Exercises 5 & 6 [Edited 2024-10-22]

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

Submission. Solutions are due **Wednesday, October 23** 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.

Recall that $\mathsf{ADD}_{n\times m}$ is the problem of adding n integers, each of which is represented by an m-bit string. In class, we proved that $\mathsf{ADD}_{n\times n} \in \mathsf{NC}^1$. In this exercise, you will prove the stronger statement $\mathsf{ADD}_{n\times n} \in \mathsf{TC}^0$.

Exercise 5 (10 points)**.** Throughout this exercise, let $k(n) = \lceil \log n \rceil$.

(a) Prove that $\mathsf{ADD}_{n\times k(n)} \in \mathsf{TC}^0$.

Hint: Convert to unary, then add in unary, then convert back to binary. For the purposes of this exercise, a "unary representation" of a number N is any bitstring with Hamming weight N.

(b) Let $n \in \mathbb{N}$, let ℓ be an odd positive integer, let $m = \ell \cdot k(n)$, and let $M \in \{0,1\}^{n\times m}$. Write it as a block matrix

$$M = \begin{bmatrix} M_{\ell-1} & M_{\ell-2} & \cdots & M_0 \end{bmatrix},$$

where $M_i \in \{0,1\}^{n\times k(n)}$ for every $i \in \{0,1,\ldots,\ell-1\}$. Prove that if $M_1 = M_3 = M_5 = \cdots = M_{\ell-2} = 0$ (the all-zeroes matrix), then we can compute $\mathsf{ADD}_{n\times m}(M)$ in TC^0.

Hint: Use part (a), and use the fact that $\mathsf{ADD}_{n\times k(n)}$ outputs strings of length $2k(n)$.

(c) Prove that $\mathsf{ADD}_{n\times n} \in \mathsf{TC}^0$.

Hint: Given $M \in \{0,1\}^{n\times n}$, split it into two matrices, $M = M^{\text{even}} + M^{\text{odd}}$.

Throughout this exercise, let p and q be fixed, distinct primes. Define $\overline{\mathsf{MOD}}_q \colon \{0,1\}^n \to \{0,1\}^q$ by the formula

$$\overline{\mathsf{MOD}}_q(x) = 0^{i-1}10^{q-i} \text{ where } i \equiv x_1 + \cdots + x_n \pmod{q}.$$

In this exercise, you will show that if p and q are distinct primes, then $\overline{\mathsf{MOD}}_q \notin \mathsf{AC}^0[p]$. The proof has the same structure as the proof that $\mathsf{PARITY} \notin \mathsf{AC}^0$ that we did in class. However, each step will be a bit trickier.

When we proved $\mathsf{PARITY} \notin \mathsf{AC}^0$, we found it convenient to work in the field $\mathbb{F}_3$. To prove $\overline{\mathsf{MOD}}_q \notin \mathsf{AC}^0[p]$, it turns out to be wise to work in the field $\mathbb{F} = \mathbb{F}_{p^{q-1}}$, the unique field with p^{q-1} elements. I realize that some of you might not be too familiar with this field,[1] but I hope the exercise will nevertheless be doable and interesting. The reason $\mathbb{F}$ is a good choice of field is that it has the following two features.

- $\mathbb{F}_p \subseteq \mathbb{F}$, where $\mathbb{F}_p$ denotes the integers modulo p.[2]
- There is a "primitive q-th root of unity" $\omega \in \mathbb{F}$, i.e., there exists $\omega \in \mathbb{F}$ such that $\omega^k = 1$ if and only if k is a multiple of q.[3]

You may take those two facts for granted.

Exercise 6 (15 points)**.**

(a) Prove that for every size-S $\mathsf{AC}^0_d[p]$ circuit $C \colon \{0,1\}^n \to \{0,1\}^q$, there exists $\vec{f} = (f_1, \dots, f_q)$, where each f_i is a multilinear polynomial over $\mathbb{F}$ of degree at most $(\log S)^{O(d)}$, such that

$$\Pr_{x \in \{0,1\}^n}\left[\vec{f}(x) = C(x)\right] \geq 0.99.$$

Hint: Use Fermat's little theorem. (You may use it without proving it.)

You may assume that $S \geq n$. It's fine if the hidden constant under the $O(\cdot)$ depends on p, since we are thinking of p and q as constants.

(b) Let $D \in \mathbb{N}$, and let $\vec{f} = (f_1, \dots, f_q)$, where each f_i is a multilinear polynomial over $\mathbb{F}$ of degree at most D. Prove that there exists a multilinear polynomial $g \in \mathbb{F}[y_1, \dots, y_n]$ of degree at most D such that

$$\Pr_{x \in \{0,1\}^n}\left[\vec{f}(x) = \overline{\mathsf{MOD}}_q(x)\right] \leq \Pr_{y \in \{1,\omega\}^n}[g(y) = y_1 y_2 \cdots y_n].$$

Hint: Let $x_i = \frac{1-y_i}{1-\omega}$.

(c) Let $g \in \mathbb{F}[y_1, \dots, y_n]$ be a multilinear polynomial of degree at most D, and define

$$\Omega = \{y \in \{1,\omega\}^n : g(y) = y_1 y_2 \cdots y_n\}.$$

Prove that every function $h \colon \Omega \to \mathbb{F}$ can be computed by a multilinear polynomial of degree at most $n/2 + D$.

Hints: Simplify the expressions $\frac{1+\omega-b}{\omega}$ and $b + \omega b - \omega$ under the assumption $b \in \{1, \omega\}$. Replace each high-degree monomial $c_S \prod_{i \in S} y_i$ of h with the low-degree polynomial $\frac{c_S \cdot g(y)}{\prod_{i \notin S} y_i}$.

(d) Prove that $\overline{\mathsf{MOD}}_q \notin \mathsf{AC}^0[p]$.

(e) (Optional; 1 point of extra credit) Prove that $\mathsf{MOD}_q \notin \mathsf{AC}^0[p]$ and $\mathsf{MAJ} \notin \mathsf{AC}^0[p]$.

[1] Caution: $\mathbb{F}$ is *not* simply the integers modulo p^{q-1}.

[2] Indeed, just like the complex numbers can be constructed by "extending" the real numbers to include an "imaginary solution" to the equation $x^2 = -1$, similarly, $\mathbb{F}$ can be constructed by "extending" $\mathbb{F}_p$ to include an "imaginary solution" to a certain equation. You can read more about finite fields on Wikipedia if you want.

[3] Proof that ω exists: The multiplicative group $\mathbb{F}^\times$ is cyclic with order $p^{q-1} - 1$, which is a multiple of q by Fermat's little theorem.