Quantum Computing

Carl

September 2023

Contents

1 Introduction

1.1

Suppose that Alice sends two different numbers to Bob. In the case that both numbers come back the same, we assume that the function is constant, if different then assume that the function is balanced. Doing this only requires two queries. The probability of getting the function correct would be

$$1 * p_c + \frac{1}{2} * p_b$$

where p_c is the probability of bob using a constant function and p_b the probability of bob using a balanced function. This is because when the function is balanced we must get $1, 0$ or $0, 1$ half of the time. Thus we will get p_b correct half the time. This method will also always get the constant valued function right since when given a constant valued function both of the values will return as the same all the time. Since we must have $p_b + p_c = 1$, and we have $2(1 * p_c + \frac{1}{2} * p_b) = p_c + p_c + p_b = p_c + 1$, we can conclude that

$$1 * p_c + \frac{1}{2} * p_b = \frac{1}{2}p_c + \frac{1}{2}$$

But $p_c \geq 0$ due to describing the probability of getting a constant function. Thus we have

$$1 * p_c + \frac{1}{2} * p_b = \frac{1}{2}p_c + \frac{1}{2} \geq \frac{1}{2}$$

meaning that we will get the correct function half the time. Thus having an error rate of $1/2$ as required.

2 Introduction to quantum mechanics

2.1

Consider $(1,2)+(1,-1)-(2,1)=(1+1-2,2-1-1)=0$. Thus we have coefficients that are not 0 which result in a sum that equals 0. Meaning the vectors are indeed linearly dependent.

2.2

We can assume that A is a 2x2 matrix because it maps from a 2 dimensional to a 2 dimensional vector space. So let

$$A=\begin{bmatrix}A_{11} & A_{12}\\ A_{21} & A_{22}\end{bmatrix}$$

Then we have $A|0\rangle=(A_{11},A_{21})$ and $A|1\rangle=(A_{12},A_{22})$. But we want $A|0\rangle=|1\rangle$. So we must have $(A_{11},A_{21})=(0,1)$ thus $A_{11}=0$ and $A_{21}=1$. Also because $A|1\rangle=|0\rangle$, we must also have $(A_{12},A_{22})=(1,0)$. Thus $A_{12}=1$ and $A_{22}=0$. So

$$A=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$$

Consider the basis vectors $|\alpha\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ and $|\beta\rangle\frac{1}{\sqrt{2}}(-|0\rangle+|1\rangle)$. We then have $A|\alpha\rangle=|\alpha\rangle$. Also $A|\beta\rangle=-|\beta\rangle$. So the transformation in this new basis will have the form

$$B=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}_{\{\alpha,\beta\}}$$

2.3

Let $1\leq l\leq i$ where i is the length of the $|v_i\rangle$ basis. Then we have the matrix $\mathcal{M}(BA)$ being defined as

$$(BA)v_l=\sum_{n=1}^{k}C_{n,k}x_n$$

where k is the length of the $|x_k\rangle$ basis. By definition of product of linear maps we have

$$(BA)v_l=B(Av_l)=B\sum_{n=1}^{j}A_{n,l}w_n$$

where j is the length of the $|w_j\rangle$ basis. But because B is a linear map we have

$$B\sum_{n=1}^{j}A_{n,l}w_n=\sum_{n=1}^{j}A_{n,l}Bw_n=$$

$$B\sum_{n=1}^{j}A_{n,l}w_n=\sum_{n=1}^{j}A_{n,l}Bw_n=\sum_{n=1}^{j}A_{n,l}\sum_{m=1}^{i}B_{m,n}v_m=\sum_{n=1}^{j}\sum_{m=1}^{i}B_{m,n}A_{n,l}v_m$$

But the last part is just the matrix representation of $\mathcal{M}(B)\mathcal{M}(A)$ Thus we can conclude that $\mathcal{M}(BA)=\mathcal{M}(B)\mathcal{A}$ as required.

2.4

The properties of the identity operator I, on any linear map T from $V \to W$ where V and W are vector spaces is $IT = TI = T$. Let $|v_j\rangle$ be a basis of V and T be a linear map from $V \to V$ The matrix representation of $\mathcal{M}(IT)$ and $\mathcal{TI}$ is

$$(IT)v_i = Tv_i = \sum_{n=1}^{j} A_{n,i}v_n$$

$$(TI)v_i = Tv_i = \sum_{n=1}^{j} A_{n,i}v_n$$

and also

$$(IT)v_i = I(Tv_i) = I\sum_{n=1}^{j} A_{n,i}v_n = \sum_{n=1}^{j} A_{n,i}Iv_n$$

$$(TI)v_i = T(Iv_i) = T\sum_{n=1}^{j} B_{n,i}v_n = \sum_{n=1}^{j} B_{n,i}Tv_n$$

Thus

$$(IT)v_i = (TI)v_i$$

$$\sum_{n=1}^{j} B_{n,i}Tv_n = \sum_{n=1}^{j} A_{n,i}Iv_n$$

$$\sum_{n=1}^{j} B_{n,i}Tv_n = \sum_{n=1}^{j} B_{n,i}\sum_{m=1}^{j} A_{m,n}v_m = \sum_{n=1}^{j}\sum_{m=1}^{j} B_{n,i}A_{m,n}v_m$$

meaning

$$\sum_{n=1}^{j} A_{n,i}v_n = \sum_{n=1}^{j}\sum_{m=1}^{j} B_{n,i}A_{m,n}v_m$$

But subtracting both sides by

$$\sum_{n=1}^{j} A_{n,i}v_n$$

results in

$$0 = \left(\sum_{n=1}^{j}\sum_{m=1}^{j} B_{n,i}A_{m,n}v_m\right) - \sum_{n=1}^{j} A_{n,i}v_n = \sum_{m=1}^{j}\left(\sum_{n=1}^{j} B_{n,i}A_{m,n}v_m\right) - A_{m,i}v_m =$$

$$\sum_{m=1}^{j}\left(\left(\sum_{n=1}^{j} B_{n,i}A_{m,n}\right) - A_{m,i}\right)v_m$$

The right hand side is just a linear combination of the basis $|v_j\rangle$ of V and so

$$\left(\sum_{n=1}^{j} B_{n,i}A_{m,n}\right) - A_{m,i} =$$

$$\left(\sum_{n=1}^{i-1} B_{n,i}A_{m,n}\right) + \left(\sum_{n=i+1}^{j} B_{n,i}A_{m,n}\right) + A_{m,i}(B_{i,i} - 1) = 0$$

for all m and i. But $A_{m,n}$ could be any value since T was an arbitrary linear transformation. Thus in order for the above equation to be fulfilled, $B_{i,i} = 1$ and $B_{n,i} = 0$ when $n \neq i$. Doing this means that we must have

$$Iv_i = \sum_{n=1}^{j} B_{n,i}v_n = v_i$$

Thus we have a matrix which is 1 only on it's diagonals as required.

2.5

Let $|w\rangle, |v\rangle, |u\rangle \in \mathbf{C}^n$ and $\lambda \in \mathbf{F}$. Then

$$(|w\rangle, |v\rangle + |u\rangle) = \sum_{i=1}^{n} w_i^*(v_i + u_i)$$

$$(|w\rangle, |v\rangle) + (|w\rangle, |u\rangle) = \left(\sum_{i=1}^{n} w_i^* v_i\right) + \left(\sum_{i=1}^{n} w_i^* u_i\right) = \sum_{i=1}^{n} w_i^*(v_i + u_i)$$

Thus $(|w\rangle, |v\rangle) + (|w\rangle, |u\rangle) = (|w\rangle, |v\rangle + |u\rangle)$

Also

$$\lambda(|w\rangle, |v\rangle) = \lambda \sum_{i=1}^{n} w_i^* v_i$$

$$(|w\rangle, \lambda|v\rangle) = \sum_{i=1}^{n} \lambda w_i^* v_i = \lambda \sum_{i=1}^{n} w_i^* v_i$$

Thus $(|w\rangle, \lambda|v\rangle) = \lambda(|w\rangle, |v\rangle)$ and so we can confirm that the defined inner product is linear in it's second argument.

We also have

$$(|w\rangle, |v\rangle) = \sum_{i=1}^{n} w_i^* v_i$$

$$(|v\rangle, |w\rangle)^* = (\sum_{i=1}^{n} v_i^* w_i)^* = \sum_{i=1}^{n} (v_i^* w_i)^* = \sum_{i=1}^{n} w_i^* v_i$$

because we have $v_i = a + bi$ and $w = c + di$, so $w_i^* v_i = ac + cbi - adi + bd = (ac + bd) + (cb - ad)i$ and also $(v_i^* w_i)^* = (ac - bci + adi + bd)^* = ((ac + bd) - (cb - ad))^* = (ac + bd) + (cb - ad)$. Thus we have $(v_i^* w_i)^* = w_i^* v_i$ and so it can be concluded that $(|w\rangle, |v\rangle) = (|v\rangle, |w\rangle)^*$ as required.

