We are all in this together

And we will get through this together.

- Use a laptop or desktop with a large screen so you can read these words clearly.
- To conserve bandwidth, please turn off your camera.
- Please mute your microphone unless I call on you.
- Please have the chat window open to ask questions.
- Reading for today: 10.3, 11.2. (The end! And Ch. 11 not on final.)
- PS11 outline due Thu; PS11 due on last day of class.
- Problem session Fri 10:30–noon.
- Today's DJ: Jiaqi.

Revisions: I'll take revisions (at least) up until Tue May 19 (last day of finals).

Final: Fri May 15, 9:45-noon
(upload starts 11:45am)

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

Take fixed a and multiply by the different h in H, compile results.

$$aH = \{ah \mid h \in H\}. \tag{1}$$

Right coset: Ha
= { ha | h in H}
If ah $\neq$ ha, get differ result.

If the context is clear, instead of saying "left multiplicative coset", we just say **coset**. (In particular, since we mainly care about abelian groups, we won't worry too much about left cosets vs. right cosets.)

In Ch 7: We saw additive cosets

r + I = { r + a | a in I }, i.e., take fixed element r and look at results when add all of different elts of I to it.

Example: $\langle 4 \rangle$ in $G = \mathbf{F}_{17}^{\times}$

$\mathbf{F}_{17} = \mathbb{Z}/(17)$

$H = \langle 4 \rangle = \{1, 4, 16, 13\}$ = all pwrs of 4

Cosets of H in G?

$4H = 4\{1,4,16,13\} = \{4,16,13,1\} = H = 1H$

$5H = 5\{1,4,16,13\} = \{5,3,12,14\} = 3H$

$15H = 15\{1,4,16,13\} = \{15,9,2,8\} = 8H$

$6H = 6\{1,4,16,13\} = \{6,7,11,10\} = 7H$

These four cosets: (1) are all the same size and (2) they hit every element of G exactly once, with no overlaps. I.e., every elt of G is in exactly one coset of H.

Partitions

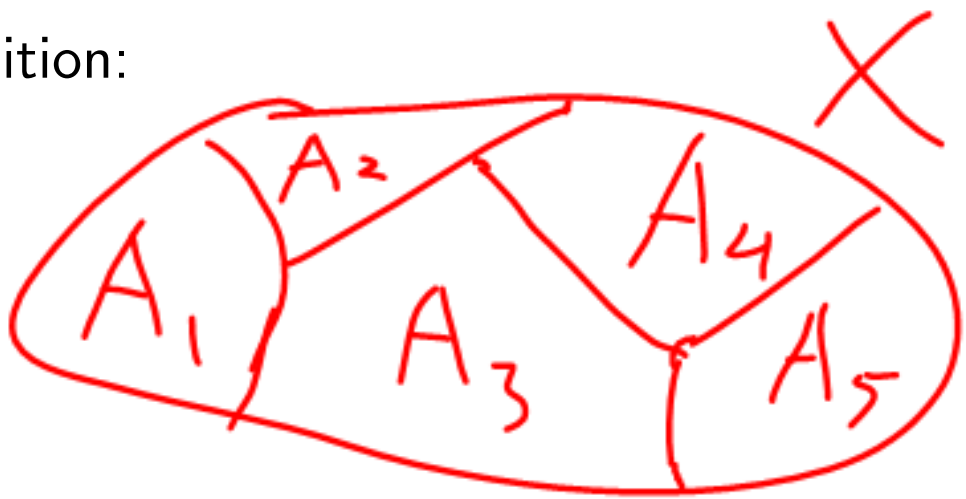
To describe the key property of cosets that we need to make money, we need the following idea.

Definition

Let X be a set, and let $\{A_1, \ldots, A_n\}$ be a collection of subsets of X. To say that $\{A_1, \ldots, A_n\}$ **partition** X means that:

1. (Nonempty) Each $A_i \neq \emptyset$;
2. (Cover) $X = \bigcup_{i=1}^{n} A_i$ (i.e., X is the union of the A_i); and
3. (Pairwise disjoint) If $i \neq j$, then $A_i \cap A_j = \emptyset$.

