CSE491/596, Fall 2023 Problem Set 6 Due 11/21/23, 11:59pm

A reminder that Prelim II will be held on **Wednesday, Nov. 29** in class period. The rules are the same as for Prelim I. It will be "cumulative" and covers material up through problem (3) of this set, but not the quantum-related material collected in problem (4). All remaining reading is out of the Lipton-Regan textbook, excerpts provided freely via non-public links on *Piazza*. For now, read chapters 1–4, and also look at the latter reading (first half of chapter 14) to see the Dirac angle-bracket notation and Bloch sphere (skimming the rest). Chapters 7–8, plus parts of 5–6, will be emphasized the week after Thanksgiving. The last four lectures from December 4 to 11 will cover chapters 9–10, and then you will be given chapters 11–13 or perhaps a lighter treatment of Shor's and Grover's algorithms, depending on how things go. Note that the final exam is as close as possible to the last lecture, so that and the previous Friday will be treated as FYI and will mix in some review.

——————-*Assignment 6, due Tue. 11/21 "midnight stretchy" on CSE Autolab*——————-

(1) The answer key for Assignment 5, problem (2), leaves a gap in its proof of the converse ("$\Longleftarrow$") direction of the reduction correctness condition "ϕ is exactly-one-satisfiable $\iff$ $f(\phi) = (G_\phi, k)$ such that the graph G_ϕ has a perfect dominating set (PDS) of size k." That is, it leaves a buggy loophole by which G_ϕ can have a PDS of size $k = n$ without it being true that ϕ has an assignment that satisfies each of its clauses exactly once. Even though the function f giving the construction is exactly the same as the one in lecture when reducing "vanilla 3SAT" to the non-perfect DOMINATING SET problem—and that construction has no bug in that reduction—it has a bug when used to reduce EXACTLY ONE 3SAT to PERFECT DOMINATING SET. *Find and fix the bug* by making a modified graph G'_ϕ and proving that $(G'_\phi, n) \in \text{PDS} \implies \phi \in$ EXACTLY ONE 3SAT. (The fix is thematic with my lecture—the part after the fire alarm on Wed. 10/25. The motivation is not to be so casual about proofs. The bug was silently ignored in grading the relatively few papers exposed to it. 18 pts. total)

(2) The following two decision problems involve directed graphs G in which every non-sink node has two out-edges labeled "right" and "left." Also specified in an instance are a source node s, a sink t, and another node u.

(i) INSTANCE: G, s, t, u as above.
QUESTION: Is there a path from s to t that goes through u, such that the number of steps from s to u equals the number of steps from u to t?

(ii) INSTANCE: G, s, t, u as above.
QUESTION: Is there a path from s to t that goes through u, such that the sequence of "right" and "left" edges taken by the path from s to u equals the sequence from u to t?

Note that problem (ii) involves a more-particular question, since in order for the right-left sequences to be the same, they must have the same number of steps.

(a) Show that problem (i) belongs to NL. A pseudocode or machine sketch that is detailed enough to show time and/or space usage is sufficient. (15 pts.)

(b) Briefly explain why your argument in (a) fails to classify problem (ii) the same way. In fact, problem (ii) is NP-complete, so please further explain by giving some consequences of its being in NL that are believed highly unlikely. (9 pts., for 24 total. Do not try to prove completeness)

(3) Show that the following problem is complete for co-NP under $\leq_m^p$:

ALL$_{NFA,n}$
INSTANCE: An NFA $N = (Q, \Sigma, \delta, s, F)$ with $\Sigma = \{0, 1\}$ and a number n.
QUESTION: Does N accept every string in $\{0, 1\}^n$?

For a hint on the reduction part, take a 3DNF formula $\psi(x_1, \dots, x_n) = T_1 \vee \cdots \vee T_m$. Then ψ is a tautology if and only if every assignment $a \in \{0, 1\}^n$ satisfies one of the terms. (Or if you prefer, think of a 3CNF formula $\phi(x_1, \dots, x_n) = C_1 \wedge \cdots \wedge C_m$ and note that ϕ is *un*satisfiable if and only if every assignment $a \in \{0, 1\}^n$ "unsatisfies" one of the clauses.) Show how to create N from ψ (or from ϕ) and give analysis to show that the reduction from 3TAUT (or from the complement of 3SAT) is correct. (27 pts. total)

(4) Some short linear algebra (for quantum) exercises.

(a) Compute the value of the tensor product matrix $A \otimes B$, where $A = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ and $B = \begin{bmatrix} 0.8 & 0.6 \\ -0.6 & 0.8 \end{bmatrix}$, on the tensor-product vector $\frac{1}{\sqrt{2}}[1, -1]^T \otimes [\frac{3}{5}, \frac{4}{5}]^T$. Do the calculation two ways:

- Show the 4×4 matrix $A \otimes B$ multiplying the length-4 product vector.
- Compute A on $[1, -1]^T$ to get one vector of length 2 (also divide it by 2 to reflect the two factors of $\frac{1}{\sqrt{2}}$) and B on $[\frac{3}{5}, \frac{4}{5}]^T$ to get another vector of length 2. Then take the tensor product of the resulting vectors.

Show that they give the same result. (12 pts. total)

(b) Prove that the state vector $\frac{1}{2}[-1, 1, 1, 1]^T$ cannot be written as a tensor product of two smaller vectors. That is, it represents an entangled quantum state. (9 pts.)

(c) Suppose A and B are self-adjoint, meaning $A^* = A$ and $B^* = B$. Show that $A \otimes B$ is self-adjoint. Use the concatenation-based indexing convention that $A[u, v]B[w, x] = (A \otimes B)[uw, vx]$. (9 pts.)

(d) Find a 2×2 unitary matrix A such that $A^2 = iY$. (The scalar multiple i doesn't matter in quantum computing and allows A to have real entries. It also doesn't matter which form of Y is used—either way, A is called the "square root of Y." 6 pts., for 36 on the problem and 105 pts. on the set)