You are encouraged to collaborate on the homework and ask for assistance. You are required to write your own solutions, list your collaborators, acknowledge all sources of help, and cite all external references.

Question 1

Call a function *k-uncertifiable* if for every subset of k inputs, no partial assignment to those inputs fixes the function value to 1. Show the following:

(a) $DISTINCT(x,y) = (x_1 \neq y_1)$ OR $\cdots$ OR $(x_n \neq y_n)$ has a decision tree of size $O(2^n)$.

(b) If ϕ is a DNF for a k-uncertifiable function then all terms of ϕ must have width more than k.

(c) A size-s DNF for a k-uncertifiable function can accept at most a $s \cdot 2^{-k-1}$-fraction of all possible inputs.

(d) The function $EQUAL =$ NOT $DISTINCT$ requires DNFs of size 2^n. Use part (c).

(e) $DISTINCT$ requires decision trees of size 2^n. Use part (d).

Question 2

Recall the INJ function from Lecture 2:

$$INJ(x_1,\ldots,x_n) = AND_{i\neq j} DISTINCT(x_i,x_j), \qquad x_i \in \{0,\ldots,m-1\}.$$

Assume $m \geq n$, n and m are both powers of 2, and elements of $\{0,\ldots,m-1\}$ are specified by their bit representation. Show the following:

(a) INJ is $(n\log n - 1)$-uncertifiable when $m = n$. (**Optional:** Is this true when $m > n$?)

(b) INJ requires DNFs of size at least $n!$ when $m \geq n$.
(**Hint:** Reduce to the case $m = n$ and use part (c) of question 1.)

(c) INJ has CNFs (ANDs of ORs of literals) of size $\binom{n}{2}m$.

(d) INJ requires CNFs of size at least m for any $n \geq 2$. (**Hint:** Use part (d) of question 1.)

Question 3

Let $f(x_1,\ldots,x_m)$ be a boolean function and $y_1,\ldots,y_n$ be another set of varaibles. A *projection* of f is a function obtained by replacing each x_i with one of the literals $y_1,\ldots,y_n,\overline{y_1},\ldots,\overline{y_n}$ or one of the constants $0,1$. We say f projects to g if there exists a projection of f that equals the function $g(y_1,\ldots,y_n)$.

(a) The AND-OR tree on n inputs is defined by the recursive formula

$$AOT(x,y,z,w) = (AOT(x) \text{ OR } AOT(y)) \text{ AND } (AOT(z) \text{ OR } AOT(w)),$$

where $x,y,z,w \in \{0,1\}^{n/4}$ and n is a power of four. The base case is $AOT(x) = x$. Show that AOT on n^2 inputs projects to PARITY on n inputs for every n that is a power of two. (**Hint:** Use induction.)

(b) Use part (a) and facts about PARITY from class to show that AND-OR requires depth-d AND/OR circuits of size $2^{\Omega(n^{1/2(d-1)})}$.

(c) Valiant's Theorem states that there exists a constant $c > 1$ for which recursive majority on at most n^c inputs projects to MAJORITY on n inputs. Recursive majority is the function

$$RMAJ(x,y,z) = MAJORITY\big(RMAJ(x), RMAJ(y), RMAJ(z)\big),$$

where $x,y,z \in \{0,1\}^{n/3}$ and n is a power of 3. The base case is $RMAJ(x) = x$. Assuming Valiant's theorem, show that AOT requires depth-d AND/OR/PARITY circuits of size $2^{\Omega(n^{\varepsilon/d})}$ for some constant $\varepsilon > 0$.

Question 4

A function $f\colon \{0,1\}^n \to \{0,1\}$ has *rational degree* at most d (over $\mathbb{F}_2$) if

$$\text{there exist polynomials } p \text{ and } q \text{ of degree at most } d \text{ such that } pf = q \text{ and } p \neq 0. \tag{1}$$

($a = b$ means $a(x) = b(x)$ for all x.) Show that for any given f,

(a) (1) implies

$$\begin{array}{l}\text{there exists } r_0 \neq 0 \text{ of degree at most } d \text{ such that for every } x,\ f(x) = 0 \text{ implies } r_0(x) = 0, \text{ or} \\ \text{there exists } r_1 \neq 0 \text{ of degree at most } d \text{ such that for every } x,\ f(x) = 1 \text{ implies } r_1(x) = 0.\end{array} \tag{2}$$

(b) (2) implies (1).

(c) (1) implies

$$\text{there exists a function } g \text{ such that for all polynomials } p \text{ and } q \text{ of degree less than } n-d,\ g \neq pf+q. \tag{3}$$

(**Hint:** Try a proof by contradiction.)

(d) (**Optional**, requires some $\mathbb{F}_2$-linear algebra) (3) implies (1).
(**Hint:** $g = pf + q$ is a system of linear equations whose variables are the coefficients of p and q.)

(e) f has rational degree at most $n/2$. Use part (d).