Quantum Information A Exam

Jake Muff
Student Number: 015361763
21/10/2020

1) 3.29 from N and C

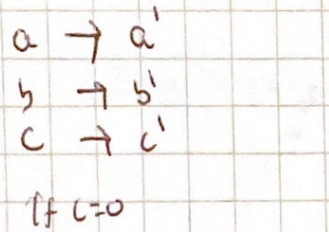
Show that applying two consecutive Fredkin gates gives same output as input

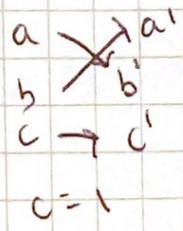
(Fredkin gate is self inverse)

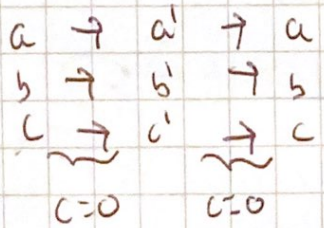
$$(x, y, z) \to (x,\ xz + \bar{x}y,\ xy + \bar{x}z)$$

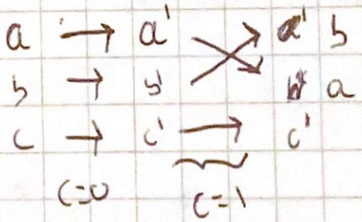
Fredkin gate only swaps bits or leaves them alone so number of 0s or 1s in the output must be same as input

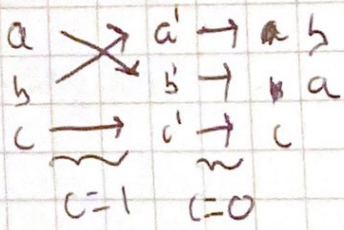
c	
0	0
0	1
1	0
1	1

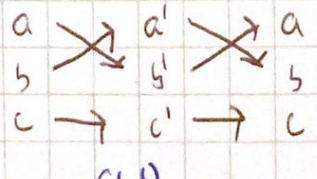












As in NC the original inputs are recovered from two consecutive gates

4.36 x and y Modulo 4

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

$x \rightarrow x_1, x_2$ $\quad$ $y \rightarrow y_1, y_2$

Circuit should have 4 inputs x_1, x_2, y_1, y_2

Should have 4 outputs x and

$x \rightarrow x_1, x_2$ and $(x+y \bmod 4) \times 2$

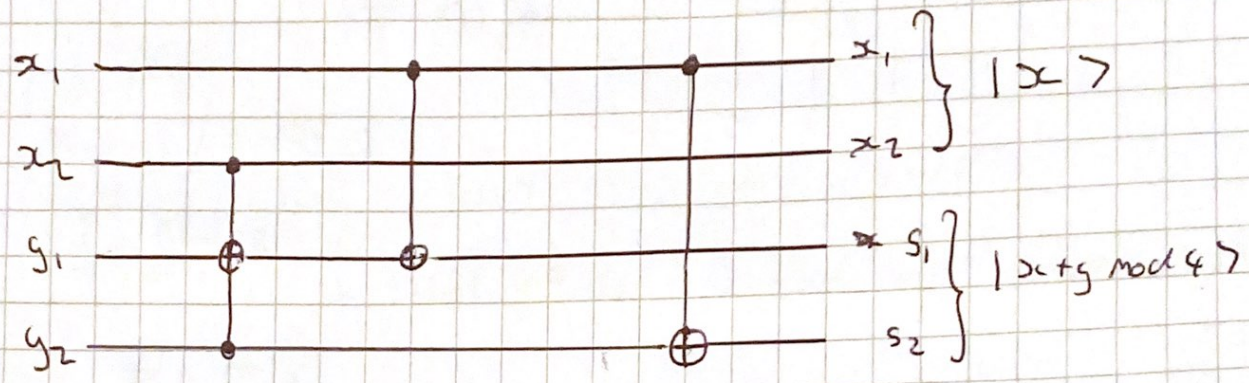
[Quantum half adder?]

