Discrete Math, 5th Problem Set (July 28)

REU 2003

Instructor: László Babai
Scribe: Ben Wieland

Exercise 0.1. If G is a nonabelian group, show that $G/Z(G)$ is not cyclic.

Definition 0.2. The *exponent* $\exp(G)$ of a group G is the least common multiple of the orders of the elements. Equivalently, the exponent is the smallest positive integer k such that $g^k = 1$ for every element g of G.

Exercise 0.3. The exponent of a group divides the order of the group. *Hint.* Recall that $g^{|G|} = 1$ (Lagrange).

Exercise 0.4. Show $\exp(S_n) = \text{l.c.m.}\,(1, \ldots, n)$. *Hint.* (1) The order of a k-cycle is k. (2) The order of a permutation is the l.c.m. of the lengths of its cycles.

Exercise 0.5. Use the Prime Number Theorem to show that

$$\ln\left(\text{l.c.m.}\,(1, \ldots, n)\right) \sim \ln\left(\prod_{p<n} p\right) \sim n.$$

Note with awe that it's the natural logarithm!

How high can the order of an individual element be? If m_n is the maximum order of an element of S_n, then we can approximate it well by taking disjoint cycles of distinct prime orders. This gives us an element with order $\prod_{p\le x} p$ where x is the greatest number with $\sum_{p\le x} p \le n$. Then $\ln m_n \sim \ln \prod_{p\le x} p$.

Exercise 0.6. $\sum_{p\le x} p \sim \frac{x^2}{2\ln x}$ (so the average value of a prime number less than x is asymptotically $\frac{x}{2}$). *Hint.* Use this form of the Prime Number Theorem: if p_k denotes the k-th prime then $p_k \sim k \ln k$.

The following theorem is nw a corollary:

Exercise 0.7. (Landau) $\ln m_n \sim \sqrt{n \ln n}$.

Note that this quantity is much smaller than the exponent of S_n.

Rubik's Cube consists of a cube with each dimension divided into thirds, so the big cube is divided into 27 *cubies*. Thus the group R of operations that can be performed by turning the sides has a homomorphism to S_{27}, or actually S_{20}, since the central cubie and the centers of each face do not move. But this homormorphism has a kernel, since a cubie can rotate while returning to its original place. A configuration is determined by the stickers. There are 54 stickers, but those on centers of the faces do not move, so R is a subgroup of S_{48}.

If we disassemble the cube, we can perform a slightly larger group of operations G, which is easier to describe. The group of rotating a corner cubie in place is $\mathbb{Z}_3$. Rotating and rearranging all corners is $\mathbb{Z}_3 \wr S_8$ (wreath product). This is the group of disassembling a $2 \times 2 \times 2$ Rubik's Cube. Similarly, the group of flipping and rearranging all edges is $\mathbb{Z}_2 \wr S_{12}$. These two operations are independent (if we are allowed to disassemble the cube), so $G = (\mathbb{Z}_3 \wr S_8) \times (\mathbb{Z}_2 \wr S_{12})$.

Exercise 0.8. Show $[G : R] \geq 12$. That is, find a group of index 12 in G containing R.
Hint. Show that there are restrictions on the positions that can be reached by turning the sides. Specifically, show that if none of the corner cubies moves, the sum of their rotations is 0. (Inside $\mathbb{Z}_3^8$, this is the subgroup of elements whose entries add up to 0 (the additive identity).) Similarly, if none of the edges move, an even number must be flipped. Finally, the image of the homomorphism $R \to S_{20}$ that ignores rotations and flips and looks only at the permutation of cubies has image in A_{20} (even permutations only).

Exercise 0.9. Show $[G : R] = 12$. That is, show that the rotations of the sides generate the group of index 12 from the previous exercise; solve the puzzle.
Hint. Find sequences of generators that perform very simple operations on the cube, such as 3-cycles of edges or vertices, flipping two edges, or rotating one corner clockwise and another counterclockwise.

Exercise 0.10. A k-cycle is a product of $k-1$ transpositions. Hence a k-cycle is even if and only if k is odd.

