6.S897, Spring 2015, Lecture 1

Note Title 1/25/2015

Administrivia:

1. Scribe
2. Project
3. Participation
4. Problem Set

- Course website:

  people.csail.mit.edu/madhu/ST15

  (ST = Spring term)

- Mailing list 6s897@csail.mit.edu

Course contents

- Quick Primer on Algebra
- Algorithms in Algebra
  - $+, *, /, --,$ GCD
  - Factorization:
    - Univariate + finite fields
    - " + rationals
    - Multivariate
  - Systems of Equations .... Primality.
- Complexity
  - Permanent vs. Determinant
  - Circuits, Formulas, Depth reduction
  - Lower bounds
  - Polynomial Identity Testing.

Today

- Membership testing in Groups.
- Motivation: "simplest algebraic problem"
- Context: Can every group on N elements be described "tractably" in $\text{polylog}\, N$ bits?
- **Still Open**

- Today will consider $G \leq S_n$, given by generators $T \subseteq S_n$.
- Can we decide if $\sigma \in S_n$ belongs to $\langle T \rangle$?
- Answer: Yes, in time $\text{poly}(n, |T|)$.

(Permutation) Group Membership

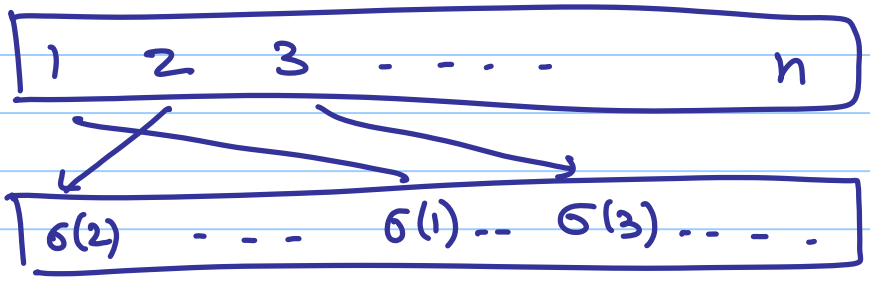
Problem: Given $\pi_1, \ldots \pi_\ell$ generating $G \leq S_n$ & $\sigma \in S_n$

decide if $\sigma \in G$

(in time poly(n, ℓ))

Visualizing the problem.

Move



to

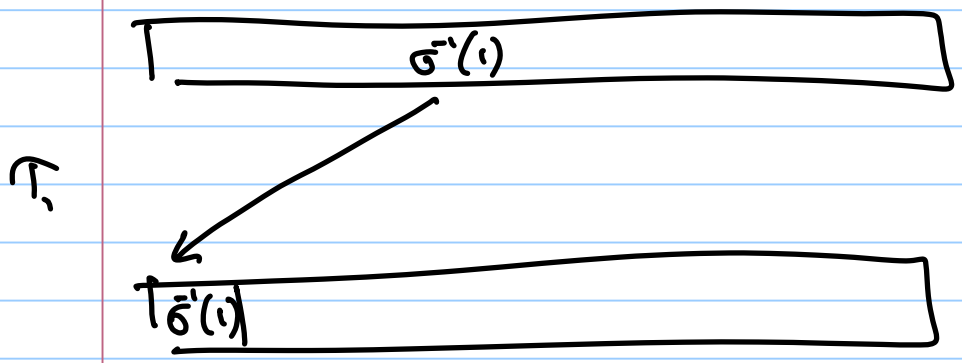
using sequence of moves from

$\pi_1, \pi_2 \ldots \pi_\ell$ (with repetitions)

Algorithm Idea

Hope to implement natural strategy

find $\tau_1 \in G$ s.t.



