2.111J/18.435J Quantum Computation Problem Set 4 Solutions
(Due: Tuesday, October 18, 2005)

1) In class we often have written down ket-bra objects $|\psi\rangle\langle\psi|$, where $|\psi\rangle$ is some arbitrary normalized state in some Hilbert space. We shall henceforth call these objects "projectors" and sometimes notate them as $\mathbb{P}(|\psi\rangle) = |\psi\rangle\langle\psi|$. Verify that the name projector for $\mathbb{P}(|\psi\rangle)$ is justified by the usual definition of projector, *i.e.*, a projector is an operator that squares to itself, which in this case requires $\mathbb{P}^2(|\psi\rangle) = \mathbb{P}(|\psi\rangle)$.

Solution: Quite simply, since

$$\mathbb{P}(|\psi\rangle) = |\psi\rangle\langle\psi|,$$

we have

$$\begin{aligned} \mathbb{P}^2(|\psi\rangle) &= |\psi\rangle\langle\psi|\psi\rangle\langle\psi| \\ &= |\psi\rangle\langle\psi| \qquad [\ \langle\psi|\psi\rangle = 1 \text{ since } |\psi\rangle \text{ is normalized. }] \\ &= \mathbb{P}(|\psi\rangle) \end{aligned}$$

---

2) Recall that $U_{CNOT} = |0\rangle\langle 0|_A \otimes \mathbb{I}_B + |1\rangle\langle 1|_A \otimes \sigma^x_B$. Verify that $U^2_{CNOT} = \mathbb{I}$.

Solution: Quite simply, since

$$U_{CNOT} = |0\rangle\langle 0|_A \otimes \mathbb{I}_B + |1\rangle\langle 1|_A \otimes \sigma^x_B,$$

we have

$$U^2_{CNOT} = |0\rangle\langle 0|0\rangle\langle 0|_A \otimes \mathbb{I}^2_B + |0\rangle\langle 0|1\rangle\langle 1|_A \otimes \mathbb{I}_B\sigma^x_B + |1\rangle\langle 1|0\rangle\langle 0|_A \otimes \sigma^x_B\mathbb{I}_B + |1\rangle\langle 1|1\rangle\langle 1|_A \otimes (\sigma^x_B)^2.$$

Remembering $\langle i|j\rangle = \delta_{ij}$ and $(\sigma^x_B)^2 = \mathbb{I}_B$, we conclude

$$\begin{aligned} U^2_{CNOT} &= |0\rangle\langle 0|_A \otimes \mathbb{I}_B + 0 + 0 + |1\rangle\langle 1|_A \otimes \mathbb{I}_B \\ &= \big(|0\rangle\langle 0|_A + |1\rangle\langle 1|_A\big) \otimes \mathbb{I}_B \\ &= \mathbb{I}_A \otimes \mathbb{I}_B \\ &= \mathbb{I}. \end{aligned}$$

---

3) Let $x = x_1x_2\ldots x_n$, $y = y_1y_2\ldots y_n$, and $z = z_1z_2\ldots z_n$ denote three n-bit binary strings. Let $\oplus$ denote bitwise addition modulo 2. That is,

$$x \oplus y = z \Longrightarrow \text{ For all } k, z_k = x_k + y_k \bmod 2.$$

Also, let $\cdot$ denote a sort of dot product for binary numbers which treats their digits as independent components

$$x \cdot y \equiv (x_1y_1 + x_2y_2 + \ldots + x_ny_n) \bmod 2.$$

Verify that this binary dot product $\cdot$ is distributive over bitwise, modulo 2 addition $\oplus$. That is, verify that

$$(x \oplus y) \cdot z = (x \cdot z) \oplus (y \cdot z).$$

Solution: The proof is trivial once one realizes that

$$(a + b + c) \bmod 2 = \{[(a + b) \bmod 2] + c\} \bmod 2 \equiv a \oplus b \oplus c$$

Thus,

$$\begin{aligned} x \cdot y &\equiv (x_1 y_1 + x_2 y_2 + \ldots + x_n y_n) \bmod 2 \\ &= x_1 y_1 \oplus x_2 y_2 \oplus \ldots \oplus x_n y_n, \end{aligned}$$

and our desired result, $(x \oplus y) \cdot z = (x \cdot z) \oplus (y \cdot z)$, follows immediately by the commutativity of modular 2 addition $\oplus$.

---

4) Recall that if a function $f = \{0,1\}^{\otimes n} \rightarrow \{0,1\}^{\otimes m}$ $(m \geq n)$ is periodic with period s with respect to bitwise, modulo 2 addition (*i.e.*, for all x, $f(x) = f(x \oplus s)$), then each run of Simon's algorithm will produce a vector y such that $s \cdot y = 0$. Explain the following statement:

With $O(n)$ runs of the algorithm, one can determine the period s with high probability.

(That is, sketch how one would determine s from the outputs of n runs of Simon's algorithm and estimate the probability that after n runs of the algorithm, one has enough data to determine s fully.)

