Introduction to Quantum Information Processing
Assignment 3 Solutions

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*.*

   Solution:

   Recall from the lectures that

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}}\sum_y(-1)^{x\cdot y}|y\rangle$$

   Thus

$$\begin{aligned} H^{\otimes n}|S+x\rangle &= \frac{1}{\sqrt{|S|}}\sum_{s\in S}H^{\otimes n}|s\oplus x\rangle \\ &= \frac{1}{\sqrt{2^n|S|}}\sum_{s\in S}\sum_z(-1)^{z\cdot(s\oplus x)}|z\rangle \\ &= \frac{1}{\sqrt{2^n|S|}}\sum_z(-1)^{z\cdot x}\left(\sum_{s\in S}(-1)^{z\cdot s}\right)|z\rangle \end{aligned}$$

   We note that $|\sum_{s\in S}(-1)^{z\cdot s}| = |S|$ if $z \in S^\perp$.

   For $z \notin S^\perp$, we note that there are equal number of elements $s$in S with $s\cdot z = 0$ as with $s \cdot z = 1$.

   Proof: If $z \notin S^\perp$*, then there must exist a* $v \in S$ *such* $z \cdot v = 1$*.*

   We define a one-to-one correspondence between elements s *of* S *that satisfy* $s\cdot z = 0$ *and those that satisfy* $s \cdot z = 1$*, by mapping* $s \mapsto s \oplus v$*; this map is self-inverse, and thus gives a one-to-one correspondence between the two sets.*

   Thus, if $z \notin S^\perp$, we have $|\sum_{s\in S}(-1)^{z\cdot s}| = 0$.

   Thus, the above superposition reduces to

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

   The normalization factor can also be written as $\frac{1}{\sqrt{|S^\perp|}}$.

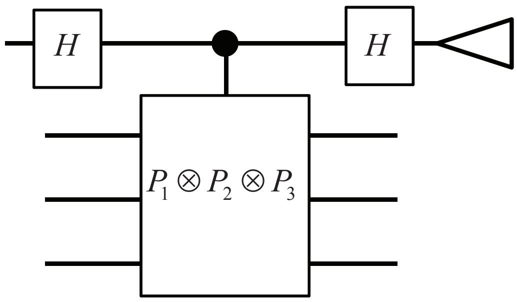
2. **4 marks** *Measuring stabilizers*

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.

Solution:

We are projecting the input space onto one of the two eigenspaces of $P_1 \otimes P_2 \otimes P_3$. We can do this using eigenvalue kickback, where the eigenvalue of $P_1 \otimes P_2 \otimes P_3$ appears as a phase in the control register. Consider the following circuit



Suppose that $|\psi\rangle = a|\psi_{-1}\rangle + b|\psi_1\rangle$, where $|\psi_{-1}\rangle$ and $|\psi_1\rangle$ are -1 and 1 eigenvectors for $P_1 \otimes P_2 \otimes P_3$, respectively. Then in the above circuit, we begin with the state

$$|0\rangle \left(a|\psi_1\rangle + b|\psi_{-1}\rangle\right).$$

Applying H to the first qubit results in

$$\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \left(a|\psi_1\rangle + b|\psi_{-1}\rangle\right).$$

Applying the controlled $P_1 \otimes P_2 \otimes P_3$ gives

$$a\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)|\psi_1\rangle + b\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)|\psi_{-1}\rangle.$$

Finally, applying H to the control qubit, we get

$$a|0\rangle|\psi_1\rangle + b|1\rangle|\psi_{-1}\rangle.$$

Now we see that measuring the control qubit will project onto one of the eigenspaces of $P_1 \otimes P_2 \otimes P_3$, with the eigenvalue revealed from the outcome of the measurement.

(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 $\frac{1}{\sqrt{2}}|0\rangle \pm \frac{i}{\sqrt{2}}|1\rangle$.)