Picture of a partition:



Lemma: If b is in aH, then bH = aH.

Proof: Suppose b in aH.

Then by defn, b = ah for some h in H.

Because H is a subgroup of G, any element of the form bh' = a(h'h) is in aH, since h'h is in H (closure of H under multiplication).

Conversely, since a = bh^{-1}, any element of the form ah' = b(h^{-1}h') is in bH.

So the two sets are equal.

(See HW problem 7.2.3.)

Cosets partition G

Theorem 3

Let G be a finite group and let H be a subgroup of G. Consider all left cosets of H, and choose one element a_i from each coset of H so that $\{a_1H, \ldots, a_nH\}$ contains each coset of H exactly once. Then $\{a_1H, \ldots, a_nH\}$ partitions G.

Proof: Check: sets nonempty, cover G, disjoint.

Nonempty: H contains 1, so a_i H contains a_i, so nonempty.

Cover: For g in H, gH must be one of these cosets, and g in gH, so g = a_i H for one of the chosen a_i.

Disjoint: If $a_iH \cap a_jH \neq \emptyset$, then $a_iH = a_jH$.

If

then $x \in a_iH \Rightarrow a_iH = xH$

& $x \in a_jH \Rightarrow a_jH = xH$

so $a_iH = a_jH$.

Transversals

Transversal = choice of a particular name for each coset of H in G.

Definition

Let G be a finite group, and let H be a subgroup of G. A choice of coset representatives like the set $\{a_1, \ldots, a_n\}$ in the statement of Theorem 3 is called a **transversal** for H in G. In other words, to say that $\{a_1, \ldots, a_n\}$ is a transversal for H in G means that

$$G = a_1 H \cup \cdots \cup a_n H \tag{2}$$

and that for $i \neq j$, $a_i H \cap a_j H = \emptyset$ (i.e., $a_i H$ and $a_j H$ are disjoint).

Example: Consider $H = \langle 4 \rangle = \{1, 4, 16, 13\}$ in $G = \mathbf{F}_{17}^{\times}$.

One transversal for H in G is: {1, 8, 10, 12} because:

1H = {1,4,16,13}
8H = {2,8,9,15}
10H = {6,7,10,11}
12H = {3,5,12,14}

each coset named once
all elts G covered.

The FFT is a clever way to compute DFT using well-chosen transversals.

Proving some previously used theory

Fact: For $H \leq G$ and $a \in G$, the coset aH has the same number of elements as H does, i.e., all cosets of H contain the same number of elements.

Corollary 1

Let G be a finite group, and let H be a subgroup of G. Then the order of H (number of elements in H) divides the order of G.

Corollary 2

G has N elements

(We used this in finite fields)

Let G be a finite group of order N, and let a be an element of G. Then the order of a divides N.

smallest positive power of a equal to 1

Sketch:

H has m elts

Cor 1: $G = a_1H \cup a_2H \cup \cdots \cup a_kH$, disjoint

each has m elts

So G has mk elts.

Cor 2: Order of a = # elts in $\langle a \rangle$.

The Discrete Fourier Transform (DFT)

$\omega^N = 1$

Definition

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. We define the DFT of f to be $\hat{f} : \mathbf{Z}/(N) \to \mathbf{C}$ given by

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

saw (sort of)

Last: We ~~say~~ that if we can compute the DFT quickly (faster than $O(N^2)$), all kinds of good stuff happens.

(fast mult. $\Rightarrow$ fast matrix?)

Goal: Fast(er) DFT.

Example: $N = 12$

Writing out the definition of $\hat{f}(k)$ for $N = 12$, we get

$$\hat{f}(0) = \frac{1}{12}(f(0) + f(1) + f(2) + \cdots + f(11))$$

$$\hat{f}(1) = \frac{1}{12}(f(0) + \omega^{-1} f(1) + \omega^{-2} f(2) + \cdots + \omega^{-11} f(11))$$

$$\hat{f}(2) = \frac{1}{12}(f(0) + \omega^{-2} f(1) + \omega^{-4} f(2) + \cdots + \omega^{-10} f(11))$$

