Math 127, Wed May 12

- 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.
- Last reading in class: 10.3, 11.2.
- Final exam, **Wed May 19**. Cumulative through Ch. 10.
- PS11 due before end of semester.

& PS10

7:15pm

Final exam review on
Tue May 18, 9:45am

Recap: The DFT

Fix $N \in \mathbf{N}$, let $\omega = e^{2\pi i/N}$ be the natural primitive Nth root of unity in $\mathbf{C}$, and let $f : \mathbf{Z}/(N) \to \mathbf{C}$ be a signal. The **DFT** of f is defined to be the function $\hat{f} : \mathbf{Z}/(N) \to \mathbf{C}$ given by

$$\hat{f}(k) = \frac{1}{N} \sum_{n=0}^{N-1} f(n)\omega^{-kn}.$$

$\mathcal{O}(N^2)$

So:

$$\hat{f}(0) = \frac{1}{N}(f(0) + f(1) + f(2) + \cdots + f(N-1)),$$

$$\hat{f}(1) = \frac{1}{N}(f(0) + \omega^{-1}f(1) + \omega^{-2}f(2) + \cdots + \omega^{-(N-1)}f(N-1)),$$

$$\hat{f}(2) = \frac{1}{N}(f(0) + \omega^{-2}f(1) + \omega^{-2(2)}f(2) + \cdots + \omega^{-2(N-1)}f(N-1)),$$

$$\hat{f}(3) = \frac{1}{N}(f(0) + \omega^{-3}f(1) + \omega^{-3(2)}f(2) + \cdots + \omega^{-3(N-1)}f(N-1)),$$

and so on.

The key example from groups for the FFT

Definition

We define C_n to be the set of all nth roots of unity in $\mathbf{C}$. I.e., $C_n = \{z \in \mathbf{C} \mid z^n = 1\}$. Recall that if $\omega = e^{2\pi i/n}$, then

$$C_n = \left\{1, \omega, \omega^2, \dots, \omega^{n-1}\right\}.$$

Theorem

For $n, k \in \mathbf{N}$, we have that:

1. *C_n is a subgroup of $\mathbf{C}^\times$, the multiplicative group of the complex numbers; and*
2. *If k divides n, then C_k is a subgroup of C_n.*

Subgroup chains like

$$C_1 \leq C_2 \leq C_4 \leq C_8 \leq C_{16}$$

describe the Fast Fourier Transform (FFT).

Cosets

Definition

Let G be a group, and let H be a subgroup of G. For $a \in G$, we define the **left multiplicative coset** aH to be

fix　　　　　　　　　　　　　　　varies over H

$$aH = \{ah \mid h \in H\}.$$

If the context is clear, instead of saying "left multiplicative coset", we just say **coset**.

Example: $G = \mathbf{F}_{19}^{\times}$ of order 18.
$H = \langle 7 \rangle = \{1, 7, 11\}$; then cosets are:

$$\begin{array}{ll} 1H = \{1, 7, 11\} & 2H = \{2, 3, 14\} \\ 4H = \{4, 6, 9\} & 5H = \{5, 16, 17\} \\ 8H = \{8, 12, 18\} & 10H = \{10, 13, 15\} \end{array}$$

Cosets partition G

Theorem

G finite group, $H \leq G$. Choose one element a_i from each coset of H so that $\{a_1 H, \ldots, a_n H\}$ contains each coset of H exactly once. Then $\{a_1 H, \ldots, a_n H\}$ partitions G.

Definition

Let G be a finite group, and let H be a subgroup of G. A choice of coset representatives like the set $\{a_1, \ldots, a_n\}$ above is called a **transversal** for H in G.

Example: In $\mathbf{F}_{19}^{\times}$:

$$\begin{aligned} 1H &= \{1, 7, 11\} & 2H &= \{2, 3, 14\} \\ 4H &= \{4, 6, 9\} & 5H &= \{5, 16, 17\} \\ 8H &= \{8, 12, 18\} & 10H &= \{10, 13, 15\} \end{aligned}$$

union of these sets is G, without any overlap

So one transversal for H in G is:

{1, 2, 4, 5, 8, 10}

Chains of C_n

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

When we have a chain like:

$$C_1 \leq C_3 \leq C_6 \leq C_{12}$$

and $N = 12$ is the size of the biggest subgroup in the chain, then we can express all of the subgroups in terms of $\boxed{\omega = \omega_{12} = e^{2\pi i/12}}$:

$C_{12} = \langle \omega \rangle = \{1, \omega, \omega^2, \omega^3, \ldots, \omega^{11}\}$

$\omega^2 = e^{\frac{2\pi i}{6}}$ so $C_6 = \langle \omega^2 \rangle = \{1, \omega^2, \omega^4, \omega^6, \omega^8, \omega^{10}\}$

$\omega^4 = e^{\frac{2\pi i}{3}}$ so $C_3 = \langle \omega^4 \rangle = \{1, \omega^4, \omega^8\}$

$\omega^{12} = e^{2\pi i}$ so $C_1 = \langle \omega^{12} \rangle = \{1\}$

(If $w = e^{\frac{2\pi i}{12}}$,

$$w^4 = \left(e^{\frac{2\pi i}{12}}\right)^4$$

$$= e^{\cancel{4}\left(\frac{2\pi i}{\underset{3}{\cancel{12}}}\right)} = e^{\frac{2\pi i}{3}}$$)

$$C_1 \le C_3 \le C_6 \le C_{12}$$

is

$$\langle w^{12} \rangle \le \langle w^4 \rangle \le \langle w^2 \rangle \le \langle w \rangle$$

The FFT: initialization

Goal is to compute DFT (Discrete Fourier Transform) using "divide and conquer" strategy in O(N log N) time.