Now fix $\sigma^{-1}(1)$ & only use permutations

$\tau_2, \tau_3, \ldots$ that fix $1, 2, \ldots$

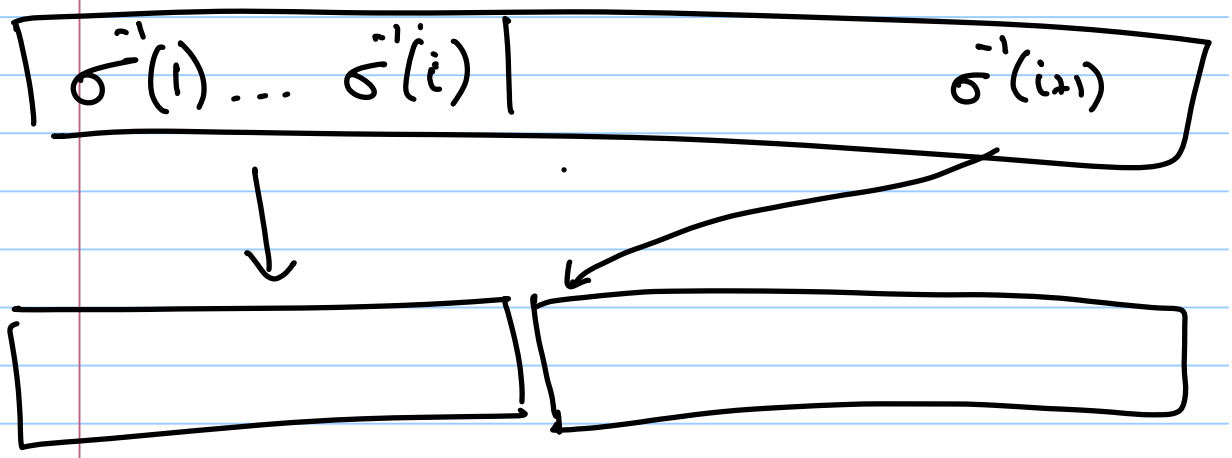
What if no such $\tau_1 \in G$?

$\Downarrow$

$\sigma \notin G$ (since σ maps $\sigma^{-1}(1) \to 1$)

Contd.

after i steps, want τ_{i+1}



Why does $\tau_{i+1} \in G$ exist? (if $\sigma \in G$)

(all moves so far can be inverted...)

$\sigma \cdot \tau_1^{-1} \cdots \tau_{i-1}^{-1} \cdot \tau_i^{-1}$ is such a τ_{i+1}!

So idea ① find generators that facilitate finding τ_i's.

② Use them to determine if $\sigma \in G$ or prove $\sigma \notin G$.

Towards Algorithm

1. Strong Generating Set : Defn.
2. Membership alg. given SGS
3. finding SGS & syzygies.

Definitions

1. $G_k \leq G$ is subgroup fixing elements $1 \dots k$

$$G_k = \{ \pi \in G \mid \pi(i) = i \quad \forall i \in [k] \}$$

2. $\text{Pairs}(G) = \{ (i,j) \mid 1 \leq i < j \leq n$ s.t. $\exists \tau_{ij} \in G_{i-1}$ $\tau_{ij}(j) = i \}$

③ S is <u>SGS</u> for G if

$\forall (i,j) \in Pairs(G)$

$\exists! \tau_{ij} \in S$ s.t $\tau_{ij} \in G_{i-1}$

$\tau_{ij}(j) = i$

SGS-Based-Membership (S, σ, i)

/* S SGS for G */

/* $\sigma \in G_i$ */

if $\sigma(i+1) = i+1$ return SGS-B-M$(S, \sigma, i+1)$

else let $j = \sigma^{-1}(i+1)$

- $\tau = \tau_{i+1,j} \in S \in G_{i+1}$

  w. $\tau(i+1) = j$

- Return $\tau \cdot \omega$ where

  $\omega =$ SGS-B-M$(S, \sigma \cdot \tau, i+1)$

Analysis: Obvious ☺

Finding SGS

① first: obviously they exist...
we proved this.

② But how to find them.

Alt. characterization

Lemma: S is SGS for $G = \langle T \rangle$

① $S \subseteq G$

② $\forall (i,j) \in Pairs(G) \quad \exists! \, T_{ij} \in S$

③ $\forall T_1, T_2 \in T \cup S$

$T_1 \cdot T_2 \in |S\rangle$ ← Ⓐ

↑ defined in four pages.

$$|S\rangle \triangleq \{ \tau_1 \cdot \tau_2 \cdots \tau_\ell \mid \tau_i \in S \quad Class(\tau_i) < Class(\tau_{i+1}) \}$$

$$Class(\tau_i) = \max \{ j \mid \tau_i \in G_j \}$$

Algorithmic Claims

① $\sigma \in |S\rangle$ can be decided efficiently (just like Member)

② for $\sigma \notin |S\rangle$ let $\sigma \perp S$ be final el't where progress can't be made.

$\sigma \perp S$ can be found eff'ly.

③ SGS(T):

$S \leftarrow \phi$

while $\exists \tau_1, \tau_2 \in S \cup T$ s.t.

