ c_{n-1} \\ c_0 \\ \vdots \\ c_{n-3} \end{bmatrix}$, and so on.

Cyclic codes, cont.

The **polynomial notation** for vectors in $\mathbf{F}_2^n$ represents $\begin{bmatrix} c_0 \\ \vdots \\ c_{n-1} \end{bmatrix}$ as

$$c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1}$$

in the ring $R = \mathbf{F}_2[x]/(x^n - 1)$ (i.e., setting $x^n = 1$). In that notation:

Theorem

Let $\mathcal{C}$ be a binary linear code of length n. In polynomial notation, $\mathcal{C}$ is cyclic if and only if it is an ideal of the ring $\mathbf{F}_2[x]/(x^n - 1)$.

Exc $= \{0000, 1100, 0110, 0011,$

$1010, 0101, 1001, 1111\}$

$\mathcal{C}$ is a subsp of $\mathbb{F}_2^4$; $\mathcal{C}$ closed + "sc mult

$c(x) = 1 + 0x + 0x^2 + 1x^3 = 1 + x^3 \in \mathcal{C}$

$c'(x) = 1 + x + x^3 = 1 + 1x + 0x^2 + 1x^3$

bc not in list $\notin \mathcal{C}$

The generator polynomial of a cyclic code

Theorem

Fix a positive integer n, and let $\mathcal{C}$ be a nonzero cyclic code of length n, i.e., let $\mathcal{C}$ be a nonzero ideal of $\overline{R} = \mathbf{F}_2[x]/(x^n - 1)$. Then $\mathcal{C}$ is principal, or in other words, $\mathcal{C} = (g(x))$ for some $g(x) \in \mathbf{F}_2[x]$. Moreover, we can choose $g(x)$ so that $g(x)$ divides $x^n - 1$.

Definition

Let $\mathcal{C}$ be a cyclic code of length n. We define the **generator polynomial** of $\mathcal{C}$ to be the minimal polynomial $g(x)$ of $\mathcal{C}$.

Again, we always assume that $g(x)$ is a divisor of $x^n - 1$.

The generator matrix of a cyclic code

Theorem

Let $\mathcal{C}$ be a cyclic code of length n generated by the divisor $g(x) \in \mathbf{F}_2[x]$ of $x^n - 1$. If $\deg g(x) = r$, then the set

$$\mathcal{B} = \left\{ g(x), xg(x), \ldots, x^{(n-1)-r} g(x) \right\}$$

is a basis for $\mathcal{C}$. Consequently, the dimension of $\mathcal{C}$ is $k = n - r$.

Example: Let $\mathcal{C}$ be the cyclic code of length 6 generated by $(1 + x)$, which divides $x^6 - 1$ (since $-1 = +1$). The theorem says:

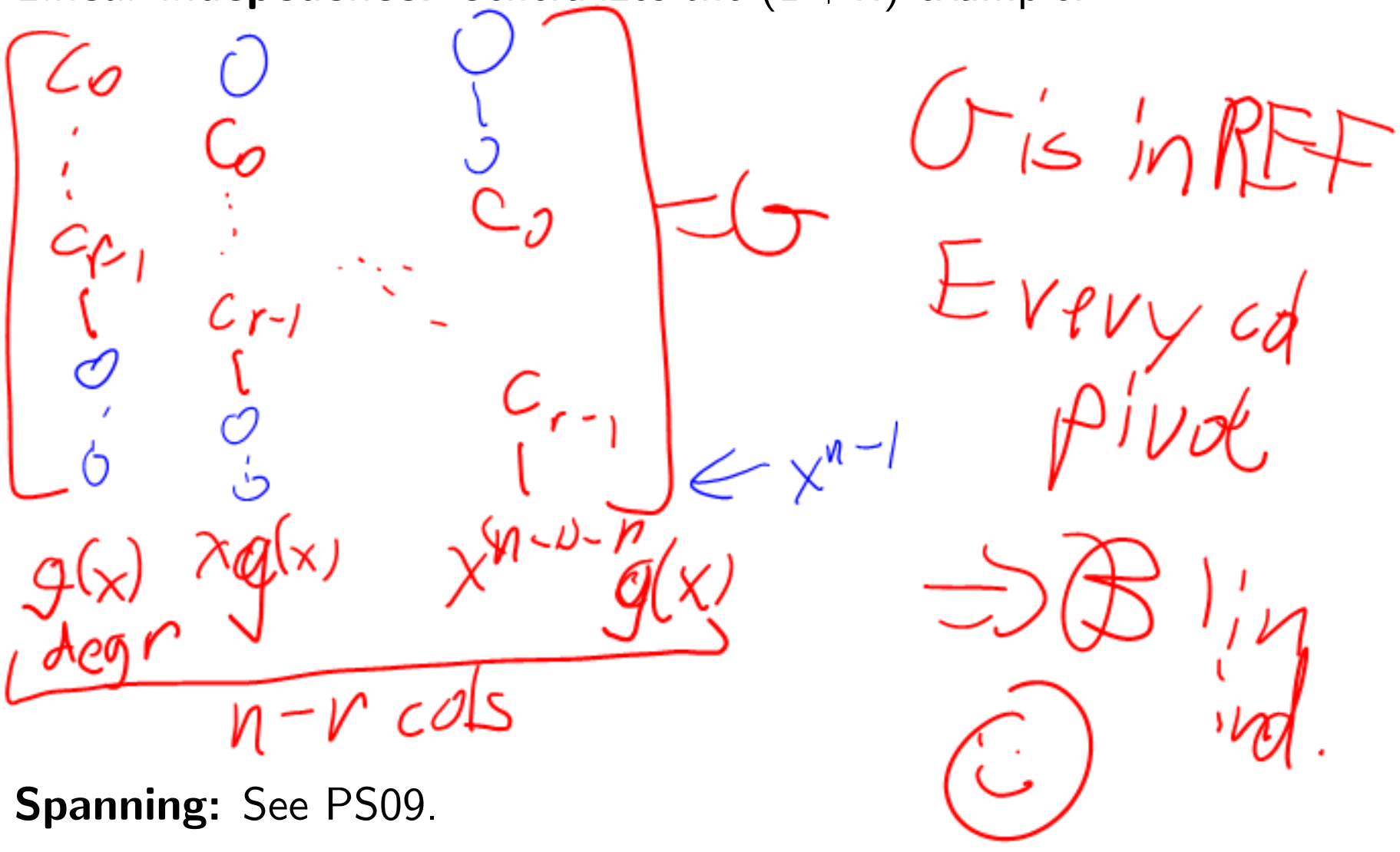
$\mathcal{B} = \{1+x, x+x^2, x^2+x^3, x^3+x^4, x^4+x^5\}$