Solution:

Let us denote
$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$, $|L\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle$, $|R\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{i}{\sqrt{2}}|1\rangle$.
Then

$$\begin{aligned}|000\rangle = & \left(\tfrac{1}{\sqrt{2}}|+\rangle + \tfrac{1}{\sqrt{2}}|-\rangle\right)\left(\tfrac{1}{\sqrt{2}}|+\rangle + \tfrac{1}{\sqrt{2}}|-\rangle\right)\left(\tfrac{1}{\sqrt{2}}|L\rangle + \tfrac{1}{\sqrt{2}}|R\rangle\right) \\ = & \tfrac{1}{\sqrt{2}}\left(\tfrac{1}{2}|+\rangle|+\rangle|L\rangle + \tfrac{1}{2}|+\rangle|-\rangle|R\rangle + \tfrac{1}{2}|-\rangle|+\rangle|R\rangle + \tfrac{1}{2}|-\rangle|-\rangle|L\rangle\right) \\ & + \tfrac{1}{\sqrt{2}}\left(\tfrac{1}{2}|-\rangle|-\rangle|R\rangle + \tfrac{1}{2}|-\rangle|+\rangle|L\rangle + \tfrac{1}{2}|+\rangle|-\rangle|L\rangle + \tfrac{1}{2}|+\rangle|+\rangle|R\rangle\right)\end{aligned}$$

where

$$\left(\frac{1}{2}|+\rangle|+\rangle|L\rangle + \frac{1}{2}|+\rangle|-\rangle|R\rangle + \frac{1}{2}|-\rangle|+\rangle|R\rangle + \frac{1}{2}|-\rangle|-\rangle|L\rangle\right)$$

is a normalized superposition of $+1$ eigenstates of $X \otimes X \otimes Y$ (since it is a product of an even number of -1 eigenstates of the single qubit operators X, X and Y), and thus is also a $+1$ eigenstate of $X \otimes X \otimes Y$.
Similarly,

$$\frac{1}{\sqrt{2}}\left(\frac{1}{2}|-\rangle|-\rangle|R\rangle + \frac{1}{2}|-\rangle|+\rangle|L\rangle + \frac{1}{2}|+\rangle|-\rangle|L\rangle + \frac{1}{2}|+\rangle|+\rangle|R\rangle\right)$$

is a normalized superposition of -1 eigenstates of $X \otimes X \otimes Y$ (since it is a product of an odd number of -1 eigenstates of the single qubit operators X, X and Y), and thus is also a -1 eigenstate of $X \otimes X \otimes Y$.
Thus one measures eigenvalue $+1$ with probability $\frac{1}{2}$ and in this case is left with the state $\left(\frac{1}{2}|+\rangle|+\rangle|L\rangle + \frac{1}{2}|+\rangle|-\rangle|R\rangle + \frac{1}{2}|-\rangle|+\rangle|R\rangle + \frac{1}{2}|-\rangle|-\rangle|L\rangle\right)$,
and one measures eigenvalue -1 with probability $\frac{1}{2}$ and in this case is left with the state $\frac{1}{\sqrt{2}}\left(\frac{1}{2}|-\rangle|-\rangle|R\rangle + \frac{1}{2}|-\rangle|+\rangle|L\rangle + \frac{1}{2}|+\rangle|-\rangle|L\rangle + \frac{1}{2}|+\rangle|+\rangle|R\rangle\right)$.

3. **2 marks** *eigenvalues of the QFT*

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

Solution:

The QFT_N maps

$$|x\rangle \mapsto \sum_{y=0}^{N-1} e^{2\pi i \frac{xy}{N}} |y\rangle$$

and applying the QFT_N again gives

$$\begin{aligned} & \textstyle\sum_{y=0}^{N-1} \sum_{z=0}^{N-1} e^{2\pi i \frac{xy}{N}} e^{2\pi i \frac{yz}{N}} |z\rangle \\ = & \textstyle\sum_{z=0}^{N-1} \left(\sum_{y=0}^{N-1} e^{2\pi i \frac{xy+zy}{N}} \right) |z\rangle \\ = & \textstyle\sum_{z=0}^{N-1} \left(\sum_{y=0}^{N-1} e^{2\pi i y \frac{x+z}{N}} \right) |z\rangle \end{aligned}$$

Note that if $x + z \neq 0 \bmod N$, then $\sum_{y=0}^{N-1} e^{2\pi i y \frac{x+z}{N}} = 0$.

Proof: Note that any element of the form $e^{2\pi i \frac{k}{N}}$ *for an integer* k *is a root of the polynomial* $x^N - 1 = 0$. *This polynomial factors as* $(x-1)(1 + x + x^2 + \ldots x^{N-1})$. *Thus any root that is not equal to* 1, *must be a root of* $1 + x + x^2 + \ldots + x^{N-1}$.