Solution: First, whatever scheme we devise to determine s may assume that the black-box function we are testing via Simon's algorithm is in fact periodic with respect to s. We do not care if a scheme produces a spurious s when the function is in fact injective. This is because we have been promised f is either injective or it is periodic with period s with respect to bitwise, modulo 2 addition $\oplus$. Hence, it only takes two simple function evaluations $f(x)$ and $f(x \oplus s)$ for any desired string x to see whether the s produced by the scheme is truly a period or merely an artifact of our scheme as f is actually injective.

The straightforward scheme to produce s comes from realizing equations of the form $s \cdot y = 0$ are linear equations. Thus, as there are n unknown digits of s, a set of $n - 1$ equations

$$\begin{aligned} s \cdot y_1 &= 0 \\ s \cdot y_2 &= 0 \\ &\vdots \\ s \cdot y_{n-1} &= 0 \end{aligned}$$

where the strings $\{y_i | i = 1, \ldots n-1\}$ are linearly independent will uniquely determine s. In order to see why only $n-1$ equations and not n equations suffices to determine s uniquely, realize that we know *a priori* that any system of equations in the form $\{s \cdot y_i = 0 | i = 1, \ldots, M\}$ must possess a trivial solution of a string of n zeros $00\ldots0$ regardless of the number of equations M. Thus, if there's $n-1$ equations, the fact there are 2 solutions, $00\ldots0$ and some nonzero string is fine. It is the nonzero string about which we care. (NB: Remember we're working in binary arithmetic mod 2. If we were dealing with reals like we normally do in linear algebra, $n-1$ linearly independent equations would leave a whole line of valid solutions through $\mathbb{R}^n$, of course.)

Thus, the question becomes: *How many times must we run the algorithm in order to have at least a probability p of obtaining $n-1$ linearly independent y_i's?*

To answer this, we first must figure out how many y_i's we could possibly measure at the end of Simon's algorithm and the probabilities with which we would measure each. Recall that the quantum computer's state at the end of Simon's algorithm is

$$|\psi_f\rangle = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y, f(x)\rangle$$

Assuming the function is periodic, then there are 2 strings x and $x \oplus s$ in function's domain for every $f(x)$ in the function's range, and thus

$$|\psi_{f,\text{per}}\rangle = \frac{1}{2^n} \sum_{\text{Range } f(x)} \sum_{y \in \{0,1\}^n} [(-1)^{x \cdot y} + (-1)^{(x \oplus s) \cdot y}] |y, f(x)\rangle$$

Using the result of Problem 3, $(x \oplus y) \cdot z = (x \cdot z) \oplus (y \cdot z)$, this expression simplifies to

$$\begin{aligned}
|\psi_{f,\text{per}}\rangle &= \frac{1}{2^n} \sum_{\text{Range } f(x)} \sum_{y \in \{0,1\}^n} [(-1)^{x \cdot y} + (-1)^{(x \cdot y) \oplus (s \cdot y)}] |y, f(x)\rangle \\
&= \frac{1}{2^n} \sum_{\text{Range } f(x)} \sum_{y \in \{0,1\}^n} \left\{ \begin{array}{c} (-1)^{x \cdot y} + (-1)^{x \cdot y} \text{ if } s \cdot y = 0 \\ (-1)^{x \cdot y} + (-1)^{(x \cdot y) \oplus 1} \text{ if } s \cdot y = 1 \end{array} \right\} |y, f(x)\rangle \\
&= \frac{1}{2^n} \sum_{\text{Range } f(x)} \sum_{y \in \{0,1\}^n} \left\{ \begin{array}{c} 2(-1)^{x \cdot y} \text{ if } s \cdot y = 0 \\ 0 \text{ if } s \cdot y = 1 \end{array} \right\} |y, f(x)\rangle
\end{aligned}$$

Thus, while there are 2^n binary strings of length n, there are only 2^{n-1} possible y_i's we can measure if the black-box function is periodic. Moreover, the probabilities of measuring any one y_i in this case are all equal, namely $1/2^{n-1}$.

If we already have obtained $k-1$ linearly independent strings $\{y_i | i = 1, \ldots, k-1\}$, then the probability of obtaining a kth linearly independent string after running Simon's algorithm once more is

$$\frac{2^{n-1} - 2^{k-1}}{2^{n-1}} = 1 - \frac{1}{2^{n-k}}$$

since 2^{k-1} is the dimension of the subspace spanned by the already obtained, linearly independent $\{y_i | i = 1, \ldots, k-1\}$.

As such, the probability of obtaining the necessary $n-1$ linearly independent y_i's with just $n-1$ runs of Simon's algorithm is

$$\prod_{k=1}^{n-1} \left(1 - \frac{1}{2^{n-k}}\right)$$

To lower bound this probability, note that the following related infinite product is convergent

$$\prod_{m=1}^{\infty} \left(1 - \frac{1}{2^m}\right) = 0.288788095086602\ldots$$

Therefore, the probability of obtaining enough information to determine s with just $n-1$ runs of Simon's algorithm is at least $28.8788095086602\ldots\%$. If we are willing to perform m sets of $n-1$ runs, then our chance of being unable to determine s approaches 0 exponentially fast:

$$\begin{aligned} [\text{Prob of failure after } m(n-1) \text{ runs}] &< (1 - 0.288788095086602\ldots)^m \\ &< (0.7112119049133976\ldots)^m \end{aligned}$$

Therefore, we have established that with $O(n)$ runs of Simon's algorithm we may determine the period s with high probability.

