Please turn in your solution in class on Tuesday September 24. You are encouraged to collaborate on the homework and ask for assistance, but you are required to write your own solutions, list your collaborators, acknowledge any sources of help, and provide external references if you used any.

All circuits in this assignment are of unbounded fan-in.

Question 1

This question is about the decision tree complexity of the recursive majority function. Recursive majority of $n = 3^d$ bits is defined by the formula

$$RMAJ_d(x, y, z) = MAJORITY_3\big(RMAJ_{d-1}(x), RMAJ_{d-1}(y), RMAJ_{d-1}(z)\big),$$

where $x, y, z \in \{0,1\}^{n/3}$ and n is a power of 3. The base case is $RMAJ_0(x) = x$.

(a) Show (by induction on d) that $RMAJ_d$ has decision tree depth 3^d.

(b) Show that $RMAJ_d$ is *not* 2^d-undetermined.

(c) Show that $\Pr[MAJORITY_3|_\rho \text{ is a constant}] = \frac{3}{2}p^2 - \frac{1}{2}p^3$, where $\rho \in \{0,1,\star\}^3$ is a $(1-p)$-random restriction (meaning each entry is a star with probability $1-\rho$).

(d) Show that $\Pr[RMAJ_d|_\rho \text{ is a constant}] \le 2^{-2^d}$, where $\rho \in \{0,1,\star\}^{3^d}$ is a 2/3-random restriction. (**Hint:** Use part (c) and induction.)

(e) Let ρ be as in part (d). Show that with probability at least 1/2, ρ can be extended by another restriction α so that $RMAJ_d|_{\rho\alpha}$ is the function $RMAJ_{d-t}$, where $t = \lceil \log d \rceil + 1$.

(f) Finally, show that $RMAJ_d$ requires decision tree *size* $2^{\Omega(3^d/d^{\log_2 3})}$. (**Hint:** Use part (a), part (e), and Theorem 5 from Lecture 1.)

Question 2

In this question you will investigate the relation between DNF, CNF, and decision tree size. Recall the function $DISTINCT\colon \{0,1\}^{2n} \to \{0,1\}$ from Lecture 1:

$$DISTINCT(x, y) = (x_1 \ne y_1) \text{ OR } \cdots \text{ OR } (x_n \ne y_n).$$

(a) Show that $DISTINCT$ has a decision tree of size $O(2^n)$.

(b) Show that the function $EQUAL = \text{NOT } DISTINCT$ requires DNFs of size 2^n, and therefore also decision trees of size 2^n.

(c) Show that every size s DNF has a decision tree of size $O(n^s)$.

(d) Show that the DNF

$$x_{11}x_{12}\cdots x_{1w} \text{ OR } x_{21}x_{22}\cdots x_{2w} \text{ OR } \cdots \text{ OR } x_{s1}x_{s2}\cdots x_{sw}$$

where $ws = n$ requires decision tree size $(n/s)^s$.

(e) **(Extra credit)** Let $f(s, n)$ be the largest possible size of the smallest decision tree among those that compute DNFs of size n on s variables. From Lecture 1 and parts (a)-(e) of this exercise we know that

$$\max\{2^{s/2}, (n/s)^s\} \le f(s, n) \le \min\{2^n, O(n^s)\}.$$

Can you improve either of these bounds?

Question 3

In Lecture 2 we claimed that any function $f\colon \{0,1\}^n \to \{0,1\}$ has a unique representation as $f(x) = p(x) \cdot MAJORITY(x) + q(x)$, where p and q have degree at most $(n-1)/2$ and n is odd. You will prove this claim.

(a) Let p be a nonzero polynomial and $a \in \{0,1\}^n$ be any string. Show that $D_a p$ has lower degree than p, where $D_a p(x) = p(x+a) + p(x)$ and $x + a$ is the bitwise XOR of x and a.

(b) Let $D_{a_0,\dots,a_d} p = D_{a_0} D_{a_1} \dots D_{a_d} p$. Prove the identity

$$D_{a_0,\dots,a_d} p(x) = \sum\nolimits_{S \subseteq \{0,\dots,d\}} p\Big(x + \sum\nolimits_{i \in S} a_i\Big).$$

(c) Use parts (a) and (b) to show that for every string x with more than d ones there exist strings $x^1, \dots, x^K$ with fewer ones than x such that $p(x) = \sum p(x^i)$ for all p of degree at most d.

(d) Use part (c) to show that if p has degree at most $(n-1)/2$ and p vanishes on all inputs with at most $(n-1)/2$ ones then p must vanish everywhere.

(e) Use part (d) to show that if p, q have degree at most $(n-1)/2$ and $p(x)MAJORITY(x) + q(x)(1 + MAJORITY(x)) = 0$ for all x, then p and q must be the zero polynomials.

(f) Use part (e) to show that every f can have at most one representation of the desired type.

(g) Prove the claim. (**Hint:** Count.)