

# ALGEBRA AND COMPUTATION

## PROBLEM SET 2

*Due date: March 3<sup>rd</sup>, 2019*

---

### INSTRUCTIONS

1. The problem set has **10 questions** with a total score of **100 points**.
2. The due date is **Sunday, March 3<sup>rd</sup>, 2019**.
3. You are welcome to discuss with other classmates **as long as these discussion are reasonable**; these are not meant for one to solve the problem for the other. You are eventually expected to find and write your own solutions and code.

If you do discuss, you are expected to explicitly mention who you discussed with and which parts of your solution came from these discussions.

4. Solutions are expected as a  $\text{\LaTeX}$  documents and sage worksheets (.ipynb files).

---

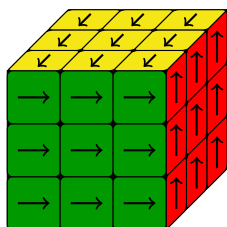
### QUESTIONS (FOR SAGE ETC.)

**Question 1. [5 points]** Build a move for the  $3 \times 3 \times 3$  Rubik's cube that flips two edges.

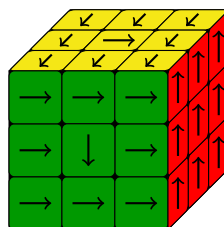


(You may use <http://alg.cubing.net>.)

**Question 2. [5 points]** Compute the generators for the group of the arrow-version of the  $3 \times 3 \times 3$  Rubik's cube:



Solved state



An unsolved state

On <http://alg.cubing.net>, the notation for the middle layer moves are M, S, E.

**[5 points]** Find a suitable commutator that *twists* some of the centres.

**Question 3. [10 points]** Consider the group for the  $4 \times 4 \times 4$  Rubik's cube (via its action on the  $16 \times 6$  stickers). Compute the orbits and minimal blocks of this action.

## QUESTIONS

**Question 4. [10 points]** Given a permutation group  $G = \langle S \rangle \leq S_n$ , give an efficient algorithm to generate a uniformly random element from  $G$ .

**Question 5. [10 points]** Prove the following lemma that we sketched in class.

**Lemma.** Suppose  $G$  acts on  $[n]$  and  $\sigma, \pi \in G$ . Then,

$$\text{Move}([\sigma, \pi]) \subseteq S \cup \sigma^{-1}(S) \cup \pi^{-1}(S),$$

where  $S = \text{Move}(\sigma) \cap \text{Move}(\pi)$ .

**Question 6. [10 points]**

Show (via a formal proof) that for any  $n \geq 3$ , the set of 3-cycles generate all even permutations on  $n$  elements.

If you have solved this in the last problem set (gave a formal proof, I mean), you do not have to write the solution again.

**Question 7. [5 points]** Consider the version of the 15-puzzle with the pieces being

A	L	G	E
B	R	A	
O	M	P	C
2	0	1	9

Can this puzzle be solved? Justify your answer. (In the solved state, the third line should read "C O M P" and the other rows are identical)

---

**Question 8. [10 points]** Using the following hint (or not), prove that any subgroup  $G \leq S_n$  has a generating set of size at most  $(n - 1)$ , and that it can be computed efficiently given a generating set for  $G$ .

For any non-trivial permutation  $g \in S_n$ , let  $\ell(g)$  be the smallest  $i \in \{1, \dots, n\}$  moved by  $g$ , i.e.  $\ell(g) = \min \{i : i^g \neq i\}$ .

Given a set  $A$  of permutations, define the graph  $X_A = (V, E_A)$  as

$$V = \{1, \dots, n\} \quad \text{and} \quad E_A = \{(i, i^g) : g \in A, i = \ell(g)\}.$$

If  $X_A$  has no cycles in it, then of course  $|A| \leq (n - 1)$ .

**Question 9.** Prove the following two facts we used in Lecture 5.

- (a). **[5 points]** If  $G$  normalizes  $H$  and  $K \leq G$ , show that  $[GH : KH] \leq [G : K]$ .
- (b). **[5 points]** If  $K \leq G$ , show that  $[G \cap H : K \cap H] \leq [G : K]$ .

**Question 10.** Nilpotent groups are groups with the following property:

A group  $G$  is *nilpotent* if there is a finite number  $k$  such that for any choice of  $g_1, \dots, g_k \in G$  we have

$$[g_1, [g_2, [\dots [g_{k-1}, g_k] \dots]]] = \text{id}$$

where  $[g_1, g_2] := g_1 g_2 g_1^{-1} g_2^{-1}$ .

for  $k = 4$ , you want  
 $[g_1, [g_2, [g_3, g_4]]] =$   
 $\text{id for every}$   
 $g_1, \dots, g_4 \in G$

(In the previous problem set, you must have observed that Sylow-subgroups are nilpotent.)

**[15 points]** Given  $G = \langle S \rangle \leq S_n$ , construct a deterministic algorithm that runs in time  $\text{poly}(n, |S|)$  to test if the group  $G$  is nilpotent.

Hint: Consider the set of all elements of the form  $[g_1, [g_2, [\dots [g_{k-1}, g_k] \dots]]]$ . What subgroup of  $G$  do they generate?

**[5 points]** Are nilpotent groups the same as solvable groups? Prove or disprove your claim.