Disclaimer: These are just notes for a lecture, not a polished writeup. In particular, references are missing. Use at your own discretion.

In this lecture we will solve the membership problem for subgroups of permutation groups.

First some notation. We use $[n]$ to denote the set $\{1, \ldots, n\}$ and $[k, n]$ to denote the set $\{k, k+1, \ldots, n\}$. A function $\pi : [n] \to [n]$ is a permutation if for every $i \neq j \in [n]$ it is the case that $\pi(i) \neq \pi(j)$.

Let S_n be the symmetric group on n elements, i.e., the group whose elements are permutations on n elements, and where $\pi \cdot \sigma$ is the composition of the two functions.

For $S \subseteq S_n$, let $\langle S \rangle$ denote the subgroup generated by S.

In this lecture we give an algorithm that takes as input $S \subseteq S_n$ and $\pi \in S_n$ and determines if $\pi \in \langle S \rangle$. (Food for thought: Among other things, this algorithm should prove $\pi \in \langle S \rangle$ or not, as the case may be. What do such proofs look like?)

This algorithm is due to Sims (Reference?). Good sources for reading this algorithm (in increasing order of simplicity) are Seress's book, Knuth's paper on perm groups, and these notes.

The central notion to this membership algorithm is a *strong generating set*. We define this notion (somewhat differently than others) below.

Throughout this lecture let n be fixed. Let $\mathrm{Sym}(k)$ denote the subgroup of S_n that fixes the set $[k+1, n]$. I.e., $\mathrm{Sym}(k) = \{\pi \in S_n | \pi(i) = i \ \forall i \in [k+1, n]\}$.

Definition 1 *For a group $G \subseteq S_n$, a set $T \subseteq G$ is a* strong generating set *for G if the following holds: For every $j < k \leq n$, if $\exists \pi \in G \cap \mathrm{Sym}(k)$ such that $\pi(k) = j$ then there exists a permutation $\sigma = \sigma_{jk} \in T \cap \mathrm{Sym}(k)$ such that $\sigma(k) = j$.*

A priori it is not clear that a strong generating set for G should even generate G. We will show however that it does do so in a strong sense.

For $\sigma \in S_n$, let $k(\sigma) = \min\{k | \sigma \in \mathrm{Sym}(k)\}$. For any set $T \subseteq G$ let $\overline{T}$ denote the set of elements that can be obtained by a multiplication of elements in T of increasing $k(\cdot)$ value. I.e., $\overline{T} = \{\sigma = \sigma_1 \cdot \sigma_2 \cdots \sigma_\ell | \sigma_i \in T, k(\sigma_i) < k(\sigma_{i+1})\}$.

Our first lemma shows that every group $G \subseteq S_n$ has a strong generating set T of size $O(n^2)$ and this generating set generates G in the strong sense that $G = \overline{T}$.

Lemma 2 *Fix group $G \subseteq \mathrm{Sym}(n)$.*

1. *G has a strong generating set of size $O(n^2)$.*
2. *For every strong generating set T of G, $G = \overline{T}$.*

Proof: For the first part, first notice that G is itself a strong generating set of G. So consider a minimal strong generating set T of G. For every $\sigma \in T$ we can associate a pair (j,k), $j < k \leq n$ such that $\sigma \in \mathrm{Sym}(k)$ and $\sigma(k) = j$. Notice that for $\sigma' \neq \sigma \in T$, the associated pairs (j',k') and (j,k) are distinct (or else we can delete one of σ or σ' and T will still be a strong generating set for G). Thus T has at most $\binom{n}{2}$ elements.

Now consider $\pi \in G$, with $k(\pi) = k$. We prove by induction on k that $\pi \in \overline{T}$. Note there must be an element $\sigma \in T$ with $k(\sigma) = k(\pi) = k$ and $\sigma(k) = \pi(k)$ (using the fact that T is a strong generating set for G). But now the element $\rho = \pi \cdot \sigma^{-1}$ satisfies the conditions $\rho \in G$, $k(\rho) < k$, and so $\rho \in \overline{T}$. Assume $\rho = \sigma_1 \cdots \sigma_\ell$. Note that $k(\sigma_\ell) = k(\rho) < k$. So $\phi = \rho\sigma = \sigma_1 \cdots \sigma_\ell \cdot \sigma$ is also in T. ∎

Note that the proof above essentially proves the correctness of the following algorithm for checking membership in G, given a strong generating set T.

Algorithm MEM: (n, T, π) /* $T \subseteq S_n, \pi \in S_n$ */

- If $\pi = 1$ return 1.
- Let $k = k(\pi)$.
- If there is a $\sigma \in T$ such that $k(\sigma) = k$ and $\sigma(k) = \pi(k)$, then return the sequence $\mathrm{MEM}(n, T, \pi \cdot \sigma^{-1})$ concatenated with σ, else return ERROR.

Thus Lemma 2, along with algorithm MEM shows how to check membership in any group $G \subseteq S_n$ given a strong generating set T, in time polynomial in $n, |T|$.

In fact, we note that the algorithm MEM is correct for checking membership in $\overline{T}$ for any set "minimal" set T, i.e., one in which for any pair $j < k$ there is at most one element $\sigma \in T$ with $k(\sigma) = k$ and $\sigma(k) = j$. This will be useful in getting an algorithm to produce a strong generating set T for a group G given by any generating set S. The following lemma gives a more recognizable characterization of a strong generating set.

