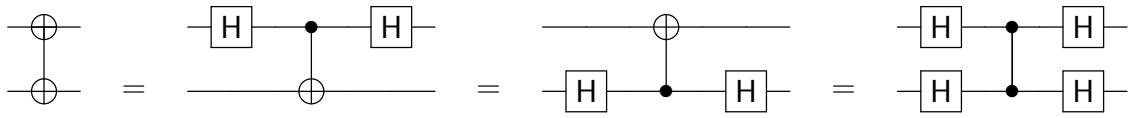
CSE439, Fall 2025 Problem Set 4 Due Sun. 10/26, 11:59pm

Reading: For next week, read Chapter 11 on Shor's Algorithm. This is tough sledding with formulas. Tuesday's lecture will be conceptual out of sections 11.1–11.3 and will follow notes at https://cse.buffalo.edu/~regan/cse439/CSE439Week9.pdf after summarixing Simon's Algorithm. Thursday's lecture will crunch down on sections 11.4–11.7.

———————*-Assignment 4, due Sun. 10/26 "midnight stretchy" on CSE Autolab*———————-

(1) Suppose we make a one-qubit circuit C completely out of the gates $\mathbf{H}, \mathbf{X}, \mathbf{Y}, \mathbf{Z}$, using an even number of Hadamard gates. Prove that this is equivalent to a circuit C' without any Hadamard gates at all. What's the maximum number of gates we need in C'? (Recall that multiplying a circuit or gate by a unit scalar is considered to be equivalent. 18 pts.)

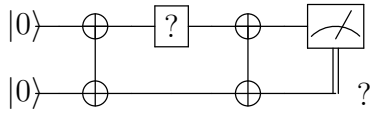
(2) Let us invent a symbol for the operation on Problem 3 of Prelim I and note one more equation for it (at far right):



Consider this to be a basic gate, which we may also call **E**. In fact, the *Quirk* simulator allows one to make this symbol using an **X** gate (which it displays as $\oplus$) and on a second qubit line, a smaller $\oplus$ from the "Toobox2" at lower left.

Now let G be any graph on some number n of vertices, undirected but with self-loops allowed. Let C_G stand for the corresponding graph-state circuit the way we have defined it: $\mathbf{H}^{\otimes n}$ at the left and right ends, and in between, a **CZ** gate for every edge of G and a **Z** gate for every self-loop (if any). Prove that C_G is equivalent to the circuit C'_G *without* the Hadamard transforms that just uses the new gate **E** for each edge and **X** for each self-loop. (*Hint:* Start with C'_G, where you just have gates for the edges and loops in the graph in whatever order, and use the rightmost above equation to substitute for **E**. For any **X** gates, use an equation you may notice in problem (1). Describe in words what you get. 18 pts.)

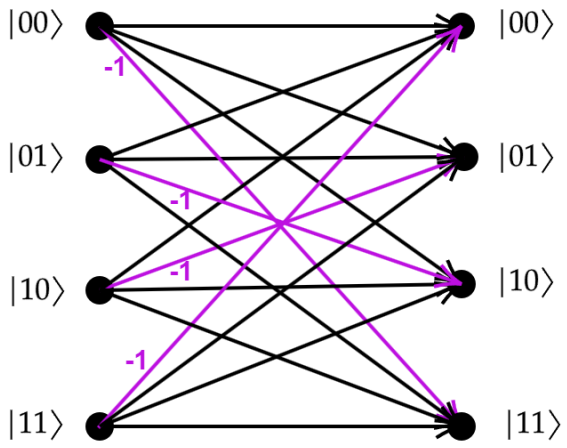
(3) Show that the mechanism of superdense coding works equally well for the following quantum circuit, again with "Alice" on qubit 1 and "Bob" on qubit 2:



To wit, Alice chooses one of the Pauli matrices $\mathbf{I}, \mathbf{X}, \mathbf{Y}, \mathbf{Z}$ to fill in between the **E** gates as defined in problem (2). She measures her qubit and sends the single classical bit result to Bob

(shown as double line). Bob is then able to tell which of the four operations Alice chose, e.g. by measuring his own qubit.

You may if you wish trace this via maze diagrams as was done for the original superdense coding circuit in lecture. For each **E** gate, you may use either of the mazes in the Prelim I problem (3) or its key, or you may use the following single-stage representation with four-way branching:



However, you can shortcut matters by applying facts you may notice from problems (1) and (2) above to the original analysis from the text section 8.3 and lecture. Either way, please also answer the following: Do you get the exact same correspondence between Bob's two bits and the $\mathbf{I}, \mathbf{X}, \mathbf{Y}, \mathbf{Z}$ choice by Alice as in the original? (18 pts.)

(4) 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:

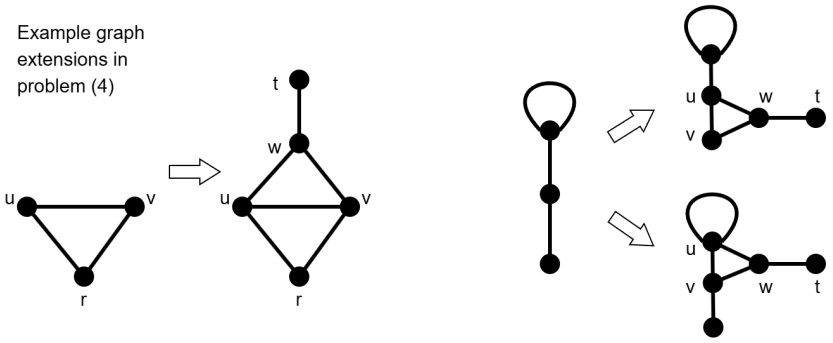
- binary strings z of length n, which correspond also to basis states $|z\rangle$;
- colorings of V, where vertex i is colored B means that bit $z_i = 1$; and
- "mice" in the "maze," since the initial $\mathbf{H}^{\otimes n}$ Hadamard transform puts one positive mouse on each row.

Thus 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:

- G is "net-zero"—meaning $\langle 0^n \,|\, C_G \,|\, 0^n \rangle = 0$—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.

- In general, 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 edge (u, v) of G. Let us connect a new node w by edges to u and v to make a triangle, and add a second new vertex t connected only to w. The resulting graph $G' = (V', E')$ has $V' = V \cup \{w, t\}$ and $E' = E \cup \{(u, w), (v, w), (t, w)\}$. Here are a few examples of this transformation:



Your task is to *prove* the following identity, for any n and graphs G and G' as above:

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

Conclude that G' is net-zero if and only if G is. (Hint: Consider separately the four possible combinations of colors for u and v in the original graph G. Show in each case how many colorings of the extra nodes w, t flip the parity of B-B edges. 24 pts., for 78 regular credit points on the set For up to 18 pts. extra credit, assuming nodes w, t 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 $x \in \{0, 1\}^n$ You are welcome to consult the answer key for last year's similar problem at https://cse.buffalo.edu/~regan/cse439/CSE439F24ps4key.pdf.)