Ph/CS 219a, Fall 2022
Quantum Computation
Prof. Alexei Kitaev

Problem set #7
Due Friday, December 2, 2022

1. Phase gates and Fourier ancillas. [10 points] In class, we discussed realization of unitary operators using these gates:

$$\text{Standard gate set:} \quad H,\ \Lambda(e^{\pm i\pi/4}),\ \mathrm{CNOT}\,. \tag{1}$$

Recall that the Toffoli gate $\Lambda^2(\sigma^x)$ has a simple exact realization, which enables classical reversible computation on superpositions of basis vectors. On the other hand, the operator $\Lambda(e^{i\varphi})$ for an arbitrary φ can only be implemented approximately and in a rather complex way (using the Solovay-Kitaev algorithm). This problem is concerned with an alternative realization and some applications of the "universal phase gate"

$$U = \Lambda(e^{2\pi i/2}) \otimes \cdots \otimes \Lambda(e^{2\pi i/2^n}), \qquad U|x\rangle = e^{2\pi i x/2^n}|x\rangle \ \text{ for } x = 0, \ldots, 2^n - 1, \tag{2}$$

where n is fixed. The idea is to first create an auxiliary Fourier state $|\psi_1\rangle$ (see below). While its construction is rather expensive, $|\psi_1\rangle$ can be used multiple times to implement U at low marginal cost.

Let $q = 2^n$ and let $\mathcal{L} = (\mathbb{C}^2)^{\otimes n}$ be the Hilbert space on n qubits. The *Fourier basis* of $\mathcal{L}$ is defined as follows:

$$|\psi_k\rangle = \frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} e^{2\pi i k x/q} |x\rangle, \qquad \text{for} \quad k = 0, \ldots, q-1. \tag{3}$$

It is clear that $|\psi_0\rangle = H^{\otimes n}|0^n\rangle$ and that $|\psi_1\rangle = U|\psi_0\rangle$. More interestingly,

$$U|x\rangle \otimes |\psi_1\rangle = W\big(|x\rangle \otimes |\psi_1\rangle\big), \tag{4}$$

where the operator

$$W:\ |x, y\rangle \mapsto |x,\, y - x \bmod 2^n\rangle \tag{5}$$

is easy to implement. Thus, if the state $|\psi_1\rangle$ has already been prepared, we can realize U and still have $|\psi_1\rangle$.

Questions:

a) Explain (in a couple of sentences) how to implement the operator W by an $O(n)$ size circuit using σ^x, $\Lambda(\sigma^x)$, and $\Lambda^2(\sigma^x)$.

b) Implement the following operator V using $O(n^2)$ such gates and a single instance of U:

$$V|x, y\rangle = e^{2\pi i\, xy/2^n}|x, y\rangle \qquad \text{for} \quad x, y = 0, \ldots, 2^n - 1. \tag{6}$$

c) Using W, copy an arbitrary n-qubit state $|\psi\rangle$ relative to the Fourier basis.

d) Find $M_a|\psi_k\rangle$, where M_a is defined as follows:

$$M_a : |x\rangle \mapsto |ax \bmod 2^n\rangle, \qquad a \in (\mathbb{Z}/2^n\mathbb{Z})^* = \{1, 3, \dots, 2^n - 1\}. \tag{7}$$

e) Construct the Fourier ancilla $|\psi_1\rangle$ from scratch. **Hint:** Begin with the state

$$|\eta\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle - |2^{n-1}\rangle\Big) = 2^{-(n-1)/2} \sum_{k \in (\mathbb{Z}/2^n\mathbb{Z})^*} |\psi_k\rangle. \tag{8}$$

Use the phase estimation procedure for the shift operator $|y\rangle \mapsto |y+1 \bmod 2^n\rangle$ to produce $|\psi_k\rangle$ with a random $k \in (\mathbb{Z}/2^n\mathbb{Z})^*$. Then turn $|\psi_k\rangle$ to $|\psi_1\rangle$. (Using the technique of problem 1 from the previous homework, this procedure can be done without leaving any garbage. You don't have to worry about garbage though.)

2. Shifted Legendre symbol. [10 points] Let $p > 2$ be a prime number. The Legendre symbol modulo p is defined for all elements $x \in \mathbb{Z}_p^* = \{1, \dots, p-1\}$.

$$\left(\frac{x}{p}\right) = \begin{cases} +1, & \text{if } x = y^2 \text{ for some } y \in \mathbb{Z}_p^*, \quad \text{i.e., if } x^{\frac{p-1}{2}} \equiv 1 \pmod{p}; \\ -1, & \text{otherwise,} \qquad\qquad\qquad\qquad\quad \text{i.e., if } x^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \end{cases} \tag{9}$$

Suppose that we have access to an oracle U such that $U|x\rangle = \left(\frac{x+\omega}{p}\right)|x\rangle$ for some unknown value of $\omega \in \mathbb{Z}_p$. Find a polynomial (i.e., $(\log p)^{O(1)}$) quantum algorithm to determine ω. (Note that $\left(\frac{0}{p}\right)$ is undefined, or we may rather set it to 0. If the oracle is called with $x = -\omega$, it signals an error, and we can learn ω immediately by measuring x.) **Hint:** Create the uniform superposition of $|x\rangle$, apply the oracle followed by the $\mathbb{Z}_p$ Fourier transform, and figure how to proceed. A key observation is that the Fourier transform of the Legendre symbol is the Legendre symbol itself (with minor modifications). This follows from the Gauss sum formula:

$$\sum_{k=0}^{p-1} \exp\left(2\pi i \frac{yk^2}{p}\right) = \sqrt{p}\, i^{\frac{(p-1)^2}{4}} \left(\frac{y}{p}\right) \qquad \text{for } y \in \mathbb{Z}_p^*. \tag{10}$$