Please turn in your solution in class on Tuesday 5 November. You are required to work and write your solutions individually.

## Question 1

Let $x_1, \dots, x_{10} \in \{0,1\}^{100}$ be 10 strings of 100 bits each. The distinctness function $DIST(x_1, \dots, x_{10})$ takes value 1 if all strings are distinct ($x_i \neq x_j$ when $i \neq j$) and 0 otherwise.

(a) Show that any deterministic read-once branching program for $DIST$ (that reads its input from left to right) must have width at least $2^{490}$.

(b) Let $h\colon \{0,1\}^{100} \to \{0,1\}^{10}$ be a random function. Show that with probability at least 95%, $DIST(h(x_1), \dots, h(x_{10})) = DIST(x_1, \dots, x_{10})$ for any fixed choice of inputs.

(c) Show that $DIST$ can be computed by a randomized read-once branching program of width at most $2^{200}$ with error at most 5%.

## Question 2

Let $X$ be an $n$ by $n$ matrix and $f\colon \{0,1\}^{n^2} \to \{0,1\}$ be the function

$$f(X) = \begin{cases} 1, & \text{if } f \text{ has \textit{exactly one} column consisting of zeros only,} \\ 0, & \text{otherwise.} \end{cases}$$

Determine the following quantities up to a constant factor (i.e., in $\Theta(\cdot)$ notation). Provide both upper and lower bound proofs.

(a) the deterministic query complexity $D(f)$

(b) the exact degree $\deg(f)$ when $f$ is viewed as a real-valued polynomial

(c) the sensitivity $\mathrm{sens}(f)$

(d) **(Extra credit)** the Monte Carlo randomized query complexity $R_{1/3}(f)$

(e) **(Mini-research project)** the quantum query complexity $Q_{1/3}(f)$

## Question 3

A *solution generator* for a search relation $R \subseteq \{0,1\}^* \times \{0,1\}^*$ is an algorithm $G$ that on input $(x, \ell)$ outputs the $\ell$-th lexicographically smallest $y$ such that $(x,y) \in R$, and the special symbol $\perp$ if such a $y$ does not exist. For example, if $(0,0), (0,10), (0,111) \in R$ but $(0,y) \notin R$ for all other $y$ then $G(0,1) = 0, G(0,2) = 10, G(0,3) = 111$, and $G(0,\ell) = \perp$ for all other $\ell$. We say that a solution generator is *efficient* if its running time is polynomial in $|x|$ and $\ell$.

(a) Prove that the search relation $R_{\mathrm{DNF}} = \{(\phi, y) : \phi \text{ is a DNF such that } \phi(y) = 1\}$ (a DNF is an OR of ANDs of literals) has an efficient solution generator.

(b) Prove that if the search relation $R_{\mathrm{CNF}} = \{(\phi, y) : \phi \text{ is a CNF such that } \phi(y) = 1\}$ (a CNF is an AND of ORs of literals) has an efficient solution generator then P = NP.

(c) Prove that if P = NP then every NP search relation has an efficient solution generator.