Fix $N \in \mathbf{N}$ and $\omega = e^{2\pi i/N}$. Let

$$C_1 = H_0 \leq H_1 \leq \cdots \leq H_{n-1} \leq H_n = C_N$$

be a chain of subgroups of C_N.

Roughly: O(N log N) because we take n steps, each O(N). And n = O(log N).

Start with $\mathbf{x} = \begin{bmatrix} f(0) \\ \vdots \\ f(N-1) \end{bmatrix}$.

At each step, $\mathbf{x}$ represents current state, $\mathbf{y}$ represents new state.

Goal is to end up with $\mathbf{x} = \begin{bmatrix} \hat{f}(0) \\ \vdots \\ \hat{f}(N-1) \end{bmatrix}$.

i=1 to n

The FFT: main loop, $i = 1$ to n H_{i-1} old, H_i new

1. *Notation.* Suppose that $H_{i-1} = \langle \omega^m \rangle$ and $H_i = \langle \omega^k \rangle$, where k divides m, so $m = kd$ for some $d > 0$. (Use the transversal $1, \omega^k, \omega^{2k}, \ldots, \omega^{(d-1)k}$ for H_{i-1} in H_i.)
2. *Fill entries corresponding to H_i.* For $j = 0$ to $(N/k) - 1$ (i.e., jk ranges over all exponents of ω appearing in H_i, or ω^{jk} ranges over all elements of H_i), set

$$y(jk) = \sum_{r=0}^{d-1} x(jm + rk)\omega^{-rkj}.$$

   Think: jm is "offset" (starting point coming from the old subgroup H_{i-1}) and rk as stepping through the exponents in the coset representatives $1, \omega^k, \omega^{2k}, \ldots, \omega^{(d-1)k}$.
3. *Translate the subgroup fill to entries corresponding to the cosets of H_i in C_N.* (Clearer to do than write out.)
4. *Set current state to new state and loop.*

Example: FFT for $C_1 \le C_2 \le C_4$

$N=4$ $\quad w = e^{\frac{2\pi i}{4}}$ $\quad w^4 = 1$

$n=2$ $\quad \langle w^4 \rangle \le \langle w^2 \rangle \le \langle w \rangle$

$i=1 \qquad i=2$

Start: $\underline{x} = \begin{bmatrix} f(0) \\ f(1) \\ f(2) \\ f(3) \end{bmatrix}$

$\{w^0, w^2\}$

$\boxed{i=1}$

$H_0 = \langle w^4 \rangle \quad \underbrace{H_1 = \langle w^2 \rangle^{k=2}}_{\text{fill entries } 0,2}$ $\quad \geq$

$n=4$

$d = \frac{4}{2} = 2$

$j = 0$ to 1:

$$y(2j) = \sum_{r=0}^{1} x(\cancel{4j} + 2r) w^{-2rj}$$

$$y = \begin{bmatrix} x(0)+x(2) \\ x(1)+x(3) \\ x(0)+x(2)\,w^{-2} \\ x(1)+x(3)\,w^{-2} \end{bmatrix}$$

H

i

Subgroup stage computes DFT correctly for H_i.

$$j=0: \quad y(0) = \sum_{r=0}^{1} x(2r) = x(0)+x(2)$$

$$j=1: \quad y(2) = \sum_{r=0}^{1} x(2r)\,w^{-2r}$$

$$= x(0)\,w^{-0} + x(2)\,w^{-2}$$

Translate step: Same thing, except increment indices of x by 1 from entry above.

End result: Set $\underline{x} = \underline{y} = \begin{bmatrix} f(0)+f(2) \\ f(1)+f(3) \\ f(0)+f(2)w^{-2} \\ f(1)+f(3)w^{-2} \end{bmatrix}$

$i=2$ $\quad H_1 = \langle w^2 \rangle$, $H_2 = \langle w \rangle = C_4$

$m=2 \qquad k=1$

$d=2 \quad j=0$ to 3

$$y(j) = \sum_{r=0}^{1} x(2j+r)\, w^{-rj}$$

$$y(0) = \sum_{r=0}^{1} x(r) = x(0)+x(1)$$

$$y(1) = \sum_{r=0}^{1} x(2+r)W^{-r} = x(2) + x(3)W^{-1}$$

$$y(2) = \sum_{r=0}^{1} x(r)W^{-2r} = x(0) + x(1)W^{-2}$$

$$y(3) = \sum_{r=0}^{1} x(2+r)W^{-3r} = x(2) + x(1)W^{-3}$$

<u>Result</u>

$$y(0) = f(0) + f(1) + f(2) + f(3) = f(0)$$

$$y(1) = f(0) + f(2)W^{-2} + f(1)W^{-1} + f(3)W^{-3}$$

Example: FFT for $C_1 \leq C_3 \leq C_6 \leq C_{12}$