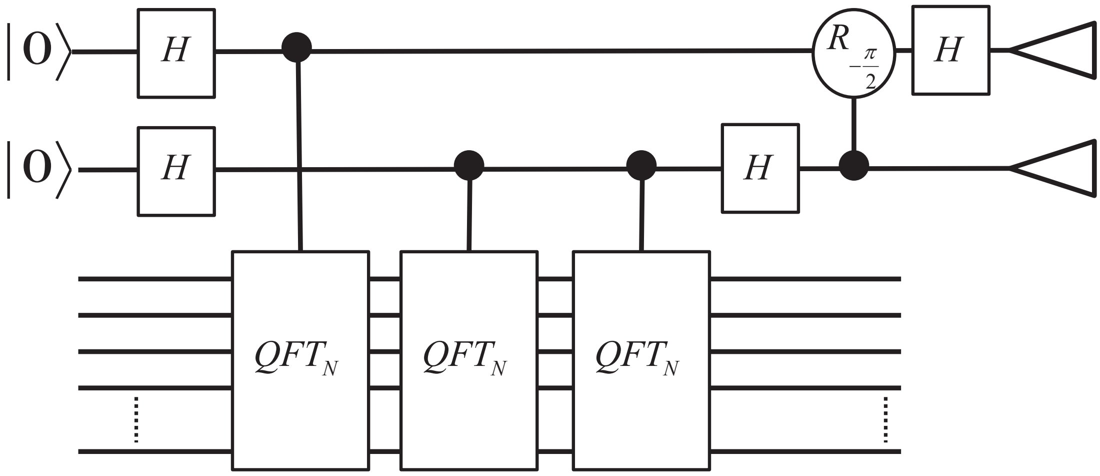
And for $x + z = 0 \bmod N$, we have $\sum_{y=0}^{N-1} e^{2\pi i y \frac{x+z}{N}} = N$.

Thus the only basis state in the above superposition that does vanish is $z = N - x \bmod N$, and has phase factor $+1$.

Thus the square of QFT_N sends $|x\rangle$ to $|N - x \bmod N\rangle$, for $0 \leq x < N$.

(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.

Solution:



Solution:

Since $QFT_N^4 = I$, the eigenvalues are of the form $e^{2\pi i \frac{k}{4}}$ for $k = 0, 1, 2, 3$.
Thus the eigenvalue estimation algorithm with a control register of two qubits will measure the eigenvalues exactly.

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?

Solution:

Since $S^3 = I$, the eigenvalues must be cube roots of 1: 1, $\omega = e^{2\pi i \frac{1}{3}}$ or $\omega^2 = e^{2\pi i \frac{2}{3}}$.
As we see in the next part, each of these values occur in the spectrum 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.)

Solution:

By inspection, $\frac{1}{\sqrt{3}}(|100\rangle + \omega^2|010\rangle + \omega|001\rangle)$ and $\frac{1}{\sqrt{3}}(|110\rangle + \omega^2|011\rangle + \omega|101\rangle)$ are eigenstates with eigenvalue ω.
By inspection, $\frac{1}{\sqrt{3}}(|100\rangle + \omega|010\rangle + \omega^2|001\rangle)$ and $\frac{1}{\sqrt{3}}(|110\rangle + \omega|011\rangle + \omega^2|101\rangle)$ are eigenstates with eigenvalue ω^2.
Note that another way to find an eigenstate of S with eigenvalue ω^j is to pick any state, say $|100\rangle$ and renormalize the state $|100\rangle + \omega^{-j}S|100\rangle + \omega^{-2j}S^2|100\rangle$. Note that by construction the operator S maps

$$|100\rangle + \omega^{-j}S|100\rangle + \omega^{-2j}S^2|100\rangle \mapsto S|100\rangle + \omega^{-j}S^2|100\rangle + \omega^{-2j}S^3|100\rangle$$

which equals (using $S^3 = I$, $\omega^{-2j} = \omega^j$, and reordering)

$$\omega^j|100\rangle + S|100\rangle + \omega^{-j}S^2|100\rangle = \omega^j(|100\rangle + \omega^{-j}S|100\rangle + \omega^{-2j}S^2|100\rangle).$$

(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.