Finally

$$(|v\rangle, |v\rangle) = \sum_{i=1}^{n} v_i^* v_i$$

But we have $v_i^* v_i = (a - bi)(a + bi) = a^2 + b^2$ which must be greater than or equal to 0. That in turn means $\sum_{i=1}^{n} v_i^* v_i$ is a sum of numbers greater than or equal to 0 and must therefore be greater than or equal to 0. Thus we have

$$(|v\rangle, |v\rangle) \geq 0$$

Now suppose $(|v\rangle, |v\rangle) = 0$. We then have

$$\sum_{i=1}^{n} v_i^* v_i = 0$$

Suppose for contradiction that $v_i \neq 0$ for some i. Then $v_i^* v_i > 0$. But that would mean $\sum_{i=1}^{n} v_i^* v_i > 0$ since all other terms besides i is greater than or equal to 0. That means we must have $v_i = 0$ for all i and thus we can conclude that $|v\rangle = 0$

Now suppose $|v\rangle = 0$. Then $v_i = 0$ and so

$$(|v\rangle, |v\rangle) = \sum_{i=1}^{n} v_i^* v_i = \sum_{i=1}^{n} v_i^* * 0 = 0$$

Therefore we can conclude that the defined operator is indeed an inner product of $\mathbf{C}^n$

2.7

We have $|w\rangle = (1, 1)$ and $|v\rangle = (1, -1)$. Then $\langle w|v\rangle = 1 * 1 - 1 * 1 = 0$. Thus we have orthogonality. The normalized vectors are $|w\rangle / ||w|| = |w\rangle / \sqrt{2} = \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right)$ and also $|v\rangle / ||v|| = |v\rangle / \sqrt{2} = \left(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}\right)$

2.9

For σ_0 we have

$$\sigma_0 = I\sigma_0 I = \sum_{m=1}^{2} \sum_{n=1}^{2} \langle w_n| \sigma_0 |v_m\rangle |w_n\rangle \langle v_m| =$$

$$\langle 0|0\rangle |0\rangle \langle 0| + \langle 1|1\rangle |1\rangle \langle 1| = |0\rangle \langle 0| + |1\rangle \langle 1|$$

For σ_x we have

$$\sigma_x = |0\rangle \langle 1| + |1\rangle \langle 0|$$

For σ_y we have

$$\sigma_y = i |1\rangle \langle 0| - i |0\rangle \langle 1|$$

For σ_z we have

$$\sigma_z = |0\rangle \langle 0| - |1\rangle \langle 1|$$

2.11

We have

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

so to find the eigenvalues

$$det\left(\begin{bmatrix} 0-\lambda & 1 \\ 1 & 0-\lambda \end{bmatrix}\right) = 0$$

This means $\lambda^2 - 1 = 0$ and so $\lambda = \pm 1$. Then the eigenvector corresponding to $\lambda = 1$ has $-v_1 + v_2 = 0$. This results in $v_1 = v_2$ and an eigenvector $\frac{1}{\sqrt{2}}(1,1)$ The eigenvector corresponding to $\lambda = -1$ has $v_1 + v_2 = 0$ thus resulting in $v_2 = -v_1$ and an eigenvector $\frac{1}{\sqrt{2}}(1,-1)$. Thus we have a diagonal matrix

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

with respect to the basis $\left(\frac{1}{\sqrt{2}}(1,1), \frac{1}{\sqrt{2}}(1,-1)\right)$. For

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

we find the eigenvalues by

$$det\left(\begin{bmatrix} 0-\lambda & i \\ -i & 0-\lambda \end{bmatrix}\right) = 0$$

meaning $\lambda^2 - 1 = 0$ which once again results in eigenvalues $\lambda = \pm 1$. The eigenvector that corresponds to $\lambda = 1$ then has the property $-v_1 + iv_2 = 0$. Thus resulting in an eigenvector of $\frac{1}{\sqrt{2}}(i,1)$. For $\lambda = -1$, we then have the property $v_1 + iv_2 = 0$ and so $v_1 = -iv_2$ thus resulting in eigenvector $\frac{1}{\sqrt{2}}(-i,1)$. This means we have a diagonal matrix

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

with respect to the basis $\left(\frac{1}{\sqrt{2}}(i,1), \frac{1}{\sqrt{2}}(-i,1)\right)$. For

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

we find the eigenvalues through

$$det\left(\begin{bmatrix} 1-\lambda & 0 \\ 0 & -1-\lambda \end{bmatrix}\right) = 0$$

meaning $-(1-\lambda)(1+\lambda) = 0$ and so $1-\lambda^2 = 0$ which results in once again $\lambda = \pm 1$. The eigenvector corresponding to $\lambda = 1$ then has the property $-2v_2 = 0$. That

means we have an eigenvector $(1,0)$. The eigenvector corresponding to $\lambda = -1$ has the property that $2v_1 = 0$ and so we have an eigenvector $(0,1)$. This results in a diagonal matrix of

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

with respect to the basis $((1,0),(0,1))$

2.12

Let

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

We have $Zv = \lambda v$. So $(Z - \lambda I)v = 0$. Solving for λ we have $\det(Z - \lambda I) = 0$. Meaning $(1-\lambda)(1-\lambda) = 0$. Thus we have $\lambda = 1$ being the only eigenvalue. We then find the eigenvector corresponding to this eigenvalue to be

$$(Z - \lambda I)v = (Z - I)v = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} v = 0$$

meaning $0v_1 + 0v_2 = 0$ and $v_1 + 0v_2 = 0$. So $v_1 = 0$ and v_2 arbitrary. So we only have the normalized eigenvector of $|1\rangle$. But $|1\rangle\langle 1| = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ which cannot represent Z thus it is not diagonalizable.

2.13

Let $|w\rangle$ and $|v\rangle$ be any two vectors. Then

$$((|w\rangle\langle v|)^\dagger |y\rangle, |x\rangle) = (|y\rangle, (|w\rangle\langle v|)|x\rangle) \text{ By definition of hermitian} =$$

$$\langle y|w\rangle\langle v|x\rangle = \langle y|w\rangle(|v\rangle, |x\rangle) = ((\langle y|w\rangle)^* |v\rangle, |x\rangle) \text{ Conjugate linear} =$$

$$(\langle w|y\rangle |v\rangle, |x\rangle) \text{ Definition of inner product} = (|v\rangle\langle w|y\rangle, |x\rangle)$$

Thus we have $(|w\rangle\langle v|)^\dagger = |v\rangle\langle w|$ as required

2.14

Let A be any linear operator on a Hilbert space V and let $|v\rangle, |w\rangle \in V$. Then

$$\left(\left(\sum_i a_i A_i\right)^\dagger |v\rangle, |w\rangle\right) = \left(|v\rangle, \sum_i a_i A_i |w\rangle\right) = \langle v| \sum_i a_i A_i |w\rangle =$$

$$\sum_i a_i(|v\rangle, A_i |w\rangle) = \sum_i a_i(A_i^\dagger |v\rangle, |w\rangle) = \left(\sum_i a_i A_i^\dagger |v\rangle, |w\rangle\right)$$

Thus we have

$$\left(\sum_i a_i A_i\right)^\dagger = \sum_i a_i A_i^\dagger$$

as required

2.15

Let A be any linear operator on a Hilbert space V and let $|v\rangle, |w\rangle \in V$. Then

$$((A^\dagger)^\dagger |v\rangle, |w\rangle) = (|v\rangle, A^\dagger |w\rangle) = (A^\dagger |w\rangle, |v\rangle)^* = (|w\rangle, A|v\rangle)^* = (A|v\rangle, |w\rangle)$$

and so $(A^\dagger)^\dagger = A$ as required.

2.16

Let P be any projector. Then

$$P^2 = \sum_i^k \sum_j^k |i\rangle \langle i| |j\rangle \langle j|$$

But we have $\langle i|j\rangle = 0$ when $i \neq j$, and $\langle i|j\rangle = 1$ when $i = j$. That means

$$\sum_i^k \sum_j^k |i\rangle \langle i| |j\rangle \langle j| = \sum_i^k |i\rangle \langle i| = P$$

Thus we have $P^2 = P$ as required.

2.24

Let A be an arbitrary operator. We have

$$A = \frac{A + A + A^\dagger - A^\dagger}{2} = \frac{(A + A^\dagger) + (A - A^\dagger)}{2} = \frac{(A + A^\dagger) + (A - A^\dagger)}{2} =$$

$$\frac{(A + A^\dagger) + (A - A^\dagger)}{2} = \frac{(A + A^\dagger) + i(iA^\dagger - iA)}{2}$$

Now define

$$B = \frac{(A + A^\dagger)}{2} \quad \textit{and} \quad C = \frac{(iA^\dagger - iA)}{2}$$

Then

$$B^\dagger = \frac{(A + A^\dagger)^\dagger}{2} = \frac{(A^\dagger + (A^\dagger)^\dagger)}{2} = \frac{(A + A^\dagger)}{2} = B$$

Meaning B is hermitian. Also

$$C^\dagger = \frac{(iA^\dagger - iA)^\dagger}{2} = \frac{(-i(A^\dagger)^\dagger + iA^\dagger)}{2} = \frac{(iA^\dagger - iA}{2} = C$$

and so C is hermitian. Since we have $A = B + iC$, we can thus conclude that any arbitrary operator can indeed be written as $A = B + iC$ where B and C are hermitian

Let P be a positive operator. Then $P = B + iC$ where B and C are hermitian. Now consider $(|\psi\rangle, A|\psi\rangle)$. We have

$$(|\psi\rangle, A|\psi\rangle) = \langle\psi| A |\psi\rangle = \langle\psi| (B + iC) |\psi\rangle = \langle\psi| B |\psi\rangle + i \langle\psi| C |\psi\rangle$$

But because A is positive, we must have $\langle\psi| B |\psi\rangle + i \langle\psi| C |\psi\rangle \geq 0$ and real. That means

$$(\langle\psi| B |\psi\rangle + i \langle\psi| C |\psi\rangle) = (\langle\psi| B |\psi\rangle + i \langle\psi| C |\psi\rangle)^* = \langle\psi| B |\psi\rangle - i \langle\psi| C |\psi\rangle$$

But

$$B - iC = A^\dagger$$

and so

$$\langle\psi| B |\psi\rangle - i \langle\psi| C |\psi\rangle = \langle\psi|A^\dagger\psi\rangle$$

We thus have $\langle\psi|A^\dagger\psi\rangle = \langle\psi|A^\dagger\psi\rangle$ and so we can conclude that $A^\dagger = A$ as required.