$\oplus$ Modulo 2 For Mod 4

Fig 3.18 NAND gate using a Toffoli gate

4.30 Cont. Two half adders can be used to build the full adder

~~Fig 3.6~~ Following Page 132 Nte we want to cascade ~~two half adders~~ a full adder w/ 2 half adders to get



$$s_1 + s_2 = x_2 \oplus g_1 \oplus g_2 + x_1 \oplus g_1 + x_1 \oplus g_2$$

$$= x_1 x_2 + g_1 g_2 \bmod 4$$

$$= x + g \bmod 4$$

Ex 4.42 Irrationality of θ

$\cos\theta = 3/5$

i) $e^{i\theta} = \frac{(3+4i)}{5}$ Show that if θ is rational then there must exist a positive integer m such that $(3+4i)^m = 5^m$

~~A rational number means that~~

θ must be a multiple of 2π

~~$e^{im\theta}$~~ Because θ must be rational we say that

$$e^{im\theta} = e^{i\frac{h}{2\pi\theta}} = 1$$

$h = 2\pi\theta$

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

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

- 442 (2) Show that $(3+4i)^n \equiv 3+4i \pmod 5$

$n > 0$

No n can exist such that $(3+4i)^n = 5^m$ can exist

So e.g $n = 2$

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

What is $(3+4i) \bmod 5$

$n = 1 \quad 3+4i \equiv 3+4i \bmod 5$

Fairly safe to say that for all $n > 0$ they're equal

so $3+4i$ is not a multiple of 5 and

$5^n \equiv 0 \bmod 5$ so there cannot exist a n which satisfies $(3+4i)^n = 5^m$

4.5] Construct a quantum circuit to [illegible] the Hamiltonian

$$H = X_1 \otimes Y_{1,2} \otimes Z_3$$

$e^{i\Delta t H}$ for any Δt

F working from Fig 4.19

Pauli X gate can be written as

$$X = HZH \qquad \text{eq(4.18)}$$

Proved Previously.

~~Pauli Y gate can be written as~~

Y = Pauli Y gate needs to be decomposed Transformed into to single qubit gate operations

e) ~~$R_z(\frac{\pi}{2})$~~ $R_z(\frac{\pi}{2})$

Using equation (4.5) and exercise 4.7 (4.6)
The Pauli Y gate can be decomposed into the Pauli X gate through applying a rotation matrix R_z

$$Y = \begin{matrix} 0 & -i \\ i & 0 \end{matrix} \quad \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

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

$\theta = \frac{\pi}{2}$ ∴

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

Thinking about this in terms of the Bloch Sphere intuitively makes sense with a rotation of 90° therefore $\theta = \frac{\pi}{2}$

$$Y = R_z(\tfrac{\pi}{2}) \times R_z(-\tfrac{\pi}{2})$$

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

we know that $X = HZH$

so

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

and both X and Y are written as single qubit ~~operation~~ gates to Z operations

& so ~~our choices~~ so the Hamiltonian is

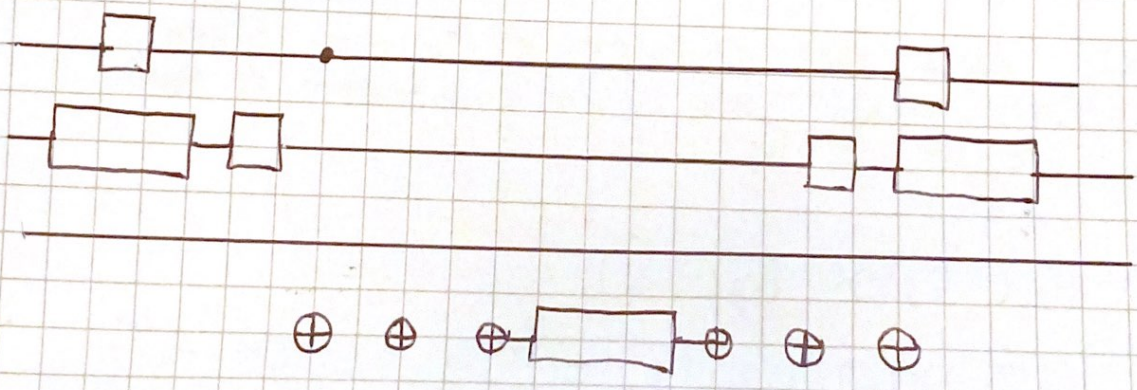
$$H = H_1 Z_1 H_1 \otimes R_{z_2}\left(\frac{\pi}{2}\right) H_2 Z_2 H_2 R_{z_2}\left(-\frac{\pi}{2}\right) \otimes Z_3$$

