AM 106: Applied Algebra **Prof. Salil Vadhan**

Problem Set 4

Assigned: Fri. Oct. 12, 2018 Due: Fri. Oct. 19, 2018 (5:00 sharp)

- You must submit your problem sets electronically on the course Canvas site. If you use LaTeX, please submit both the source (`.tex`) and the compiled file (`.pdf`).
- For SAGE problems, also submit a pdf version of your SAGE notebook.
- Aim for clarity and conciseness in your solutions, emphasizing the main ideas over low-level details. Please reread the parts of the syllabus about Problem Sets and the Collaboration Policy.

Problem 1. (Isomorphisms of Specific Groups, 15pts) For each of the following pairs of groups (G, H), determine whether or not they are isomorphic. If not, determine whether one is isomorphic to a subgroup of the other. Justify your answers.

1. $\mathbb{Z}_5$ vs. S_5.
2. $\mathbb{Z}_8^*$ vs. $\mathbb{Z}_{12}^*$.
3. $\mathbb{Z}_{15}^*$ vs. D_4.
4. D_{12} vs. S_4.
5. $\mathbb{Z}$ vs. $\mathbb{Q}$.

Problem 2. ($\mathbb{C}^*$, Gallian 7.12 & 7.30, 10pts)

1. Let $\mathbb{C}^*$ be the group of nonzero complex numbers under multiplication and let $H = \{a + bi \in \mathbb{C}^* : a^2 + b^2 = 1\}$. Give a geometric description of the coset $(3 + 4i)H$. Give a geometric description of the coset $(c + di)H$ for arbitrary $c + di \in \mathbb{C}^*$.
2. Determine all finite subgroups G of $\mathbb{C}^*$. Justify your answer. (Hint: what are the solutions to $a^n = 1$ in $\mathbb{C}^*$?)

Problem 3. (Orbits and Stabilizers for the Cube, 10pts) Let G be the group of rotational symmetries of a regular cube in $\mathbb{R}^3$. (We do not include reflections in G.)

1. Among points s on the surface of the cube (including edges and corners), what are the possible orbit sizes? For each answer a you give, provide an example of a point s with $|\mathrm{orb}_G(s)| = a$.
2. For each point s above, describe $\mathrm{stab}_G(s)$.

Problem 4. (Solving the Cube, 25pts) For a group G and elements $g_1, \ldots, g_k \in G$, the *subgroup generated by* $g_1, \ldots, g_k$ is defined to be the set of all elements of G that can be obtained by multiplying the g_i's and their inverses a finite number of times. That is:

$$\langle g_1, \ldots, g_k \rangle = \{g_{i_1}^{j_1} g_{i_2}^{j_2} \cdots g_{i_m}^{j_m} : m \geq 0, i_1, \ldots, i_m \in [k], j_1, \ldots, j_m \in \mathbb{Z}\}.$$

It can be verified that $\langle g_1, \ldots, g_k \rangle$ is in fact a subgroup of G, just as in the case of cyclic subgroups (which is the case $k = 1$).

Providing a set of generators in this way can give a very compact description of a large group. Surprisingly, for the case of $G = S_n$, many computations about the group $H = \langle g_1, \ldots, g_k \rangle$ can be done in time $\mathrm{poly}(n, k)$, even though the group itself can be of size up to $n!$. For example, we can efficiently determine whether a permutation g is in H (and if so, write it in terms of the generators), calculate $|H|$, find the orbit of an element $i \in [n]$, and determine generators for the stabilizer of an element $i \in [n]$.

These algorithms are implemented in SAGE, and in this problem, you will see how to use them to solve puzzles like the Rubik's Cube. See PS4 Tips at `http://seas.harvard.edu/~salil/am106/fall18/SAGE.html` for the relevant and allowable SAGE commands. If you're interested in how the algorithms work, see Lecture 9 from the 2017 offering of AM 106 (`http://seas.harvard.edu/~madhusudan/courses/Fall2017/`).

Look at your Rubik's cube, preferably in the "solved" state where each face is monochromatic. (If you haven't picked up your cube, see the flattened picture of a cube at `https://en.wikipedia.org/wiki/Rubik%27s_Cube#/media/File:Rubik%27s_cube_colors.svg`. If you have accidentally scrambled your cube, it is possible to forcibly disassemble it and reassemble it into the solved state.) Fixing the positions of the 6 colored center squares (white, blue, red, yellow, green, orange) on the cube, we use the first letters of the colors (W, B, R, Y, G, O) to name the corresponding faces. (To avoid a conflict of notation, we will *not* use G to name a group in the rest of this problem!) Then we can name the other 48 squares using (a variant of) "Singmaster notation" by first specifying the face the square is on, and then specifying the one or two other faces that the square is adjacent to (corner squares are adjacent to two other faces, edge squares are adjacent to one other face). For example, the 8 non-center squares on the W face would be named (in clockwise fashion) *WBR*, *WR*, *WRG*, *WG*, *WGO*, *WO*, *WOB*, *WB*. (For corner squares, we always write the 3 faces in clockwise order, e.g. *WBR* and *BRW* rather than *WRB* or *BWR*.)

The basic moves on a Rubik's cube are rotating one of the six faces 90 degrees clockwise. Each of these 6 moves can be described by a permutation of X, which we also denote by the corresponding face. For example, the permutation W takes *WBR* to *WRG* and *RW* to *GW*. The Rubik's Cube Group is thus $H = \langle W, B, R, Y, G, O \rangle \leq Sym(X)$. Some of the SAGE functions we want require that the set X is of the form $\{1, \ldots, n\}$, so following the model in the SAGE PS4 tips, you should arbitrarily number the 48 elements of X so that $Sym(X) = S_{48}$ (assigning variables like `WBR=1`, `WR=2`, etc. so that you can use Singmaster notation in place of the numbers).

1. In SAGE, construct the 6 generators as elements of S_{48} in cycle notation and use these to construct Cube Group H as a subgroup of S_{48} following the model in the PS4 tips. You can check your answer by verifying that $|H| \approx 43 \times 10^{18}$.

2. Is H contained in A_{48}?

3. For each of the following permutations, determine whether they are in the group H, and if so, describe how they can be written as a product of basic moves.

(a) $(WR\ RW)$

(b) $(RYG\ BRW\ YRB\ GRY\ WBR\ BYR\ YGR\ RWB\ RBY)$
$(RG\ WG\ OG\ OY\ OB\ OW\ YG\ RW\ RB\ RY)$
$(RGW\ WGO\ WRG\ OWG\ GWR\ GOW)$
$(GYO\ YBO\ BWO\ OGY\ OYB\ OBW\ YOG\ BOY\ WOB)$
$(GO\ YO\ BO\ WO\ GY\ WR\ BR\ YR\ GR\ GW)$.

(c) $(WRG\ RGW\ GWR)$

(d) $(WR\ RW)(OB\ BO)$.

For those that are in the group H, verify the decompositions into basic moves using the Rubik's Cubes we've provided you (starting from a solved cube)! (Although it is known that 20 moves suffice for any reachable permutation of the Rubik's Cube, SAGE will often generate very long sequences of moves. There are no known polynomial-time algorithms for finding a minimum-length product of generators to obtain a given element of a permutation group.)

4. Explain in words how, if you were given a scrambled cube, how you could use SAGE find a sequence of moves to solve the cube.

5. By repeatedly applying basic moves, to how many different locations can we move the square WR?

6. By repeatedly applying basic moves, to how many different locations can we move the square WR while bringing all of the other white squares back to their original position? (Hint: start by a sequence of stabilizer computations.)