2.25

Let A be any operator. Then $A = B + iC$ where B and C are hermitian. Then

$$AA^\dagger = (B+iC)(B+iC)^\dagger = (B+iC)(B-iC) = (B+iC)(B-iC) = B^2 + C^2$$

Since B is hermitian and C is hermitian, we have a spectral decomposition such that $B = \sum_i \lambda_i |v_i\rangle \langle v_i|$ and $C = \sum_i \gamma_i |w_i\rangle \langle w_i|$ where λ_i, γ_i are real and $|v_i\rangle$, $|w_i\rangle$ are orthonormal bases. Then

$$AA^\dagger = \sum_i \lambda_i |v_i\rangle \langle v_i| \sum_i \lambda_i |v_i\rangle \langle v_i| + \sum_i \gamma_i |w_i\rangle \langle w_i| \sum_i \gamma_i |w_i\rangle \langle w_i| =$$

$$\sum_i \lambda_i^2 |v_i\rangle \langle v_i| + \sum_i \gamma_i^2 |w_i\rangle \langle w_i|$$

So

$$\langle\psi| AA^\dagger |\psi\rangle = \sum_i \lambda_i^2 \langle\psi| |v_i\rangle \langle v_i| |\psi\rangle + \sum_i \gamma_i^2 \langle\psi| |w_i\rangle \langle w_i| |\psi\rangle =$$

$$\sum_i \lambda_i^2 |\langle\psi|v_i\rangle|^2 + \sum_i \gamma_i^2 |\langle\psi|w_i\rangle|^2$$

But we have $\gamma_i^2 |\langle\psi|w_i\rangle|^2, \lambda_i^2 |\langle\psi|v_i\rangle|^2 \geq 0$ are both real and positive. Thus

$$\langle\psi| AA^\dagger |\psi\rangle = \sum_i \lambda_i^2 |\langle\psi|v_i\rangle|^2 + \sum_i \gamma_i^2 |\langle\psi|w_i\rangle|^2 \geq 0$$

and so $AA^\dagger$ is indeed a positive operator as required.

2.26

We have

$$|\psi\rangle^{\otimes 2} = \frac{(|0\rangle + |1\rangle)}{\sqrt{2}} \otimes \frac{(|0\rangle + |1\rangle)}{\sqrt{2}} = \frac{1}{2}((|0\rangle + |1\rangle) \otimes |0\rangle + (|0\rangle + |1\rangle) \otimes |1\rangle) =$$

$$\frac{1}{2}(|0\rangle |0\rangle + |0\rangle |1\rangle + |0\rangle |1\rangle + |1\rangle |1\rangle)$$

With the Kronecker product, we have

$$|\psi\rangle^{\otimes 2} = \frac{1}{\sqrt{2}} \begin{bmatrix} |\psi\rangle \\ |\psi\rangle \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

2.34

We first look for the spectral decomposition of

$$A = \begin{bmatrix} 4 & 3 \\ 3 & 4 \end{bmatrix}$$

So we solve for the eigenvalues. We have $(4-\lambda)^2 - 9 = 0$. Thus $\lambda = 4 \pm 3$, meaning $\lambda_1 = 1$ and $\lambda_2 = 7$ are the two eigenvalues of A. Solving for the eigenvector we obtain

$$\begin{bmatrix} 3 & 3 \\ 3 & 3 \end{bmatrix} |v\rangle = 0 \quad \begin{bmatrix} -3 & 3 \\ 3 & -3 \end{bmatrix} |w\rangle = 0$$

meaning we have $v_1 + v_2 = 0$, thus $v_2 = -v_1$ and so $|v\rangle = \frac{1}{\sqrt{2}}(1, -1)$ is a normalized eigenvector. We also have $-w_1 + w_2 = 0$, so $w_1 = w_2$, and $|w\rangle = \frac{1}{\sqrt{2}}(1, 1)$ is another normalized eigenvector. The two are also orthogonal since $\langle w|v\rangle = 0$. We then have

$$A = 7\,|w\rangle\langle w| + |v\rangle\langle v|$$

Thus

$$\sqrt{A} = \sqrt{7}\,|w\rangle\langle w| + |v\rangle\langle v| = \frac{1}{2} \begin{bmatrix} \sqrt{7}+1 & \sqrt{7}-1 \\ \sqrt{7}-1 & \sqrt{7}+1 \end{bmatrix}$$

and

$$\log(A) = \frac{1}{2} \begin{bmatrix} \log 7 + 1 & \log 7 - 1 \\ \log 7 - 1 & \log 7 + 1 \end{bmatrix}$$

2.42

$$\frac{[A,B] + \{A,B\}}{2} = \frac{AB - BA + AB + BA}{2} = \frac{2AB}{2} = AB$$

as required

2.44

We have $AB - BA = 0$ and $AB + BA = 0$. So $AB = BA$ and $-AB = BA$. Meaning $AB = -AB$. So $AB + AB = 0$. Then $A(2B) = 0$. Applying A^{-1} to both sides we then get $2B = 0$. Thus $B = 0$ as required.

2.45

We have $[A,B]^\dagger = (AB - BA)^\dagger = (AB)^\dagger - (BA)^\dagger = B^\dagger A^\dagger - A^\dagger B^\dagger = [B^\dagger, A^\dagger]$

2.48

The polar decomposition of a positive matrix P has $J = \sqrt{P^\dagger P}$ and $K = \sqrt{PP^\dagger}$, but because P is positive, we have $P = P^\dagger$. So $J = P$ and $K = P$. Meaning $P = UP = PU$. But the identity matrix $I = U$ is unitary and satisfies this so $P = IP = PI$. The polar decomposition of a unitary matrix U has $J = \sqrt{U^\dagger U}$ and $K = \sqrt{UU^\dagger}$. But because U is unitary we have $UU^\dagger = I = U^\dagger U$ thus $J = I$ and $K = I$. So we have $U = UI = IU$. The polar decomposition of a hermitian matrix H has $J = \sqrt{H^\dagger H}$ and $K = \sqrt{HH^\dagger}$. But H is hermitian so $H^\dagger = H$ thus $J = H$. We have $H = UH = HU$. The identity matrix I which is also unitary satisfies $H = IH = HI$.

2.49

Consider the normal matrix N. We then have $J = \sqrt{N^\dagger N}$ and $K = \sqrt{NN^\dagger}$. But because N is normal we have $J = K$ and so $N = UJ = JU$ for some unitary matrix U. Let $\sum_i a_i |i\rangle \langle i|$ be the spectral decomposition of J and let $\sum_j b_j |j\rangle \langle j|$ be the spectral decomposition of U. Then the outer product representation is $\sum_i a_i |i\rangle \langle i| \sum_j b_j |j\rangle \langle j|$

2.51

The Hadamard gate

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

has

$$H^\dagger = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

We then have

$$H^\dagger H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Thus H is unitary as required

2.52

Since $H^\dagger = H$, we can conclude from 2.51 that $H^2 = H^\dagger H = I$ as required.

2.53

For the eigenvalues we have $(\frac{1}{\sqrt{2}} - \lambda)(-\frac{1}{\sqrt{2}} - \lambda) - \frac{1}{2} = 0$. So $\lambda^2 - 1 = 0$. Leaving us with $\lambda_1 = 1$ and $\lambda_2 = -1$ as eigenvalues. That in turn results in

$$\begin{bmatrix} \frac{1}{\sqrt{2}} - 1 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} - 1 \end{bmatrix} v = 0$$

Thus $(\frac{1}{\sqrt{2}} - 1)v_1 + \frac{1}{\sqrt{2}} v_2 = 0$, and $\frac{1}{\sqrt{2}} v_1 + (-\frac{1}{\sqrt{2}} - 1)v_2 = 0$. Then $(1 - \sqrt{2})(-\frac{2}{\sqrt{2}} - 1)v_2 = \frac{1}{\sqrt{2}} v_2$. Meaning v_2 is arbitrary, and since $v_1 = (1 + \sqrt{2})v_2$, we have $(1 + \sqrt{2}, 1)$ as an eigenvector with eigenvalue $\lambda_1 = 1$. For $\lambda_2 = -1$, we have

$$\begin{bmatrix} \frac{1}{\sqrt{2}} + 1 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} + 1 \end{bmatrix} w = 0$$

That results in $(\frac{1}{\sqrt{2}} + 1)w_1 + \frac{1}{\sqrt{2}} w_2 = 0$ and $\frac{1}{\sqrt{2}} w_1 + (-\frac{1}{\sqrt{2}} + 1)w_2 = 0$. Then $\frac{1}{\sqrt{2}} w_2 = (1 + \sqrt{2})(-\frac{1}{\sqrt{2}} + 1)w_2$ which once again means w_2 is arbitrary. Since

$w_1 = (1-\sqrt{2})w_2$, we have $(1-\sqrt{2}, 1) = w$ being the other eigenvector with eigenvalue $\lambda_2 = -1$.

2.54

Since A and B are commuting Hermitian operators, we then have A and B being simultaneously diagonalizable. So $A = \sum_i a_i |i\rangle \langle i|$ and $\sum_i b_i |i\rangle \langle i|$. Then

$$\exp(A)\exp(B) = (\sum_i \exp(a_i)|i\rangle\langle i|)(\sum_i \exp(b_i)|i\rangle\langle i|) =$$

$$\sum_{ij} \exp(a_j)|j\rangle\langle j|\exp(b_i)|i\rangle\langle i| = \sum_{ij}\exp(a_j)\exp(b_i)|j\rangle\langle j|i\rangle\langle i|$$

But because $|i\rangle$ is an orthonormal set of eigenvectors, we have

$$\exp(A)\exp(B) = \sum_i \exp(a_i)\exp(b_i)|i\rangle\langle i| = \exp(A)\exp(B) =$$

$$\sum_i \exp(a_i+b_i)|i\rangle\langle i| = \exp(A+B)$$

as required

2.55

We have

$$U^\dagger(t_1,t_2) = \exp\left[\frac{iH^\dagger(t_2-t_1)}{\hbar}\right]$$

Then due to H being Hermitian

$$U^\dagger U = \exp\left[\frac{iH^\dagger(t_2-t_1)}{\hbar}\right]\exp\left[\frac{-iH(t_2-t_1)}{\hbar}\right] = \exp[0] = I$$

as required.

