CS 121: Introduction to Theoretical Computer Science Fall 2019

Programming Assignment 1

Prof. Boaz Barak

Programming Question: Multiply Circuit (40 points + 20 points extra bonus): Let $S_{C,n} : \{0,1\}^n \to \{0,1\}^n$ be the following function: on $x \in \{0,1\}^n$, let $X \in \mathbb{N}$ be the natural number represented by x in the binary basis (i.e., $X = \sum_{i=0}^{n-1} x_i \cdot 2^i$), then $S_{C,n}(x)$ is the binary representation of the number $C \cdot X \pmod{2^n}$. That is, it is the representation of the number in $[2^n]$ obtained by multiplying X with C and then taking the remainder modulo 2^n. For this problem, we will take $n = 128$ and $C = 83077384819225213653292785468473349$ (These numbers will also be given in the code sample so you won't need to copy and paste them).

Write a Python function `nandmultiply()` that outputs a string which is the code of a valid NAND program that computes the function $S_{C,128}$. You will submit this through gradescope, and four collaborators can submit the same code. The authors that produce the shortest valid program in the class will get 20 points extra bonus. Any submission that is at most z percent longer than the best submission will get bonus of $\max\{0, 20 - z\}$ points.

We will supply skeleton code as well as code to test your programs.

Important Details:

- This problem can be solved by groups of up to 4 students.
- You submit the solution to a separate assignment through gradescope.
- While you should not copy any code, feel free to research online for clever algorithmic ideas, though remember that "premature optimization is the root of all evil": first get something working before you try to minimize the number of lines.
- You will have up to two late days, but late days will be taken off of every person in the group.
- This assignment will be due October 2nd at midnight.