$\tau_1 \cdot \tau_2 \notin |S\rangle$

$S \leftarrow S \cup (\tau_1 \cdot \tau_2 \perp S)$

Clearly SGS makes $\leq n(n-1)$ iterations

④ $|S\rangle \triangleq \{ \sigma_\ell \sigma_{\ell-1} \cdots \sigma_1 \mid \sigma_i \in S$, $\text{type}(\sigma_i) < \text{type}(\sigma_{i+1}) \}$

$\text{type}(\sigma) \triangleq \max k$ s.t. $\sigma \in G_k$.

Proof of Lemma

Complex Induction / Contradiction.

- Will prove that for all

$\tau, \sigma \in |S\rangle$, we have

$\tau \cdot \sigma \in |S\rangle$

- Suffices: Why? $|S\rangle$ is a subgroup of S_n;

$T \in |S\rangle \Rightarrow |S\rangle = \langle T \rangle$

- Proof that $|S\rangle \cdot |S\rangle \subseteq |S\rangle$:

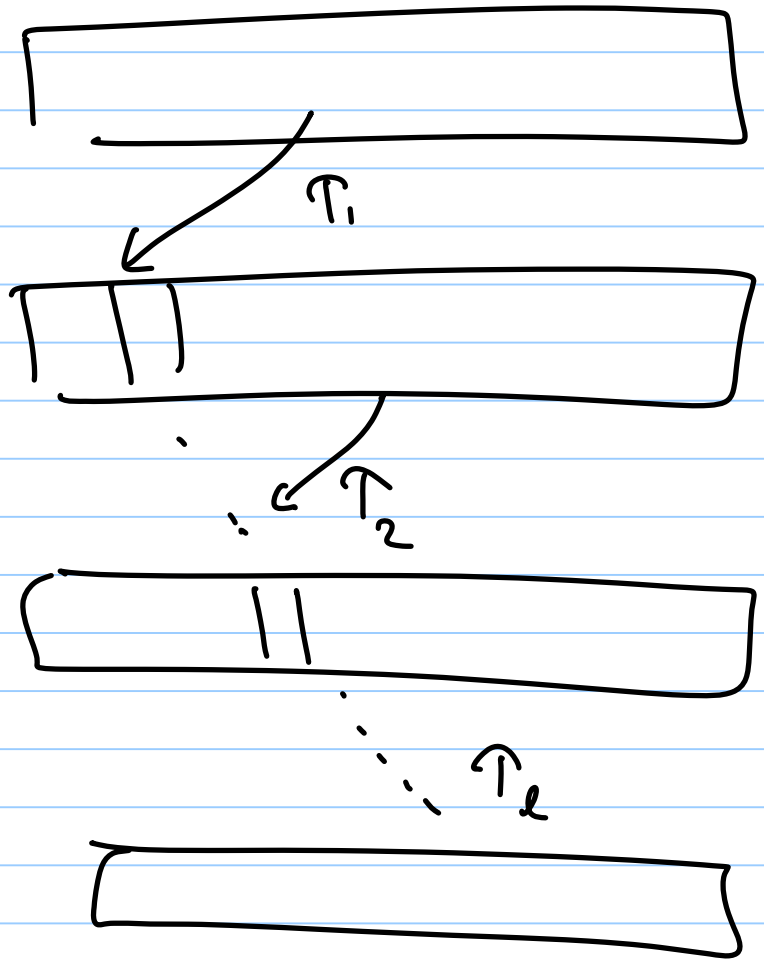
Key idea: induction on complexity of $\tau \cdot \sigma$;

say $\tau = \tau_\ell \cdots \tau_1 \quad \tau_i \in S$

$\sigma = \sigma_m \cdots \sigma_1 \quad \sigma_i \in S$

- What is type $(\tau_\ell \dots \tau_2)$?

- strictly > type $(\tau_\ell \dots \tau_2 . \tau_1)$



Either $\tau_1 . \sigma \notin |S|$

Or we have counterexample with smaller type (τ).

But we know $\tau \cdot \sigma_m \in |S\rangle$

(hypothesis)

& $\text{type}(\tau \cdot \sigma_m) = \text{type}(\tau)$

so $(\tau \cdot \sigma_m) \cdot (\sigma_{m-1} \cdots \sigma_1)$ gives

$\tau' \quad \sigma'$.

Counterexample with $\text{type}(\tau') = \text{type}(\tau)$

& $\text{length}(\sigma') < \text{length}(\sigma)$.

$\boxtimes$