Problem Set 1: Part B

- Due Date: **3 Mar, 2022**
- The points for each problem is indicated on the side. The total for this part of the set is **60** points.
- The problem set has a fair number of questions so please do not wait until close to the deadline to start on them. Try and do one question every couple of days.
- Turn in your solution to this part electronically (PDF; either LaTeXed or scanned etc.) on Acadly.
- Collaboration is encouraged, but all writeups must be done individually and must include names of all collaborators.
- Referring to sources other than the class notes is strongly discouraged. But if you do use an external source (eg., other text books, lecture notes, or any material available online), ACKNOWLEDGE all your sources (including collaborators) in your writeup. This will NOT affect your grades. However, not acknowledging will be treated as a serious case of academic dishonesty.
- Be clear in your writing.

1. **[Nilpotent groups]** (3 + 3 + 4)

   Recall the definition on *nilpotent* groups that we briefly discussed in class.

   Definition (Nilpotent groups)**.** *A group G is nilpotent if there exists a positive integer k such that for any $g_1, \ldots, g_k \in G$, we have*

   $$[g_1, [g_2, [g_3, [\ldots [g_{k-1}, g_k] \ldots]]]] = \mathrm{id}\,.$$

   The goal of this question is to construct a polynomial time algorithm for checking if a permutation group (given via generators $S \subseteq \mathrm{Sym}([n])$) is nilpotent.

   For all $i \geq 1$, define the groups G_i inductively via as

   $$G_0 = G$$
   $$G_i = [G, G_{i-1}] = \langle [g, h] \ : \ g \in G \ , \ h \in G_{i-1} \rangle \quad \text{for all } i \geq 1$$

   (a) Can you give an informal explanation of why this definition is different from the notion of a group being *solvable*? Provide an example of a group that shows this separation.

   (b) Prove that $G_i \trianglelefteq G$ for all $i \geq 0$.

   (c) In fact, like in the case of commutator subgroups, if we have generating sets S and T for G and G_i respectively, G_{i+1} is the smallest normal subgroup of G that contains all the commutators of the form $\{[s, t] \ : \ s \in S \ , \ t \in T\}$.

   Use this to construct a polynomial time algorithm to for testing nilpotence.

Base version: (2022-02-17 15:54:27 +0530) , dbba884

2. **[Membership as expressions using the generators]** (2 + 4 + 4 + 10)

Let $p_1, \ldots, p_m$ be the first m distinct primes, and let $n = \sum p_i$ (a loose estimate gives $n \approx p_m^2$). Let $\sigma_1, \ldots, \sigma_m \in \mathrm{Sym}([n])$ be disjoint cycles of length $p_1, p_2, \ldots, p_m$ respectively (that is, $\sigma_1 = (1\ 2)$, $\sigma_2 = (3\ 4\ 5)$, $\sigma_3 = (6\ 7\ 8\ 9\ 10)$ etc.).

(a) Let $\tau = \sigma_1\sigma_2\cdots\sigma_m$. Show that the order of τ (i.e., the smallest positive integer k such that $\tau^k = \mathrm{id}$) is $\prod p_i$.

(b) Show that $\langle \sigma_1, \ldots, \sigma_k \rangle = \langle \tau \rangle$.

(c) If $\sigma_1 = \tau^a$ for an integer a, show that $|a| = \exp(\Omega(m))$.

(d) Suppose you were to run the membership algorithm to check if an input permutation σ is in the group $G = \langle S \rangle$, and suppose σ is indeed in the group. The algorithm would keep "modifying" σ while trying to insert it in the tableau, until at some point it is "modified" to id and it accepts. This might seem to suggest that we can write σ as a short expression involving the generators.

But let's just revisit the same with $\sigma = \sigma_1$ and $S = \{\tau\}$. The previous subdivision just argued that there is no "short" expression for σ_1 using τ. How do you resolve this "contradiction"?

3. **[Subtlety in subgroup chains]** (10)

Consider the following argument to show that claims to prove $\mathrm{GraphAut} \in \mathsf{P}$.

> Let $G_0 = \mathrm{Sym}([n])$. Let us order the edges of the graph X as $e_1, \ldots, e_i$ with $e_i = (u_i, v_i)$ and define the following tower of subgroups:
>
> $$G_i = \{\sigma \in G_{i-1} \ : \ (\sigma(u_i), \sigma(v_i)) \in X\}\,.$$
>
> That is, each $G_0 = \mathrm{Sym}([n])$ shuffles all the vertices with no regard for edge structure, and each G_i just ensures additionally that edge e_i is mapped only to an edge.
>
> The following are relatively obvious:
>
> - Certainly, $G_{|E|} = \mathrm{Aut}(X)$ as this is precisely the set of all permutations that preserve all the edges.
> - G_{i+1} is a recognisable subgroup of G_i as we only need to check the image of the edge e_{i+1}.
> - $[G_i : G_{i+1}] \leq n^2$ as the edge e_{i+1} only has n^2 possible other edges it may be mapped to by any element of G_i and hence there are at most n^2 cosets of G_{i+1} in G_i.
>
> Thus, by using Schreier's lemma for tower of subgroups, we can efficiently find a generating set for $\mathrm{Aut}(X)$.

What is wrong with this argument?

4. **[Smaller generating sets for subgroups]** (10)

In this question, you are required to show that any subgroup $G \leq \mathrm{Sym}([n])$ has a generating set of just n elements (instead of the bound of $n \log n$ that we proved in class). A sketch of the procedure is provided:

For any $\mathrm{id} \neq \sigma \in \mathrm{Sym}([n])$, let $\ell(\sigma)$ be the smallest i such that $\sigma(i) \neq i$ (that is, $\ell(\sigma)$ is the smallest index moved by σ).

Given a generating set S, let us construct the following graph on n vertices as follows. We will run through each $\sigma \in S$ and add an edge from $\ell(i)$ to $\sigma(\ell(i))$ (and keep σ as the edge label for book-keeping). But as soon as adding a new edge for a σ creates a cycle in this graph, we will replace the permutation σ by [something] and add it back to S.

Once we have processed all of S, we have a graph with no cycles in it and hence has at most $(n-1)$ edges. Return all those edge labels as the new generating set.

Fill in the details, and also prove the correctness of the algorithm.

5. **[Properties of blocks]** (3 + 3 + 4)

Recall the definition of *blocks* that we saw in class.

Definition. *A subset $\Delta \subseteq \Omega$ is a block of the G-action on Ω if for any $g \in G$ we have either $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \emptyset$.*

Formally prove the following properties about blocks.

(a) For any pair of elements g_1, g_2, we have that either $\Delta^{g_1} = \Delta^{g_2}$ or $\Delta^{g_1} \cap \Delta^{g_2} = \emptyset$.

(b) If Δ_1 and Δ_2 are blocks, then so is $\Delta_1 \cap \Delta_2$.

(c) Suppose $\Gamma = \{\Delta_1, \ldots, \Delta_r\}$ be the block-system generated by a block Δ (i.e., $\Gamma = \{\Delta^g : g \in G\}$). Prove that the *block-kernel* $B = \{g \in G : \Delta^g = \Delta \text{ for all } \Delta \in \Gamma\}$ is a normal subgroup of G.
