CSE696, Spring 2021 Problem Set 4 Due Mon. 5/10

Reading:

After Chapter 13, please read Chapter 19 (which finally defines BQP) in advance of a presentation by Frank Tsai on Wednesday on sections 19.3–19.6. This is a short HW in advance of the take-home final, which will run from 5/10 to 5/17. The take-home final will be like homeworks except for the open-ended aspects of the latter.

(1) Consider undirected n-vertex graphs G as given by their $n \times n$ adjacency matrices $A = A_G$. To any permutation π of $\{1, \ldots, n\}$ we can associate the permutation matrix P with entries $P[i, \pi(i)] = 1$, $P[i, j] = 0$ for the other $n - 1$ values j. Then $A_\pi = PAP^{-1}$ is another adjacency matrix for the same graph G with the labels of the nodes permuted. Then π is an *automorphism* of G if the matrices A_π and A are identical. Note that you can consider the matrices to be binary strings in $\{0,1\}^m$ where $m = n^2$—or if you care to minimize redundancy, you can consider the upper triangle as a string in $\{0,1\}^m$ with $m = \binom{n}{2} = n(n-1)/2$ instead.

(a) Say briefly why the automorphisms form a subgroup of the permutation group S_n. The subgroup is standardly called $\mathsf{Aut}(G)$. (6 pts.)

(b) Let L_0 be the language of graphs with *no* automorphisms other than the identity. Let L_1 denote the graphs having exactly *one* automorphism besides the identity, i.e., with $||\mathsf{Aut}(G)|| = 2$. Finally let L_3 comprise all other strings in $\{0,1\}^m$, which all denote graphs having two or more automorphisms besides the idenitity. None of these languages is currently known to belong to P, but this problem will lead into reasons why they are not believed to be NP-hard either. Say whether you can put each of L_0, L_1, L_2 into any of NP, $\mathsf{co\text{-}NP}$, UP, $\mathsf{co\text{-}UP}$, or the class US; recall that a language L belongs to US iff there is a function $f \in \#\mathsf{P}$ such that $L = \{x : f(x) = 1\}$. (9 pts.)

(c) Given any n-vertex graph $G \in L_0$, say exactly how many strings in $\{0,1\}^m$ denote the same graph. Same question given $G \in L_1$. Finally, if $G \in L_2$, what is an upper limit on the number of such strings? (9 pts.)

(d) Prove that L_0 belongs to $\mathsf{BP}[\mathsf{NP}]$, that is, to AM. Use the same hashing idea as in the set cardinality protocol, which is akin to the calculations we have seen with the Valiant-Vazirani theorem on HW3. (18 pts.)

(e) Can you get $L_1 \in \mathsf{AM}$ in a similar manner? Finally say why it is silly to ask whether $L_2 \in \mathsf{AM}$. (Open-ended, but with a baseline of 12 pts., for 54 on the problem.)

(2) With reference to problem(1): given any individual graph $G \notin L_2$ (in the form of some adjacency matrix A_G for it), show how to define a function f_G that is 1-to-1 if $G \in L_0$ and 2-to-1 if $G \in L_1$. Then give a relation $R(x, y)$ such that $f_G(x) = f_G(y) \iff R(x, y)$ holds, where $x, y \in \{0,1\}^m$. Show that if $R(x, y)$ could always have the form that there exists a

string z_G, depending only on G, such that $f_G(x) = f_G(y) \iff x \oplus y = z_G$, then L_0 would belong to BQP. (18 pts. total—plus possible open-ended as this is IMHO the most accessible basic open question about concrete problems and BQP)

(3) Over all input lengths n, consider products $M = M_1 \cdot M_2 \cdots M_s$ of $N \times N$ matrices, where $N = 2^n$, such that:

- $s = s(n)$ is polynomial in n;
- every entry $M_k[i, j]$ is 0, 1, or -1; and
- the function $\mu(i, j, k) = M_k[i, j]$ is computable in $O(n)$ time, where $0 \leq i, j < 2^n$ and $1 \leq k \leq s$.

The third condition says that the families of matrices are polynomially uniformly presented. They could come from a uniform family $[C_n]_{n=1}^{\infty}$ of quantum circuits (of Hadamard, CNOT, and Toffoli gates only, say), but the setting of this problem is more general. Show that there are two functions $f, g \in \#\mathsf{P}$ such that $M[i, j] = f(i, j) - g(i, j)$. Note that

$$M[i, j] = \sum_{\ell_1, \ldots, \ell_{s-1}} M_1[i, \ell_1] M_2[\ell_1, \ell_2] \cdots M_{s-1}[\ell_{s-2}, \ell_{s-1}] M_s[\ell_{s-1}, j].$$

Have f count the positive products and g the negative ones. Conclude from this that any language defined by the condition that $M[0, 0] \neq 0$, for instance, belongs to P^{PP}. (The proof that it belongs to PP is harder, I think... 18 pts., for 90 total)