# 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

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

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 $2n$-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 $x_1, \dots, x_n$ (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 $\langle \pi_1, \pi_2, \dots \rangle$ where each $\pi_i$ is a pair of the form $(x_{i_1}, b_1)$ where each $b_i$ is a 0/1 value):

- $\mathcal{D}_1(T)$: Draw $\boldsymbol{\rho} \sim \mathcal{R}_p$ and consider $T\restriction_{\boldsymbol{\rho}}$. A draw from $\mathcal{D}_1(T)$ is obtained by outputting a branch $\boldsymbol{\sigma} \sim \mathcal{W}(T\restriction_{\boldsymbol{\rho}})$, i.e. $\boldsymbol{\sigma}$ is a branch obtained by doing a random walk down from the root of $T\restriction_{\boldsymbol{\rho}}$.
- $\mathcal{D}_2(T)$: Draw $\boldsymbol{\pi} = \langle \boldsymbol{\pi}_1, \dots, \boldsymbol{\pi}_k \rangle \sim \mathcal{W}(T)$. Output the sub-list of $\boldsymbol{\pi}$ obtained by going through $\boldsymbol{\pi}$ and independently including each element $\boldsymbol{\pi}_i$ with probability $p$.

**Problem 5.** (2024/02/06) As defined in class, let $\boldsymbol{X} \in \{w, w+1, \dots\}$ 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 $\mathbf{E}[\boldsymbol{X}^t] \le (7wt2^w)^t$. (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 $DNFTRIBES(a_1, \dots, a_n) \vee CNFTRIBES(b_1, \dots, b_n)$ 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 $|\mathbb{F}| = n = 2^j$ and let $i \le j$. Show how to generate $n$ random elements $\boldsymbol{X}_1, \ldots, \boldsymbol{X}_n$ 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 $\mathrm{IP} : \{0,1\}^n \to \{-1, +1\}$, $\mathrm{IP}(x_1, \ldots, x_n) = (-1)^{x_1 x_2 + \cdots + x_{n-1} x_n \mod 2}$. Argue from this that for any degree-1 $\mathbb{F}_2$-polynomial $p$, we have $\mathbf{Pr}_{\boldsymbol{U}}[\mathrm{IP}(\boldsymbol{U}) = p(\boldsymbol{U})] = 1/2 \pm 2^{-n/2}$.

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

**Problem 10.** (2024/03/26) Let $f : \{-1,1\}^n \to \{-1,1\}$. Show that for fixed $J, S \subseteq [n]$ and uniform random $\boldsymbol{z} \sim \{-1,1\}^{\bar{J}}$, we have

$$\mathop{\mathbf{E}}_{\boldsymbol{z} \sim \{-1,1\}^{\bar{J}}} \left[ \widehat{f}_{J,\boldsymbol{z}}(S) \right] = \mathbf{1}[S \subseteq J] \cdot \widehat{f}(S)$$
$$\mathop{\mathbf{E}}_{\boldsymbol{z} \sim \{-1,1\}^{\bar{J}}} \left[ \widehat{f}_{J,\boldsymbol{z}}(S)^2 \right] = \mathbf{1}[S \subseteq J] \cdot \sum_{T \subseteq \bar{J}} \widehat{f}(S \cup T)^2,$$

where $f_{J,z}$ is the restriction that leaves variables in $J$ "alive" and fixes variables in $[n] \setminus J$ to the values specified by $z$.

**Problem 11.** (2024/03/26) Let $f : \{-1,1\}^n \to \{-1,1\}$. Show that

$$\mathop{\mathbf{E}}_{(\mathbf{J}, \boldsymbol{z}) \sim \mathcal{R}_p} \left[ \widehat{f}_{\mathbf{J},\boldsymbol{z}}(S) \right] = p^{|S|} \cdot \widehat{f}(S)$$
$$\mathop{\mathbf{E}}_{(\mathbf{J}, \boldsymbol{z}) \sim \mathcal{R}_p} \left[ \widehat{f}_{\mathbf{J},\boldsymbol{z}}(S)^2 \right] = \sum_{U \subseteq [n]} \widehat{f}(U)^2 \cdot \mathbf{Pr}[U \cap \mathbf{J} = S],$$

where "$(\mathbf{J}, \boldsymbol{z}) \sim \mathcal{R}_p$" means that every variable is independently put into $\mathbf{J}$ with probability $p$ and $\boldsymbol{z}$ is uniform random over $\{-1,1\}^{\bar{J}}$.

**Problem 12.** (2024/03/26) Let $f : \{-1,1\}^n \to \{-1,1\}$. Show that

$$\mathop{\mathbf{E}}_{\mathbf{J}, \boldsymbol{z} \sim \mathcal{R}_p} \left[ W^{\ge k}[f_{\mathbf{J},\boldsymbol{z}}] \right] = \sum_{r \ge k} W^r[f] \cdot \mathbf{Pr}[\mathrm{Bin}(r, p) \ge k],$$

where $\mathrm{Bin}(r, p)$ denotes a draw from a Binomial random variable with success probability $p$.