2.57 (U)

We have an application of L_l on some state $|\psi\rangle$ being

$$\frac{L_l|\psi\rangle}{\sqrt{\langle\psi|L_l^\dagger L_l|\psi\rangle}}$$

Then an application of M_m results in

$$\frac{M_l L_l|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}\sqrt{\langle\psi|L_l^\dagger L_l|\psi\rangle}} = \frac{M_l L_l|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}\sqrt{\langle\psi|L_l^\dagger L_l|\psi\rangle}}$$

2.58

The average observed value would be $\langle\psi|M|\psi\rangle$. Since $|\psi\rangle$ is in an eigenstate of M, we have $\langle\psi|M|\psi\rangle = \langle\psi|m|\psi\rangle = m\langle\psi|\psi\rangle = 1$. The standard deviation is then $\langle M^2\rangle - \langle M\rangle^2 = \langle\psi|M^2|\psi\rangle - m^2\langle\psi|\psi\rangle = m^2\langle\psi|\psi\rangle - m^2\langle\psi|\psi\rangle = 0$.

2.59

The average value would be $\langle 0| X |0\rangle = \langle 0|1\rangle = 0$. The standard deviation is then $\langle X^2\rangle - \langle X\rangle^2 = \langle X^2\rangle = \langle 0| X^2 |0\rangle = \langle 0|0\rangle = 1$.

2.60

We have

$$\vec{v}\cdot\vec{\sigma} = \begin{bmatrix} v_3 & v_1 - iv_2 \\ v_1 + iv_2 & -v_3 \end{bmatrix}$$

So

$$\det\left(\begin{bmatrix} v_3 - \lambda & v_1 - iv_2 \\ v_1 + iv_2 & -v_3 - \lambda \end{bmatrix}\right) = 0$$

Thus we have $-(v_3 - \lambda)(v_3 + \lambda) - (v_1 - iv_2)(v_1 + iv_2) = 0$. This results in $-v_3^2 + \lambda^2 - v_1^2 - v_2^2 = 0$ and so $\lambda^2 = v_3^2 + v_1^2 + v_2^2$. But since $\vec{v}$ is a unit vector, we have $\lambda^2 = 1$ and so $\lambda = \pm 1$ as eigenvalues. We then have $(v_3 \mp 1)w_1 + (v_1 - iv_2)w_2 = 0$ as well as $(v_1 + iv_2)w_1 - (v_3 \pm 1)w_2 = 0$. Thus we have

$$w_1 = \frac{(v_3 \pm 1)}{v_1 + iv_2} w_2$$

and so the eigenvectors are

$$\begin{bmatrix} v_3 \pm 1 \\ v_1 + iv_2 \end{bmatrix}$$

which has a magnitude of $\sqrt{v_3^2 \pm 2v_3 + 1 + v_1^2 + v_2^2} = \sqrt{\pm 2v_3 + 2} = \sqrt{2(1 \pm v_3)}$ resulting in normalized eigenvectors of

$$\frac{1}{\sqrt{2}}\begin{bmatrix} \frac{v_3 \pm 1}{\sqrt{1 \pm v_3}} \\ \frac{v_1 + iv_2}{\sqrt{1 \pm v_3}} \end{bmatrix}$$

Since $v_1^2 + v_2^2 = 1 - v_3^2 = (1 - v_3)(1 + v_3)$, we then have

$$P_\pm = \frac{1}{2}\begin{bmatrix} \frac{v_3 \pm 1}{\sqrt{1 \pm v_3}} \\ \frac{v_1 + iv_2}{\sqrt{1 \pm v_3}} \end{bmatrix}\begin{bmatrix} \frac{v_3 \pm 1}{\sqrt{1 \pm v_3}} & \frac{v_1 - iv_2}{\sqrt{1 \pm v_3}} \end{bmatrix} =$$

$$\frac{1}{2}\begin{bmatrix} 1 \pm v_3 & \pm(v_1 - iv_2) \\ \pm(v_1 + iv_2) & 1 \pm v_3 \end{bmatrix} = \frac{1}{2}\left(I \pm \vec{v}\cdot\sigma\right)$$

as required

2.61

The probability of getting $+1$ would be

$$\frac{1}{2}\langle 0|\left(I + \vec{v}\cdot\sigma\right)|0\rangle = \frac{1}{2}(1 + \langle 0|\vec{v}\cdot\sigma|0\rangle) = \frac{1}{2}(1 + v_3)$$

and if $+1$ is measured, we have a state

$$\frac{P_+|\psi\rangle}{\sqrt{\frac{1}{2}(1 + v_3)}} = \frac{1}{\sqrt{\frac{1}{2}(1 + v_3)}}\begin{bmatrix} 1 + v_3 \\ v_1 + iv_2 \end{bmatrix}$$

2.63

We have $E_m = M_m^\dagger M_m$. Using polar decomposition, we have $J = \sqrt{M^\dagger M} = \sqrt{E_m}$. Thus we have $M_m = U_m\sqrt{E_m}$ for some unitary matrix U_m as required.

2.65

Consider the basis

$$|v\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad |w\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

In this basis we have the two states as $(1,0)$ and $(0,1)$. Suppose for contradiction that they differ by a relative phase in this basis. Then we have $1 = \exp(i\theta) * 0 = 0$, a contradiction. Therefore they are not the same up to a relative phase in this basis.

2.66

The average value is defined as

$$\frac{1}{2}\left(|00\rangle + |11\rangle, X_1 Z_2(|00\rangle + |11\rangle)\right) =$$

$$\frac{1}{2}\left(|00\rangle + |11\rangle, X_1|0\rangle Z_2|0\rangle + X_1|1\rangle Z_2|1\rangle\right) =$$

$$\frac{1}{2}\left(|00\rangle + |11\rangle, |1\rangle|0\rangle + |0\rangle(-|1\rangle)\right) =$$

$$\frac{1}{2}\begin{bmatrix}1 & 0 & 0 & 1\end{bmatrix}\begin{bmatrix}0\\-1\\1\\0\end{bmatrix} = 0$$

as required.

2.71

Suppose ρ is a density operator. Then $tr(\rho) = 1$ and is also a positive operator. It then has a spectral decomposition $\sum_i \lambda_i |i\rangle\langle i|$, where $\sum_i \lambda_i = 1$ and $\lambda_i \geq 0$. So $\rho^2 = \sum_i \lambda_i |i\rangle\langle i| \sum_j \lambda_j |j\rangle\langle j| = \sum_{ij} \lambda_j\lambda_i |i\rangle\langle i|j\rangle\langle j| = \sum_i \lambda_i^2 |i\rangle\langle i|$. Thus $tr(\rho^2) = \sum_i \lambda_i^2$. But we must have $0 \leq \lambda_i \leq 1$ and so $0 \leq \lambda_i^2 \leq \lambda_i \leq 1$ meaning $\sum_i \lambda_i^2 \leq \sum_i \lambda_i = 1$. Thus we have $tr(\rho^2) \leq 1$.

Suppose $tr(\rho^2) = 1$. Then we have $\sum_i \lambda_i^2 = \sum_i \lambda_i$. But we have $\lambda_i^2 \leq \lambda_i \leq 1$. So $\lambda_i^2 = \lambda_i$. Which is only possible when $\lambda_i = 1$ or $\lambda_i = 0$. Since $\sum_i \lambda_i = 1$, we must have $\lambda_i = 1$ for some i, and 0 for all other i. Meaning we are left with $\rho = |i\rangle\langle i|$ for some i. So by definition is a pure state as required.

Now suppose ρ is a pure state. Then $\rho = |\psi\rangle\langle\psi|$ where $|\psi\rangle$ is a state vector. We then have $tr(\rho) = \langle\psi|\psi\rangle = 1$ as required.

2.72

1) Let ρ be a density matrix for a mixed state qubit. Then $\rho = a_1 I + a_2 X + a_3 Y + a_4 Z$. Since ρ is positive, it must also be hermitian. Thus $\rho = a_1^* I + a_2^* X^\dagger + a_3^* Y^\dagger + a_4^* Z\dagger$. But the Pauli matrices are Hermitian thus $\rho = a_1^* I + a_2^* X + a_3^* Y + a_4^* Z$. But that in turn means $a_i = a_i^*$ due to the Pauli matrices being linearly independent. Thus we have a_i is real. We must also have $tr(\rho) = 1$. Meaning

$1 = a_1 tr(I) + a_2 tr(X) + a_3 tr(Y) + a_4 tr(Z) = 2a_1 + 0 + 0 + 0 = 2a_1$. Meaning $a_1 = 1/2$ and $a_2..a_4$ can be arbitrary reals. So letting $\vec{r} = (2a_2, 2a_3, 2a_4)$ and $\sigma = (X, Y, Z)$, we have

$$\rho = \frac{1}{2}I + a_2 X + a_3 Y + a_4 Z = \frac{1}{2}I + \frac{1}{2}\vec{r} \cdot \vec{\sigma} = \frac{I + \vec{r} \cdot \vec{\sigma}}{2}$$

as required

2) We have $\vec{r} = (0, 0, 0)$. Since $0 \cdot \vec{\sigma} = 0$. So

$$\rho = \frac{1}{2}I + \frac{1}{2}\vec{r} \cdot \vec{\sigma} = \frac{1}{2}I$$

3) Suppose ρ is pure. Then $\rho = |\psi\rangle \langle\psi|$ for some pure state $|\psi\rangle$. We have

$$\rho = \frac{I + \vec{r} \cdot \vec{\sigma}}{2} \quad tr(\rho^2) = 1$$

Since

$$tr(\rho^2) = tr\left(\frac{I + \vec{r} \cdot \vec{\sigma}}{2} \frac{I + \vec{r} \cdot \vec{\sigma}}{2}\right) = tr\left(\frac{I + 2\vec{r} \cdot \vec{\sigma} + (\vec{r} \cdot \vec{\sigma})(\vec{r} \cdot \vec{\sigma})}{4}\right) =$$

$$\frac{1}{4} tr\left(I + 2\vec{r} \cdot \vec{\sigma} + (r_1 X + r_2 Y + r_3 Z)(r_1 X + r_2 Y + r_3 Z)\right) =$$

$$\frac{1}{4} tr(I + 2\vec{r} \cdot \vec{\sigma} + r_1^2 X^2 + r_2 r_1 YX + r_3 r_1 ZX + r_1 r_2 XY +$$

$$r_2^2 Y^2 + r_3 r_2 ZY + r_1 r_3 XZ + r_2 r_3 YZ + r_3^2 Z^2) =$$

$$\frac{1}{4} tr(I + 2\vec{r} \cdot \vec{\sigma} + r_1^2 X^2 + r_2^2 Y^2 + r_3^2 Z^2) =$$

$$\frac{1}{4}(tr(I) + 2tr(\vec{r} \cdot \vec{\sigma}) + r_1^2 tr(X^2) + r_2^2 tr(Y^2) + r_3^2 tr(Z^2) = \frac{1}{4}(2 + 2r_1^2 + 2r_2^2 + 2r_3^2)$$

That means $\frac{1}{2}(1 + r_1^2 + r_2^2 + r_3^2) = 1$ and so we have $||\vec{r}|| = r_1^2 + r_2^2 + r_3^2 = 1$ as required.