---

5) Verify that the quantum Fourier transform

$$QFT|j\rangle \equiv \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i jk/N} |k\rangle$$

is a unitary operation.

(*Hint*: Recall that the inverse quantum Fourier transform is

$$QFT^{-1}|k\rangle \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{-2\pi i jk/N} |j\rangle$$

and recall that if an operator U is unitary, then $U^{-1} = U^\dagger$.)

Solution: The above rules allow us to write down the matrix representation of QFT and

QFT^{-1} in any orthonormal basis $|n\rangle$.

$$\begin{aligned} QFT_{mn} &\equiv \langle m|QFT|n\rangle \\ &= \left\langle m \left| \left(\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ink/N} \right| k \right\rangle \right) \\ &= \frac{e^{2\pi inm/N}}{\sqrt{N}} \quad \text{since } \langle m|k\rangle = \delta_{mk} \end{aligned}$$

$$\begin{aligned} QFT^{-1}_{mn} &\equiv \langle m|QFT^{-1}|n\rangle \\ &= \left\langle m \left| \left(\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{-2\pi ink/N} \right| k \right\rangle \right) \\ &= \frac{e^{-2\pi inm/N}}{\sqrt{N}} \quad \text{since } \langle m|k\rangle = \delta_{mk} \end{aligned}$$

Therefore, we conclude $QFT^{-1}_{mn} = QFT^{\dagger}_{nm}$ and thus QFT is unitary.

---

6) Verify the product representation of the quantum Fourier transform on a n-qubit state

$$\begin{aligned} QFT|j\rangle &\equiv \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi ijk/N}|k\rangle \\ &= \frac{1}{2^{n/2}} \left[|0\rangle_1 + e^{2\pi i(0.j_n)}|1\rangle_1\right] \otimes \left[|0\rangle_2 + e^{2\pi i(0.j_{n-1}j_n)}|1\rangle_2\right] \otimes \ldots \otimes \left[|0\rangle_n + e^{2\pi i(0.j_1 \ldots j_n)}|1\rangle_n\right] \end{aligned}$$

where we have used the binary equivalent of decimal point notation:

$$0.j_l j_{l+1} \ldots j_n \equiv \frac{j_l}{2} + \frac{j_{l+1}}{4} + \ldots + \frac{j_n}{2^{n-l+1}}.$$

(*Hint*: Write out j explicitly in binary, $j = j_1 2^{n-1} + j_2 2^{n-2} + \ldots + j_n 2^0$, and remember that the tensor product is distributive over addition.)

Solution: We first explicitly write out the tensor product state $|k\rangle = \bigotimes_{i=1}^{n} |k_i\rangle$ and explicitly write out in binary the number $k = k_1 2^{n-1} + k_2 2^{n-2} + \ldots + k_n 2^0$.

$$\begin{aligned} QFT|j\rangle &\equiv \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n}|k\rangle \\ &= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \exp\left[\frac{2\pi ij}{2^n} \sum_{l=1}^{n} k_l 2^{n-l}\right] \left(\bigotimes_{m=1}^{n} |k_m\rangle\right) \end{aligned}$$

Next, we use the fact the exponential of sum $e^{\sum_i x_i}$ is a product of exponentials $\prod_i e^{x_i}$.

$$QFT|j\rangle = \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} \left(e^{2\pi i j k_l 2^{-l}} |k_l\rangle \right)$$

Now, we invoke the fact that the tensor product is distributive over addition and explicitly evaluate the sums.

$$QFT|j\rangle = \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left(|0\rangle_l + e^{2\pi i j 2^{-l}} |1\rangle_l \right)$$

Then, we write out j explicitly in binary, $j = j_1 2^{n-1} + j_2 2^{n-2} + \ldots + j_n 2^0$.

$$QFT|j\rangle = \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[|0\rangle_l + \exp\left(2\pi i \sum_{m=1}^{n} j_n 2^{n-m-l} \right) |1\rangle_l \right]$$

Finally, we realize that since $e^{2\pi i z} = 1$ for any integer z, the only nontrivial terms in the sum in the exponent above are those for which $n - m - l < 0$. Using this fact and the binary equivalent of decimal point notation then yields the desired product representation

$$QFT|j\rangle = \frac{1}{2^{n/2}} \left[|0\rangle_1 + e^{2\pi i (0.j_n)} |1\rangle_1 \right] \otimes \left[|0\rangle_2 + e^{2\pi i (0.j_{n-1} j_n)} |1\rangle_2 \right] \otimes \ldots \otimes \left[|0\rangle_n + e^{2\pi i (0.j_1 \ldots j_n)} |1\rangle_n \right].$$