CS 281: Challenge #1

Professor Alexander Sherstov

Nakul Khambhati

Problem 1

While constructing the polynomial to compute $\texttt{MOD}_m$, we raise the polynomial to the m-th degree so that every non-zero element evaluates to 1. If m was not a prime number, this would not work for all non-zero elements. It would only work for the ones that are relatively prime to m.

Problem 2

Problem 3

We can prove that there is no polynomial-size circuit of constant depth that computes the majority function on n bits by proving the following proposition:
$\exists$ *a poly-size const depth circuit that computes* `MAJORITY` $\implies$ $\exists$ *exists a poly-size const depth circuit that computes* `PARITY`
Then the result follows by contraposition and Razborov-Smolensky.

Proof. Assume that C is a poly-size const depth circuit that computes `MAJORITY`. Consider the problem of determining whether $\#x = k$ where $\#x$ denotes the number of 1's in x and $0 \leq k \leq n$. We will now construct another circuit C' that is built out of C to solve this problem.

We can use C to decide $\#x \geq k$. This part is easier to explain by introducing some numbers. Assume $n = 5, x = 11010$ such that $\#x = 3$. Suppose we want to check whether $\#x \geq 4$ i.e. the case $k = 4$. We can simply append 00 to x and compute $C(x00) = 1 \iff \#x \geq 4$ since $|x00| = 7$. This way, we can compute any $\#x \leq k$ by appending a suitable number of 1's and 0's.
Similarly, we can compute $\#x \leq k$. For example, let's decide $\#x \leq 2$. It can be verified that $C(x) = 0 \iff \#x \leq 2$.
Then we can construct C' as $\#x = k \iff \#x \leq k \wedge \#x \geq k$. Since C' depends on k, let's denote it C'_k

Now, we can easily compute $\texttt{PARITY} = \bigvee_{k \text{ odd}} C'_k$ since `PARITY` returns `TRUE` if and only if there is an odd number of 1's in x. This only increase the depth by a constant factor and the size remains polynomial so we have proved the proposition. ☐

Problem 4