Lemma 3 *T is a strong generating set for $\langle S \rangle$ if and only if (1) $T \subseteq \langle S \rangle$, (2) $S \subseteq \overline{T}$, and (3) $\forall \sigma, \tau \in T$, $\sigma \cdot \tau \in \overline{T}$.*

Proof: The forward direction (i.e., that a strong generating set satisfies (1)-(3)) is obvious. So we prove the reverse, namely that if T satisfies conditions (1)-(3) then it is a strong generating set for $\langle S \rangle$. We prove this indirectly. First we prove that $\overline{T}$ is closed under multiplication (using only condition (3)). This, along with the conditions (1) and (2) immediately imply $\overline{T} = \langle S \rangle$. We then use this equivalence to show that T satisfies the definition of a strong generating set for $\langle S \rangle$.

Stage 1: Consider $\sigma, \tau \in \overline{T}$. Let $\sigma = \sigma_1 \cdots \sigma_\ell$, where $\sigma_i \in T$ with $k(\sigma_i) < k(\sigma_{i+1})$ and let $k = k(\sigma)$. Similarly let $\tau = \tau_1 \cdots \tau_m$ with $\tau_i \in T$ and $k(\tau_i) < k(\tau_{i+1})$. We prove by double induction on k and then on m that $\sigma \cdot \tau \in \overline{T}$. (I.e. for any other pair σ', τ' with associated (k', m') with $k' < k$ or with $k' = k$ and $m' < m$, we assume the claim is true.)

Now if $k(\sigma_\ell) < k(\tau_1)$, then there is nothing to prove since $\sigma_1 \cdots \sigma_\ell \cdot \tau_1 \cdots \tau_j$ is syntactically in $\overline{T}$. So consider the case when $k(\tau_1) \leq k(\sigma_\ell)$. By property (3), we have $\sigma_\ell \cdot \tau_1 \in \overline{T}$ and so $\sigma_\ell \cdot \tau_1 = \alpha_1 \cdots \alpha_m$

with $\alpha_i \in T$ and $k(\alpha_i) < k(\alpha_{i+1})$. Now, since $k(\sigma_\ell), k(\tau_1) \leq k$, we have $\alpha_m \in \mathrm{Sym}(k)$ and $k(\alpha_i) < k$ for all $i < m$. Letting $\sigma' = \sigma_1 \cdots \sigma_{\ell-1}$ and $\alpha' = \alpha_1 \cdots \alpha_{m-1}$, we get $\sigma \cdot \tau_1 = \sigma' \cdot \alpha' \cdot \alpha_m$. Since $\sigma', \alpha' \in \overline{T}$ with $k(\sigma') < k$, we have $\sigma' \cdot \alpha' \in \overline{T}$. Furthermore $k(\sigma' \cdot \alpha') < k$ (since $k(\sigma'), k(\alpha') < k$) and so once again by induction we have $\sigma' \cdot \alpha' \cdot \alpha_m \in \overline{T}$ and thus $\sigma \cdot \tau_1 \in \overline{T}$. Furthermore $k(\sigma \cdot \tau_1) \leq k$ and so by induction on m, we have $(\sigma \cdot \tau_1) \cdot \tau_2 \cdots \tau_m \in \overline{T}$. We conclude that $\overline{T}$ is closed under multiplication.

Stage 2: We are now ready to do the cleaning up. Since T is contained in $\langle S \rangle$ (by (1)), we also have $\overline{T} \subseteq \langle S \rangle$. Since $S \subseteq \overline{T}$ (condition (2)), and $\overline{T}$ is closed under multiplication, we conclude that $\langle S \rangle \subseteq \overline{T}$. Thus $\overline{T} = \langle S \rangle$.

Stage 3: Consider $\pi \in \langle S \rangle$ with $k(\pi) = k$ and $\pi(k) = j < k$. Since $\overline{T} = \langle S \rangle$, we know that there exist $\pi_1 \ldots \pi_\ell \in T$ such that $\pi = \pi_1 \cdots \pi_\ell$ with $k(\pi_i) < k(\pi_{i+1})$. We conclude that $k(\pi_\ell) = k$ and $\pi_\ell(k) = \pi(k)$, showing that π_ℓ satisfies the conditions of the σ_{jk} as needed in the definition of the strong generating set. ∎

Based on the lemma above, the following algorithm suggests itself for finding a strong generating set for $\langle S \rangle$. (Below we use the notation $T \cdot T$ to denote the set $\{\tau_1 \cdot \tau_2 | \tau_1, \tau_2 \in T\}$.)

Algorithm SGS: (n, S) /* $S \subseteq S_n$ */

- Initialize $T \leftarrow \emptyset$.
- While there exists $\sigma \in S \cup T \cdot T - \overline{T}$ do
  - $T \leftarrow T \cup$ ADD-ELEMENT(n, T, σ).

Subroutine ADD-ELEMENT: (n, T, σ)

- If $\sigma = 1$ return 1;
- Else if $\exists \rho \in T$ with $k(\rho) = k(\sigma) = k$ and $\rho(k) = \sigma(k)$ return ADD-ELEMENT$(n, T, \sigma \cdot \rho^{-1})$.
- Else return σ.

To argue the correctness, we argue that T is always minimal (the only elements σ added to T satisfy the condition that T does not have any element σ' with $k(\sigma) = k(\sigma')$ and $\sigma(k) = \sigma(k')$). Furthermore, T is always a subset of $\langle S \rangle$, since any element added to T is a product of elements in the current set T, with possibly some element of S. Finally, when the algorithm concludes we have $S \subseteq \overline{T}$ and $T \cdot T \subseteq \overline{T}$, satisfying the characterization of a strong generator.

To analyze the running time of the algorithm SGS, we recall that the membership test $\sigma \in \overline{T}$? takes poly(n) time for minimal sets T. The while loop executes at most $\binom{n}{2}$ times since the size of T increases every time we execute it. Finally the subroutine ADD-ELEMENT takes polynomial time in n, since each recursive call reduces $k(\sigma)$.