6.885 Algebra and Computation	September 21, 2005
Lecture 4	
Lecturer: Madhu Sudan	*Scribe: Karola Mészáros*

Membership algorithm for the permutation group

In the last lecture we only sketched the proof of Gauss's lemma.

Exercise 1. Prove Gauss's lemma rigorously.

The problem we are considering today is as follows: given a group G, subgroup of the symmetric group S_n, and an element $\pi \in S_n$, we would like to know whether π belongs to G. In order to ask this question we must have a way to represent the group G, and the most natural way to do so is by giving a set $S = \{\pi_1, \ldots, \pi_l\}$ such that $\pi_i \in S_n$ for all $i \in [l]$, and $G =< S >$, generated by the set S. Moreover, we represent every permutation π by specifying the image of any $k \in [n]$ under π (given such a representation we can also easily verify if it is really a permutation). Back to our original question of whether π is in G, one way to show that π is in G is to write π as a product of elements in S. However, as it turns out this is not a very efficient way, since:

Exercise 2. Given $G \subset S_n$, generated by less than or equal to n elements, there is a permutation $\pi \in G$ such that the shortest product of its generators representing π is exponential in n.

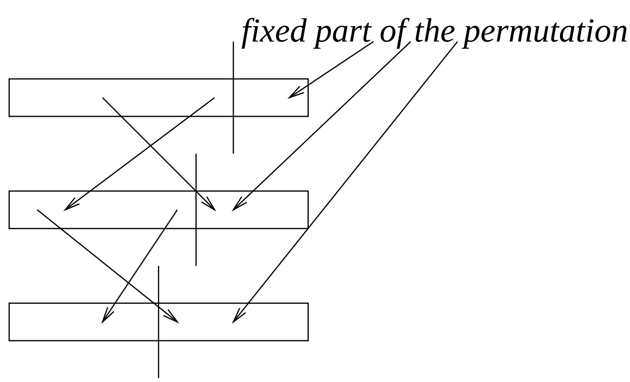
Exercise 3. Express the towers of Hanoi as a permutation group problem.

Since we saw that if G is given by just any set of generators S it won't be efficient to look for a representation of elements as product of the given generators, we will shortly introduce the notion of a strong generating set of G. The idea is that we would like to have a (relatively) short representation for any π, and by adding some special elements to our set of generators we might be able to do this (start with the empty set and successively add suitable generators).

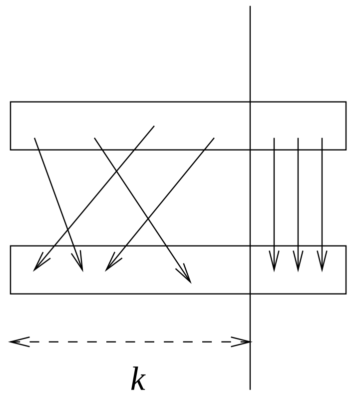
Definition. $T \subset G$ is a *strong generating set* (SGS) of G if for every $j < k \leq n$ we have the following: if there exists a $\tau \in G$ such that $\tau(k+1) = k+1, \ldots, \tau(n) = n, \tau(j) = k$, then there exists a $\sigma = \sigma_{jk}$ in T such that $\sigma(k+1) = k+1, \ldots, \sigma(n) = n, \sigma(j) = k$.

Lemma. (a) Every group G has a SGS T with cardinality $O(n^2)$.
(b) $< T >= G$.

Proof. (a) It is clear that any group G has a SGS since G itself is a SGS. Moreover, we see from the definition of SGS that for every $j, k, j \neq k$ there is at most one generator in T. This, $|T|$ is less than or equal to n choose 2.
(b) To prove this we introduce the following concept.
For $T \subset G$ define $\bar{T}$ as the elements obtained by greedy (right-to-left) movements using elements of T. See the illustration:



Definition. For every permutation $\sigma \in S_n$, let $k(\sigma)$ be the largest k such that $\sigma(k) \neq k$. Then, for a SGS T of G we define $\bar{T} = \{\sigma_1\sigma_2 \ldots \sigma_t | \sigma_1, \sigma_2, \ldots, \sigma_t \in G\}$.



