Activity Lecture 4

1. Notation Recall that a control Z gate is a 2 qubit gate that sends $|1\rangle|1\rangle$ to $-|1\rangle|1\rangle$ and acts as identity on all other basis vectors. A control Z gate is sometimes written as in Fig. 1. Is this a reasonable notation? Why or why not?

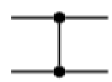


Figure 1: Circuit diagram for Control Z gate

2. Flipping control and target In lecture 2 we constructed a circuit as in Fig. 2 for the Fourier transform over $\mathbb{Z}_{16}$. In this figure we are using the notation shown in Fig. 3.

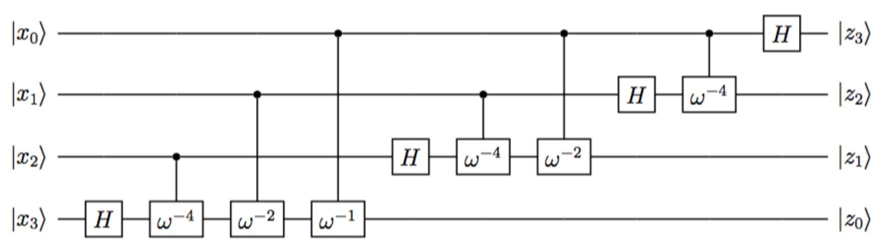
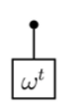


Figure 2: Circuit for the FT over $\mathbb{Z}_{16}$



$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \omega^t \end{bmatrix}$$

Figure 3: Controlled phase gate

Argue that the Fourier transform circuit can equivalently written as in Fig. 4.

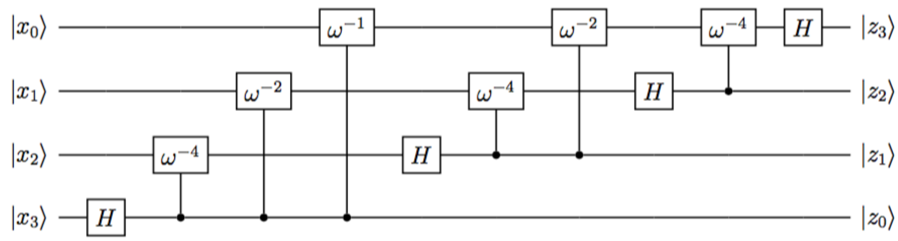


Figure 4: Alternative representation of the circuit for the FT over $\mathbb{Z}_{16}$

3. Measuring right after In the representation of Fig. 4, notice that after a Hadamard is applied to it each qubit only acts as a control qubit. Now suppose that, as in Shor's algorithm, we immediately measure the output of the Fourier transform. Show that you obtain equivalent measurement results if you measure each qubit after its Hadamard, and use the outcome to control the phase gates as in Fig. 5.

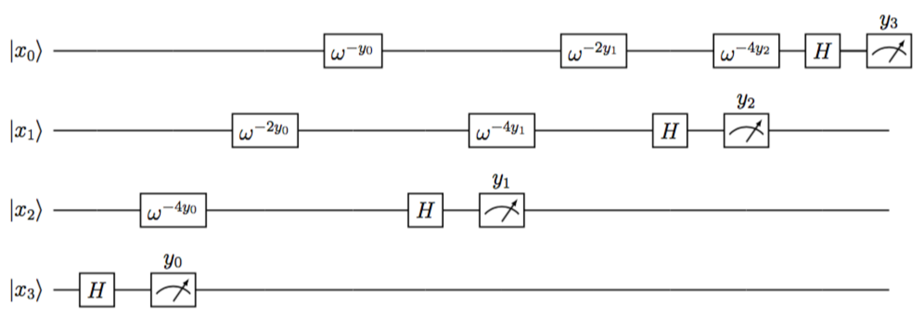


Figure 5: Semi-classical Fourier transform

4. Application What implications might this have for implementing Shor's algorithm?

5. Crossing lines What is going on in the representation of the semi-classical Fourier transform in Fig. 6?

5. References This "semi-classical" version of the Fourier transform is from the paper Semi-classical Fourier Transform for Quantum Computation by Griffiths and Niu. It is discussed in the textbook *Quantum Computer Science: An Introduction* by Mermin, from which Fig. 6 is taken. I adapted this exercise from Ryan O'Donnell's course, weekly work 8.

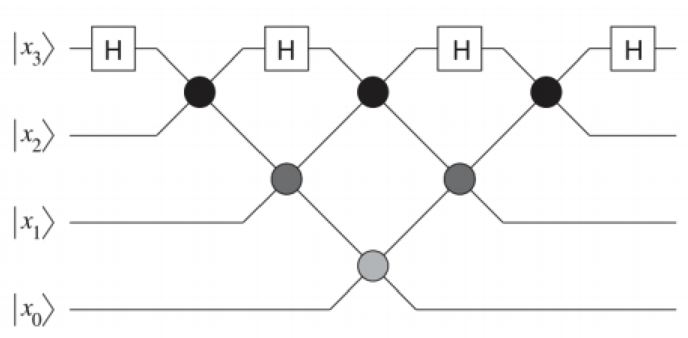


Figure 6: Artistic representation of the semi-classical Fourier transform