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

Problem set #6
Due Thursday, November 17, 2022

1. Accuracy of quantum subroutines. [15 points] It was stated in class that the accuracy of state vectors, probability distributions, unitary gates, and density matrices is characterized by the Euclidean norm, ℓ_1 norm, operator norm, and trace norm, respectively:

$$\begin{aligned} \big\||\xi\rangle\big\| &= \sqrt{\langle\xi|\xi\rangle}, & \|w\|_1 &= \sum_a |w_a|, \\ \|X\| &= \sup_{|\xi\rangle\neq 0} \frac{\big\|X|\xi\rangle\big\|}{\big\||\xi\rangle\big\|} = \max_j \lambda_j, & \|X\|_1 &= \sum_j \lambda_j. \end{aligned} \tag{1}$$

(Here, $\lambda_j \geq 0$ are the singular values of the operator X, i.e. λ_j^2 are the eigenvalues of $X^\dagger X$.) In all cases, one should consider the norm of the difference between the actual state vector (probability distribution, unitary operator, or density matrix) and the ideal one. These norms fit together nicely. For example, $\big\||\tilde\psi\rangle\langle\tilde\psi| - |\psi\rangle\langle\psi|\big\|_1 \leq 2\big\||\tilde\psi\rangle - |\psi\rangle\big\|$. Now, suppose that the same measurement $(\Pi_1, \ldots, \Pi_l)$ is applied to density matrices ρ and $\tilde\rho$ such that $\|\tilde\rho - \rho\|_1 \leq 2\varepsilon$. Then the probability distributions of the measurement outcomes, $w_a = \operatorname{Tr}\Pi_a\rho$ and $\tilde w_a = \operatorname{Tr}\Pi_a\tilde\rho$, satisfy the condition $\|\tilde w - w\|_1 \leq 2\varepsilon$. As a consequence, the overall error probability of a quantum computation is bounded by the sum of the errors in each individual step (up to a factor of 2).

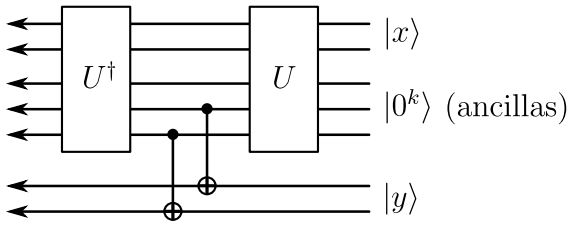
However, for particular types of quantum algorithms more special techniques give tighter error bounds. This problem is concerned with errors in quantum subroutines that are similar to reversible classical computation: we compute $f(x)$ for a given x, copy the result, and run the computation backward to remove any intermediate data. The difference is that the computation is quantum, and thus, may give an incorrect result with some probability. Furthermore, we intend to apply the whole procedure to an arbitrary superposition of basis states $|x\rangle$.

Let $f : \{0,1\}^n \to \{0,1\}^m$ and let us consider the unitary operator $W = \widehat{f_\oplus}$ acting on $n+m$ qubits:

$$\widehat{f_\oplus} : \ |x, y\rangle \mapsto |x, y \oplus f(x)\rangle, \tag{2}$$

An approximate realization $\tilde W$ of $\widehat{f_\oplus}$ uses k ancillas and is organized as follows. We apply some unitary U to the input state $|x, 0^k\rangle$ (or a superposition of such states), add each of the last m bits to the corresponding bit of y (modulo 2), and apply $U^{-1} = U^\dagger$:

$$\begin{aligned} &\tilde W = \sum_a P_a \otimes R_a, \quad \text{where} \\ &P_a = U^\dagger\big(I \otimes |a\rangle\langle a|\big)U, \\ &R_a \ : |y\rangle \mapsto |y \oplus a\rangle. \end{aligned} \tag{3}$$



If we were not interested in working with superpositions, we could use just use U once and measure the last m bits. Suppose that the error probability of this simpler procedure is small:

$$\forall x \sum_{a \neq f(x)} p(a|x) \leq \varepsilon, \qquad \text{where} \quad p(a|x) = \langle x, 0^k | P_a | x, 0^k \rangle. \tag{4}$$

Our goal is to estimate how well the operator $\tilde{W}$ approximates $\widehat{f_\oplus}$. Specifically, we want to obtain an upper bound for the norm of the "error operator"

$$E = \tilde{W} V - V \widehat{f_\oplus}, \tag{5}$$

where V augments the input qubits with ancillas: $V|x, y\rangle = |x, 0^k, y\rangle$.

