Quantum Algorithms
Homework 8 Solutions

Patrick Canny

Due: 2019-04-02

1 Book Problems

1. Exercise 9.1

Solution:

Proof. The proof that the choice of ε does not matter is similar to an argument made earlier in the class about the class BPP.

It may be useful to note that I will define an operator called M whose job is to compute the result of $MAJ_{\oplus}$ with ancillas.

First, take k many applications of the circuit U as described in the textbook ($U = U_L \dots U_2 U_1$) because the problem requires that the input to $MAJ_{\oplus}$ be the output qubits of k many copies of U.

Now, we need to apply M a number of times to the resulting output of U. This number of inputs does not necessarily have to equal k, so let's call it m. The reason for doing this is in order to determine if an answer apprears as the result of k-many applications of U.

It is important to note that U computes a function F with a given probability, specifically:

$$\sum_x |\langle F(x), z| U \left|x, 0^{N-m}\right\rangle|^2 \geq 1 - \varepsilon$$

So by choosing a sufficiently large value for k, the probability of at least $k/2$ of the same result produced by U will increase. □

2. Exercise 9.3

Solution: To answer this question, I will show and explain the result of changing the basis oon each of the two input qubits.

First, consider the controlled qubit. From the circuit provided in the problem, we can see that the controlled qubit can be represented by $H[2]\Lambda(\sigma^x)H[2] = (I \otimes H)\Lambda(\sigma^x)(I \otimes H)$ which can be used to compute:

$$
\begin{aligned}
(H \otimes I)\Lambda(\sigma^x)(H \otimes I) &= 1/\sqrt{2} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} 1/\sqrt{2} \\
&= 1/2 \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \\
&= 1/2 \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & -2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}
\end{aligned}
$$

This implies that when the basis is changed for the controlled qubit, it is equivilent to leaving the basis unchanged aside from $|1,1\rangle$, which is multiplied by -1. This matrix is actually the same as $\Lambda(\sigma^z)$, which can be seen by extending the pattern of adding 1s on the diagonal above the Unitary operator σ^z as seen with $\Lambda(\sigma^x)$.

Now, we can consider the case of $H[1]\Lambda(\sigma^x)H[1] = (H \otimes I)\Lambda(\sigma^x)(H \otimes I)$, representing a change of basis on the control qubit:

$$
\begin{aligned}
(H \otimes I)\Lambda(\sigma^x)(H \otimes I) &= 1/\sqrt{2} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} 1/\sqrt{2} \\
&= 1/2 \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix} \\
&= 1/2 \begin{pmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{pmatrix}
\end{aligned}
$$

This seems to represent multiple rotations about the x axis for a given input qubit.

2 Additional Problems

1. Recall the operator Z from page 85 of the text,

$$Z\left|a_0,\ldots,a_n\right\rangle = \left|a_0 \oplus f(a_1,\ldots,a_n), a_1,\ldots,a_n\right\rangle, \qquad \text{where}$$
$$f(a_1,\ldots,a_n) = \begin{cases} 1 & \text{if } a_1 = \cdots = a_n = 0, \\ 0 & \text{if } \exists j : a_j \neq 0. \end{cases}$$

Find the matrix for Z when $n = 2$ and prove that it is unitary.

Solution: Take the definition of Z when $n = 2$:

$$Z\left|a_0,a_1,a_2\right\rangle = \left|a_0 \oplus f(a_1,a_2),(a_1,a_2)\right\rangle$$
$$f(a_1,a_2) = \begin{cases} 1 & \text{if } a_1 = a_2 = 0, \\ 0 & \text{if } \exists j : a_j \neq 0. \end{cases}$$

From here, we can build the matrix representation for Z by considering all 3-qubit basis vectors:

$$\begin{aligned} Z\left|0,0,0\right\rangle &= \left|1,0,0\right\rangle \quad Z\left|0,0,1\right\rangle = \left|0,0,1\right\rangle \\ Z\left|0,1,0\right\rangle &= \left|0,1,0\right\rangle \quad Z\left|0,1,1\right\rangle = \left|0,1,1\right\rangle \\ Z\left|0,0,0\right\rangle &= \left|1,0,0\right\rangle \quad Z\left|1,0,1\right\rangle = \left|1,0,1\right\rangle \\ Z\left|1,1,0\right\rangle &= \left|1,1,0\right\rangle \quad Z\left|1,1,1\right\rangle = \left|1,1,1\right\rangle \end{aligned}$$

So, the columns of the matrix representation of Z can be given by considering these resulting vectors as columns for the matrix. For example, the first column of the matrix will be given by $Z\left|0,0,0\right\rangle$ because the basis for the new matrix will be lexigraphically ordered in terms of the previous computations. This yields:

$$Z = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

To prove that it is a unitary matrix, we must show that it's rows and columns are orthonormal.

Claim 2.1. *Z is orthonormal*

Proof of claim. Z is a matrix where every column and every row has exactly a single 1. To show that each column is normal, take it's inner product with itself.

Take $\left|\chi\right\rangle$ to be a given column in Z.

$$\left\langle \chi \mid \chi \right\rangle = 1$$

To show that all the columns are orthogonal to each other, consider that the inner product of a pair of columns. Column a has single 1 in position i vs column b where that 1 exists in position j, $i \neq j$.