$= \left\{ \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} \right\}$ dim $= 5 = 6 - 1$

Note Since $\dim \mathcal{C} = n - r$,
where $r = \deg(g(x))$, want $\deg g$
as small as possible (more data)

Generator matrix of a cyclic code (proof)

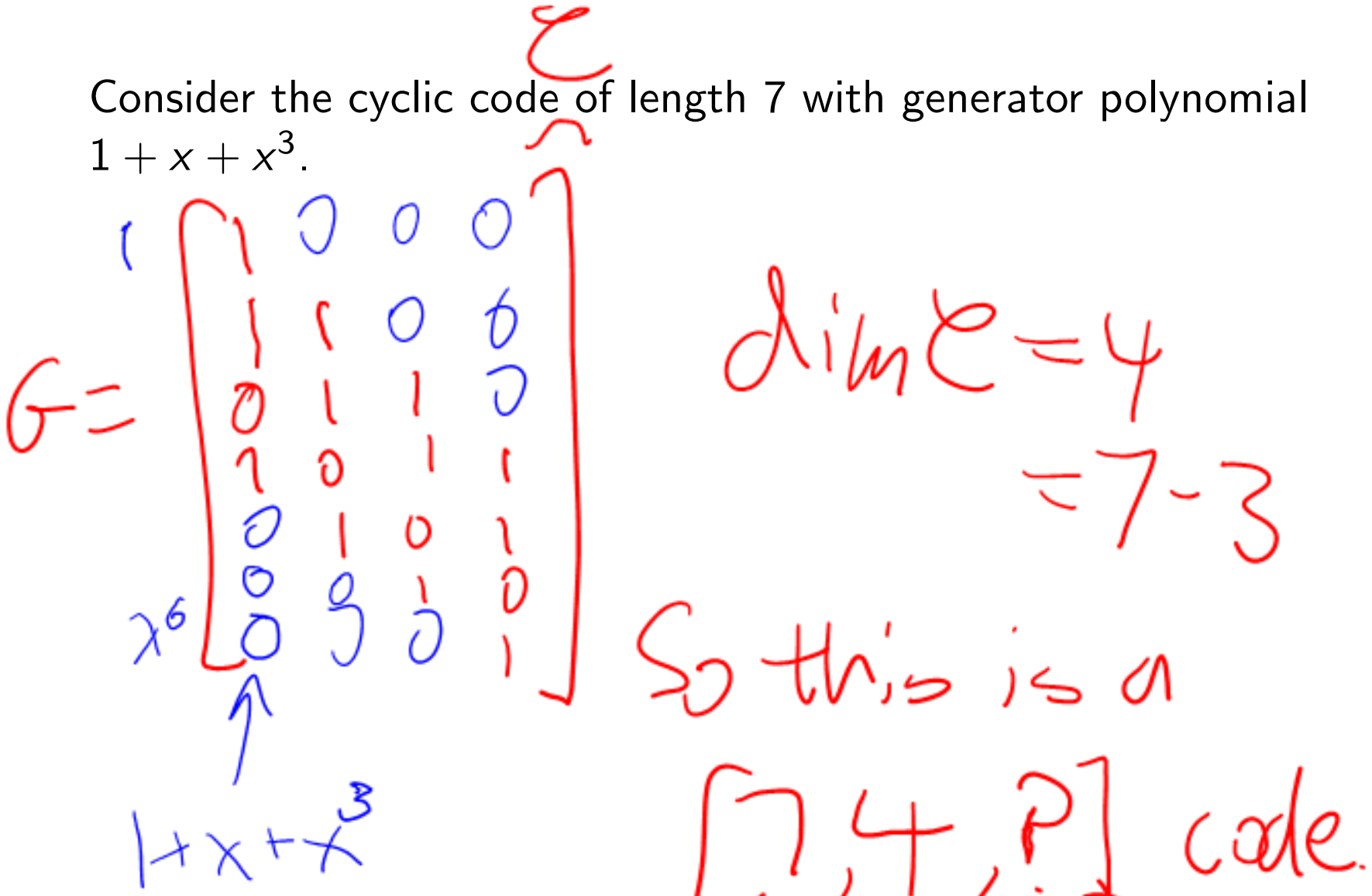
Linear indepedence: Generalizes the $(1 + x)$ example:



Spanning: See PS09.

The Hamming 7-code as a cyclic code

Consider the cyclic code of length 7 with generator polynomial $1 + x + x^3$.



Generators of cyclic codes: The upshot

$r = \deg g(x)$

Suppose $g(x)$ divides $x^n - 1$ in $\mathbf{F}_2[x]$. Let $\overline{R} = \mathbf{F}_2[x]/(x^n - 1)$.

- The principal ideal of $\overline{R}$ generated by $g(x)$ defines a cyclic code $\mathcal{C}$ of length n.
- The set $\{g(x), xg(x), \ldots, x^{(n-1)-r}g(x)\}$ is a basis for $\mathcal{C}$, and so the dimension of $\mathcal{C}$ is $k = n - r$.

Note: Coding and reading correctly received codewords can be done using polynomial multiplication and division, so we'll concentrate on being able to correct errors in principle (i.e., because of having a large minimum distance).

Big and difficult question: How can we compute the minimum distance of a cyclic code $\mathcal{C}$? Or at least, how can we ensure some kind of lower bound for the minimum distance of $\mathcal{C}$?

Answer: Use field extensions of $\mathbf{F}_2$. (!!!)

What does it mean:

$\mathbb{F}_8$ ext of $\mathbb{F}_2$?

$\mathbb{F}_8 = \mathbb{F}_2[\alpha]/(\alpha^3+\alpha+1=0)$, so $\alpha^3 = \alpha+1$

$2 = 3-1$

$\mathbb{F}_8 = \{$polys of deg ≤ 2 in $\alpha\}$

$= \{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\}$

Ch. 7

$\mathbb{F}_2$

Factoring over $\mathbf{F}_2$ vs. factoring over an extension

Example

The polynomial $x^3 + x + 1$ is irreducible over $\mathbf{F}_2$, but if α is a root of $x^3 + x + 1$ in $\mathbf{F}_8$, then

$$x^3 + x + 1 = (x + \alpha)(x + \alpha^2)(x + \alpha^4).$$

The BCH Theorem

Let $\mathcal{C}$ be a cyclic code of length n generated by the divisor $g(x) \in \mathbf{F}_2[x]$ of $x^n - 1$.
Suppose E is an extension of $\mathbf{F}_2$ such that for some $\delta \in \mathbf{N}$ and some $\alpha \in E$ with the order of α exactly equal to n, we have that

$$0 = g(\alpha) = g(\alpha^2) = g(\alpha^3) = \cdots = g(\alpha^{\delta-1}).$$

Then the minimum distance d of $\mathcal{C}$ is at least δ, i.e., $d \geq \delta$.

So we need to find E, α of order n, and $g(x)$ such that $g(\alpha^k) = 0$ for as many consecutive k as possible (error correction) while keeping $\deg g$ as low as possible (higher dimension of code).

Example: $n = 7$, $g(x) = x^3 + x + 1$.

The Frobenius automorphism

Solution to problem above is the following automorphism (!!).

Theorem

Let E be a finite extension of $\mathbf{F}_2$, and define a function $\rho : E \to E$ by the formula

$$\rho(\beta) = \beta^2.$$

1. *If E is a finite extension of $\mathbf{F}_2$, then $\beta \in E$ is a root of $x^2 - x$ if and only if $\beta \in \mathbf{F}_2$.*
2. *The map ρ is an automorphism of E. Furthermore, ρ fixes exactly the subfield $\mathbf{F}_2$; in other words, for $\beta \in E$, $\rho(\beta) = \beta$ if and only if $\beta \in \mathbf{F}_2$.*

Why: See PS08 and text.