Questions:

a) Show that for each x and y, the corresponding error is bounded as follows: $\big\|E|x, y\rangle\big\| \leq \sqrt{2\varepsilon}$. Using this result, prove that $\|E\| \leq 2^{(n+m)/2}\sqrt{2\varepsilon}$. **Hint:** It is clear that

$$E|x, y\rangle = |\tilde{\psi}_{x,y}\rangle - |\psi_{x,y}\rangle, \quad \text{where} \quad |\psi_{x,y}\rangle = |x, 0^k, y \oplus f(x)\rangle, \quad |\tilde{\psi}_{x,y}\rangle = \tilde{W}|x, 0^k, y\rangle. \tag{6}$$

Use the fact that if $|\psi\rangle$ and $|\tilde{\psi}\rangle$ are unit vectors, then $\big\||\tilde{\psi}\rangle - |\psi\rangle\big\|^2 = 2 - 2\,\mathrm{Re}\langle\psi|\tilde{\psi}\rangle$.

b) Show that

$$\big\|E\big(|x\rangle \otimes |\xi\rangle\big)\big\| \leq \sqrt{4\varepsilon}\,\big\||\xi\rangle\big\| \tag{7}$$

for any vector $|\xi\rangle$ and prove this bound: $\|E\| \leq 2^{n/2}\sqrt{4\varepsilon}$. **Hint:** Write $E\big(|x\rangle \otimes |\xi\rangle\big)$ as $|\tilde{\psi}_{x,\xi}\rangle - |\psi_{x,\xi}\rangle$ and try to express $\langle\psi_{x,\xi}|\tilde{\psi}_{x,\xi}\rangle$ in terms of $1 - R_{a\oplus f(x)}$.

c) The factor $2^{n/2}$ is not so easy to dispense with because the errors from different values of x may interfere constructively. Modify the circuit (3) so as to exclude any such interference. The new implementation should satisfy the inequality $\|E\| \leq O\left(\sqrt{\epsilon}\right)$.

2. [10 points] Consider a generalized version of the Grover oracle:

$$U_\xi = I_n - 2|\xi\rangle\langle\xi|, \tag{8}$$

where I_n is the identity operator on n qubits, and $|\xi\rangle$ is an absolutely arbitrary quantum state. We will not attempt to find $|\xi\rangle$, but rather, to distinguish U_ξ from I_n. The standard Grover algorithm will work in most but not all cases: think what happens when $|\xi\rangle = |+\rangle = 2^{-n/2}\sum_x |x\rangle$. To remedy the situation, let us replace $|+\rangle$ with a maximally entangled state of $2n$ qubits:

$$|\Psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x, x\rangle, \qquad \text{where} \quad N = 2^n. \tag{9}$$

The oracle will be applied to the first n qubits.

a) Implement the operators

$$Q = \big(I_{2n} - |\Psi\rangle\langle\Psi|\big) \otimes I_1 + |\Psi\rangle\langle\Psi| \otimes \sigma^x, \qquad V = I_{2n} - 2|\Psi\rangle\langle\Psi|. \tag{10}$$

b) Construct a circuit that uses $O\big(\sqrt{N}\big)$ instances of an unknown operator U and outputs 0 if $U = I_n$ and 1 if $U = U_\xi$ for some $|\xi\rangle$. (Note that the circuit should not depend on $|\xi\rangle$ because it's not known.) A small error probability, vanishing in the limit of large N, is acceptable. **Hint:** A properly designed algorithm should be easy to analyze because the quantum state will remain in the linear span of $|\Psi\rangle$ and $\big(|\xi\rangle\langle\xi| \otimes I_n\big)|\Psi\rangle$ at all times. Please be careful about the final measurement: it is not as straightforward as for the usual Grover search.