**2.111J/18.435J Quantum Computation Problem Set 4**
(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 $\mathbb{P}^2(|\psi\rangle) = \mathbb{P}(|\psi\rangle)$.

---

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

---

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 $\bullet$ denote a sort of dot product for binary numbers which treats their digits as independent components

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

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

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

---

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 $s \bullet y = 0$. 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.)

---

5) Verify that the quantum Fourier transform

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

is a unitary operation.

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

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

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

---

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.)