Now suppose $||\vec{r}|| = r_1^2 + r_2^2 + r_3^2 = 1$. We had shown that

$$tr(\rho^2) = \frac{1}{4}(2 + 2r_1^2 + 2r_2^2 + 2r_3^2)$$

meaning

$$tr(\rho^2) = \frac{1}{4}(2 + 2) = 1$$

as required thus proving the equality

4) We have for pure states, $\rho = |\psi\rangle \langle\psi|$ and the Bloch vector having the property $||\vec{r}|| = 1$. Since $|\psi\rangle$ is a qubit, we have $|\psi\rangle = a|0\rangle + b|1\rangle$ and $|| |\psi\rangle ||^2 = 1$. So we have $\rho = (a|0\rangle + b|1\rangle)(a^* \langle 0| + b^* \langle 1|) = a^* a |0\rangle \langle 0| +$

2.74

Suppose $|a\rangle$ and $|b\rangle$ are pure states of their respective systems and the composite system is in state $|a\rangle |b\rangle$. Then the density operators for A is $\rho_A = |a\rangle \langle a|$ and for B is $\rho_B = |b\rangle \langle b|$. The density operator of the composite system is then $|ab\rangle \langle ab|$. Then we have $\rho^A = tr_b(|ab\rangle \langle ab|) = |a\rangle \langle a| \langle b|b\rangle$, but since $|b\rangle$ is a pure state we have $\langle b|b\rangle = 1$ and so $\rho^A = |a\rangle \langle a| = \rho_A$ which we established as a pure state as required.

2.75

For the bell state

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

we have

$$\rho = \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)\left(\frac{\langle 00| + \langle 11|}{\sqrt{2}}\right) = \frac{|00\rangle \langle 00| + |00\rangle \langle 11| + |11\rangle \langle 00| + |11\rangle \langle 11|}{2}$$

The reduced density operator for A has already been shown in the textbook so we have

$$\rho^B = tr_A\left(\frac{|00\rangle \langle 00| + |00\rangle \langle 11| + |11\rangle \langle 00| + |11\rangle \langle 11|}{2}\right) =$$

$$\frac{tr_A(|00\rangle \langle 00|) + tr_A(|00\rangle \langle 11|) + tr_A(|11\rangle \langle 00|) + tr_A(|11\rangle \langle 11|)}{2} =$$

$$\frac{|0\rangle \langle 0| + |1\rangle \langle 1|}{2} = \frac{I}{2}$$

For the bell state

$$\frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

We have

$$\rho = \left(\frac{|00\rangle - |11\rangle}{\sqrt{2}}\right)\left(\frac{\langle 00| - \langle 11|}{\sqrt{2}}\right) = \frac{|00\rangle \langle 00| - |00\rangle \langle 11| - |11\rangle \langle 00| + |11\rangle \langle 11|}{2}$$

And so

$$\rho^B = tr_A\left(\frac{|00\rangle \langle 00| - |00\rangle \langle 11| - |11\rangle \langle 00| + |11\rangle \langle 11|}{2}\right) =$$

$$\frac{tr_A(|00\rangle \langle 00|) - tr_A(|00\rangle \langle 11|) - tr_A(|11\rangle \langle 00|) + tr_A(|11\rangle \langle 11|)}{2} =$$

$$\frac{|0\rangle \langle 0| + |1\rangle \langle 1|}{2} = \frac{I}{2}$$

The same can be said about ρ^A due to symmetry.

3 Introduction to Computer Science

3.3

Suppose we have a turing machine with two tapes. The top one takes as it's input x and the rest is blanks, while the second tape starts off as all blanks, b. The alphabet we consider will have $0, 1, b, \triangleright$, we will have states q_s, f, r, b_0, q_h and our program lines will be

$$\langle q_s, \triangleright, \triangleright, f, \triangleright, \triangleright, 1, 1\rangle$$

$$\langle f, 1, b, f, 1, b, 1, 0\rangle$$

$$\langle f, 0, b, f, 0, b, 1, 0\rangle$$

$$\langle f, b, b, r, b, b, -1, 0\rangle$$

$$\langle r, 1, b, r, b, 1, -1, 1\rangle$$

$$\langle r, 0, b, r, b, 0, -1, 1\rangle$$

$$\langle r, \triangleright, b, q_h, \triangleright, b, 0, 0\rangle$$

This will have the reverse of the input on the second tape

3.5

Suppose for contradiction that there exists an algorithm, H which can determine if the turing machine M will halt when given a blank tape. Let H return true if M does halt for a blank tape and false otherwise. Let M be defined so that when H is true, M does not halt for a blank tape, and when H is false M does halt for a blank tape. In the case M does halt, H would have returned true, meaning M doesn't halt, a contradiction. In the case M doesn't halt H would have returned false, meaning M does halt, a contradiction. In both cases we have a contradiction and so there does not exist such an algorithm to determine if a turing machine halts.

3.6

Suppose for contradiction there does exist a probabilistic turing machine, M which outputs $h_p(x)$ with probability of correctness strictly greater than $1/2$ for all x. Let x be the machine defined as such, x halts if M outputs 0 otherwise it doesn't halt. In the case M outputs 0, we have two cases. In the case M is correct, we would have M returning 0 greater than $1/2$ of the time. But that would mean, x halts greater than $1/2$ of the time, a contradiction. In the case M is wrong, then M would return 0 less than $1/2$ and halt less than $1/2$ of the time but that would mean M is correct, a contradiction. In the case M returns 1, we have two cases. In the case M is correct, M would return 1, greater than $1/2$ of the time leading to x not halting more than $1/2$ of the time and so it would halt less than $1/2$ of the time, a contradiction since M returning 1 being correct means x halts $1/2$ of the time or greater. In the case M is wrong, we would have halting greater than $1/2$ the time, but that would mean M is right, a contradiction. Therefore such an M cannot exist as required.

3.9

Suppose $f(n) \in O(g(n))$ then $f(n) \leq cg(n)$ for some constant c and all $n \geq n_0$ for some n_0. But that also means, $\frac{1}{c}f(n) \leq g(n)$. Since $\frac{1}{c}$ is a constant, we now have $g(n) \in \Omega(f(n))$. Suppose $g(n) \in \Omega(f(n))$ Then $cg(n) \leq f(n)$ for some constant c and all $n \geq n_0$ for some n_0. That then means $g_(n) \leq \frac{1}{c}f(n)$ and so we can conclude $g(n) \in \Omega(f(n))$ as required. This proves the equivalence relationship. Now $f(n) \in \Theta(g(n))$ if and only if $f(n) \in O(g(n))$ and $f(n) \in \Omega(g(n))$. This is true if and only if $g(n) \in \Omega(f(n))$ and $g(n) \in O(f(n))$, which is true if and only if $g(n) \in \Theta(f(n))$ as required.

3.10

Suppose $g(n)$ is a polynomial of degree k. Let $l \geq k$, then $n^l \geq n^k$ for all $n \geq 1$. Since we have

$$g(n) = \sum_{i=0}^{k} a_i n^i$$

and $a_i n^l \geq a_i n^i$ for all $n \geq 1$, we can conclude that

$$\sum_{i=0}^{k} a_i n^i \leq n^l \sum_{i=0} a_i$$

for all $n \geq 1$. So $g(n) \in O(n^l)$ for any $l \geq k$.

3.11

Suppose $k \geq 0$, we have $2^{\log(n)} = n$, and $n \leq 2^n$ for all n. Then $\log(n) \leq n$. Since $n \leq n^k$ for all $k > 0$ and $n \geq 1$, we can thus conclude $\log(n) \leq n^k$ for all $k > 0$ and $n \geq 1$ meaning $\log(n) \in O(n^k)$ for all $k > 0$ as required.