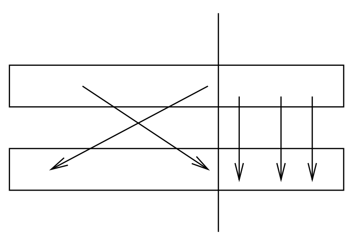
It is clear that if $T \subset G$ then $\bar{T} \subset < T > \subset G$. If T is a SGS for G then $G \subset \bar{T}$. Now, returning to our original problem of whether or not π belongs to G, we can give the following algorithm:

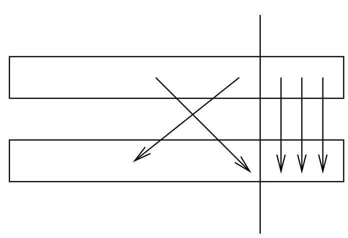
MEM-WITH-SGS(π, G, T) // Does the group G with SGS T conain π?
let $k = k(\pi)$
let $j = \pi^{-1}(k)$
let $\sigma_t \in T$ such that $\sigma_t(j) = k, k(\sigma_t) = k$
let $\sigma_1, \sigma_2, \ldots, \sigma_{t-1}$ generate $\pi{\sigma_k}^{-1}$ in $\bar{T}$
Output($\sigma_1, \sigma_2, \ldots, \sigma_t$)

Note that this algorithm also shows $G \subset \bar{T}$. For a proof see Professor Sudan's notes.

Since the above algorithm is very efficient, we see that if we had a SGS for G then we could easily tell whether π belongs to G or not. Thus, given G with some set of generators S we will construct a SGS. Once we do this, we solve our problem of deciding $\pi \in G$.

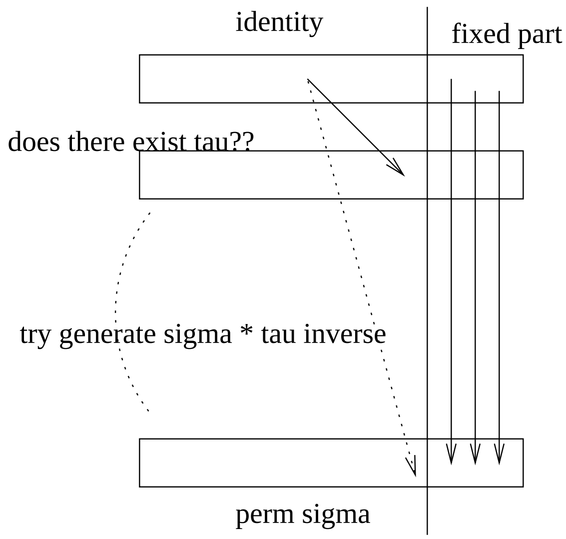
The idea for building a SGS for T is to start with the empty set and successively add in suitable elements, where suitable means that we will get a SGS at the end. Basically while there are elements that are not in $\bar{T}$ but are in $< T \cup S >$, we will add some suitable σ to T. Note that there is a big difference in the notion of $< T >$ and $\bar{T}$ in that in $\bar{T}$ we can only "jugle right to left". Indeed, if in the illustration below $\sigma_2 \in T \cup S$ is the upper permutation and $\sigma_1 \in T \cup S$ the lower one, then we can tell that $\sigma_1\sigma_2 \in < T \cup S >$, whereas it is not sure that $\sigma_1\sigma_2$ is in $\bar{T}$.





We can obtain a SGS for G is by the followong procedure. Set $T = \emptyset$ at the beginning, then:

ADD-ELEM(S, T, σ)
if there is $\tau \in T$ such that $k(\tau) = k(\sigma) = k$ and $j = \sigma^{-1}(k) = \tau^{-1}(k)$
then ADD-ELEM$(S, T, \sigma\tau^{-1})$
else add σ to T.
See illustration for an explanation of the algorithm:



Lemma. If (1) $T \subset < S >$,
(2) $S \subset \bar{T}$,
(3) for every $\sigma_1, \sigma_2 \in T$, $\sigma_1\sigma_2 \in \bar{T}$,
then T is a SGS for $< S >$.
For a careful proof take a look at Professor Sudan's notes.
An idea here how to prove this:
Part 1. It follows from (1), (2), (3), that $< S > \subset \bar{T}$.
$\bar{T}$ closed under multiplication; use subtle induction.
Part 2. Using above we claim that T is a SGS for $< S >$.
Given $\pi \in < S >$, $k(\pi) = k, \pi(j) = k$, we need to show that there exists $\pi' \in T$ such that $k(\pi') = k, \pi'(j) = k$. If $\pi = \pi_1\pi_2 \ldots \pi_l$, with $\pi_1, \pi_2, l \ldots, \pi_l \in T$ then π_l satisfies the condition.