Example: The Frobenius automorphism on $\mathbf{F}_8$

Recall that $\mathbf{F}_8 = \mathbf{F}_2(\alpha)$, where α is a root of $x^3 + x + 1$ (i.e., $\alpha^3 = \alpha + 1$).

$\rho(\alpha) = \alpha^2$

$\alpha^3 = \alpha + 1$

$\alpha^4 = \alpha^2 + \alpha$

$\rho(\alpha^2) = \alpha^4 = \alpha^2 + \alpha$

$\rho(\alpha^4) = \rho(\alpha^2 + \alpha) = \rho(\alpha^2) + \rho(\alpha)$

$= \alpha^2 + \alpha + \alpha^2 = \alpha$

Alt: α is a primitive element, and therefore has order

$|\mathbb{F}_8^\times| = 7 \Rightarrow \alpha^7 = 1$

exps of α mod 7

$\{\alpha, \alpha^2, \alpha^4\}$

$\alpha^8 = \alpha$

Frob: $\{\alpha, \alpha^2, \alpha^4\}$

orbit

Minimal polynomial of $\beta \in E$

Theorem

Let E be an extension of $\mathbf{F}_2$, fix some $\beta \in E$, and let

$$I = \{f(x) \in \mathbf{F}_2[x] \mid f(\beta) = 0\}.$$

Then I is an ideal of $\mathbf{F}_2[x]$, and consequently, $I = (m(x))$ for some $m(x) \in \mathbf{F}_2[x]$ (the **minimal polynomial** *of β).*

m is smallest poly w/ β as a root.

Definition

E an extension of $\mathbf{F}_2$, $\beta \in E$. Define

$$\beta_n = \rho^n(\beta),$$

e.g., $\beta_3 = \rho(\rho(\rho(\beta)))$. The **Frobenius orbit of** β is the set

$$\{\beta_0 = \beta, \beta_1, \beta_2, \dots\}.$$

Note that since some finite power of ρ is the identity, every Frobenius orbit is finite.

The Orbit Theorem

Let E be an extension of $\mathbf{F}_2$, let β be in $E^\times$, and suppose the Frobenius orbit of β is $\{\beta_0, \ldots, \beta_{s-1}\}$, where $\beta_k = \rho^k(\beta)$ and $\rho^s(\beta) = \beta$. Then the minimal polynomial of β over $\mathbf{F}_q$ is

$$m(x) = (x - \beta_0)(x - \beta_1)\ldots(x - \beta_{s-1}).$$

Furthermore, if β has order n, then $m(x)$ divides $x^n - 1$.

Why:

- Because β is a root of $m(x)$, and the Frobenius automorphism preserves zeros, each β_k must be a root of $m(x)$, which means that $(x - \beta_k)$ must be a factor of $m(x)$. By the same argument, each of the $(x - \beta_k)$ must be a factor of $x^n - 1$.
- Conversely, the above product is invariant under Frobenius, so it must have coefficients in $\mathbf{F}_2$.

Examples of minimal polymomials

Example: $E = \mathbf{F}_8$, α primitive root of E, so order of α is: 7

Frob orbit of α: $\{\alpha, \alpha^2, \alpha^4\}$

Min poly of α is $m_\alpha(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4)$

Always true: $m_\alpha(x) \in \mathbf{F}_2[x]$

Example: Let $E = \mathbf{F}_{2048}$, β primitive root of E, so β has order $2047 = 23 \cdot 89$, $\alpha = \beta^{89}$. Order of α is:

Why we use x^3+x+1

The BCH algorithm

1. Choose an extension E of $\mathbf{F}_2$, $|E| = 2^e$.
2. Choose $\alpha \in E$ of order n. Code will have length n.
3. Choose a **designed distance** $\delta \in \mathbf{N}$.
4. Let $g(x) = \operatorname{lcm}(m_1(x), \ldots, m_{\delta-1}(x))$, i.e., remove repetitions of minimal polynomials and take the resulting product.

Let $\mathcal{C}$ be the cyclic code of length n generated by $g(x)$. Then

- Length of $\mathcal{C}$ is n.
- $\dim \mathcal{C} = n - \deg g(x)$.
- Minimum distance $d \geq \delta$. (So guaranteed distance is at least δ, and is sometimes better.)

See text for proof of the last fact (the hard part).

Example: $E = \mathbf{F}_{32}$, α primitive, $\delta = 5, 7$

Example: $E = \mathbf{F}_{256}$, β primitive, $\alpha = \beta^3$, $\delta = 5, 7, 9$