Math 127, Mon May 10

Revisions: PS01-04 due Fri May 21. Other revisions due Wed May 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: 10.1–10.3. Last reading in course: 11.1–11.2.
- Final exam, **Wed May 19**.

Final will be cumulative.
I'll try to catch up on grading as much as possible before the final.
New material: Definitely Chs 9 and 10, maybe Ch 11?
Study guide on Wed.

Recap: The DFT

$\omega^N = 1$

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

$k=3$

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

ω^{-3n}

Punchline: This is an $O(N^2)$ algorithm, that, if we can speed it up to $O(N \log N)$, we can use to make serious money.

Solution comes from, of all places, some even more abstract algebra: **groups**.

$N=4$ $\quad w^4=1$ $\quad w^{-4}=1$

DFT

$$\hat{f}(0)=\frac{1}{4}\left(f(0)+f(1)+f(2)+f(3)\right)$$

$$\hat{f}(1)=\frac{1}{4}\left(f(0)+f(1)w^{-1}+f(2)w^{-2}+f(3)w^{-3}\right)$$

$$\hat{f}(2)=\frac{1}{4}\left(f(0)+f(1)w^{-2}+f(2)+f(3)w^{-2}\right)$$

$$\hat{f}(3)=\frac{1}{4}\left(f(0)+f(1)w^{-3}+f(2)w^{-2}+f(3)w^{-1}\right)$$

Groups and abelian groups

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 $aa^{-1} = 1 = a^{-1}a$.

Some important groups don't have commutative multiplication, but:

Definition

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

All of the groups we're really interested in are abelian.

In this class:

Our favorite example of a group

irr

$F = \mathbb{C}, \mathbb{Z}/(p) = \mathbb{F}_p, \mathbb{F}_p[x]/(m(x))$

Let F be a field, and let $F^\times$ be the **multiplicative group of** F (i.e., $F - \{0\}$).

1. For $a, b, c \in F^\times$, $(ab)c = a(bc)$ because multiplication is associative in all of F, and therefore in $F^\times$.
2. $1 \neq 0$, so $F^\times$ has an identity element.
3. By the definition of field, every nonzero element of F has an inverse, which is itself nonzero, so every element of $F^\times$ has an inverse in $F^\times$.

Or actually: We're going to use certain **subgroups** of $F^\times$.

Ch. 11: $F^\times = \mathbb{C}^\times = \mathbb{C} - \{0\}$

Subgroups

In the study of "foo" theory: A subFOO of a FOO is a subset of a FOO that is itself a FOO under the same operation(s) of the big FOO. True in all kinds of abstract algebra.

Definition

Let G be a group. A **subgroup** of G is a subset of G that is itself a group, using the same operation as G.

Notation: $H \leq G$ means H is a subgroup of a group G.

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 $a^{-1} \in S$.*

Compare Subspace Test: subspace contains 0, closed +, closed sc mult.

The key example for the FFT

$\omega^n = 1$

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

$$C_n = \{1, \omega, \omega^2, \ldots, \omega^{n-1}\}.$$

See PS10

$\omega^n = 1$

See PS10

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.*

E.g.: Every 3rd root of unity is also a 12th root of unity.

We'll use subgroup chains like

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

to describe the Fast Fourier Transform (FFT).

Details on $C_1 \le C_2 \le C_4 \le C_8 \le C_{16}$

Fix $N = 16$, $w = e^{\frac{2\pi i}{16}}$, $w^N = w^{16} = 1$

$w = w_{16}$

$C_1 = \{1\}$

$C_2 = \{1, -1\} = \{1, w^8\}$

$C_4 = \{1, w^4, w^8, w^{12}\}$

$w^2 = e^{2\pi i/8}$

$C_8 = \{1, w^2, w^4, w^6, w^8, \ldots, w^{14}\}$

$C_{16} = \{1, w, w^2, \ldots, w^{15}\}$

Cyclic (sub)groups

Definition

Let G be a group and a an element of G. We define the **cyclic subgroup generated by** a to be

$$\langle a \rangle = \{a^n \mid n \in \mathbf{Z}\}, = \{\ldots, a^{-1}, \overset{1}{\overset{\parallel}{a^0}}, a, a^2, \ldots\}$$

the set of all powers of a, positive, negative, and zero. If $\langle a \rangle$ happens to be equal to the entirety of G, we say that G is **cyclic**, and that G is **generated by** a.

