In class, we analyzed the number $q(n)$ of gates needed to construct the n-qbit quantum Fourier transform gate $T^{(n)}$. We developed a recurrence relation for $q(n)$ with initial condition $q(1) = 1$. We quickly concluded that $q(n)$ is $\mathcal{O}(n^2)$, and then I told you what $q(n)$ was exactly.

Unfortunately, my analysis included the SWAP gates used in $S^{(n)}$ but omitted the SWAP gates used in $Q^{(n)}$. We should be consistent. So let's fix that now.

A. In each part of this problem, figure out the recurrence relation for $q(n)$ exactly, and state the asymptotics of $q(n)$ using big-$\mathcal{O}$ notation. You are not expected to compute what $q(n)$ is exactly.

1. What if we don't count any SWAPs anywhere? What is the recurrence relation, and what is the resulting $\mathcal{O}$ complexity?
2. Let's count all of the SWAPs. The ones in $Q^{(n)}$ arise from controlled one-qbit gates, where the control qbit is not always next to the data qbit. If there are k qbits inserted between the control qbit and the data qbit, then we can implement this controlled gate using $2k$ SWAPs (plus the two-qbit cU gate itself). If we follow this strategy, then what is the recurrence relation, and what is the resulting complexity? This fact from algebra might help:
$$\sum_{j=0}^{q} j = \frac{q(q+1)}{2}.$$
3. The previous answer was overly pessimistic, in that it used more SWAPs than necessary. Draw circuits for $n = 2, 3, \ldots$, simplifying the SWAPs in each one, until you see the pattern of how many SWAPs are actually needed. Then tell me the recurrence relation and the resulting complexity.

(This is a fairly long problem. The first part is short, while the other two parts are medium-length.)

Let U be the five-qbit circuit, that we used to implement the four-qbit cccZ operation. We checked that this gate works correctly for a few classical input states. We did not check all of the cases. Nor did we prove my most important assertion, that the ancillary qbit remains unentangled from the other qbits (so that we can legitimately talk about the state of those other qbits).

B. Assume that U works correctly on all 32 classical states. That is,

$$U \cdot (|\gamma\rangle \otimes |\alpha_2\alpha_1\alpha_0\rangle \otimes |\beta\rangle) = |\gamma\rangle \otimes |\alpha_2\alpha_1\alpha_0\rangle \otimes Z^{\alpha_2 \odot \alpha_1 \odot \alpha_0} |\beta\rangle .$$

Prove the unentanglement claim — that is, for any one-qbit state $|\chi\rangle$ and four-qbit state $|\psi\rangle$, the first qbit is unentangled from the other four qbits in the output state $U \cdot (|\chi\rangle \otimes |\psi\rangle)$. (This is a medium-length problem.)

C. (This problem is optional. Do not hand it in.) Check that U works correctly on all 32 classical cases. (There is some educational value in mindlessly checking the cases. There is more educational value in figuring out how to save yourself some work by combining cases.)

D. (This problem is optional. Do not hand it in.) Write out the seven-qbit multiply-controlled-Z gate, following the pattern established in class.