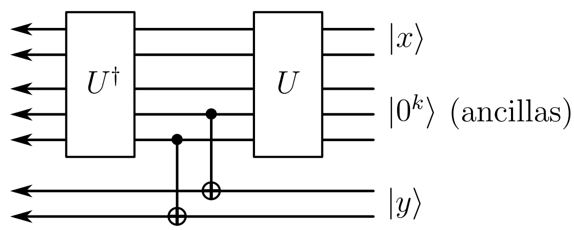
**Solutions to problem set #6**

**1. Accuracy of quantum subroutines.** [15 points] *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:*

$$\widehat{f_\oplus} : \ |x,y\rangle \mapsto |x, y \oplus f(x)\rangle, \tag{1}$$

*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 $U^{-1} = U^\dagger$:*

$$\tilde{W} = \sum_a P_a \otimes R_a, \quad \textit{where}$$
$$P_a = U^\dagger\big(I \otimes |a\rangle\langle a|\big)U,$$
$$R_a \ : |y\rangle \mapsto |y \oplus a\rangle.$$




(2)

*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:*

$$\forall x \sum_{a \neq f(x)} p(a|x) \leq \varepsilon, \qquad \textit{where} \quad p(a|x) = \langle x, 0^k | P_a | x, 0^k \rangle. \tag{3}$$

*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"*

$$E = \tilde{W}V - V\widehat{f_\oplus}, \tag{4}$$

*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*

$$E|x,y\rangle = |\tilde{\psi}_{x,y}\rangle - |\psi_{x,y}\rangle, \quad \textit{where} \quad |\psi_{x,y}\rangle = |x, 0^k, y \oplus f(x)\rangle, \quad |\tilde{\psi}_{x,y}\rangle = \tilde{W}|x, 0^k, y\rangle. \tag{5}$$

*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*

$$\big\|E\big(|x\rangle \otimes |\xi\rangle\big)\big\| \leq \sqrt{4\varepsilon}\,\big\||\xi\rangle\big\| \tag{6}$$

*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 (2) so as to exclude any such interference. The new implementation should satisfy the inequality $\|E\| \leq O\left(\sqrt{\epsilon}\right)$.*

**Answers:**

a) Following the hint, we calculate the inner product between the vectors $|\psi_{x,y}\rangle$ and $|\tilde{\psi}_{x,y}\rangle$ defined by Eq. (5). In this calculation, we use the fact that $\tilde{W} = \sum_a P_a \otimes R_a$ (see Eq. (2)).

$$\begin{aligned}\langle\psi_{x,y}|\tilde{\psi}_{x,y}\rangle &= \left\langle x, 0^k, y\oplus f(x)\middle|\tilde{W}\middle|x, 0^k, y\right\rangle = \sum_a \underbrace{\langle x, 0^k|P_a|x, 0^k\rangle}_{p(a|x)}\underbrace{\langle y\oplus f(x)|R_a|y\rangle}_{\delta_{a,f(x)}} \\ &= p(f(x)|x) \geq 1-\varepsilon.\end{aligned} \tag{7}$$

Hence,

$$\big\|E|x,y\rangle\big\| = \big\||\tilde{\psi}_{x,y}\rangle - |\psi_{x,y}\rangle\big\| = \sqrt{2 - 2\,\mathrm{Re}\langle\psi_{x,y}|\tilde{\psi}_{x,y}\rangle} \leq \sqrt{2\varepsilon}. \tag{8}$$

Let us now apply the operator $E$ to an arbitrary superposition of basis states, $|\psi\rangle = \sum_{x,y} c_{x,y}|x,y\rangle$:

$$E|\psi\rangle = \sum_{x,y} c_{x,y}\big(|\tilde{\psi}_{x,y}\rangle - |\psi_{x,y}\rangle\big), \tag{9}$$

$$\big\|E|\psi\rangle\big\| \leq \sum_{x,y} |c_{x,y}|\,\big\||\tilde{\psi}_{x,y}\rangle - |\psi_{x,y}\rangle\big\| \leq \left(\sum_{x,y}|c_{x,y}|\right)\sqrt{2\epsilon}. \tag{10}$$

