Math 127, Mon Apr 26

- Use a laptop or desktop with a large screen so you can read these words clearly.
- In general, please turn off your camera and mute yourself.
- Exception: When we do groupwork, please turn both your camera and mic on. (Groupwork will not be recorded.)
- Please always have the chat window open to ask questions.
- Reading for today: 8.5, 9.2–9.3. Reading for Wed: 9.4–9.5, 10.1. (Reload again after tonight!)
- PS09 due Wed night.
- Exam 3 in one week, Mon May 03.
- Exam review Fri Apr 30, 10am–noon.

Covers Chs 7 and 8
= PS07, PS08, PS09
Sample exam and study guide posted tonight.

The BCH Theorem

$\mathcal{C}$ = all multiples of g(x) with degree <= n-1.

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).

$E = \mathbb{F}_2[\alpha] = \mathbb{F}_2[x]/(m(x))$

The Orbit Theorem

Let E be an extension of $\mathbf{F}_2$, let β be in $E^\times$, and let $\rho(x) = x^2$ be the Frobenius automorphism of E.
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 $\mathbf{F}_q$ 2 is

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

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

The BCH algorithm

This is how you choose a BCH code with a desired amount of error correction.

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.
- $\dim \mathcal{C} = n - \deg g(x)$.

Works for any cyclic code with gen g(x)

- Minimum distance $d \geq \delta$. (So guaranteed distance is at least δ, and is sometimes better.)

See text for proofs.

min polynomials of alpha^k

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

$|E| = 32 = 2^5$, α has order $q - 1 = 31$

$q = 2^5$

$\alpha^{31} = 1$

$\boxed{\delta = 5}$ Want min polys of

$\alpha^1, \alpha^2, \alpha^3, \alpha^4$

By Orbit Theorem, find min polys from squaring orbits.

$\mathrm{orb}(\alpha^1) = \{\alpha^1, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}\}$

$\alpha^{32} = \alpha$

$\mathrm{orb}(\alpha^1) = \mathrm{orb}(\alpha^2) = \mathrm{orb}(\alpha^4)$

$\operatorname{orb}(\alpha^3) = \{\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{17}\}$

$48 \pmod{31} = 17$

$\alpha^{34} = \alpha^3$

$$m_1(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)(x-\alpha^{16})$$

$$m_3(x) = (x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^{24})(x-\alpha^{17})$$

$g(x) = m_1(x)\,m_3(x)$ $\quad \deg g = 10$

$\mathcal{C}$ has: length $= 31$ $\quad$ dim $= 31 - 10 = 21$

min dist ≥ 5 (BCH)

$\boxed{\mathcal{E} \text{ is } [31, 21, 5]}$

errs corr $= \dfrac{5-1}{2} = 2$

3 errs corr

$\boxed{\delta = 7}$ Need $g(\alpha^k) = 0$ for $1 \le k \le 6$

Only missing α^5:

$m_5(x) = [5, 10, 20, 9, 18]$

double mod 31

$36 \equiv 5 \pmod{31}$

$g(x) = m_1(x)\, m_3(x)\, m_5(x)$ $\quad$ deg $g = 15$

$\dim \mathcal{E} = 31 - 15 = 16$ $\quad \boxed{\mathcal{E} \text{ is } [31, 16, 7]}$

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

$256 = 2^8$, $\mathrm{ord}(\beta) = 255 = 5 \cdot 3 \cdot 17$

$(\beta^3)^{5 \cdot 17} = \beta^{255} = 1$

$\mathrm{ord}(\alpha) = \frac{255}{3} = 85$

$\alpha = \beta^3$ Codes length 85

$\alpha^{85} = 1$, so doubling mod 85.

$\boxed{\delta = 5}$ $\underbrace{\alpha^1, \alpha^2, \alpha^3, \alpha^4}$

$\mathrm{orb}(\alpha^1) = [1, 2, 4, 8, 16, 32, 64, 43]$

$86 = 1 \pmod{85}$

$orb(\alpha^3) = [3, 6, 12, 24, 48, 11, 22, 44]$

$88 \equiv 3 \pmod{85}$

$96 \equiv 11 \pmod{85}$

$\deg m_1(x) = 8 \quad \deg m_3(x) = 8$

$g(x) = m_1(x) m_3(x) \Rightarrow \deg g = 16$

So $\mathcal{E}$ has: $n = 85 \quad k = 85 - 16 = 69$

$d \geq \delta = 5$

$\boxed{\delta = 7}$ $\quad orb(\alpha^5) = [5, 10, 20, 40, 80,$

$90 \bmod 85$

$160 \bmod 85 \longrightarrow 75, 65, 45]$

$\deg m_5(x) = 8$

$g(x) = m_1(x)\, m_3(x)\, m_5(x)$

$\deg g = 24 \quad k = 85 - 24 = 61$

$\mathcal{C}$ is $[85, 61, 7]$ code.