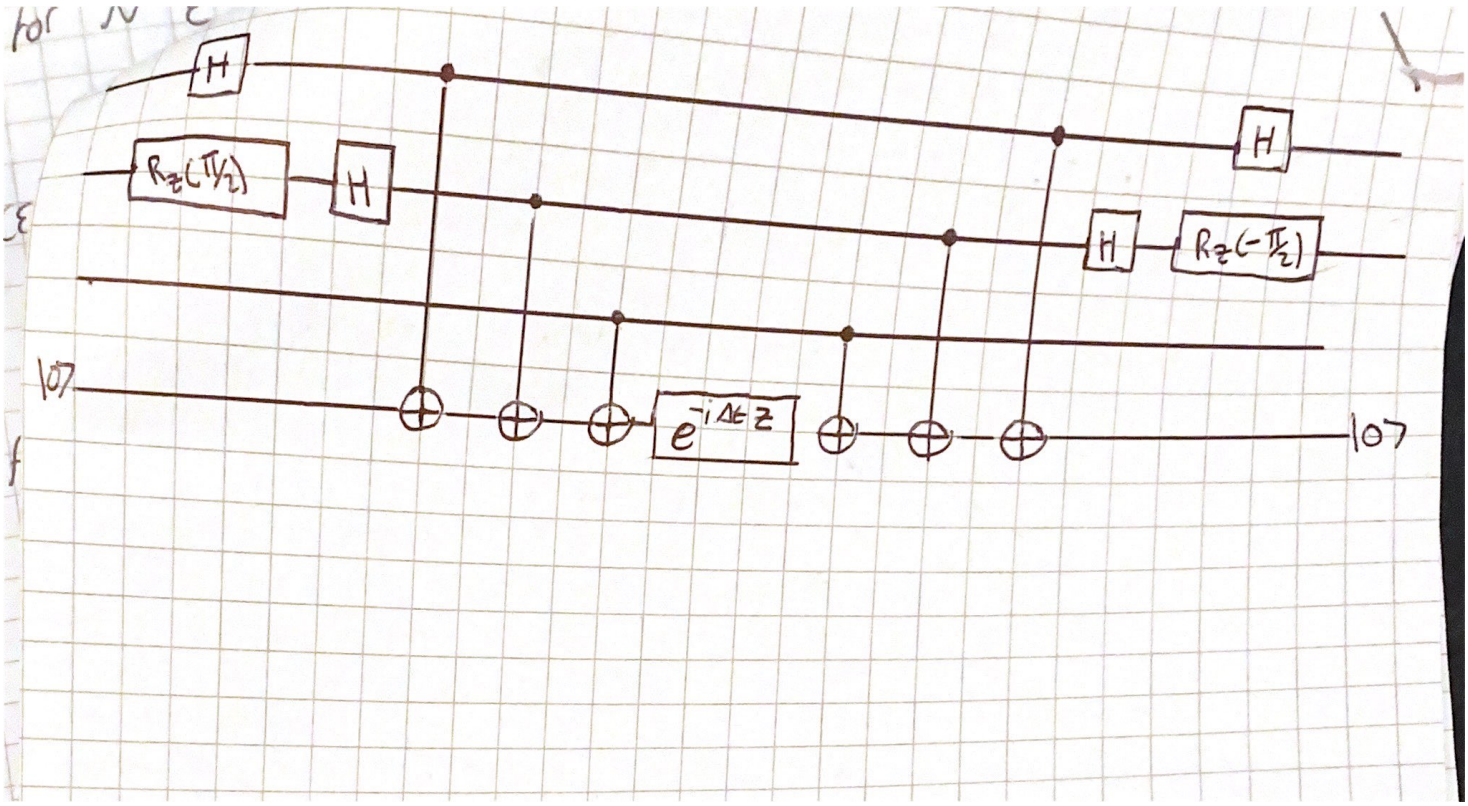
1st line → H_1 ⊕ ⊕ H_1

2nd line → $R_z(\pi/2)$ H ⊕ ⊕ H $R_z(-\pi/2)$

3rd line → ⊕ ⊕

4th line → $|0\rangle$ — $e^{-i\Delta t Z}$ — $|0\rangle$




H
$R_z(\pi/2)$
H
H
H
$R_z(-\pi/2)$
$e^{-i\Delta E z}$
107
107

Ex 5.18 Factoring N = 91

Step 1 → Is N even? NO

Step 2 → Does $N = a^b$ for $a \geq 1$ and $b \geq 2$

Closest we get is $9^2 = 81$ or $3^4 = 81$

Step 3 → $x = 4$ $\quad gcd(x, N) = gcd(4, 91) = 1$

So ~~for~~ step 3 skipped

Step 4 → Find order r of x mod 91

4 mod 91

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

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

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

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

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

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

$\therefore r = 6$ $\quad r$ is even (step 5)

$4^{r/2} = 4^3 = 64 \qquad 64 \neq 90$

Note Typo in Book

$-1 \pmod{91} = 90$ so $gcd(64 - 1, N) = 7$