Exercises 3 & 4 [Mistake corrected 2024-10-15]

Circuit Complexity, Autumn 2024, University of Chicago
Instructor: William Hoza (williamhoza@uchicago.edu)

Submission. Solutions are due **Wednesday, October 16** at 5pm Central time. Submit your solutions through Gradescope. You are encouraged, but not required, to typeset your solutions using a LaTeX editor such as Overleaf.

The policies below can also be found on the course webpage.

Collaboration. You are encouraged to collaborate with your classmates on homework, but you must adhere to the following rules.

- Work on each exercise on your own for at least fifteen minutes before discussing it with your classmates.
- Feel free to explain your ideas to your classmates in person, and feel free to use whiteboards/chalkboards/etc. However, do not share any written/typeset solutions with your classmates for them to study on their own time. This includes partial solutions.
- Write your solutions on your own. While you are writing your solutions, do not consult any notes that you might have taken during discussions with classmates.
- In your write-up, list any classmates who helped you figure out the solution. The fact that student A contributed to student B's solution does not necessarily mean that student B contributed to student A's solution.

Permitted Resources for Full Credit. In addition to discussions with me and discussions with classmates as discussed above, you may also use any slides or notes posted in the "Course Timeline" section of the course webpage, and you may also use Wikipedia. If you wish to receive full credit on an exercise, you may not use any other resources.

Outside Resources for Partial Credit. If you wish, you may use outside resources (ChatGPT, Stack Exchange, etc.) to solve an exercise for partial credit. If you decide to go this route, you must make a note of which outside resources you used when you were working on each exercise. You must disclose using a resource even if it was ultimately unhelpful for solving the exercise. Furthermore, if you consult an outside resource while working on an exercise, then you must not discuss that exercise with your classmates.

A *monotone circuit* uses only AND gates, OR gates, variable gates, and constants. Negations are prohibited. A function $f\colon \{0,1\}^* \to \{0,1\}^*$ is in mNC^i if it can be computed by monotone circuits of depth $O(\log^i n)$ and size $\mathrm{poly}(n)$ (with bounded fan-in). In class, we prove $\mathsf{MAJ} \in \mathsf{NC}^1$. In this exercise, you will prove the stronger statement $\mathsf{MAJ} \in \mathsf{mNC}^1$.

Exercise 3 (~~10 points~~ 7 points)**.**

(a) (Optional; 3 points extra credit) Let $\varepsilon_0, \delta \in (0,1)$. Inductively define a sequence $\varepsilon_0 \le \varepsilon_1 \le \varepsilon_2 \le \cdots$ by letting

$$\varepsilon_{i+1} = \mathbb{E}[\mathrm{sign}(X_1 + X_2 + X_3)],$$

where $X_1, X_2, X_3 \in \{\pm 1\}$ are independent random variables such that $\mathbb{E}[X_1] = \mathbb{E}[X_2] = \mathbb{E}[X_3] = \varepsilon_i$. Prove that there is a value $k = O(\log(1/\varepsilon_0) + \log\log(1/\delta))$ such that $\varepsilon_k \ge 1 - \delta$.

~~*Hints:* Let $\delta_i = 1 - \varepsilon_i$ and prove that $\delta_{i+1} \le \delta_i^2$. Then use the inequality $1 + x \le e^x$, which holds for all $x \in \mathbb{R}$.~~

Hints: First show that there is a value $k_1 = O(\log(1/\varepsilon_0))$ such that $\varepsilon_{k_1} \ge 0.4$. Then let $\delta_i = 1.5 \cdot (1 - \varepsilon_i)$ and show that $\delta_{i+1} \le \delta_i^2$.

(b) Let $C_k\colon \{0,1\}^{3^k} \to \{0,1\}$ be a depth-k ternary tree in which each node is a MAJ_3 gate and each variable is used exactly once at the bottom. Let $n \in \mathbb{N}$ be odd and let $x \in \{0,1\}^n$. Pick $i_1, i_2, \ldots, i_{3^k} \in [n]$ independently and uniformly at random. Prove that there is a value $k = O(\log n)$ such that

$$\Pr[C_k(x_{i_1}, x_{i_2}, \ldots, x_{i_{3^k}}) = \mathsf{MAJ}_n(x)] > 1 - 2^{-n}.$$

You may take part (a) for granted even if you did not solve it.

(c) Prove that $\mathsf{MAJ}_n \in \mathsf{mNC}^1$. For simplicity's sake, you may assume that n is odd.

Hint: Use Adleman's trick to get rid of the randomness from part (b).

In class, we use the fact that $\mathsf{MAJ} \in \mathsf{NC}^1$ to convert randomized NC^1 circuits into deterministic NC^1 circuits. In this exercise, you will convert randomized AC^0 circuits into deterministic AC^0 circuits, despite the fact that MAJ is *not* in AC^0.

Exercise 4 (10 points)**.**

(a) Let $\delta \in (0,1)$. Prove that there exists $m \in \mathbb{N}$ and an AC^0_3 circuit $C\colon \{0,1\}^m \to \{0,1\}$ of size $\operatorname{polylog}(1/\delta)$ such that for every $p \in [0,1]$, if we sample $X_1, X_2, \ldots, X_m \in \{0,1\}$ independently with $\mathbb{E}[X_1] = \cdots = \mathbb{E}[X_m] = p$, then

$$\begin{aligned} p \le 1/4 &\implies \mathbb{E}[C(X_1,\ldots,X_m)] < \delta \\ p \ge 3/4 &\implies \mathbb{E}[C(X_1,\ldots,X_m)] > 1-\delta. \end{aligned}$$

Hint: Let $n = \ln(1/\delta^2)$. Let A be the conjunction of $O(\log n)$ variables, and show that it amplifies the gap from $(1/4, 3/4)$ to $(1/n^C, 1/n^c)$ for some constants $c < C$. Then let OA be the disjunction of $\operatorname{poly}(n)$ copies of A on disjoint variables, and show that it amplifies the gap to $(1/\operatorname{poly}(n), 1-e^{-n})$. Finally, let AOA be the conjunction of $\operatorname{poly}(n)$ copies of OA on disjoint variables, and show that it amplifies the gap to $(\delta, 1-\delta)$.

(b) Prove that there exists a function $\widetilde{\mathsf{MAJ}}\colon \{0,1\}^* \to \{0,1\}$ such that $\widetilde{\mathsf{MAJ}} \in \mathsf{AC}^0$, and for every $n \in \mathbb{N}$ and every $x \in \{0,1\}^n$,

$$\begin{aligned} x_1 + \cdots + x_n \ge 3n/4 &\implies \widetilde{\mathsf{MAJ}}(x) = 1 \\ x_1 + \cdots + x_n \le n/4 &\implies \widetilde{\mathsf{MAJ}}(x) = 0. \end{aligned}$$

Hint: Apply C to m variables chosen independently and uniformly at random from among $x_1, \ldots, x_n$. Then use Adleman's trick to get rid of the randomness.

(c) Let $f\colon \{0,1\}^* \to \{0,1\}$. Assume that f can be computed by "randomized AC^0 circuits," i.e., for every $n \in \mathbb{N}$, there exists a constant-depth $\operatorname{poly}(n)$-size circuit $C\colon \{0,1\}^n \times \{0,1\}^r \to \{0,1\}$ such that for every $x \in \{0,1\}^n$, we have

$$\Pr_{y \in \{0,1\}^r}[C(x,y) = f(x)] \ge 0.9.$$

Prove that $f \in \mathsf{AC}^0$.