Introduction to Quantum Information Processing
Assignment 3
Due at 11:59pm on Wednesday 13 February 2013 using the LEARN dropbox, or the dropbox located outside the tutorial centre, MC 4066, BOX 2, Slot 11 (please submit a confirmation of submission online in this case)
(will constitute 10% out of the 50% assignment marks)

1. **3 marks** For any subspace S of the vector space $\{0,1\}^n$ (over $\mathbf{Z}_2$) define $S^\perp = \{\mathbf{t} \in \{0,1\}^n \mid \mathbf{s}\cdot\mathbf{t} = 0 \text{ for all } \mathbf{s} \in S\}$.

   Let $|\mathbf{x}+S\rangle = \frac{1}{\sqrt{|S|}}\sum_{\mathbf{y}\in S}|\mathbf{x}\oplus\mathbf{y}\rangle$. Show that

   $$H^{\otimes n}|\mathbf{x}+S\rangle = \sqrt{\frac{|S|}{2^n}}\sum_{\mathbf{z}\in S^\perp}(-1)^{\mathbf{x}\cdot\mathbf{z}}|\mathbf{z}\rangle.$$

   Hint: Show that for any $\mathbf{z} \in Z_2^n$, either $\mathbf{z} \in S^\perp$ or $\mathbf{z}$ is perpendicular to exactly half of the elements of S.

2. **4 marks** *Measuring stabilizers*

   In Section 4.5 it is shown how to implement a parity measurement using a quantum circuit. In Exercise 3.4.4, it is shown how the parity measurement is equivalent to measuring the observable $Z^{\otimes n}$.

   (a) Describe an alternative algorithm (and draw the corresponding circuit diagram) for measuring any Pauli observable $P_1\otimes P_2\otimes P_3$ using one application of a c-$(P_1\otimes P_2\otimes P_3)$ gate, where $P_1, P_2, P_3 \in \{I, X, Y, Z\}$, and not all three equal I.

   (b) What are the two possible outcomes, and their respective probabilities, of measuring the observable $X\otimes X\otimes Y$ on input $|000\rangle$? (Note that the eigenvectors of Y are $\frac{1}{\sqrt{2}}|0\rangle \pm \frac{i}{\sqrt{2}}|1\rangle$.)

3. **4 marks** *eigenvalues of the QFT*

   (a) Find a concise description of the operation formed by the square of QFT_N.

   (b) Note that the order of the QFT_N is 4, for $N \geq 3$. That is, $QFT_N^4 = I$. For $N \geq 3$, give a circuit for exactly measuring the eigenvalues of the QFT_N operation. You may use a controlled-QFT operation, and other elementary quantum gates.

4. **4 marks** Consider the cyclic shift operator S on three qubits:

   $$|x\rangle|y\rangle|z\rangle \mapsto |z\rangle|x\rangle|y\rangle$$

   for all $x, y, z \in \{0,1\}$.

   (a) What are the eigenvalues of S?

(b) Note that $|000\rangle$, $|111\rangle$, $\frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle)$, and $\frac{1}{\sqrt{3}}(|110\rangle + |011\rangle + |101\rangle)$ are eigenvectors with eigenvalue 1.

For the remaining eigenvalues, write a basis of eigenvectors for the corresponding eigenspace. (Hint: you can find eigenvectors that are superpositions of strings with the same Hamming weight.)

(c) Express the state

$$(\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle)$$

as a linear combination of the given eigenvectors.

(d) Express the state $|0\rangle|0\rangle|1\rangle$ as a linear combination of the given eigenvectors.

5. **3 marks** *Modular arithmetic and factoring*

Let r be the order of 3 mod 65.

(a) **1 mark** Find r.

(b) **1 mark** What is 3^{123} mod 65?

(c) **1 mark** Find $\mathrm{GCD}(65, 3^{\frac{r}{2}} - 1)$ and $\mathrm{GCD}(65, 3^{\frac{r}{2}} + 1)$.

6. **2 marks**

Let $s \in \{0,1\}^n$ be a secret string of length n.

Suppose you have a black-box that outputs states of the form $\frac{1}{\sqrt{2}}|0\rangle|x\rangle + \frac{1}{\sqrt{2}}|1\rangle|x \oplus s\rangle$ for random values of x.

Describe an algorithm that will find s with high probability using $O(n)$ calls to the black-box.

(Hint: Use ideas from Simon's algorithm.)