3.15 (U)

We will do proof using induction. For base case $n = 1$, we will have 1 possible initial ordering and after $k \geq 0$ swaps, we would have the 1 possible initial ordering sorted. Thus we have at most 2^k initial offering sorted. Now suppose as inductive hypothesis that for $n > 0$ we have $S_{nk} \leq 2^k$, where S_{nk} is the amount of initial orderings that have been sorted after k compare and swaps of an element list with n elements. Now consider a list of $n + 1$ elements. We first consider sorting the first n elements. By inductive hypothesis, we would have $S_{nk} \leq 2^k$ for k swap operations. But in order for the $n + 1$ elements to be sorted, we must also have the last element being in the correct place, so given the first n elements, are sorted, only $1/(n + 1)$ of the possible combinations would be fully sorted. So we have $S_{nk}/(n + 1) \leq 2^k$ will be sorted when the first n elements are sorted. For the final element to be sorted, we would have at most $n+1$ extra swaps, each swap only bringing in one additional permutation, This would still mean that the amount sorted after k swaps is at most 2^k as required. Since we can sort at most 2^k permutations, after k swaps, and a list of n element, has $n!$ permutations, we would need at least $2^k \geq n!$, so

$$k \geq \log(n!) = \sum_{i=1}^{n} \log(i)$$

and since we have for $n \geq 1$, we have

$$\sum_{i=1}^{n} \log(i) = \log(n!) \leq n \log(n)$$

We then have $n! \leq n^n$ for $n \geq 1$

3.17

Suppose a polynomial-time algorithm for finding the factors of a number m exists. Then the factoring decision problem is easily answered if we apply the given algorithm and compare its results to see if there are any factors less than l that aren't 1. This would add at most a factor of l to the time complexity. Thus the factoring decision problem is still polynomial-time. Therefore we can conclude that it is in **P** by definition of **P**. Now suppose the factoring decision problem is in **P**. Then given a composite integer m and $l < m$, we can determine if m has a non-trivial factor less than l in polynomial time. Now consider the algorithm defined as so, check inductively starting from 1, if there are any non-trivial factors of m less than l. At the lowest l that returns true, we would know that $l-1$ is a factor of m. This will take no more than m factoring decisions, so we have $m*T$ where T is the time for a factoring decision. We then divide m by $l-1$ and obtain a new factor s. Applying the factoring decision algorithm as we did for m, except with s as the new number, we obtain a factor p of both s and m. Dividing s by p we get another factor of m lets call n. We then apply the above process to n and continue until the factoring decision can't find anymore factors. This will take at most m more uses of m more factoring decisions and $m * m * T + m * T$. But $T \leq Cm^k$ for some k since it is a polynomial-time algorithm. Thus $m * m * T + m * T \leq Cm^{k+2} + Cm^{k+1}$ which is in the class $O(m^{k+2})$ and is still polynomial time as required.

3.19

Let m,n be the vertices we are considering for reachability. Start at m and consider the recursive method defined as so. Mark current node as visited. Check if any of the edges connected to the current vertex lead to n. if there is, we are done. if not traverse an edge that does not lead to a visited vertex. If none of the edges lead to a vertex that hasn't been visited, return to the previous vertex or in the case that there is no previous vertex, we are done and conclude that n cannot be reached. Repeat above steps until one of the stopping cases are met. This algorithm will determine reachability in $O(n^2)$ time since at each node we will have visited each vertex at most $n-1$ times and with a total of n vertices, we would have $n(n-1)$ visits and a complexity of $O(n^2)$ as required. Then by checking from vector m if all the other $n-1$ nodes are reachable, we can confirm if the graph is connected. This would be in the class $O(n^3)$ as required.

3.20

Let G be a connected graph of t vertices. Suppose G contains a Euler cycle. Suppose for contradiction that one of the vertex has an odd number $m = 2n-1$ edges. Since G contains a Euler cycle, there exists a cycle v_j, such that each of the m edges are traversed exactly once. Then for any edge of the vertex, we

must have $l = \{v_k, v_{k+1}\}$ for some k and $l \neq \{v_j, v_{j+1}\}$ where $j \neq k$. So when also considering the definition of a cycle, we must have $\{v_k, v_{k+1}\} \neq \{v_{k-1}, v_k\}$. These two are edges of the vertex which are different. So by following the above procedure $n-1$ times, we will be left with one edge which has not been paired off. We must have for some k, $\{v_k, v_{k+1}\}$ being the edge. But we must have $\{v_k, v_{k+1}\} = \{v_{k-1}, v_k\}$ since all other edges have been paired off. But this is also a contradiction since that would mean the same edge appeared twice in the cycle. Therefore we have a contradiction and the vertex must have an even number of edges at each vertex. Now suppose every vertex has an even number of edges. We can create a cycle through the following procedure. Start at any vertex. Traverse a non-traversed edge that does not go back to the starting vertex and mark it as traversed, also add it to the sequence. If the only non-traversed edge is to the starting vertex, traverse that edge and we are done. Repeat until stopping case is reached and the sequence will be a eulur cycle.

3.21

Suppose L_1 is reducible to L_2 and L_2 is reducible to L_3. Then there exists a Turing machine operating in polynomial time such that given an input x, it outputs $R(x)$, and $x \in L_1$ if and only if $R(x) \in L_2$ and there exists a Turing machine operating in polynomial time such that given an input x, it outputs $F(x)$, and $x \in L_2$ if and only if $F(x) \in L_3$. We then have a Turing machine which first applies $R(x)$ and then applies $F(x)$ to $R(x)$ for a composition $F(R(x))$. This is in polynomial time since the turing machines that output $R(x)$ and $F(x)$ are in polynomial time and the composition is just the addition of the two times which would also be polynomial time. Now suppose $x \in L_1$ then $R(x) \in L_2$ and $F(R(x)) \in L_3$ as required. Now suppose $z \in L_3$. Then there is a $y \in L_2$ such that $F(y) = z$. Since $y \in L_2$, we have an $x \in L_1$ such that $R(x) = y$ and so $z = F(R(x))$ where $x \in L_1$ as required. Therefore we can conclude that L_1 is reducible to L_3.

3.22

Suppose L is complete for a complexity class, and L' is another language in the complexity class such that L reduces to L'. Let X be a language in the same complexity class as L. Then X can be reduced to L but since L can be reduced to L' we have by transitivity that X can be reduced to L'. Since X was arbitrary in the complexity class, we can conclude that all languages in the complexity class can be reduced to L' making L' complete as required.

3.29

We have from the application of the fredkin gate on inputs a, b, and c, two cases. In the case c is 1, the output after the first fredkin gate will be b, a, c. Since c doesn't change, the application of the second fredking gate will then result in a swap and so a, b, c which is just the input. In the case $c = 0$, we have no swap resulting in an output of a, b, c after the first fredkin gate. Since c stays the same, we would have no swap from the second fredkin gate, meaning the output is a, b, c as required. Thus we can conclude that applying the fredkin twice results back in the input.

4 Quantum Circuits

4.1

The normalized eigenvectors of X is $\left(\frac{1}{\sqrt{2}}(1,1), \frac{1}{\sqrt{2}}(1,-1)\right)$. The eigenvector $\frac{1}{\sqrt{2}}(1,1)$ can be expressed as

$$|D\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

This means $\cos(\theta/2) = \frac{1}{\sqrt{2}}$ and $e^{i\varphi}\sin(\theta/2) = \frac{1}{\sqrt{2}}$ and so $\theta/2 = \pi/4$ resulting in $\theta = \pi/2$. That makes $\sin(\theta/2) = \frac{1}{\sqrt{2}}$ and so $e^{i\varphi}\sin(\theta/2) = e^{i\varphi}\frac{1}{\sqrt{2}}$ resulting in $\varphi = 0$. This means we have the Bloch vector of $(1,0,0)$ for $|D\rangle$. The eigenvector $\frac{1}{\sqrt{2}}(1,-1)$ can be expressed as

$$|E\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

In this case we would have $\theta = \pi/2$ but we must have $e^{i\varphi} = -1$ and so $\varphi = \pi$. Thus we have $(-1,0,0)$ as the Bloch vector for $|E\rangle$

The normalized eigenvectors of Y is $\left(\frac{1}{\sqrt{2}}(1,-i), \frac{1}{\sqrt{2}}(1,i)\right)$. We can express the first eigenvector as

$$|F\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{i}{\sqrt{2}}|1\rangle$$

This results in $\cos(\theta/2) = 1/\sqrt{2}$ and $e^{i\varphi}\sin(\theta/2) = -i/\sqrt{2}$. This means $\theta = \pi/2$ resulting in $e^{i\varphi} = -i$. Thus $\varphi = 3\pi/2$ and so we have $(0,-1,0)$ as the Bloch vector for $|F\rangle$. The second eigenvector can be expressed as

$$|G\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle$$

which following from the previous eigenvector has $\theta = \pi/2$ and so $e^{i\varphi} = i$. Thus $\varphi = \pi/2$ and so a Bloch vector of $(0,1,0)$ representing $|G\rangle$

The normalized eigenvectors of Z is $((1,0),(0,1))$. Thus for $|1\rangle$ we must have $\cos(\theta/2) = 1$ and so we have $\theta = 0$. This results in the Bloch vector $(0,0,1)$ for $|1\rangle$. For $|0\rangle$ we must have $\cos(\theta/2) = 0$ and so $\theta = \pi$ which would result in the Bloch vector $(0,0,-1)$ corresponding to $|0\rangle$

4.2

We have

$$exp(iAx) = \cos(Ax) + i\sin(Ax) = \sum_{n=0}^{\infty}\frac{(-1)^n(Ax)^{2n}}{(2n)!} + i\sum_{n=0}^{\infty}\frac{(-1)^n(Ax)^{2n+1}}{(2n+1)!} =$$

$$\sum_{n=0}^{\infty}\frac{(-1)^n Ix^{2n}}{(2n)!} + i\sum_{n=0}^{\infty}\frac{(-1)^n Ax^{2n+1}}{(2n+1)!} = I\sum_{n=0}^{\infty}\frac{(-1)^n x^{2n}}{(2n)!} + iA\sum_{n=0}^{\infty}\frac{(-1)^n x^{2n+1}}{(2n+1)!} =$$

$$\cos(x)I + i\sin(x)A$$

as required

4.3

We have

$$R_z(\pi/4) = \begin{bmatrix} \exp(-i\pi/8) & 0 \\ 0 & \exp(i\pi/8) \end{bmatrix} \quad T = \begin{bmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{bmatrix}$$

But

$$\exp(i\pi/8)R_z(\pi/4) = \begin{bmatrix} \exp(-i\pi/8 + i\pi/8) & 0 \\ 0 & \exp(i\pi/8 + i\pi/8) \end{bmatrix} =$$

$$\begin{bmatrix} \exp(0) & 0 \\ 0 & \exp(i\pi/4) \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{bmatrix} = T$$

Thus $R_z(\pi/4) = T$ up to a global phase factor.