Recall $x$ and $y$ have $N = 2^n$ and $M = 2^m$ possible values, respectively. If all the terms in the last sum are equal, $c_{x,y} = (NM)^{-1/2}$, then they add up to $\sqrt{NM}$. This is, actually, an upper bound, which follows from the Cauchy-Schwarz inequality:

$$\left(\sum_{x,y}|c_{x,y}|\right)^2 \leq \left(\sum_{x,y}|c_{x,y}|^2\right)\left(\sum_{x,y}1\right) = 1\cdot NM = 2^{n+m}. \tag{11}$$

Thus, $\big\|E|\psi\rangle\big\| \leq 2^{(n+m)/2}\sqrt{2\epsilon}$ for all unit vectors $|\psi\rangle$, and hence $\|E\| \leq 2^{(n+m)/2}\sqrt{2\epsilon}$.

b) The solution to this part is a simple modification of the previous argument.[1] We first calculate the inner product between the vectors $|\psi_{x,\xi}\rangle = \widehat{f_\oplus}\big(|x,0^k\rangle\otimes|\xi\rangle\big)$ and $|\tilde{\psi}_{x,\xi}\rangle = \tilde{W}\big(|x,0^k\rangle\otimes|\xi\rangle\big)$:

$$\begin{aligned}\langle\psi_{x,\xi}|\tilde{\psi}_{x,\xi}\rangle &= \big(\langle x,0^k|\otimes\langle\xi|\big)\widehat{f_\oplus}\,\tilde{W}\big(|x,0^k\rangle\otimes|\xi\rangle\big) = \sum_a \langle x,0^k|P_a|x,0^k\rangle\,\langle\xi|R_{f(x)}R_a|\xi\rangle \\ &= \sum_a p(a|x)\langle\xi|R_{a\oplus f(x)}|\xi\rangle = p(f(x)|x)\langle\xi|\xi\rangle + \sum_{a\neq f(x)} p(a|x)\langle\xi|R_{a\oplus f(x)}|\xi\rangle \\ &= \langle\xi|\xi\rangle - \sum_{a\neq f(x)} p(a|x)\,\langle\xi|(I - R_{a\oplus f(x)})|\xi\rangle \geq (1-2\varepsilon)\langle\xi|\xi\rangle,\end{aligned} \tag{12}$$

[1] It doesn't look so simple if you start from scratch. When I first used quantum subroutines in some algorithms, I struggled to get rid of the exponential factor and had to compensate it by probability amplification. I tried to make the problem easier for you by structuring it and defining the operators $P_a$, $R_a$, and $E$. I hope that helped. -A.K.

where we have used the fact that $I - R_{a\oplus f(x)}$ is a Hermitian operator with norm less than or equal to 2. Since both $|\psi_{x,\xi}\rangle$ and $|\tilde{\psi}_{x,\xi}\rangle$ have the same norm as $|\xi\rangle$,

$$\big\||\tilde{\psi}_{x,\xi}\rangle - |\psi_{x,\xi}\rangle\big\| = \sqrt{2\langle\xi|\xi\rangle - 2\,\mathrm{Re}\langle\psi_{x,\xi}|\tilde{\psi}_{x,\xi}\rangle} \le \sqrt{(2-2(1-2\varepsilon))\langle\xi|\xi\rangle} = \sqrt{4\varepsilon}\,\big\||\xi\rangle\big\|. \quad (13)$$

Now, let us represent an arbitrary initial state $|\psi\rangle$ as $\sum_x |x\rangle \otimes |\xi_x\rangle$ and slightly change our previous notation: $|\psi_x\rangle = \widehat{f_\oplus}\big(|x,0^k\rangle \otimes |\xi_x\rangle\big)$, $|\tilde{\psi}_x\rangle = \tilde{W}\big(|x,0^k\rangle \otimes |\xi_x\rangle\big)$. We have the bound $\big\||\tilde{\psi}_x\rangle - |\psi_x\rangle\big\| \le \sqrt{4\varepsilon}\,\big\||\xi\rangle_x\big\|$, therefore the error in the final state can be estimated as follows:

$$E|\psi\rangle = \sum_x \big(|\tilde{\psi}_x\rangle - |\psi_x\rangle\big), \quad (14)$$

