Complexity Theory, WS 13/14: Solution Hints 4.

Markus Bläser, Thatchaphol Saranurak

Exercise 4.1 a) If σ is a 5-cycle, then the graph of σ^{-1} can be obtained by reversing the edges of σ's graph. Such graph is a 5-cycle as well.

b) Let $\sigma = (13245), \tau = (14325)$. Verify. This step seems ad-hoc, but we will have a similar situation for any non-solvable group G. In this case, $G = S_5$.

Exercise 4.2 Since τ, σ are both 5-cycle, they have the same "cycle-type". Thus, they are in the same conjugation class of S_5. That is, there is $g \in S_5$ where $\tau = g\sigma g^{-1}$.

Suppose that B is a permutation program σ-deciding L. We create a permutation program B' as follows: for every permutation $\pi_i \in B$, we set $\pi'_i = g\pi_i g^{-1} \in B'$. Thus the length of B' is same as of B.

Since $B'(x) = \pi'_1\pi'_2 \cdots \pi'_l = (g\pi_1 g^{-1})(g\pi_2 g^{-1}) \cdots (g\pi_l g^{-1}) = g(\pi_1\pi_2 \cdots \pi_l)g^{-1}$, we conclude if $B(x) = \sigma$, then $B'(x) = \tau$, and if $B(x) = \text{id}$, then $B'(x) = \text{id}$.

Exercise 4.3 We will prove by induction that for any gate g in the circuit C at level d, there exists a permutation program of width 5 and of length 4^d that π-decides "the language of g" where π is a 5-cycle. (By exercise 4.2, we can choose π to be any 5-cycle.)

Base case: trivial.

Inductive case: if g is an AND-gate with children g_1 and g_2, then by induction hypothesis there are

- B_1 σ-deciding the language of g_1,
- B'_1 σ^{-1}-deciding the language of g_1,
- B_2 τ-deciding the language of g_2,
- B'_2 τ^{-1}-deciding the language of g_2,

where they all are of width 5 and of length at most 4^{d-1}. We chose σ and τ such that $\sigma\tau\sigma^{-1}\tau^{-1} = \pi$ is some 5-cycle. We define $B = B_1 \circ B_2 \circ B'_1 \circ B'_2$. B has length at most $4 \cdot 4^{d-1} = 4^d$. Moreover, if $g_1(x) = 0$ or $g_2(x) = 0$, then $B(x) = \text{id}$. Otherwise, $B(x) = \pi$. Thus, B π-decides the language of g.

If g is a NOT-gate with a child g', then there exist B' π^{-1}-deciding the language of g'. $B = \pi \circ B'$ will do the job. We can construct B such that it has the same length as B' by composing π to the last permutation of B'.

If g is an OR-gate, then we can just use DeMorgan's law because, by the last paragraph, there is a program B deciding the complement of a language of another program B' where B has the same length as B'.

Exercise 4.4 If $L \in \mathsf{NC}_1$, then by the last exercise we have a family of permutation programs of width 5 and length $4^{O(\log n)} = n^{O(1)}$ that decides L.

Conversely, as a program has constant width, a permutation can be represented using a constant number of bits, and we compute a composition of two permutations (with cases) using a constant number of gates and levels. We use divide and conquer. Thus, for any bounded width permutation program of length $\ell = n^{O(1)}$, there is a circuit of depth $O(\log \ell) = O(\log n)$ and size $O(\ell) = n^{O(1)}$ deciding the same language.