Unconditional Lower Bounds & Derandomization, Spring 2024
Official Homework Problems

**Problem 1.** (2024/01/23) We proved in class that at least a $1 - 1/2^n$ fraction of all $2^n$ Boolean functions have de Morgan formula size at least $2^n/(2 \log n)$, for $n$ sufficiently large. In this problem you’ll prove a related average-case lower bound: Show that at least a $1 - 1/2^n$ fraction of all $2^n$ Boolean functions $f$ are such that any Boolean formula $F$ of size at most $2^n/(\log n)^2$ satisfies

$$\Pr_{U \sim \{0,1\}^n}[F(U) = f(U)] \leq 1/2 + \varepsilon(n)$$

for some function $\varepsilon(n) = o_n(1)$. How small can you make the function $\varepsilon(n)$?

**Problem 2.** (2024/01/23) Show that the $2^n$-variable Andre’ev function $A(x, y)$, defined in class, is computed by an $O(n)$-size Boolean circuit.

**Problem 3.** (2024/01/30) Give a construction of depth-$d$ circuits computing the $n$-variable parity function. Try to make the circuit size as small as you can, and analyze the circuit size of your construction. (You can assume $d$ is not too large, say at most $c \log(n)/\log\log(n)$ for an absolute constant $c$.)

**Problem 4.** (2024/02/06) Let $T$ be a proper decision tree over variables $x_1, \ldots, x_n$ (so no variable occurs twice on any root-to-leaf path). Prove that the following two distributions over branches are equivalent (recall that a branch is a sequence $\langle \pi_1, \pi_2, \ldots \rangle$ where each $\pi_i$ is a pair of the form $(x_i, b_i)$ where each $b_i$ is a 0/1 value):

- $D_1(T)$: Draw $\rho \sim \mathcal{R}_p$ and consider $T\upharpoonright\rho$. A draw from $D_1(T)$ is obtained by outputting a branch $\sigma \sim \mathcal{W}(T\upharpoonright\rho)$, i.e. $\sigma$ is a branch obtained by doing a random walk down from the root of $T\upharpoonright\rho$.

- $D_2(T)$: Draw $\pi = (\pi_1, \ldots, \pi_k) \sim \mathcal{W}(T)$. Output the sub-list of $\pi$ obtained by going through $\pi$ and independently including each element $\pi_i$ with probability $p$.

**Problem 5.** (2024/02/06) As defined in class, let $X \in \{w, w+1, \ldots\}$ be a random variable corresponding to the first time that $w$ consecutive heads come up in a sequence of i.i.d. fair coin flips. Prove that $E[X^t] \leq (7wt2^n)^t$. (Hint: One way to do this is by induction on $t$.)

**Problem 6.** (2024/02/13) Show that any depth-2 circuit that computes the $2n$-variable function $\text{DNFTRIBES}(a_1, \ldots, a_n) \lor \text{CNFTRIBES}(b_1, \ldots, b_n)$ correctly on 99% of all $2^{2n}$ many possible $2n$-bit inputs must have size at least $2^{\Omega(n/\log n)}$. You may use any of the results we proved in class to do this.
**Problem 7.** (2024/02/27) Let $\mathbb{F}$ be a field with $|\mathbb{F}| = n = 2^i$ and let $i \leq j$. Show how to generate $n$ random elements $X_1, \ldots, X_n$ of $\{0, 1, \ldots, 2^i - 1\}$ which are $k$-wise uniform using $kj$ independent uniform random bits. You may use any results from lecture.

**Problem 8.** (2024/02/27) Write down an explicit expression for the Fourier representation of $IP : \{0, 1\}^n \to \{-1, +1\}$, $IP(x_1, \ldots, x_n) = (-1)^{x_1x_2\cdots + x_{n-1}x_n \mod 2}$. Argue from this that for any degree-1 $\mathbb{F}_2$-polynomial $p$, we have $\Pr_U[IP(U) = p(U)] = 1/2 \pm 2^{-n/2}$.

**Problem 9.** (2024/02/27) Let $f : \{0, 1\}^n \to \{0, 1\}$ be a conjunction of literals over distinct variables. Show that $L_1(f) = 1$. 
