Math 127, Wed May 11

Midterms: 8Q, 75 min
Final: 14 (+1) Q, 135 min

- Reading for today: 10.3, 11.1.
- Reading for Wed May 11: 11.2.
- PS10 outline due ~~today(-ish)~~ tomorrow (-ish)
- **FINAL EXAM** on **THU MAY 19**. Study guide and sample posted tomorrow.

9:45 - noon } Plan to use entire time
Here (MH 233)

Mon: PS10, FFT

Recap 1: Groups and abelian groups

Ex G is $F^\times$ or subgps

Definition

A **group** is a set G along with a binary operation $\cdot$, usually written as multiplication, such that the following axioms are satisfied.

1. *(Associativity)* For any $a, b, c \in G$, $(ab)c = a(bc)$.
2. *(Identity)* There exists an element $1 \in G$ such that $1a = a = a1$ for all $a \in G$.
3. *(Inverses)* For every $a \in G$, there exists some $a^{-1} \in G$ such that $aa^{-1} = 1 = a^{-1}a$.

Definition

Let G be a group. To say that G is **abelian** means that for all $a, b \in G$, we have that $ab = ba$.

Recap 2: Subgroups and cyclic subgroups

Theorem (Subgroup Theorem)

Let G be a group, and let S be a subset of G. Then S is actually a subgroup of G if and only if all three of the following conditions hold.

1. *(Identity) $1 \in S$ (i.e., S contains the multiplicative identity of G).*
2. *(Multiplicative closure) S is closed under the operation of G, i.e., if $a, b \in S$, then $ab \in S$.*
3. *(Inverse closure) S is closed under taking inverses, i.e., if $a \in S$, then $a^{-1} \in S$.*

Important special case: Cyclic subgroup generated by a is $\langle a \rangle = \{a^n \mid n \in \mathbf{Z}\}$, e.g., if $\omega_n = e^{2\pi i/n}$, then $C_n = \langle \omega_n \rangle$.

Orders of elements

Request of Ch. 3, Ch. 7

(See Scream 5)

Definition

Let G be a group and let a be an element of G. If $a^n = 1$ for some positive integer n, we define the **order** of a to be the *smallest* possible n such that $a^n = 1$.

Theorem

(Ch. 7)

Let G be a group and let a be an element of G of finite order n. Then the order of a^k is $\dfrac{n}{\gcd(k,n)}$. Special case: If d divides n, then the order of a^d is n/d.

Example: Suppose $\mathrm{ord}(a) = 14$.

What is $\mathrm{ord}(a^5)$?

1. Direct method $b = a^5$

Compute b^k until get 1.

$\mathrm{ord}(a) = 14$

$b^1 = a^6$

$b^2 = a^{12}$ $\cdot a^6$

$b^3 = a^{18} = a^4$ $\cdot a^6$

$b^4 = a^{10}$

$b^5 = a^{16} = a^2$

$b^6 = a^8$

$b^7 = a^{14} = 1$

ord(b) = 7

$a^{14} = 1$ so exps mod 14

Reduce every time!

Yay!

2. Thm

$$\text{ord}(a^6) = \frac{14}{\gcd(6,14)} = \frac{14}{2} = 7$$

Note: 6, 12, 4, 10, 2, 8, 14 = 0 is all mults of 2 (mod 14)

How do you go from b^3 to b^4?

Ans $b^4 = b^3 \cdot b$

So to take powers of $b = a^6$, you mult each result in turn by $b = a^6$, reduce each time.

Cosets

Believe it or not, the following idea is what makes the FFT work.

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

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

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

Example: $G = \mathbf{F}_{19}^{\times}$ of order 18, $H = \langle 7 \rangle$. Cosets:

$H = \langle 7 \rangle = \{1, 7, 7^2 = 11, 7^3 = 77 = 1\}$

$H = \{1, 7, 11\}$

$3H = 3\{1,7,11\}$

$= \{3(1), 3(7), 3(11)\}$ $\{2,3,14\}$

$= \{3, 21, 32\} = \{3, 2, 14\}$

$7H = 7\{1,7,11\}$

$= \{7, 7^2 = 11, 7^3 = 1\} = \{1,7,11\} = H$

$2H = 2\{1,7,11\} = \{2,14,22\} = \{2,14,3\}$

$= 3H$

(In gen'l, if $b \in aH$, $bH = aH$)

1H = {1, 7, 11} = 7H = 11H

3H = {2, 3, 14} = 2H = 14H

5H = {5, 35, 55} = {5, 16, 17} = 16H = 17H

4H = {4, 28, 44} = {4, 9, 6}

8H = {8, 56, 88} = {8, 18, 12}

10H = {10, 70, 110} = {10, 13, 15} = 13H = 15H

{1, 7, 11}, {2, 3, 14}, {4, 6, 9} = $\mathbb{F}_{19}^{\times}$

{5, 16, 17}, {8, 12, 18}, {10, 13, 15}

Can start w/ any H

and pick a's until ally

exhaust all elts of G.

