Quantum Algorithms
Homework 6 Solutions

Patrick Canny

Due: 2019-03-19

1 Book Problems

1. Exercise 7.1
   Prove that negation and the Toffoli gate form a complete basis for reversible circuits.

Solution:

Claim 1.1. *The assertion of Problem 7.1 is true.*

Proof of claim. To prove that a basis is complete, we've generally considered bases that are known to be complete and then shown that that basis can be created from elements of the new basis. The procedure here will be similar, but reversibility will need to be considered.

Take the complete boolean basis $\{\neg, \wedge\}$. From Lemma 7.1 (page 62 in the text)it is possible to create permutations for the elements of the basis, allowing realizations of the following mappings:

$$\neg_{\oplus} : (x, y) \mapsto (x, x \oplus y \oplus 1)$$
$$\wedge_{\oplus} : (x, y, z) \mapsto (x, y, z \oplus xy)$$
$$\bigoplus : (x, y) \mapsto (x, x \oplus y)$$

By Lemma 7.1, these functions form a complete basis for reversible boolean circuits. From here, we need to show that this basis can be represented using only the Toffoli gate and negation. Fortunately, the Toffoli gate is already present in this new basis. It is now required to show that the other two functions can be represented using the Toffoli and negation.

The permuted not, $\neg_{\oplus}$, can actually be formed using the controlled not and negation in the following way:

$$\neg_{\oplus}[1, 2] = \neg[2] \bigoplus [1, 2]$$

So, if it is possible to show that the controlled not, $\bigoplus$, can be realized using the Toffoli and negation, it suffices to prove the claim. Fortunately, due to Lemma 7.2(page 63), it is possible to introduce ancillary bits, which allows the realization of $\bigoplus$. Take new ancillary bit n and use it to realize $\bigoplus[1, 2]$, for instance:

$$\bigoplus[1, 2] = \neg[n] \wedge_{\oplus} [n, 1, 2]\neg[n]$$

Since we have represented the elements of a complete basis for reversible boolean circuits using the Toffoli and Negation, this proves that $\{\wedge_{\oplus}, \neg\}$ is a complete basis for revesible boolean circuits as well. •

2. Exercise 8.2
Prove that any operator of the form $\Lambda(U), U \in U(\mathcal{B})$ can be realized (without ancillas) by a constant size circuit over the basis of one-qubit gates and the gate $\Lambda(\sigma^x)$.

Solution: First, take $U = e^{i\varphi}Z$ where $Z \in SU(2)$. The reason that this is done is that this allows for elements in the group U to be easily decomposed into elements in SU.

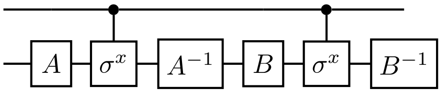
So, $\Lambda(U) = \Lambda(e^{i\varphi})\Lambda(Z)$. The first part ($\Lambda(e^{i\varphi})$) will act only on the control qubit, so the second piece is more significant as it acts on the operator that belongs to the Special Unitary Group.

Any operator $Z \in SU(2)$ can be represented as

$$Z = A\sigma^x A^{-1} B\sigma^x B^{-1} \qquad A, B \in SU(2)$$

This is due to the geometric properties of these operators. This representation is representative of 2 consecutive rotations being applied. For example, the A operator represents some modified rotation about the y axis, whie the B operator represents a vertical rotation. This is due to the fact that applying an operator (such as A) to σ^x yields operator $\sigma^x *$. When this new operator is applied to an input qubit, the resulting position on the Bloch sphere represents the result of the desired operations being performed on the input. The reason that two of these transformations must be applied is that with two rotations of varying degree, any position on the Bloch sphere can be accessed.

From here this produces circuit



which follows from the above explanations: the input qubit is being applied at both of the $\sigma^x *$ gates in the circuit.

3. Exercise 8.4
Suppose that a unitary operator $U : \mathcal{B}^{\otimes n} \to \mathcal{B}^{\otimes n}$ satisfies the condition $U|0\rangle = |0\rangle$. Construct a circuit of size $6n+1$ realizing $\Lambda(U)$ over the basis $\{U, \Lambda^2(\sigma^x)\}$, using ancillas. The gate U need only be applied once.

Solution: To do this, we will implement an n-qubit controlled exchange. This can be done by consindering the definition of a bit exchange given in the text:

$$(\leftrightarrow)[j,k] = \bigoplus[j,k] \bigoplus [k,j] \bigoplus [j,k]$$

By the definition of $\Lambda^2(\sigma^x)$ (from here referred to as $\Lambda_\oplus$), it follows that we can extrapolate this definition:

$$(\leftrightarrow)[j,k] = \Lambda_\oplus[j,k]\Lambda_\oplus[k,j]\Lambda_\oplus[j,k]$$

Now, in order to introduce control to the equation, another qubit must be added. This allows for the qubits to be swapped if the control is hi, and leaves them be if the control is lo. With qubits a, b and control qubit c, the definition of the controlled bit exchange is as follows:

$$(\leftrightarrow)[c,a,b] = \Lambda_\oplus[c,a,b]\Lambda_\oplus[c,b,a]\Lambda_\oplus[c,a,b]$$

So, for an n-qubit input, by the equation above, there will be $3n$ many applications of $\Lambda_\oplus$ required to exchange the input qubits. Then, the gate U will be applied to the exchanged input if the control qubit is hi, and will not be applied if the control is lo. This is a constant addition of 1 gate to the circuit. From here, the input must be exchanged back to its original state. This is done with another $3n$ many applications of $\Lambda_\oplus$. So, the final size of this exchange circuit will be $6n + 1$ many gates.

2 Additional Problems

1. Suppose that $F : \{0,1\}^2 \to \{0,1\}^2$ is a reversible function. Prove that there are constants $a, b, c, d, e, f \in \{0,1\}$ such that

$$F(x,y) = \big(ax \oplus by \oplus c, dx \oplus ey \oplus f\big)$$

for all $x, y \in \{0,1\}$. Recall that we interpret multiplication and addition ($\oplus$) as taking place in $\mathbb{Z}/2\mathbb{Z}$ so that multiplication is bitwise "and" and addition is bitwise "or".

Solution:

Claim 2.1. *The assertion of AP 1 is true, and constants a, b, c, d, e, f can be found*

Proof of claim. Since the output of F is a 2-bit pair, and the structure given for computing these two bits is the same, I will prove the assertion using only one bit, but it is important to realize that the same can be done for the second bit.

First, consider the equation

$$G(x,y) = \big(ax \oplus by \oplus c\big)$$

We seek to show that G always has a solution, and that any version of G can evaluate to either 0 or 1.

$$\begin{aligned}
G(0,0) &= a0 + b0 + c = c \\
G(0,1) &= a0 + b + c = b + G(0,0) \to b = G(0,1) - G(0,0) \\
G(1,0) &= a + b0 + c = a + G(0,0) \to a = G(1,0) - G(0,0) \\
G(1,1) &= a + b + c = G(1,0) - G(0,0) + G(1,0) - G(0,0) + G(0,0) \\
&= G(1,0) + G(0,1) + G(0,0)
\end{aligned}$$

It's unclear that the last equation has a solution, but the solution can be created when considering that all of these equations will evaluate to some number in $\mathbb{Z}/x\mathbb{Z}$. Now, we can establish

$$s = a + b + c \quad | \quad s, a, b, c \in \mathbb{Z}/2\mathbb{Z}$$

Now, if s is to be 1, choose $a = s = 1, b = c = 0$. If s is to be 0, choose $s = b = 0, a = c = 1$. Since this equation is solvable, its analog that computes the other bit is also solvable by the same rationale. This is enough to show that the claim is true. •