$\boxed{\delta = 9}$ Need α^7

112 mod 85

112 mod 85

128 mod 85

$\text{orb}(\alpha^7) = [7, 14, 28, 56, 27, 54, 23, 46]$

$$g(x) = \overset{8}{m_1(x)}\,\overset{8}{m_3(x)}\,\overset{8}{m_5(x)}\,\overset{8}{m_7(x)}$$

$\deg g = 32$

$\dim \mathcal{C} = 85 - 32 = 53$

$\mathcal{C}$ is $[85, 53, \geq 9]$ code

In fact! also $\alpha^{10}, \alpha^{11}, \alpha^{12}$

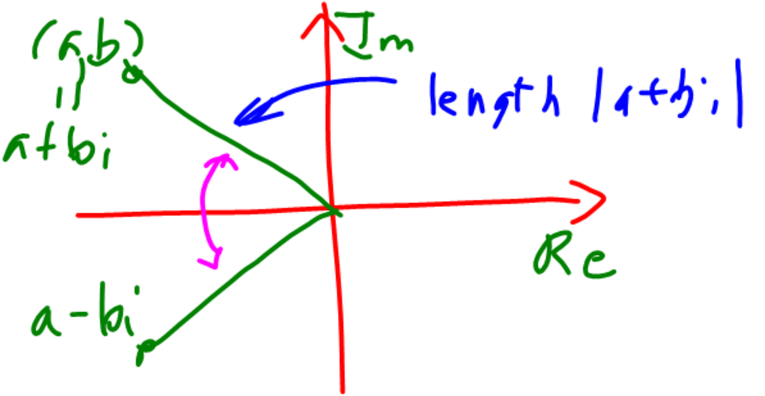
$\mathcal{C}$ is $[85, 53, 13]$ code

Complex numbers and roots of unity

Ch. 9

Towards: The Fast Fourier Transform

Recall: Complex numbers have form $a + bi$, $a, b \in \mathbf{R}$, where $i^2 = -1$. Drawn in the **complex plane:**

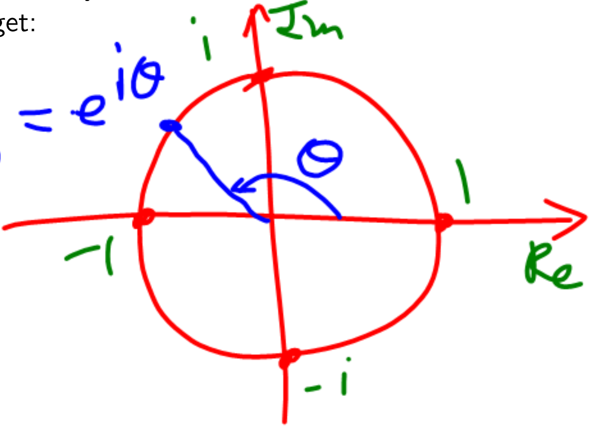


The **modulus**, or **absolute value**, of $a + bi$ is $|a + bi| = \sqrt{a^2 + b^2}$ and the (complex) **conjugate** of $a + bi$ is $\overline{a + bi} = a - bi$.

The complex exponential $e^{i\theta}$

Euler's formula says $e^{i\theta} = \cos\theta + i\sin\theta$. Drawn in the complex plane, we get:

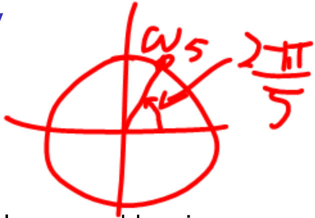
$$\cos\theta + i\sin\theta = e^{i\theta}$$



Important: To multiply two complex exponentials, add their angles:

$$e^{i\theta} e^{i\gamma} = e^{i(\theta+\gamma)} \qquad (e^{i\theta})^n = e^{in\theta}$$