4.5

We have $(\hat{n} \cdot \vec{\sigma})^2 = (n_x X + n_y Y + n_z Z)(n_x X + n_y Y + n_z Z) = n_x^2 X^2 + n_x n_y YX + n_x n_z ZX + n_x n_y XY + n_y^2 Y^2 + n_z n_y ZY + n_x n_z XZ + n_y n_z YZ + n_z^2 Z^2$. But because the Pauli matrices are anti-commutative, all cross terms cancel out and we are left with, $n_x^2 X^2 + n_y^2 Y^2 + n_z^2 Z^2$. Since the inverse of pauli matrices is itself, we have $(n_x^2 + n_y^2 + n_z^2)I$. Since $\hat{n}$ is normal we can thus conclude $(\hat{n} \cdot \vec{\sigma})^2 = I$ as required.

4.7

We have

$$XYX = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} -i & 0 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = -Y$$

as required. Then we have

$$XR_y(\theta)X = \cos(\theta/2)X^2 - i\sin(\theta/2)XYX =$$

$$\cos(\theta/2)I + i\sin(\theta/2)Y = \cos(-\theta/2)I - i\sin(-\theta/2)Y = R_y(-\theta)$$

as required

4.13

$$HXH = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = Z$$

$$HYH = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \frac{1}{2}\begin{bmatrix} -i & i \\ i & i \end{bmatrix} = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix} = Y$$

$$HZH = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = X$$

4.14

Since $T = R_z(\pi/4) = \cos(\pi/4)I - i\sin(\pi/4)Z$ up to a global phase factor, we have $HTH = HR_z(\pi/4)H = \cos(\pi/4)H^2 - i\sin(\pi/4)HZH = \cos(\pi/4)I - i\sin(\pi/4)X = R_x(\pi/4)$ as required.

4.16

Since the Hadamard gate on the x_2 qubit will have the effect of

$$|00\rangle \to \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$$

$$|01\rangle \to \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle)$$

$$|10\rangle \to \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle)$$

$$|11\rangle \to \frac{1}{\sqrt{2}}(|01\rangle - |11\rangle)$$

The 4×4 matrix that would represent the given operation would be

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}$$

The Hadamard gate on the x_1 qubit will have the effect of

$$|00\rangle \to \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$$

$$|01\rangle \to \frac{1}{\sqrt{2}}(|00\rangle - |01\rangle)$$

$$|10\rangle \to \frac{1}{\sqrt{2}}(|10\rangle + |11\rangle)$$

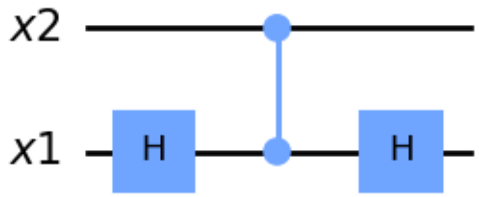
$$|11\rangle \to \frac{1}{\sqrt{2}}(|10\rangle - |11\rangle)$$

and so we have the 4×4 matrix

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}$$

4.17

Consider the two qubits x_1 and x_2. Let x_2 be the control qubit of Z and x_1. Apply H to x_1 before $C - Z$ and apply another H to x_1 after the $C - Z$. We have $|00\rangle$ becomes $|00\rangle$ since Z is not applied on the second qubit resulting in $HH = I$ being applied on the second qubit. The $|01\rangle$ becomes $|01\rangle$ by the same reasoning as above. For $|10\rangle$, it becomes $|11\rangle$ since we would have HZH applied on x_1 but $HZH = X$ which is a not gate. We have $|11\rangle$ becomes $|10\rangle$ by the same reasoning. This is a $C - NOT$ gate with control qubit x_2 and target qubit x_1 as required.



4.19

A density matrix of the state $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ will be $\rho = a_1 |00\rangle\langle 00| + a_2 |01\rangle\langle 01| + a_3 |10\rangle\langle 10| + a_4 |11\rangle\langle 11|$ where $a_1^2 + a_2^2 + a_3^2 + a_4^2 = 1$. Since the $C - NOT$ gate is

$$U = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

and $U = U^\dagger$. We have the evolution of ρ being $U\rho U = a_1 U |00\rangle\langle 00| U + a_2 U |01\rangle\langle 01| U + a_3 U |10\rangle\langle 10| U + a_4 U |11\rangle\langle 11| U = a_1 |00\rangle\langle 00| + a_2 |01\rangle\langle 01| + a_3 |11\rangle\langle 11| + a_4 |10\rangle\langle 10|$

4.20

The quantum circuit can be thought of as $(I \otimes H)(H \otimes I)U(I \otimes H)(H \otimes I)$ where U is the $C - NOT$ gate. We then have $(I \otimes H)(H \otimes I)U(I \otimes H)(H \otimes I) = (H \otimes H)U(H \otimes H)$ Since we have

$$H \otimes H = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

We have

$$(H \otimes H)U(H \otimes H) =$$

$$\frac{1}{4} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} =$$

$$\frac{1}{4} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

as required. We are trying to find $U|{+}{+}\rangle$ Since $(H \otimes H)U(H \otimes H)|00\rangle = (H \otimes H)U|{+}{+}\rangle$ and $(H \otimes H)U(H \otimes H)|00\rangle = |00\rangle$, we have $(H \otimes H)U|{+}{+}\rangle =$

$|00\rangle$ meaning $(H \otimes H)(H \otimes H)U\,|{+}{+}\rangle = (H \otimes H)\,|00\rangle$. That in turn means $U\,|{+}{+}\rangle = |{+}{+}\rangle$. The rest follows from similar reasoning.

4.21

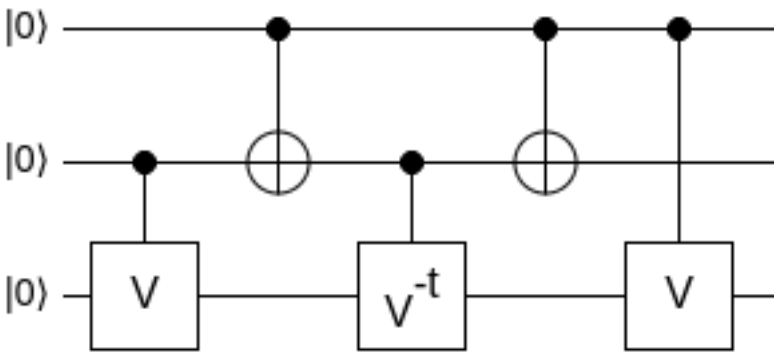
We have

$$\begin{aligned} |000\rangle \to |000\rangle \quad & |001\rangle \to |001\rangle \\ |010\rangle \to |010\rangle \quad & |011\rangle \to |011\rangle \\ |100\rangle \to |100\rangle \quad & |101\rangle \to |101\rangle \\ |110\rangle \to |11\rangle\,U\,|0\rangle \quad & |111\rangle \to |11\rangle\,U\,|1\rangle \end{aligned}$$

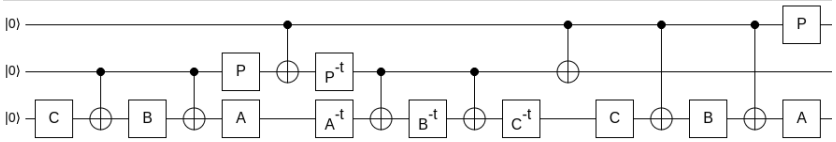
for the $C^2(U)$ gate. Now consider the right side. We have $|000\rangle$ won't apply any of the controlled gates meaning we are left with $|000\rangle$ after going through the right. For $|001\rangle$ the same can be said because the control parts are in x_1 and x_2 resulting in $|001\rangle$. For $|010\rangle$, the first V and $V^\dagger$ gates are applied resulting in $|01\rangle\,VV^\dagger\,|0\rangle$. But since V is unitary we have $VV^\dagger = I$. This results in $|010\rangle$ still. For $|011\rangle$ we have the same situation as $|010\rangle$ and so we are left with $|011\rangle$. For $|100\rangle$ the first not gate is applied flipping the second qubit to $|1\rangle$ which means $V^\dagger$ is applied to the third qubit. Then the second qubit is flipped back to $|0\rangle$. Finally the final V gate to the third qubit. This results in $|1\rangle\,XX\,|0\rangle\,VV^\dagger\,|0\rangle = |100\rangle$. For $|101\rangle$ we have the same situation as $|100\rangle$ and we are thus left with $|101\rangle$. For $|110\rangle$, we have V first applied to the third qubit, then X applied to the second, this makes it so that $V^\dagger$ is not applied, X is then applied again to the second qubit and the final V is applied to the third qubit resulting in $|1\rangle\,XX\,|1\rangle\,VV\,|0\rangle = |11\rangle\,U\,|0\rangle$. For $|111\rangle$ we have the same situation as $|110\rangle$ and thus resulting in $|11\rangle\,U\,|1\rangle$. Therefore we can conclude that the two sides are equivalent.