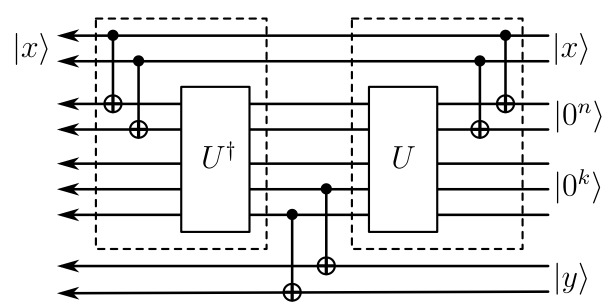
$$\big\|E|\psi\rangle\big\| \le \sum_x \big\||\tilde{\psi}_x\rangle - |\psi_x\rangle\big\| \le \sqrt{4\epsilon}\sum_x \big\||\xi_x\rangle\big\|. \quad (15)$$

But $\big(\sum_x \big\||\xi_x\rangle\big\|\big)^2 \le N \sum_x \big\||\xi_x\rangle\big\|^2 = 2^n$ by Cauchy-Schwarz, hence $\big\|E|\psi\rangle\big\| \le 2^{n/2}\sqrt{4\varepsilon}$.

c) The last upper bound can be improved if the errors for different values of $x$ are mutually orthogonal. Indeed, in this case,

$$\big\|E|\psi\rangle\big\|^2 = \sum_x \big\||\tilde{\psi}_x\rangle - |\psi_x\rangle\big\|^2 \le 4\epsilon \sum_x \big\||\xi_x\rangle\big\|^2 = 4\epsilon. \quad (16)$$

The orthogonality condition holds in many concrete examples due to a special form of the operator $U$. To satisfy it without making any assumptions, we keep an extra copy of $x$ that is not changed by $U$:




(17)

The modified versions of $U$ and $U^\dagger$ are shown by dotted boxes.

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

$$U_\xi = I_n - 2|\xi\rangle\langle\xi|, \quad (18)$$

*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 $U_\xi$ 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:*

$$|\Psi\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x,x\rangle, \qquad \textit{where} \quad N = 2^n. \quad (19)$$

*The oracle will be applied to the first $n$ qubits.*

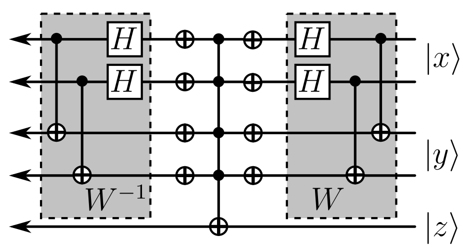
*a) Implement the operators*

$$Q = \big(I_{2n} - |\Psi\rangle\langle\Psi|\big) \otimes I_1 + |\Psi\rangle\langle\Psi| \otimes \sigma^x, \qquad\qquad V = I_{2n} - 2|\Psi\rangle\langle\Psi|. \tag{20}$$

*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.*

a) The operator $Q$ flips the last qubit if and only if the first $2n$ qubits contain $|\Psi\rangle$. To implement this, we first apply some unitary $W$ such that $W|\Psi\rangle = |0^{2n}\rangle$, check for the presence of $2n$ zeros, and apply $W^{-1}$. The operator $W$ can be realized as the bitwise CNOT: $|x, y\rangle \mapsto |x, y \oplus x\rangle$ followed by the Hadamard gates applied to qubits $1, \ldots, n$. This is the complete circuit:

$Q =$




(21)

To implement $V$, we use the $|-\rangle$ ancilla in place of $|z\rangle$.