The natural primitive Nth root of unity



For a positive integer N, this is

$$\omega_N = e^{2\pi i/N}.$$

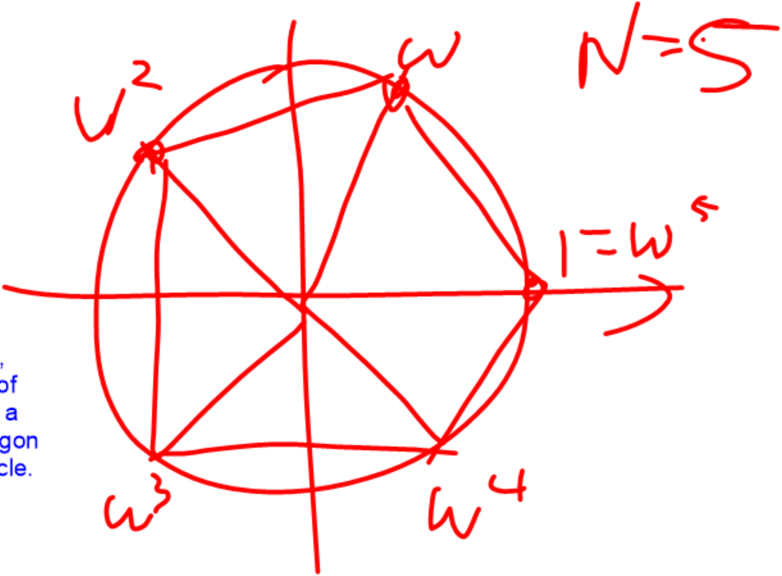
When N is fixed, or the context is otherwise clear, we abbreviate ω_N as ω. Called Nth root of unity because:

$$(\omega_N)^N = \left(e^{\frac{2\pi i}{N}}\right)^N = e^{2\pi i} = 1$$

Thm: Let N be a positive integer, and let $\omega = \omega_N = e^{2\pi i/N}$. The zeros of the polynomial $z^N - 1$ (i.e., the solutions to $z^N = 1$) are precisely the powers $1, \omega, \omega^2, \ldots, \omega^{N-1}$ of ω.

Proof: See PS10.

A picture of $1, \omega, \omega^2, \ldots, \omega^{N-1}$



In general,
Nth roots of
unity form a
regular N-gon
on unit circle.

Recap/foreshadowing: What you really need to know about ω

Let N be a positive integer, and let $\omega = \omega_N = e^{2\pi i/N}$.

1. The solutions to $z^N = 1$ are precisely the powers $1, \omega, \omega^2, \ldots, \omega^{N-1}$.
2. Because of the Orthogonality Lemma (coming up next), we have that

$$1 + \omega + \cdots + \omega^{N-1} = 0.$$

Signals

Definition

Fix $N \in \mathbf{N}$. We define a **signal** to be a function $f : \mathbf{Z}/(N) \to \mathbf{C}$, or in other words, a complex-valued function with domain $\mathbf{Z}/(N)$. Note that a signal f is defined by its N values $f(0), \ldots, f(N-1) \in \mathbf{C}$, so we sometimes represent a signal f in vector form as $\begin{bmatrix} f(0) \\ \vdots \\ f(N-1) \end{bmatrix}$.

Example: Let $\omega = e^{2\pi i/N}$ be the natural primitive Nth root of unity in $\mathbf{C}$. We define the **basic trigonometric signal** $e_k : \mathbf{Z}/(N) \to \mathbf{C}$ by $e_k(n) = \omega^{kn}$. We can also represent e_k in vector form as $\begin{bmatrix} 1 \\ \omega^k \\ \vdots \\ \omega^{(N-1)k} \end{bmatrix}$.

Examples: e_k for $N = 12$, $k = 0, 1, 2, 3, 4$

Orthogonality Lemma

Fix $N \in \mathbf{N}$ and let $\omega = \omega_N = e^{2\pi i/N}$ be the natural primitive Nth root of unity in $\mathbf{C}$. For $t \in \mathbf{Z}/(N)$, we have:

$$\sum_{k=0}^{N-1} \omega^{tk} = \begin{cases} N & \text{if } t = 0 \pmod{N}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof: See PS10.

In particular, if $t = 1$:

A motivating problem

Motivating Problem

Fix $N \in \mathbf{N}$. How can we express any signal on $\mathbf{Z}/(N)$ as a linear combination of the basic trigonometric signals e_k, $0 \leq k \leq N-1$?

Solving this problem has many applications (e.g., analysis of music/sound production) but we'll concentrate on one: making multiplication faster. (!!)