Conjecture 0.11. *For any set S that generates of S_n,* $\operatorname{diam}(S_n, S) < n^C$. *Maybe even* $\operatorname{diam}(S_n, S) = (n^2)$. *(*$\operatorname{diam}(G, S)$ *denotes the diameter of the Cayley graph* $\Gamma(G, S \cup S^{-1})$*.)*

Theorem 0.12 (Even-Goldreich). *If $G \cong \mathbb{Z}_2^m$ and $G < S_n$ is generated by a set S (described as element of S_n), the problem of computing* $\operatorname{diam}(G, S)$ *is NP-hard.*

Theorem 0.13 (Jerrum). *Finding the shortest word representing $g \in G \leq S_n$ in terms of a generating set S is PSPACE-hard.*

Jerrum does not assume that $S^{-1} = S$, so what he measures is the *directed* distance in the Cayley graph. It is expected that this result remains true if we require $S = S^{-1}$.

Theorem 0.14 (B–Seress). *Let S generate S_n.* $\operatorname{diam}(S_n, S) < m_n^{1+o(n)}$.

This result suffers from the "element-order bottleneck." The two tricks used are commutators and raising elements to powers. A recent result gives a polynomial upper bound under the condition that one of the generators fixes 70% of the permutation domain. So now all is left to prove is that we can reach such a permutation in a polynomially bounded number of steps. Somebody in this audience may be able to do this with a fresh idea.

Theorem 0.15 (B–Beals–Seress). *Let S generate S_n. If $\exists s \in S$ with the* degree $\deg s < 0.3n$ *then* $\operatorname{diam}(S_n, S) < n^C$ *($C = 12$?). (Recall that the* degree *of a permutation is size of its* support*, the set of elements that it actually moves.)*

We really only need to care about reaching the even permutations. Indeed, if we can always reach the even permutations quickly, here is how we handle an odd target permutations σ. We multiply σ by the inverse of an odd generator; the product is even so we can get there quickly, finally multiply by the odd generator. Thus the diameter of S_n is at most 2 more than cost of reaching the even permutations.

Exercise 0.16. 3-cycles generate A_n. In fact, any connected set of 3-cycles (a set that connects all the points) is a generating set.

Exercise 0.17. For $\sigma \in S_n$, $(1\ 2\ 3)^\sigma = (1^\sigma\ 2^\sigma\ 3^\sigma)$. (Compare this to the geometric argument that the conjugate of a rotation is still a rotation, with the new center the image under the conjugating map of the old center.)

The plan is to get a 3-cycle and conjugate it to get a connected set of 3-cycles.

Definition 0.18. If $a, b \in G$ then the **commutator** of a, b is the element $[a, b] = a^{-1}b^{-1}ab$. Note that $[a, b] = 1$ if and only if $ab = ba$.

Exercise 0.19. If $|\operatorname{supp}\sigma \cap \operatorname{supp}\tau| = 1$ then σ and $\tau]$ cannot commute.

Exercise 0.20. If $|\operatorname{supp}\sigma \cap \operatorname{supp}\tau| = 1$ then $[\sigma, \tau]$ is a 3-cycle.

Exercise 0.21. $\deg[\sigma, \tau] \leq 3|\operatorname{supp}\sigma \cap \operatorname{supp}\tau|$. Show that this exercise also solves the preceding one.

Exercise 0.22. If σ and τ are cycles and $|\operatorname{supp}\sigma \cap \operatorname{supp}\tau| = 1$, then σ and τ generate either the symmetric or alternating group on the union of their support, which has $\deg\sigma + \deg\tau - 1$ elements.

Exercise 0.23. If $H < G$ and $[G : H] = 2$, then $H \triangleleft G$.

Exercise 0.24. If $H < G$ and $[G : H] = 2$, then $(\forall g \in G)(g^2 \in H)$.

Exercise 0.25. If $H < S_n$ and $[S_n : H] = 2$ then $H = A_n$. *Hint.* Every 3-cycle is a square (of its own square).

Exercise 0.26. If $H < G$ and $[G : H] = k$, then the kernel K of $G \to Sym(H\backslash G)$ satisfies $K \triangleleft H, G$ and $[G : K] \leq k!$. *Hint.* The image of G is a subgroup of S_k.

Exercise 0.27. If $H \leq S_n$, $n \geq 5$, and $H \neq A_n, S_n$, then $[S_n : H] \geq n$. So S_{n-1} is the second largest subgroup of S_n.
Hint. Use that A_n is simple.

Remark 0.28. More generally, for n large, the largest few subgroups of S_n are variants on $S_k \times S_{n-k}$. These are the point stabilizers of the action of S_n on k-element subsets. "Variants" refers to restrictions on parity, e. g., $A_n \cap (S_k \times S_{n-k})$ and $A_k \times A_{n-k}$ have index 2 and 4, respectively, in $S_k \times S_{n-k}$.