b) Like in the usual Grover search, we begin with $|\Psi\rangle$ and apply the operator $R = -V(U \otimes I_n)$ a certain number of times. If $U = I_n$, the initial state will not change. If $U = I_n - 2|\xi\rangle\langle\xi|$, the state will evolve, and we need to understand how. Since both $U$ and $V$ preserve the linear span of $|\Psi\rangle$ and $\big(|\xi\rangle\langle\xi| \otimes I_n\big)|\Psi\rangle$, the problem is two-dimensional. If $|\xi\rangle = \sum_x c_x |x\rangle$, then

$$\big(|\xi\rangle\langle\xi| \otimes I_n\big)|\Psi\rangle = \left(\sum_{x,x'} c_x c_{x'}^* |x\rangle\langle x'| \otimes I_n\right)\left(\frac{1}{\sqrt{N}}\sum_y |y, y\rangle\right) = \frac{1}{\sqrt{N}}|\eta\rangle, \tag{22}$$

$$\text{where} \quad |\eta\rangle = \sum_{x,x'} c_x c_{x'}^* |x, x'\rangle = |\xi\rangle \otimes |\bar{\xi}\rangle, \qquad |\bar{\xi}\rangle = \sum_x c_x^* |x\rangle. \tag{23}$$

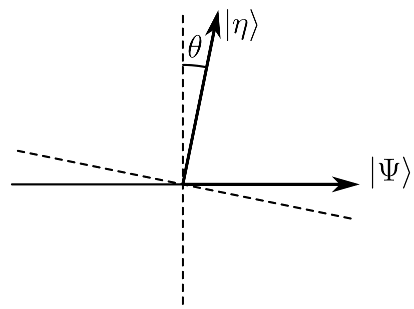
Note that the vector $|\eta\rangle$ has unit norm. The purpose of doubling the number of qubits in the algorithm was to make the angle between $|\Phi\rangle$ and $|\eta\rangle$ independent of the unknown vector $|\xi\rangle$. Let us write this angle as $\frac{\pi}{2} - \theta$ and find $\theta$:

$$\sin\theta = \cos\left(\frac{\pi}{2} - \theta\right) = \langle\Psi|\eta\rangle = \frac{1}{\sqrt{N}}\sum_x c_x c_x^* = \frac{1}{\sqrt{N}}. \tag{24}$$

The analysis of the algorithm is analogous to that of Grover's with multiple solutions. Let us repeat it for completeness. We first show that the operator $|\xi\rangle\langle\xi| \otimes I_n$ acts in the two-dimensional subspace exactly as $|\eta\rangle\langle\eta|$:

$$\begin{aligned} \big(|\xi\rangle\langle\xi| \otimes I_n\big)|\Psi\rangle &= \frac{1}{\sqrt{N}}|\eta\rangle = \big(|\eta\rangle\langle\eta|\big)|\Psi\rangle, \\ \big(|\xi\rangle\langle\xi| \otimes I_n\big)|\eta\rangle &= \big(|\xi\rangle\langle\xi| \otimes I_n\big)\Big(\sqrt{N}\big(|\xi\rangle\langle\xi| \otimes I_n\big)|\Psi\rangle\Big) = |\eta\rangle = \big(|\eta\rangle\langle\eta|\big)|\eta\rangle. \end{aligned} \tag{25}$$

Thus, we may replace the operator $U \otimes I_n$ with $I - 2|\eta\rangle\langle\eta|$. The latter is the reflection about the line that is perpendicular to vector $|\eta\rangle$. Similarly, $-V = -I + 2|\Psi\rangle\langle\Psi|$ is the reflection about $|\Psi\rangle$.

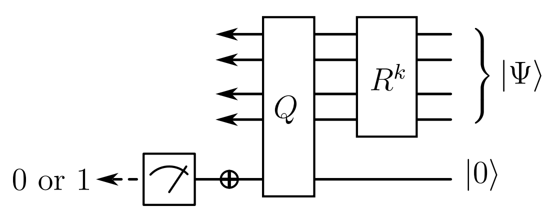



(26)

The operator $R \equiv -V\big(I - 2|\eta\rangle\langle\eta|\big)$ rotates counterclockwise by angle $2\theta$. After

$$k \approx \frac{\pi}{4\theta} \leq O\big(\sqrt{N}\big) \tag{27}$$

iterations, the state will become (almost) orthogonal to $|\Psi\rangle$, and we can do the final measurement. Instead of checking that we have found a solution, we check the orthogonality to $|\Psi\rangle$ using the previously implemented operator $Q$:




(28)