HW1

Mathematical Methods in TCS: Boolean Functions (Fall 2026)
University of Toronto
Swastik Kopparty

Due: Wednesday, November 4, 2026

Think about all questions, submit **handwritten** (not typed) answers to any 2 questions.

Do not use AI to give you answers to these questions.

1. Let N be a positive integer. We will be working with circuits whose wires contain elements of $[N] = \{1, 2, \ldots, N\}$. N is going to go to infinity. This question is about computing 3-input functions using arbitrary 2-input gates.

   Let $s(N)$ be the smallest s such that every function $f : [N]^3 \to [N]$ can be computed by a circuit whose wires carry elements of $[N]$, using $\leq s$ 2-input gates, where each gate can compute an arbitrary function from $[N]^2$ to $[N]$.

   Prove the best upper bound and lower bound on $s(N)$ that you can. (We care about the asymptotics in N).

   (For the upper bound, it will be okay if you give an upper bound on $s(N)$ only for the case where N a power of 2.)

2. Show that if $f : \{0,1\}^n \to \{0,1\}$ has a decision tree with at most M leaves, then:

$$\Pr_{x \in \{0,1\}^n}[f(x) = PARITY(x)] \leq \frac{1}{2} + M \cdot 2^{-n}.$$

3. Let $f : \{0,1\}^{[k] \times [k]} \to \{0,1\}$ be the function:

$$f(M) = \begin{cases} 1 & \exists i \in [k] \text{ such that } M_{ij} = 1 \text{ for all } j \in [k] \\ 0 & \text{otherwise} \end{cases}.$$

   (The input to f is viewed as a $k \times k$ Boolean matrix).

   Show that the 0-certificate complexity and 1-certificate complexity of f are both equal to k.

   Show that the decision tree depth of f equals k^2 as follows. Suppose there was a decision tree of depth $D < k^2$ that computes f. Let us (the lower bound provers) design an M where it fails. Start running the decision tree algorithm. Every time it queries some bit M_{ij}, we (the lower bound provers) have to decide what the value of M_{ij} is. We keep deciding the bits of M in such a way that even after D bits of M have been revealed, the value of f is not yet determined by what has been revealed (both 0 and 1 are still possible values).

4. We say that $f : \{0,1\}^n \to \{0,1\}$ depends on the i'th variable if there exists some input $x \in \{0,1\}^n$ such that $f(x \oplus e_i) \neq f(x)$. ($e_i \in \mathbb{F}_2^n$ denotes the i'th elementary basis vector, and $\oplus$ denotes bitwise XOR, which is the same as vector sum in $\mathbb{F}_2^n$).

Let $S \subseteq [n]$ be the set of variables on which f depends. Suppose $|S| \leq k$.

Show that for all $T \subseteq [n]$:

$$\widehat{f}(T) \neq 0 \qquad \Rightarrow \qquad T \subseteq S.$$

$$\widehat{f}(T) \neq 0 \qquad \Rightarrow |\widehat{f}(T)| \geq 2^{-k}.$$

Thus show that there is a $\mathsf{poly}(2^k, n)$ time randomized algorithm to find S given oracle access to f.