FFfFF: The multiplicative group of a finite field is cyclic.

Example

For a positive integer n, let $\omega_n = e^{2\pi i/n}$. Then $C_n = \langle \omega_n \rangle$, and therefore, C_n is cyclic.

Orders of elements

$$\omega_n = e^{\frac{2\pi i}{n}}$$

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 $a^n = 1$. Ex $\text{order}(\omega_n) = n$

Theorem

Let G be a group and let a be an element of G of order n. Then $k = \ell$ in $\mathbf{Z}/(n)$ if and only if $a^k = a^\ell$.

I.e., exponents are computed mod order of element a. See: BCH codes.

Corollary

Let G be a group, $a \in G$ of order n. Then $a^k = 1$ if and only if and only if $k = 0$ in $\mathbf{Z}/(n)$, or in other words, if and only if k is a multiple of n.

Orders of elements, cont.

(Explanation of some of those facts about finite fields)

Corollary

Let G be a group, $a \in G$ of order n. Then the cyclic subgroup $\langle a \rangle$ contains n elements (i.e., has order n).

Theorem

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.

See: BCH codes

Example:

If α prim elt of $\mathbb{F}_{64}$

$\operatorname{ord}(\alpha) = 63$

$\operatorname{ord}(\alpha^7) = \frac{63}{7} = 9$

So this is where we get an element of order 9 to construct a BCH code of length 9.

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

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

a fixed, h varies over all elements of subgroup H

If the context is clear, instead of saying "left multiplicative coset", we just say **coset**. $= \mathbb{Z}/(19)$ (mod 19)

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

$49 = 11$

$77 = 1$

$\mathrm{ord}(7) = 3$

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

$$5H = \{5 \cdot 1, 5 \cdot 7, 5 \cdot 11\} = \{5, 16, 17\}$$

$$= 16H = 17H$$

$$8H = \{8\cdot 1, 8\cdot 7, 8\cdot 11\} = \{8, 18, 12\} = 18H = 12H$$

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

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

$$4H = \{4, 9, 6\}$$

$$10H = \{10\cdot 1, 10\cdot 7, 10\cdot 11\}$$

$$= \{10, 13, 15\}$$

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 element of G. Then aH and bH are either disjoint or equal.

Previous example, revisited:

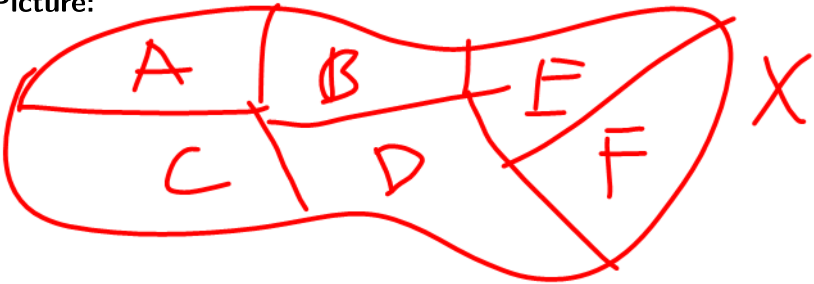
Partitions

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.

$G = \mathbb{F}_{19}^{\times}$

Example:

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

$5H = \{5, 16, 17\}$ $\quad 4H = \{4, 6, 9\}$

$8H = \{8, 12, 18\}$ $\quad 10H = \{10, 13, 15\}$

$G = H \cup 2H \cup 4H \cup 5H \cup 8H \cup 10H$

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 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

$$G = a_1 H \cup \cdots \cup a_n H$$

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).

Previous example, revisited one more time: