Quantum Information A Fall 2020 Exam Solutions

Jake Muff
Student number: 015361763
21/10/2020

1. **Exercise 3.29 from Nielsen & Chuang.**
   Show that applying two consecutive Fredkin gates gives the same output as input. (Fredkin gate is self inverse)
   Fredkin gate only swaps bits or leaves them alone so number of 1's or 0's in the output must be the same as input i.e

$$(x, y, z) \rightarrow (x, xz + \tilde{x}y, xy + \tilde{x}z)$$

   So the only thing that changes the output is the control bit c which, for two consecutive inputs as 4 different permutations

c	
0	0
0	1
1	0
1	1

Table 1: Table showing that different permutations or values the control bit can be with two consecutive Fredkin gates.

a	→	a'	a	→	b'
b	→	b'	b	→	a'
c	→	c'	c	→	c'

Table 2: If c=0(left) and c=1(right), for 1 Fredkin gate.

a	→	a'	→	a
b	→	b'	→	b
c	→	c'	→	c

Table 3: Two consecutive Fredkin gates where c=(0,0)

   Each of the tables shows a different combination of the control bits as different combinations will provide different outputs, however as shown, no matter what the combination of control bits with two consecutive Fredkin gates, the outputs are the same as inputs.
   N.B: I have also attached a scan of my working out for this question which included better drawn diagrams to show the swapping of the bits after each Fredkin gate.

a	$\rightarrow$	a'	$\rightarrow$	b
b	$\rightarrow$	b'	$\rightarrow$	a
c	$\rightarrow$	c'	$\rightarrow$	c

Table 4: Two consecutive Fredkin gates where c=(0,1)

a	$\rightarrow$	b'	$\rightarrow$	b
b	$\rightarrow$	a'	$\rightarrow$	a
c	$\rightarrow$	c'	$\rightarrow$	c

Table 5: Two consecutive Fredkin gates where c=(1,0)

a	$\rightarrow$	b'	$\rightarrow$	a
b	$\rightarrow$	a'	$\rightarrow$	b
c	$\rightarrow$	c'	$\rightarrow$	c

Table 6: Two consecutive Fredkin gates where c=(1,1)

2. **Exercise 4.36 from Nielsen & Chuang.**
Constructing a quantum circuit to add two two-bit numbers that performs the transformation

$$|x, y\rangle \rightarrow |x, x + y \ mod \ 4\rangle$$

So, as per the transformation, the circuit should have 4 inputs x_1, x_2, y_1, y_2 and 4 outputs $x_1, x_2, (x + y \ mod \ 4) \times 2$.
Taking inspiration from page 132 which showed gate diagrams for the half adder and full adder circuit as well as figure 3.18. These show that two half adders can be used to build a full adder using the casding effect and that $CNOT$ gates can be used to create modulo 2 addition circuits. So we have the circuit

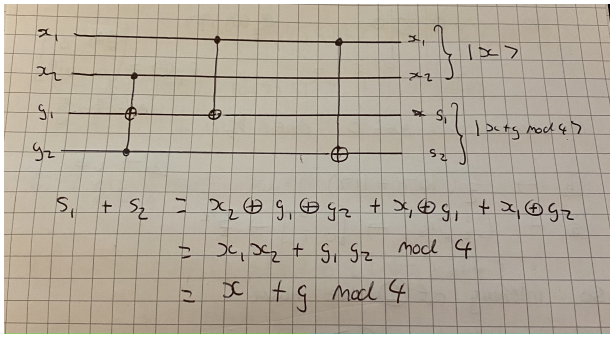

Figure 1: Quantum circuit for Ex 4.36 to add two two-bit numbers mod 4. The text below the circuit verifies that the outputs combine to give $x + y \ mod \ 4$. This image is also attached separately.

3. **Exercise 4.42 from Nielsen & Chuang.**
Irrationality of θ with $cos(\theta) = 3/5$

(a) (1)

$$e^{i\theta} = \frac{3+4i}{5}$$

Because θ must be rational (as given in the question θ must be a multiple of 2π) we can say that

$$e^{im\theta} = e^{ik} = 1$$

Where $k = 2\pi\theta$ so that

$$e^{im\theta} = \frac{(3+4i)^m}{5^m}$$

$$1 \times 5^m = (3+4i)^m$$

Such that we get that there must be a positive integer m such that

$$(3+4i)^m = 5^m$$

(b) (2) Showing that $(3+4i)^m = 3+4i(mod\ 5)$ for all $m > 0$
So for $m = 1$, trivially we have

$$3+4i = 3+4i\ mod\ 5$$

and for $m = 2$ we have

$$(3+4i)^2 = (3+4i)(3+4i) = 9+12i+12i+16i^2 = -7+24i = (3+4i)\ mod\ 5$$

It is (fairly?) safe to say that $m > 0$ they're equal. This is saying that $3+4i$ is not a multiple of 5, therefore we can say

$$5^m = 0 \mod 5$$

So there cannot exist a m which satisfies $(3+4i)^m = 5^m$

4. **Exercise 4.51 from Nielsen & Chuang.**
Construct a quantum circuit to simulate the Hamiltonian

$$H = X_1 \otimes Y_2 \otimes Z_3$$

Performing $e^{-i\Delta t H}$ for any Δt
Using Fig 4.19 in the book as a reference, we can transform the X_1 and Y_1 into Pauli Z gates so the quantum circuit will be an alteration of fig 4.19.
The Pauli X gate can be written as

$$X = HZH$$

As proved earlier in N & C (eq 4.18). The Pauli Y gate requires additional thought but it can be transformed into single qubit gate operations using equations 4.5 and 4.6 and exericse 4.7 in the book.
So the Pauli Y gate can be decompised into the Pauli X gate through applying a rotation matrix R_z and then transforming the X gate into a Z gate through the equation above. (Similar to Toffoli gate transformation shown in Problem Set 6, which helped me in realising this.)

$$R_z(\theta) = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}$$

$$R_z(-\theta) = \begin{pmatrix} e^{i\theta/2} & 0 \\ 0 & e^{-i\theta/2} \end{pmatrix}$$

If we take $\theta = \frac{\pi}{2}$ we get back to Y such that

$$Y = R_z(\theta) X R_z(-\theta)$$

Which, if we think about in terms of the bloch sphere representation intuitively makes sense with a rotation of 90 degrees, which is why $\theta = \frac{\pi}{2}$ was applied.

$$Y = R_z(\frac{\pi}{2}) X R_z(-\frac{\pi}{2})$$

$$= \begin{pmatrix} e^{-i\frac{\pi}{4}} & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} e^{i\frac{\pi}{4}} & 0 \\ 0 & e^{-i\frac{\pi}{4}} \end{pmatrix} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

Which, using $X = HZH$ makes this

$$Y = R_z(\frac{\pi}{2}) HZH R_z(-\frac{\pi}{2})$$

Now both X and Y are written as single qubit gates to Z operations, the Hamiltonians is

$$H = H_1 Z_1 H_1 \otimes R_{z_2}(\frac{\pi}{2}) H_2 Z_2 H_2 R_{z_2}(-\frac{\pi}{2}) \otimes Z_3$$

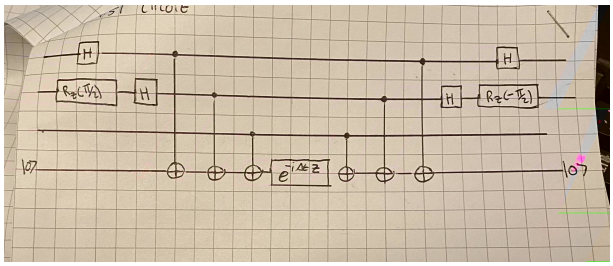

Figure 2: Quantum circuit for Ex 4.51.This image is also attached separately.

5. **Exercise 5.18 from Nielsen & Chuang.**
Factoring $N = 91$. Following the algorithm for reduction of factoring to order finding.
Step 1: Is N even? No.
Step 2: Does $N = a^b$ for $a \geq 1$ and $b \geq 2$. Using a quick python check (not necessary but quick), the closest we get is $9^2 = 81$ or $3^4 = 81$. $N \neq a^b$ for integers a and b.
Step 3: $x = 4$

$$gcd(x, N) = gcd(4, 91) = 1$$

So step 3 is also skipped.
Step 4: Find order r of $x \ mod \ 91$. Again using python

$$4^1 = 4 \rightarrow 4 \ mod \ 91 = 4$$

$$4^2 = 16 \rightarrow 16 \ mod \ 91 = 16$$

$$4^3 = 64 \rightarrow 64 \ mod \ 91 = 64$$

$$4^4 = 256 \rightarrow 256 \ mod \ 91 = 74$$

$$4^5 = 1024 \rightarrow 1024 \ mod \ 91 = 23$$

$$4^6 = 4096 \rightarrow 4096 \ mod \ 91 = 1$$

So $r = 6$ and r is even so for Step 5 we have

$$4^{\frac{r}{2}} = 4^3 = 64 \neq -1(mod \ 91) \neq 90$$

And

$$gcd(64 - 1, 91) = 7$$

And the algorithm succeeds.