CS 235: Algebraic Algorithms **Assignment 6**

Due: March 27, 2008

1 Commutativity of Inverse (20 points)

Let G be a (not necessarily commutative) group. For any $x \in G$, our group axioms claim that there is an inverse, x^{-1}, such that $xx^{-1} = e$. Strictly, though, we should perhaps define a *left inverse* and *right inverse* as values x_l^{-1} and x_r^{-1} such that $x_l^{-1}x = xx_r^{-1} = e$, since in a non-commutative group we might have $xx^{-1} \neq x^{-1}x$.

Fortunately, this is redundant: prove that x always commutes with its inverse, that is, if $xx^{-1} = e$, then $x^{-1}x = e$. (Hint: Remember that if $b \neq e$, then $ab \neq a$.)

2 Permutation Groups

Consider the group S_n of permutations of n elements. We can think of these as bijective functions $\sigma : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$. It is convenient to write a permutation as a set of *cycles*: for example, we can write (012) for the permutation that sends 0 to 1, 1 to 2, and 2 to 3. By composing these, we can write more complicated permutations: (012)(34) is the permutation that behaves as described for 0,1,2, and also exchanges 3 and 4. We usually leave out elements that permute to themselves, so if we're in S_6, then (012)(34) sends 5 to itself.

If you have trouble thinking about this problem in the general case, try working out some examples for yourself in a small case like S_5 or S_6 (drawing permutations as arrow diagrams like we did in class), and try to see from this how to proceed in general.

2.1 Cycling individual elements (20 points)

Prove that for any permutation $\sigma \in S_n$, and any $i \in \mathbb{Z}_n$, every i corresponds to a cycle under σ as described. (Be careful: you need to show not just that σ will eventually cycle when applied to i, but that it cycles back exactly to i itself).

2.2 Disjointness of cycles (20 points)

Prove that every element $i \in \mathbb{Z}_n$ is in a *unique* such cycle: that is, the cycles of i and j under σ are either identical or completely disjoint.

2.3 Combining cycles (10 points)

Prove that every element of S_n can be written as described by composing disjoint cycles. (Just apply the previous parts.)

2.4 Generators (30 points)

Consider the subset $\{(ij)\}_{i \neq j}$ of S_n, that is, the elements (ij) of S_n that just swap two distinct elements i and j, while leaving everything else fixed. Prove that this subset generates all of G. (Hint: Given any desired permutation, start with the identity permutation, and show how to transform it one swap at a time into the permutation you need.)

2.5 Parity of cycles (30 points extra credit)

Show that we can split S_n up into two subsets, the *even* permutations and the *odd* ones, corresponding to whether the permutations require an even or odd number of individual flips (ij). Show that the even and odd permutations are disjoint, that is, no "even" element can be reached by an odd number of flips, and vice versa. Conclude that the set of all even permutations is a subgroup of S_n. (This subgroup is called the *alternating group*, and is written as A_n.)