CSE439, Fall 2024 Problem Set 4 Due Fri. 11/01, 11:59pm

Next week has an evening Zoom lecture **Tuesday 10/29, 7:30–8:50pm** to make up for the canceled lecture on Thursday. Zoom coordinates will be given on *Piazza* and it will be recorded. It will cover the analysis of the classical part of Shor's algorithm and how knowing the period enables one to factor, from Chapter 12, after the regular Tuesday lecture in class that day covers the analysis in Chapter 11 of the quantum part. *Please read those chapters over the weekend.* The Thursday lecture will likely include coverage of Grover's algorithm, so please also read chapter 13 and look at the notes https://cse.buffalo.edu/˜regan/cse491596/CSE491596lect121123GroverExtra.pdf.

The assignment is due on Friday Nov. 1 because Thursday of next week is Halloween.

——————-*Assignment 4, due Fri. 11/1 "midnight stretchy" on CSE Autolab*——————-

(1) This problem is midway between the "maze diagram" analysis of small quantum circuits—graph state circuits in particular—and the kind of linear algebra done in the proofs of Deutsch-Jozsa and Simon's algorithm. Recall from lecture that the analysis of n-qubit graph state circuits C_G can be reckoned in terms of colorings of the associated graph $G = (V, E)$, $|V| = n$, where each vertex in V is colored either black (B) or white (W). Call a coloring "even" if it makes an even number of B-B edges (counting zero as an even number) and "odd" otherwise. Note that if the node of a self-loop is colored B, then the loop counts as a B-B edge. The point is that there are 1-to-1 correspondences between:

- binary strings z of length n, which correspond also to basis states $|z\rangle$;
- colorings of V, where vertex i is colored B means that bit $z_i = 1$; and
- "mice" in the "maze," since the initial $\mathbf{H}^{\otimes n}$ Hadamard transform puts one positive mouse on each row.

The gist is that a coloring makes an odd number of B-B edges if and only if the mouse along the corresponding row ends up negative. In consequence:

- $\langle 0^n \,|\, C_G \,|\, 0^n \rangle = 0$ if and only if the number of positive mice equals the number of negative mice, which is the same as G having 2^{n-1} even colorings and 2^{n-1} odd colorings.
- The amplitude of $\langle 0^n \,|\, C_G \,|\, 0^n \rangle$ equals the number of even colorings minus the number of odd colorings, divided by 2^n.

Now, let us take any n-node undirected graph $G = (V, E)$ and vertex u of G and add a "stick" at u using two new vertices v, w and two new edges (u, v) and (v, w). The resulting graph $G' = (V', E')$ has $V' = V \cup \{v, w\}$ and $E' = E \cup \{(u, v), (v, w)\}$. For example, the "lollipop" graph, which is on the very last page of the notes https://cse.buffalo.edu/˜regan/cse439/CSE439Week5.pdf, can be regarded as obtained by adding the "stick" of vertices 2 and 3 to the simple loop graph on vertex 1. *Your task* is to *prove* the following identity, for any n and graphs G and G' as above:

$$\left\langle 0^{n+2} \,\middle|\, C_{G'} \,\middle|\, 0^{n+2} \right\rangle = \frac{1}{2} \left\langle 0^n \,|\, C_G \,|\, 0^n \right\rangle .$$

Conclude that G' is net-zero if and only if G is. (Hint: Consider separately the colorings χ of the original graph G that make $\chi(u) = B$ and those that make $\chi(u) = W$. Show in each case how many colorings of the extra nodes v, w flip the parity of B-B edges. 24 pts. For up to 18 pts. extra credit, assuming nodes v, w are numbered $n+1$ and $n+2$, prove the answer to whether we get $\langle x00 \,|\, C_{G'} \,|\, x00 \rangle = \frac{1}{2} \langle x \,|\, C_G \,|\, x \rangle$ for all $x \in \{0,1\}^n$.)

(2) Consider the 2×2 Hadamard matrix together with its three rotations—for fun, let's call them all the "Damhard" matrices:

$$H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}; \qquad H_2 = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}; \qquad H_3 = \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}; \qquad H_4 = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}.$$

Begin a quantum circuit C with 2 qubits by placing an Hadamard gate on line 1 followed by CNOT with control on 1 and target on line 2. As shown in lecture from ch. 7, on input e_{00} this creates an entangled pair of qubits—say the one on line 1 is owned by "Alice" while the second qubit is sent to "Bob." Now add to line 1 a "black box" in which Alice has placed one of the four Damhard matrices. Your task is to finish C with some gates so that by measuring both qubits, Bob can learn *exactly* which one Alice used. You must include analysis showing that fact. (30 pts. total)

Some possibly-helpful chitchat: This contrasts with the situation with the four matrices in Deutsch's original problem, where it is *not* possible to learn exactly which one was used—only whether its corresponding Boolean function f is "constant" or "balanced." This would be so even if we added a third qubit to the circuit that could be entangled with the others and kept by "Bob." There is an intuitive linear-algebraic reason reason: the four Deutsch matrices are not linearly independent when regarded as "unrolled" into vectors of length 4. This is because

$$U_I + U_X = U_T + U_F.$$

Thus if you have any vector u, the four vectors $v_1 = U_I u$, $v_2 = U_X u$, $v_3 = U_T u$, and $v_4 = U_F u$ resulting from them are linearly dependent. Hence the vectors w_1, w_2, w_3, w_4 you would get from later stages of the circuit are also linearly dependent. This means in particular that their nonzero entries must overlap in some indices, and any such overlap prevents 100% certainty that a single measurement will distinguish them.

However, the Damhard matrices *are* linearly independent. For a help in building the rest of C, try multiplying each of H_2, H_3, H_4 by H. Then relate the results to the four "Pauli matrices" which the text uses for its demonstration of "superdense coding" in section 8.3. The final helpful fact from lecture is that a scalar unit constant like -1 or i never changes any measurement, so you can disregard it.

(3) Lipton-Regan text, problem 8.4 in chapter 8. Be sure to explain how you got the simple inequalities—just "plonking them down" is not enough for full credit. (12 pts., for 66 regular-credit points besides the possible extra credit.)