Solution:

$$\begin{aligned}
& (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle) \\
= \quad & \alpha^3|000\rangle + \alpha^2\beta|001\rangle + \alpha^2\beta|010\rangle + \alpha^2\beta|100\rangle \\
& +\alpha\beta^2|011\rangle + \alpha\beta^2|101\rangle + \alpha\beta^2|110\rangle + \beta^3|111\rangle \\
= \quad & \alpha^3|000\rangle + \sqrt{3}\alpha^2\beta(\tfrac{1}{\sqrt{3}}|100\rangle + \tfrac{1}{\sqrt{3}}|010\rangle + \tfrac{1}{\sqrt{3}}|001\rangle) \\
& +\sqrt{3}\alpha\beta^2(\tfrac{1}{\sqrt{3}}|110\rangle + \tfrac{1}{\sqrt{3}}|011\rangle + \tfrac{1}{\sqrt{3}}|101\rangle) + \beta^3|111\rangle
\end{aligned}$$

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

Solution:

$$\begin{aligned}
|001\rangle = \quad & \frac{1}{\sqrt{3}}\frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle) + \frac{\omega^2}{\sqrt{3}}\frac{1}{\sqrt{3}}(|100\rangle + \omega^2|010\rangle + \omega|001\rangle) \\
& + \frac{\omega}{\sqrt{3}}\frac{1}{\sqrt{3}}(|100\rangle + \omega|010\rangle + \omega^2|001\rangle)
\end{aligned}$$

We can see that the coefficient for a given eigenvector is just the conjugate of the coefficient of $|001\rangle$ in that eigenvector. This is what we obtain when we take the inner product of the given state and the corresponding eigenvector.

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

   Let r be the order of 3 mod 65.

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

   Solution 1:

   If we compute the powers of 3 mod 65, we get $3, 9, 27, 16, 48, 14, 42, 61, 53, 29, 22, 1, \ldots$, with the first element equal to 1 being the one in position number 12. Therefore, the order of 3 mod 65 is 12.

   Note that to obtain an element of this list, we can just multiply the previous element by 3, and reduce the result modulo 65.

   Solution 2:

   By direct calculation, 4 is the order of 3 modulo 5 (so $3^4 = 1 \bmod 5$), and 3 is the order of 3 modulo 13 (so $3^3 = 1 \bmod 13$). By the Chinese Remainder theorem we have $3^{12} = 1 \bmod 5 * 13 = 65$, and 12 is the smallest power of 3 that is congruent to 1 modulo both 5 and 13.

   (b) **1 mark** What is $3^{123} \bmod 65$?

   Solution:

   Since $3^{12} = 1 \bmod 65$, then $3^{12k} = 1 \bmod 65$ for any positive integer k, and thus $3^{123} = 3^{123 \bmod 12} \bmod 65$. Now, $123 = 3 \bmod 12$. Therefore, $3^{123} = 3^3 = 27 \bmod 65$.

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

   Solution:

   We have $3^{\frac{r}{2}} - 1 = 13 \bmod 65$ and $2^{\frac{r}{2}} + 1 = 15 \bmod 65$. Thus $\mathrm{GCD}(65, 2^{\frac{r}{2}} - 1) = 13$ and $\mathrm{GCD}(65, 3^{\frac{r}{2}} + 1) = 5$.

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.)

   Solution:

   Apply $H^{\otimes n}$ to the second register. This gives

$$\sum_{y \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} \left(\frac{(-1)^{y \cdot x}}{\sqrt{2}} |0\rangle|y\rangle + \frac{(-1)^{y \cdot (x \oplus s)}}{\sqrt{2}} |1\rangle|y\rangle \right).$$

If we measure the second register we get a random y and the first qubit is left in the state $\frac{(-1)^{y\cdot x}}{\sqrt{2}}|0\rangle + \frac{(-1)^{y\cdot(x\oplus s)}}{\sqrt{2}}|1\rangle = (-1)^{y\cdot x}(\frac{1}{\sqrt{2}}|0\rangle + \frac{(-1)^{y\cdot s}}{\sqrt{2}}|1\rangle)$.

If we apply a Hadamard gate to this qubit, we obtain $(-1)^{y\cdot x}|y\cdot s\rangle$. Thus we know y and the value of $y \cdot s$ for a random string y.

If we sample $n + O(1)$ such random strings, $y_1, y_2, \ldots$, with $y_i \cdot s = b_i$, then with high probability s will be the only solution to the linear system $y_1 \cdot s = b_1, y_2 \cdot s = b_2, \ldots$, and we can find s by solving the linear system.