

Reading: For next week, read Chapter 10 on Simon’s Algorithm and then read up through section 11.3 in the Shor’s Algorithm chapter. My lecture on Thu. 10/22 will also draw on the famous blog post “Shor, I’ll do it” by Scott Aaronson, so please read that as well. Note this is due on a **Monday**, not Friday, ten days from now on October 26 with the usual “midnight stretchy” grace period.

(1) Let C be the graph state circuit for the two-node graph with one edge, except that (for simplicity) we omit the second Hadamard gate on line 2. Let “Alice” control qubit line 1 and give it a general qubit $\mathbf{c} = [a, b]^T$ which she wishes to teleport to “Bob,” who starts with $|0\rangle$ on line 2. Alice then measures her qubit on the other side of C and sends the resulting bit e classically to Bob. Show that if Alice gets $e = 0$ then Bob’s qubit already holds the value $\mathbf{c}$, whereas if Alice gets $e = 1$ then Bob only has to apply $\mathbf{X}$ to his qubit. (If we included the second Hadamard gate on line 2, then Bob would have to apply $\mathbf{H}$ again to undo it, before applying $\mathbf{X}$ in the $e = 1$ case. For a footnote, this lacks one meaningful feature of the three-qubit teleportation circuit in chapter 8: There the connection between Alice and Bob using qubits 2 and 3 happens “before” Alice does anything with her qubit $\mathbf{c}$ on line 1. But it is still an often-used trick with graph states, worth 18 pts. here.)

(2) Consider a graph state circuit C on n qubits for a general n -vertex graph G . Let $\mathbf{a}_0$ denote the input vector—which we may consider to be any of the standard basis vectors $|x\rangle = \mathbf{e}_x$ for $x \in \{0, 1\}^n$, not just $|0^n\rangle$. Let $\mathbf{a}_1$ be the vector after the first Hadamard transform $\mathbf{H}^{\otimes n}$, which is given by the general formula

$$\mathbf{a}_1[u] = \frac{1}{\sqrt{N}} \sum_{t \in \{0,1\}^n} (-1)^{t \bullet u} \mathbf{a}_0[t],$$

where $N = 2^n$ and $u \in \{0, 1\}^n$. Note that if $\mathbf{a}_0 = |0^n\rangle$ then every entry is $+1$ divided by $\sqrt{N}$, so that $\mathbf{a}_1 = |+\rangle^n$, but for other inputs $\mathbf{a}_0$ it will have some negative entries. And $\mathbf{a}_0 = \mathbf{e}_x$ implies that every entry $\mathbf{a}_0[t]$ is 0 except for the case $t = x$.

Then let $\mathbf{a}_2$ be the state after the graph part. Since we strictly have only $\mathbf{CZ}$ and $\mathbf{Z}$ gates, there is no “crossover” of locations as we would get with $\mathbf{X}$ and $\mathbf{CNOT}$ gates, for instance. Thus values $\mathbf{a}_2[u]$ depend only on $\mathbf{a}_1[u]$ for all $u \in \{0, 1\}^n$. The dependence may only flip the $\pm$ sign. We can represent this as $(-1)^{g(u)}$ where the function g corresponds to the graph G . Thus we get

$$\mathbf{a}_2[u] = (-1)^{g(u)} \mathbf{a}_1[u].$$

Finally, for any index $z \in \{0, 1\}^n$, we compute the amplitude $\mathbf{a}_3[z]$ via a full Hadamard transform of $\mathbf{a}_2$, similar to how we got $\mathbf{a}_1$ from $\mathbf{a}_0$.

- (a) Give the amplitude value for $\mathbf{a}_3[z]$ when the input $\mathbf{e}_x$ is given to C , for any $x, z \in \{0, 1\}^n$. Your formula should incorporate the function $g(\cdot)$ without specifying it further, and may involve sums over other variables, but it should not have any “ $\mathbf{a}_i$ ” vector notation. This value can be denoted by $\langle z|C|x\rangle$ or by $\langle \mathbf{e}_z|C|\mathbf{e}_x\rangle$. (18 pts.)

- (b) Deduce from your formula that $\langle \mathbf{e}_x | C | \mathbf{e}_x \rangle = \langle 0^n | C | 0^n \rangle$ for all x . Thus for graphs like the triangle with $n = 3$ where $\langle 0^n | C | 0^n \rangle = 0$, we actually get $\langle x | C | x \rangle = 0$ for all x . (6 pts.)
- (c) Explain further why inserting one or more $\mathbf{Z}$ gates between the two $\mathbf{H}^{\otimes n}$ transforms has the same effect as changing the input x to another string w . In particular, if we let C' be the graph-state circuit obtained after inserting the $\mathbf{Z}$ gates and fix $x = 0^n$, then there is a string w such that for all possible outputs z , $\langle z | C | 0^n \rangle = \langle z | C' | w \rangle$. And that this equals $\langle (z \oplus w) | C | 0^n \rangle$, where $z \oplus w$ is bitwise XOR. Conclude that inserting $\mathbf{Z}$ gates never changes the number of nonzero terms in the final quantum state $\mathbf{a}_3$, only which possible outputs they denote. (*Hint*: use the identity $\mathbf{ZH} = \mathbf{HX}$, which follows from $\mathbf{HZH} = \mathbf{X}$. 18 pts. total, making 42 on the problem)

(3) Let $G = (V, E)$ be any graph with a self-loop at some node $u \in V$. In the corresponding graph-state circuit C_G , the self-loop is implemented by a standalone $\mathbf{Z}$ gate on the qubit corresponding to node u . (Since the $\mathbf{Z}$ and $\mathbf{CZ}$ operators are diagonal and hence all commute with each other, the order doesn't matter and we may suppose the $\mathbf{Z}$ comes first.) Now make a new graph G' by adding two new vertices v and w , adding three new edges (u, v) , (v, w) , and (w, u) to make a triangle, and finally removing the self-loop at u . In the corresponding circuit C' , the $\mathbf{Z}$ gate on line u is removed and replaced by three $\mathbf{CZ}$ gates involving line u and the two new lines for v and w . Prove that

$$\langle 0^{n+2} | C' | 0^{n+2} \rangle = \frac{1}{2} \langle 0^n | C | 0^n \rangle.$$

(Hint: Consider separately the cases when u is colored white (W) and when it is black (B). Show in each case how many colorings of the extra nodes v, w flip the parity of B-B edges, meaning the count of edges with both nodes colored black and whether it is even or odd. 24 pts., for 84 on the set.)