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.

Solution: This is true for $d = 0$ because $RMAJ_0$ is not constant. Suppose it is true for $d-1$. For any ordering of the 3^n inputs, by inductive assumption there exists an assignment of values so that $RMAJ_{d-1}(x)$ is undetermined until all of the bits of x are queried, and the same is true for y and z. By symmetry we may assume that the last bits in x and y are queried before the last bit of z. If the last queried bits in x and y are assigned opposite values then the value of $RMAJ_d$ is undetermined until the last bit of the input is queried by the decision tree.

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

Solution: This is true by induction on d: $RMAJ_0$ can be set to zero by restricting its input to zero. Assuming $RMAJ_{d-1}$ can be set to zero by resticting 2^{d-1} of its input, so can $RMAJ_d$ by restricting its x and y inputs accordingly.

(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 $1-p$).

Solution: $MAJORITY_3$ restricts to a constant if the restriction has at least two zeros or at least two ones. The probability ρ has exactly two zeros is $3(p/2)^2(1-p/2)$ and the probability it has three zeros is $(p/2)^3$. The probabilities are the same for at least two ones, so the desired probability is $2(3(p/2)^2(1-p/2) + (p/2)^3) = 3p^2/2 - p^3/2$.

(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.)

Solution: If p_d is the desired probability then by part (c) $p_d = \frac{3}{2}p_{d-1}^2 - \frac{1}{2}p_{d-1}^3$, so $\frac{3}{2}p_d \le (\frac{3}{2}p_{d-1})^2$. Unwinding this recursion, we get that $p_d \le \frac{2}{3}(\frac{3}{2}p_0)^{2^d} \le 2^{-2^d}$ for $p_0 = 1/3$.

(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 $t = \lceil \log d \rceil + 1$.

Solution: $RMAJ_d$ can be written as $RMAJ_{d-t}$ of 3^{d-t} $RMAJ_t$ functions on distinct inputs. By part (d) and a union bound, the probability that any one of these $RMAJ_t$ functions restricts to a constant under ρ is at most $3^{d-t}\cdot 2^{-2^t} = 2^{(d-t)\log 3 - 2^{\log d + 1}} \le 2^{-0.415d - 1.584t} \le 1/2$. Assuming none restrict to a constant, all but one of their inputs can be fixed by some α so that this property is preserved. Then $RMAJ_d|_{\rho\alpha}$ is the recursive majority of depth $d-t$.

(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.)

Solution: Combining the three parts we get the inequality $s \cdot (5/6)^{3^{d-t}} \geq 1/2$, from where $s \geq \frac{1}{2} \cdot (6/5)^{3^d/3^t} \geq \frac{1}{2} \cdot (6/5)^{3^d/9d^{\log_2 3}}$.

Question 2

Recall the function $DISTINCT\colon \{0,1\}^{2n} \to \{0,1\}$ from Lecture 1:

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

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

Solution: The following decision tree solves $DISTINCT$. Read x_1 and then y_1. If they are different output zero, if they are equal recursively solve $DISTINCT$ on $2n-2$ inputs. The size of this decision tree satisfies the recurrence $s(n) = 2s(n-1)+2$ with initial condition $s(1) = 4$ which solves to $s(n) = 3 \cdot 2^n - 2$.

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

Solution: We show that any term in any DNF for $EQUAL$ must include all $2n$ variables. Suppose there is a term that misses at least one variable and let (x,y) be an assignment that satisfies this term. By possibly flipping the value of the missing variable we can always obtain an assignment that the term still accepts but in which x and y are not equal. So such a DNF cannot compute $EQUAL$.

Each term that includes all $2n$ variables accepts a random assignment with probability 2^{-2n}. Since the probability that x equals to y is 2^{-n} there must be at least 2^n clauses in the DNF.

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

Solution: We describe the decision tree recursively. Given any clause of the DNF, the decision tree queries the variables in that term one by one. If the answer to the i-th query makes the term reject, the decision tree recursively computes the remaining DNF of size $s-1$. If the answers to all queries satisfy the term, the decision tree outputs 1. For the base case, when $s = 0$ the decision tree outputs 0.

The size of the decision tree satisfies the recurrence $t(s) = nt(s-1)+1$ with base case $s(0) = 1$ which solves to $t(s) = O(n^s)$.

(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 $(n/s)^s$.

Solution: Consider the set X of inputs that have exactly one zero in each term. An element of X can be described by specifying the positions of the zeros so X has size w^s. We argue that in any decision tree for this DNF, no two inputs in X follow the same path in the tree. Assume some two inputs do. These inputs differ by the values of two variables in the same term, so these two variables cannot be queried on the path. But the value of the function on both inputs is then undetermined so the inputs must lead to different leaves. So the tree must have at least w^s leaves.

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.

Solution: By linearity it is enough to prove this for monomials. When p is a monomial $p(x+a)$ is not, but its highest degree monomial is p. The highest degree monomials in $p(x)$ and $p(x+a)$ cancel out so $D_a p$ has strictly lower degree.

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

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

Solution: This can be proved by induction. The base case $d = 0$ is immediate. For the inductive step from $d-1$ to d:

$$\begin{aligned} D_{a_0} D_{a_1,\ldots,a_d} p(x) &= D_{a_0} \sum_{S \subseteq \{1,\ldots,d\}} p\left(x + \sum\nolimits_{i \in S} a_i\right) \\ &= \sum_{S \subseteq \{1,\ldots,d\}} p\left(x + a_0 + \sum\nolimits_{i \in S} a_i\right) + \sum_{S \subseteq \{1,\ldots,d\}} p\left(x + \sum_{i \in S} a_i\right) \end{aligned}$$

so the identity holds for all d.

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

Solution: Let a_i be the string obtained that is zero everywhere except in the position of the i-th one entry of x. Then all strings of the form $x^S = x + \sum_{i \in S} a_i$ have fewer ones than x. By part (b) they all add up to zero, so $p(x) = p(x^\varnothing)$ can be represented as a sum of the others.

(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.

Solution: By induction on the number of ones, any string x with *at least* d ones satisfies the property in part (c). The right-hand side $\sum p(x^i)$ is a sum of zeros so $p(x)$ is also zero.

(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.

Solution: This polynomial has value $q(x)$ at every x such that $MAJORITY(x) = 0$, namely on all inputs with at most $(n-1)/2$ ones. By part (c) q must vanish everywhere so $p(x)MAJORITY(x)$ is the zero polynomial. So is the polynomial $p(1+x)MAJORITY(1+x)$, where 1 is the all-ones input. The polynomial $p(1+x)$ has degree at most $(n-1)/2$ and vanishes on all inputs with at most $(n-1)/2$ ones so by part (c) $p(1+x)$ too must vanish everywhere, and so must p.

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

Solution: If f has two such representations (p, q) and (p', q'), then their difference $(p - p', q - q')$ would be a representation of zero, so $p - p'$ and $q - q'$ must be zero, so the two representations are identical.

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

Solution: To describe p we need to list all its coefficients. There is one coefficient for every set of size less than $n/2$, of which there are $2^n/2$ (since each set and its complement match all subsets of $\{1, \ldots, n\}$). So there are $2^{2^n/2}$ choices for p and as many for q, or $(2^{2^n/2})^2 = 2^{2^n}$ choices for the pair (p, q). This is equal to the number of functions from n bits to one bit. If a function has no reperesntation then some other function must have more than one, which is impossible by part (f).