Cosets are either equal or disjoint

Theorem

Let H be a subgroup of a group G, and let a be an element of G. If b is an element of aH, then $aH = bH$.

Definition

Let H be a subgroup of a group G, and let a be an element of G. A **representative** of the coset aH is an element b of aH. Note that if b is a representative of aH, then bH is an alternative name for aH.

Corollary

Let H be a subgroup of a group G, and let a and b be an elements of G. Then aH and bH are either disjoint or equal.

Previous example, revisited:

$10H = 13H$, but $10H \cap 4H = \emptyset$

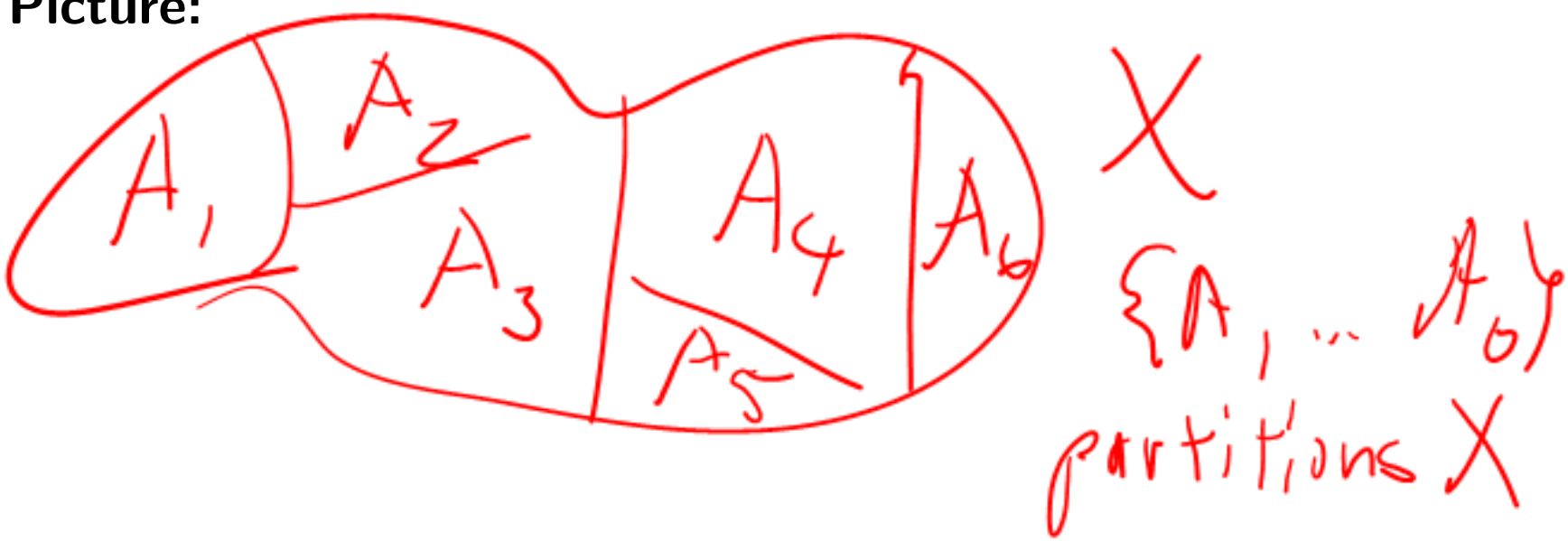
Partitions

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:



Cosets partition G

Theorem

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.

Example:

$14 = \{1, 7, 11\}, \{2, 3, 14\}, \{4, 6, 9\}$

$= \{5, 16, 7\}, \{8, 12, 18\}, \{10, 13, 15\}$

$2H$ $4H$ H $5H$ $8H$ $10H$

partition of H in G

Transversals

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 the "cosets partition" theorem 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

$$G = a_1H \cup \cdots \cup a_nH$$

and that for $i \neq j$, $a_iH \cap a_jH = \emptyset$ (i.e., a_iH and a_jH are disjoint).

Previous example, revisited one more time:

$H = \{1, 7, 11\}$ $G = H, aH, a^2H$

Then $\{1, 2, 4, 5, 8, 10\}$

is a transversal for H in G.

Chains of C_n

When we have a chain like:

$\leq$ is a subgp of

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

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

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

$C_6 = \langle e^{\frac{2\pi i}{6}} \rangle = \langle \omega^2 \rangle$ $N=12$

$= \{1, \omega^2, \omega^4, \omega^6, \omega^8, \omega^{10}\}$

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

$$= \{1, w^4, w^8\}$$

$$C_1 = \{1\}$$

The FFT: initialization

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.

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

The FFT: main loop, $i = 1$ to n

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 $C_1 \leq C_2 \leq C_4$

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