Endterm
Computational Complexity

Solve all 6 questions. The solutions are due on Monday, May 12. Some hints are given on the last page.

Problems

1. A DNF formula in (boolean) variables $x_1, x_2, \ldots, x_n$ is of the form

$$\phi = D_1 \vee D_2 \cdots \vee D_m$$

$$\text{where for } 1 \leq i \leq m, \quad D_i = y_{i_1} \wedge y_{i_2} \ldots \wedge y_{i_k}$$

and each y_j is a variable or its negation. Show that deciding if a DNF formula is satisfiable is in P but counting the number of satisfying solutions is $\#\mathsf{P}$-complete.

2. Let L be the language accepted by a family of circuits $\{C_n\}$ which consist of AND, NOT and PARITY gates such that

   - Circuit C_n has n inputs, size $2^{n^{O(1)}}$ and depth $O(1)$.
   - AND gates have fan-in bounded by poly(n).
   - PARITY gates have unbounded fanin.
   - The circuits C_n are uniformly generated by a polynomial time DTM M.

   Show that $L \in \oplus\mathsf{P}$. In other words show that there is a polynomial time NTM N which has an odd number of accepting computations on input x iff $x \in L$.

3. Let $\mathbb{Z}_3 = \{0, 1, -1\}$ be the field of integers modulo 3. We say that a polynomial $P(X_1, \cdots, X_n)$ in n variables is multilinear if the degree of each X_i in P is at most 1. For instance $P(X_1, X_2, X_3) = X_1X_2 + X_2X_3$ is multilinear but $X_1^2 + X_2^2$ is not.

   - Show that every function $f : \{0, 1\}^n \to \mathbb{Z}_3$ is computed by a unique multilinear polynomial in $\mathbb{Z}_3[X_1, \cdots, X_n]$.
   - Consider all Boolean functions $f : \{0, 1\}^n \to \{0, 1\}$. Let the degree of function f be the degree of the unique polynomial computing f. Show that AND and OR functions have degree n.
   - The MOD-k function is 1 if $\sum_{i=1}^{n} x_i$ is divisible by k, and 0 otherwise. Show that MOD-2 (PARITY) has degree n but MOD-3 has degree 2.

4. Let $\omega(G)$ denote the size of the largest clique in graph G. Assume that there is a polynomial time reduction A that takes as input a SAT instance ϕ and outputs a graph G on n vertices such that

   - If ϕ is satisfiable, $\omega(G) \geq \alpha n$.
   - If ϕ is unsatisfiable, $\omega(G) \leq \beta n$.

   Here α, β are constants such that $0 < \beta < \alpha < 1$. Use this to show that, for any constant C, there is no polynomial time algorithm that approximates $\omega(G)$ within a factor C unless $\mathsf{P} = \mathsf{NP}$.

5. Assume that there is an unknown Boolean function $f : \{0,1\}^n \to \{0,1\}$ which is 1 at exactly K inputs. Give an algorithm to find (some) input x with $f(x) = 1$ which asks $O(\sqrt{N/K})$ queries in the Quantum Query Model ($N = 2^n$). A single query Q is defined as the unitary operator:

$$Q\,|x\rangle \;=\; (-1)^{f(x)}\,|x\rangle \qquad \forall x \in \{0,1\}^n.$$

6. The set-disjointess function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is defined as

$$f(x,y) = 1 \qquad \Longleftrightarrow \qquad x_i \wedge y_i = 0 \;\; \forall\, i = 1, \cdots, n$$

   In other words, think of x and y as incidence vectors of sets $S(x)$ and $S(y)$ respectively. Then $f(x,y) = 1$ iff the sets $S(x)$ and $S(y)$ are disjoint. Let M_f denote the matrix of values of f.

   - Show that any 1-monochromatic rectangle in M_f has size at most 2^n.
   - Show that the deterministic communication complexity of f is $\Omega(n)$.

Hints

1. A CNF formula in variables $x_1, x_2, \ldots, x_n$ is of the form

$$\phi = C_1 \wedge C_2 \cdots \wedge C_m$$

$$C_i = y_{i_1} \vee y_{i_2} \cdots \vee y_{i_k}$$

First show that counting the number of solution to CNF formula is #P-complete.

2. Define the non-deterministic machine N as follows

   - At an AND gate, evaluate all the inputs (recursively). Accept only if all the computations accept.
   - At a PARITY gates, non-deterministically select an input and evaulate it. Accept if that computation accepts.
   - At a NOT gate, non-deterministically do one of the following (i) Accept (ii) Evaluate the input to the NOT gate and accept if that computation accepts.

3. To write PARITY as a polynomial over $\mathbb{Z}_3$, note that it is easy to write in $\{+1, -1\}$-notation. Then convert it into $\{0, 1\}$-notation.

4. Consider the following graph product. Given a graph $G(V, E)$ the graph G^2 has vertex set $V^2 = V \times V$. The edges are defined as

$$(v_1, v_2) \sim (w_1, w_2) \quad \text{if} \quad \begin{cases} v_1 \sim w_1 & \text{and} \quad v_2 \sim w_2 \\ v_1 = w_1 & \text{and} \quad v_2 \sim w_2 \\ v_1 \sim w_1 & \text{and} \quad v_2 = w_2 \end{cases}$$

Use this product to boost the gap between $\omega(G)$ in the given reduction.

5. Show that a modification to Grover's Algorithm works. Choose an appropriate pair of mutually orthogonal vectors in the plane.