It holds in Z that all pairs of columns hold this property. In computing the inner product of two columns that share this property, a 0 will exist in column b at position i, and a 0 will exist in column a at position j. This implies that any 1 will become a 0 when computing the inner product of a and b. Since all the inner products are 0, it holds that Z is orthogonal.

Since Z is orthonormal, Z is unitary. ∘

2. Define the Boolean function $f : \{0,1\}^2 \to \{0,1\}$ by the table below (variable x is the horizontal variable and y is vertical).

(x,y)	0	1
0	1	0
1	1	1

(i) Find a boolean circuit that computes $f_\oplus$ over the usual basis.

(ii) Find the matrix for $\widehat{f_\oplus}$ relative to the standard computational basis.

(iii) Find a quantum circuit that computes $\widehat{f_\oplus}$. You may use any 2-qubit gate as well as controlled gates. There is a solution without ancillas, but you may use ancillas if you need to.

Solution:

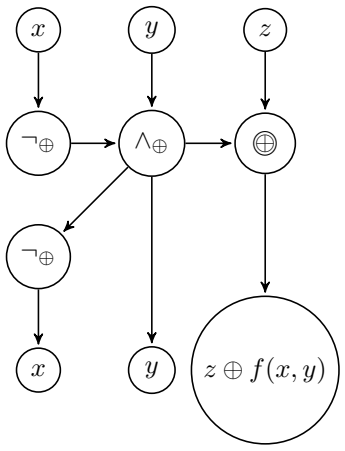
(i) $f_\oplus(x,y,z) = (x,y,z \oplus f(x,y))$, so:

$$f_\oplus(0,1,z) = (0,1,z)$$
$$f_\oplus(x,y,z) = (x,y,\neg z)$$

If we consider the usual basis to be $\{\wedge, \vee, \neg\}$, the reversible basis can be defined as:

$$\{\wedge_\oplus, \vee_\oplus, \neg_\oplus, \circledcirc\}$$

We can now use these gates to construct a reversible boolean circuit:



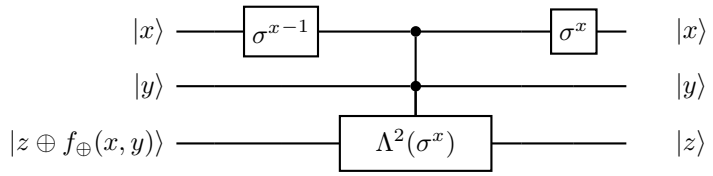
(ii) Similarly to AP 1, $\widehat{f_\oplus}$ can be represented in the 3-qubit space by considering the solution bits as the result of $f_\oplus$ applied to a 3-qubit basis vector representing the input to $f_\oplus$:

$$\begin{aligned} Z\,|0,0,0\rangle &= |0,0,1\rangle \quad Z\,|0,0,1\rangle = |0,0,0\rangle \\ Z\,|0,1,0\rangle &= |0,1,1\rangle \quad Z\,|0,1,1\rangle = |0,1,0\rangle \\ Z\,|1,0,0\rangle &= |1,0,1\rangle \quad Z\,|1,0,1\rangle = |1,0,0\rangle \\ Z\,|1,1,0\rangle &= |1,1,1\rangle \quad Z\,|1,1,1\rangle = |1,1,0\rangle \end{aligned}$$

Using the same rationale as AP 1, the resulting matrix for $\widehat{f_\oplus}$ can be established as:

$$f_\oplus = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

(iii) The quantum circuit for $\widehat{f_\oplus}$ can be represented as:



Where both $|x\rangle, |y\rangle$ are inputs to the Toffoli gate.

3. Let $g : \{0,1\}^n \to \{0,1\}^n$ be a reversible boolean function. Prove that $\widehat{g}$ is unitary.

Solution:

Proof. $\widehat{g}$ provides insight into a pattern that is present when considering a concrete implementation of $g_\oplus$:

$$\begin{aligned} g(a_0, a_1 \ldots, a_n, c) &= (c \oplus g(a_0, a_1, \ldots, a_n), a_0, a_1, \ldots, a_n) \\ \widehat{g}\,|a_0, a_1 \ldots, a_n, c\rangle &= |c \oplus g(a_0, a_1, \ldots, a_n), a_0, a_1, \ldots, a_n\rangle \end{aligned}$$

So, it holds that the application of $\widehat{g}$ must preserve the original input into g.

If we recall that the application of any operator to an input qubit represents a rotation in the quantum space, it follows that whatever operator rotates the input must also be able to rotate it back its original position. Call the operator that acts on the qubit $|\alpha\rangle$ U, the result of this application $|\beta\rangle$, and the operator that rotates $|\beta\rangle$ back to $|\alpha\rangle$, G. The following relationship can be established:

$$GU\,|\alpha\rangle = |\alpha\rangle$$

So it holds that $GU = I$. Recall that unitary operators have the property

$$U^\dagger U = UU^\dagger = I$$

U also has the property where $U^{-1} = U^\dagger$. U also preserves the norm of a vector, so the result of applying U to a vector will represent a pure rotation about the Bloch sphere without any changes to the length of the vector. This implies that GU will only allow $|\beta\rangle$ to remain on the Bloch sphere if both G and U are unitary.

Since U has a unique inverse that which must also be unitary (in order to retain a position on the bloch sphere), it holds that G must be $U^\dagger = U^{-1}$. □