$$\hat{f}(3) = \frac{1}{12}(f(0) + \omega^{-3} f(1) + \omega^{-6} f(2) + \cdots + \omega^{-9} f(11))$$

$$\hat{f}(4) = \frac{1}{12}(f(0) + \omega^{-4} f(1) + \omega^{-8} f(2) + \cdots + \omega^{-8} f(11))$$

$$\hat{f}(11) = \frac{1}{12}(f(0) + \omega^{-11} f(1) + \omega^{-10} f(2) + \cdots + \omega^{-1} f(11))$$

pwrs of ω^{-1}

pwrs of ω^{-2}

$k=0$

$k=1$

$k=2$

pwrs of ω^{-k}

$\hat{f}(k) = \frac{1}{12}(f(0) + \omega^{-k} f(1) + \omega^{-2k} f(2) + \cdots)$

B/C $\omega^{12} = 1$, all pwrs of ω are (mod 12)

Keeping the exponents of the omegas negative is a convention of this class. We could choose to make them positive, but formula for DFT naturally uses negative exponents. (Rather: the generalization of DFT to integrals very naturally uses negative exponents.)

Note that inverse DFT uses positive exponents, consistent with our using negative exponents for DFT.

Subgroups of C_N

$C_6 = \langle w_6 \rangle$

$w_6 = e^{\frac{2\pi i}{6}}$

Theorem

Fix a positive integer N and let $\omega = e^{2\pi i/N}$. If $N = dq$ for positive $d, q \in \mathbf{Z}$, then C_d (the group of complex dth roots of unity) is precisely $\langle \omega^q \rangle$, the subgroup of C_N generated by ω^q.

Example: $N = 12$, $\omega = \omega_{12} = e^{2\pi i/12}$, so $\omega^{12} = 1$.

$\langle \omega \rangle = \{1, w, w^2, w^3, \cdots, w^{10}, w^{11}\} = C_{12}$

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

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

$\langle \omega^{12} \rangle = \{1\} = C_1$

Smaller subgroup is generated by a bigger power of omega.

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

This is the algebraic structure we need for FFT, N=12.

The Fast Fourier Transform based on $H_0 \leq \cdots \leq H_n$

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

$$C_1 = H_0 \leq H_1 \leq \cdots \leq H_{n-1} \leq H_n = C_N \tag{3}$$

As we go through algorithm:

$\mathbf{x} = \begin{bmatrix} x(0) \\ \vdots \\ x(N-1) \end{bmatrix}$ is current state, $\mathbf{y} = \begin{bmatrix} y(0) \\ \vdots \\ y(N-1) \end{bmatrix}$ new state.

Initialize: Let $\mathbf{x} = \begin{bmatrix} f(0) \\ \vdots \\ f(N-1) \end{bmatrix}$.

(I.e., we start with data for original signal f and step-by-step, turn it into the date for the DFT $\hat{f}$.)

Main loop of the FFT

For $i = 1$ to n: Suppose $H_{i-1} = \langle \omega^m \rangle$, $H_i = \langle \omega^k \rangle$.
Since $H_{i-1} \leq H_i$, $m = kd$ for some $d \in \mathbf{Z}$. Use the standard transversal $1, \omega^k, \omega^{2k}, \ldots, \omega^{(d-1)k}$ for H_{i-1} in H_i.
Fill subgroup: For $j = 0$ to $(N/k) - 1$ (i.e., ω^{jk} ranges over all elements of H_i), set

$$\begin{aligned} y(jk) &= \sum_{r=0}^{d-1} x(jm + rk)\omega^{-rkj} \\ &= x(jm) + x(jm + k)\omega^{-kj} + x(jm + 2k)\omega^{-2kj} + \ldots. \end{aligned}$$

Translate: For $\ell = 1$ to $k - 1$ and $j = 0$ to $(N/k) - 1$, we set

$$y(jk + \ell) = \sum_{r=0}^{d-1} x(jm + rk + \ell)\omega^{-rkj}. \tag{4}$$

Set current state to new state and loop. Set $\mathbf{x} = \mathbf{y}$ and loop.
Rescale. Divide every entry of $\mathbf{x}$ by N.

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