**CSE610C, Fall 2021** **Problem Set 5 (Take-Home Final)** **Due Mon. Dec. 20**

**(1) (30 pts.)**

Consider the $2 \times 2$ Hadamard matrix together with its three rotated forms—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. 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.

For a footnote relating to lecture, it is *not* possible to learn exactly in the case of the four matrices in Deutsch's problem, even if we added a third qubit to the circuit that could be entangled with the others and kept by "Bob." The reason is that those four matrices are not linearly independent: $U_I + U_X = U_T + U_f$. 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. Try combining them with $H$ and/or the Pauli matrices, remembering also that multiplication by a scalar unit constant such as $-1$ or $i$ never changes any measurement, so you can disregard it.

**(2) (18 + 12 = 30 pts.)**

Define $|\mu\rangle = \frac{1}{2}[1, -1, -1, 1]^T$ and $A = \pi\,|\mu\rangle\,\langle\mu|$. The $\pi$ is not a typo—so $A$ is not a density matrix but it remains Hermitian. Find a $4 \times 4$ unitary matrix $U$ such that $U = e^{iA}$. (Possibly up to multiplying by a unit scalar, $U$ is a matrix seen in the course.) Verify your calculation by showing how if $U$ were given, one can obtain $A$.

Now for an exercise in the other direction, take $U = \frac{1}{2}\begin{bmatrix} -1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$. Find a Hermitian matrix $A$ such that $U = e^{iA}$. (Note that $U$ is not symmetric, so the procedure in section 18.1 will introduce complex entries even though $U$ has none. The latter matrix $U$ comes from the recent *Nature* paper Markiewicz et al. in E.R.'s presentation on interferometers, but this exercise is not directly connected to the paper. It is also "yucky" but only 12 pts.)

**(3) (9 + 6 + 9 + 6 = 30 pts.)**

Consider the 4-cycle graph $G$ with edges $(1, 2)$, $(2, 3)$, $(3, 4)$, and $(1, 4)$. Construct the corresponding graph state $|\Phi_G\rangle$ without the second bank of Hadamard gates. Call the nodes Alice, Bob, Charlie, and Donna in that order (Donna = 4).

(a) Construct the density matrix $\boldsymbol{\rho}_G$. Then show the result of tracing out nodes 3 and 4. Is the result a completely mixed state of two qubits? Is it pure?

(b) Now let Charlie and Donna each apply a single-qubit Hadamard gate locally and then post-select on 0. Show the calculations for the state Alice and Bob are left with, as well as verifying it on *Quirk*. Are Alice and Bob entangled?

(c) Now trace out nodes 2 and 4 instead. Are Alice and Charlie left with the completely mixed state in this case?

(d) Now instead of traciong out Donna and Bob, let them each apply a single-qubit Hadamard gate locally and then post-select on 0. Are Alice and Charlie left entangled? (This has some of the flavor of S.W.'s presentation.)

**(4) (12 + 18 = 30 pts.)**

Let $G$ be the five-node graph with edges $(u_1, u_2)$, $(u_2, u_3)$, $(u_2, u_4)$, $(u_3, u_4)$, $(u_3, u_5)$, and $(u_4, u_5)$. With the inputs and outputs of the corresponding graph-state circuit $C_G$ fixed to $0^5$, the polynomial $q$ in I.J.'s presentation becomes simply the sum of $u_i u_j$ over all edges $(u_i, u_j)$. Evaluating the polynomial on an argument $w \in \{0,1\}^n$ with arithmetic modulo 2 gives the same answer as counting the (parity of the) number of black-black edges in the coloring that corresponds to $w$ (with 0 for white, 1 for black).

(a) Show that $\langle 0^5 | C_G | 0^5 \rangle = 0$, i.e., the graph is "net-zero." (Going thru the colorings may be tedious, but less so IMHO than using matrices or a maze diagram with 32 rows. And see the next part.)

(b) Compute all the points $w$ where $\frac{\partial q}{\partial u_i}(w) = 0 \pmod{2}$ for each $i$. (They correspond to colorings in which each node has an even number of black neighbors, but IMHO it is easier to solve this one arithmetically.) Then verify that the amplitude summed only over those points is zero—as it should be under the theorem about the *least action principle* in the paper presented by I.J.

**(5) (24 + 6 = 30 pts.)**

Let Alice and Bob play the CHSH game portion of the Ekert 1991 QKD protocol, begun by Alice sending Bob half of the entangled state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Consider a play where Alice uses angle 0 to mean "yes" and Bob uses $\pi/8$ to mean "yes," so that they win if their answers agree. Suppose the eavesdropper Eve intercepts the qubit transmitted by Alice to Bob and measures it at angle $\pi/6$ first. Compute the win expectation for Alice and Bob in this case. For the last 6 pts., do the case where Bob uses $3\pi/8$ to mean "yes," so that now he and Alice win if their answers *disagree*, keeping Eve at $\pi/6$ which is almost midway between them. Does this change the expectation? (This makes 150 total points.)