4.22(U)

Since V is a unitary operator we can express it as $V = e^{i\alpha}AXBXC$ where $ABC = I$ and are also unitary matrices. That means $V^\dagger = e^{-i\alpha}C^\dagger XB^\dagger XA^\dagger$. We then have



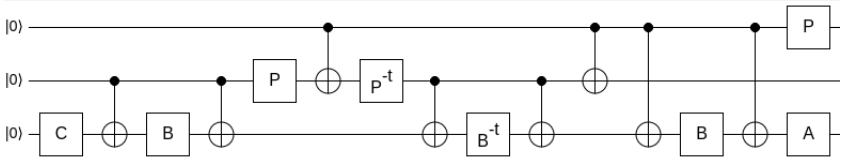
is equivalent to



where

$$P = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{bmatrix}$$

Since A and C are both unitary, we have $AA^\dagger = I$ and $C^\dagger C = I$. This results in



4) this can then be

4.23

We have

$$R_x(\theta) = \begin{bmatrix} \cos(\theta/2) & -i\sin(\theta/2) \\ -i\sin(\theta/2) & \cos(\theta/2) \end{bmatrix} =$$

$$e^{i\alpha}R_z(\beta)R_y(\gamma)R_z(\delta) = \begin{bmatrix} e^{i(\alpha-\beta/2-\delta/2)}\cos(\gamma/2) & -e^{i(\alpha-\beta/2+\delta/2)}\sin(\gamma/2) \\ e^{i(\alpha+\beta/2-\delta/2)}\sin(\gamma/2) & e^{i(\alpha+\beta/2+\delta/2)}\cos(\gamma/2) \end{bmatrix}$$

So $\cos(\theta/2) = e^{i(\alpha-\beta/2-\delta/2)}\cos(\gamma/2)$, $-i\sin(\theta/2) = -e^{i(\alpha-\beta/2+\delta/2)}\sin(\gamma/2)$, $-i\sin(\theta/2) = e^{i(\alpha+\beta/2-\delta/2)}\sin(\gamma/2)$, and $\cos(\theta/2) = e^{i(\alpha+\beta/2+\delta/2)}\cos(\gamma/2)$. Thus we have

$$e^{-i(\alpha+\beta/2+\delta/2)} = e^{i(\alpha+\beta/2+\delta/2)}$$

meaning

$$-(\alpha+\beta/2+\delta/2) = (\alpha+\beta/2+\delta/2)$$

which is only true when

$$(\alpha+\beta/2+\delta/2) = 0$$

That would then mean $\gamma = \theta$ and since we have

$$-e^{i(\alpha-\beta/2+\delta/2)} = e^{i(\alpha+\beta/2-\delta/2)}$$

This results in

$$i(\pi+\alpha-\beta/2+\delta/2) = i(\alpha+\beta/2-\delta/2)$$

and so we have

$$\pi+\alpha-\beta/2+\delta/2 = \alpha+\beta/2-\delta/2$$

resulting in $\pi = \beta - \delta$. That then means

$$-a-\pi/2 = \delta \quad \beta = \frac{\pi}{2} - \alpha$$

Thus we have

$$R_x(\theta) = e^{i\alpha} R_z\left(\frac{\pi}{2} - \alpha\right) R_y(\theta) R_z\left(-\alpha - \frac{\pi}{2}\right)$$

where α is arbitrary. So we choose $\alpha = 0$ and obtain

$$R_x(\theta) = R_z\left(\frac{\pi}{2}\right) R_y(\theta) R_z\left(-\frac{\pi}{2}\right)$$

We then set

$$A = R_z\left(\frac{\pi}{2}\right) R_y\left(\frac{\theta}{2}\right) \quad B = R_y\left(\frac{-\theta}{2}\right) R_z(0) \quad C = R_z\left(\frac{-\pi}{2}\right)$$

and obtain the decomposition

$$R_x(\theta) = e^{\alpha} AXBXC = R_z\left(\frac{\pi}{2}\right) R_y\left(\frac{\theta}{2}\right) X R_y\left(-\frac{\theta}{2}\right) X R_z\left(-\frac{\pi}{2}\right)$$

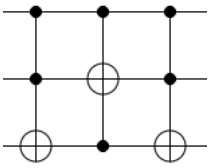
There does not seem to be any way to make this have only two single qubit gates. Now consider $R_y(\theta)$, we have $R_y(\theta) = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$, where clearly, $\alpha = 0$, $\beta = 0$, $\gamma = \theta$, and $\delta = 0$. By letting $A = R_z(0) R_y(\theta/2)$, $B = R_y(-\theta/2) R_z(0)$, and $C = R_z(0)$. Thus we have

$$R_y(\theta) = e^{i\alpha} AXBXC = R_y(\theta/2) X R_y(-\theta/2) X$$

which only has two single qubit gates.

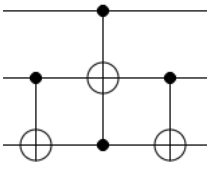
4.25

1)



represents a fredkin gate, as can be seen by supplying all possible inputs.

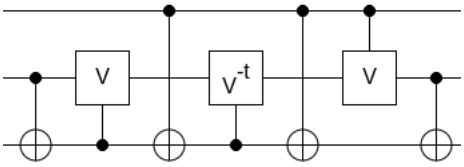
2)



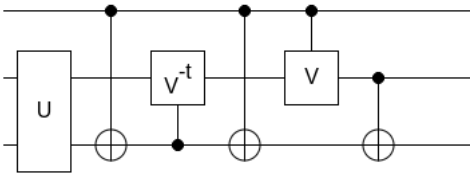
represents a fredkin gate as well. For the input $0, 0, 0$, we have $0, 0, 0$ after the first cnot, then after the toffoli gate, we still have $0, 0, 0$ and finally after the second cnot, we are left with $0, 0, 0$ as required. For $0, 0, 1$, we have after the first cnot, $0, 0, 1$, after the toffoli, $0, 0, 1$, and after the second cnot $0, 0, 1$ as

required. For $0,1,0$ we have after the first cnot, $0,1,1$, after the toffoli, $0,1,1$, and after the second cnot $0,1,0$ as required. For $0,1,1$, we have $0,1,0$ after the first cnot, then $0,1,0$ after the toffoli, and after the second cnot $0,1,1$ as required. For $1,0,0$ we have $1,0,0$ after the first cnot, $1,0,0$ after the toffoli, and $1,0,0$ after the second cnot as required. For $1,0,1$, we have after the first cnot, $1,0,1$ after the toffoli, $1,1,1$ and after the second cnot, $1,1,0$ as required. For $1,1,0$, we have after the first cnot, $1,1,1$, after the toffoli, we have $1,0,1$ and after the second cnot, $1,0,1$ as required. For $1,1,1$ we have after the first cnot, $1,1,0$, after the toffoli $1,1,0$ and after the second cnot $1,1,1$ as required. Thus we can conclude that the above circuits action is the same as a fredkin gate.

3)

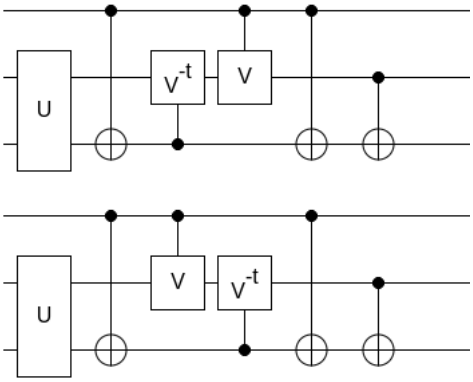


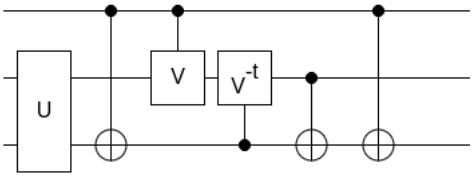
where $V = (1-i)(I+iX)/2$ also represents a fredkin gate this can be simplified to



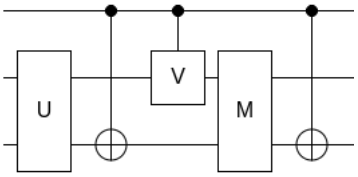
Where U represents the application of the *cnot* and *cv* gates.

4)



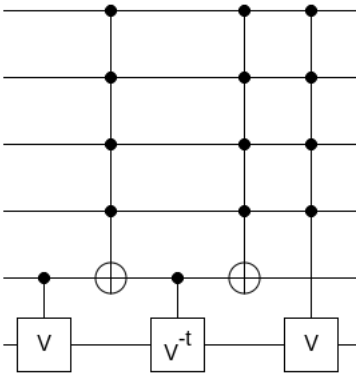


The above are equivalent to a fredkin gate. The first one because the cnot and cv gates don't affect each other, allowing it to be swapped. The second because of the unitary nature of V, thus making it normal and commutes with each other. The third is because the control qubits are not affected and X commutes with itself. From the above we can replace the cv^{-t} and cnot gate with a single two qubit gate M and obtain



which has only five 2 qubit gates as required.

4.27



Is equivalent since this is basically the same as the ccu gate except conditional on 5 qubits rather than 2.

4.32

We would have after measurement, but with no knowledge of the measurement, the state $\rho' = \sum_m p(m)\rho_m = \sum_m M_m \rho M_m^\dagger = P_0\rho P_0 + P_1\rho P_1$. Since we have by schmidt decomposition

$$\rho = \sum_i \lambda_i^2 \left|i_a i_b\right\rangle \left\langle i_a i_b\right| = \sum_i \lambda_i^2 \left|i_a\right\rangle \left\langle i_a\right| \otimes \left|i_b\right\rangle \left\langle i_b\right|$$

then

$$tr_2(\rho) = \sum_i \lambda_i^2 \left|i_a\right\rangle \left\langle i_a\right| \left\langle i_b | i_b\right\rangle = \sum_i \lambda_i^2 \left|i_a\right\rangle \left\langle i_a\right|$$

since $|i_b\rangle$ is orthonormal. Also

$$tr_2(\rho') = tr_2(P_0\rho P_0 + P_1\rho P_1) =$$

$$tr_2\left(\sum_i \lambda_i^2 |i_a\rangle\langle i_a| \otimes P_0 |i_b\rangle\langle i_b| P_0 + \sum_i \lambda_i^2 |i_a\rangle\langle i_a| \otimes P_1 |i_b\rangle\langle i_b| P_1\right) =$$

$$\sum_i \lambda_i^2 |i_a\rangle\langle i_a| (tr(P_0 |i_b\rangle\langle i_b| P_0) + tr(P_1 |i_b\rangle\langle i_b| P_1)) =$$

$$\sum_i \lambda_i^2 |i_a\rangle\langle i_a| (tr(|0\rangle\langle 0| |i_b\rangle\langle i_b| |0\rangle\langle 0|) + tr(|1\rangle\langle 1| |i_b\rangle\langle i_b| |1\rangle\langle 1|)) =$$

$$\sum_i \lambda_i^2 |i_a\rangle\langle i_a| (\langle 0| |i_b\rangle\langle i_b| |0\rangle + \langle 1| |i_b\rangle\langle i_b| |1\rangle)$$

But we have $i_b = a|0\rangle + b|1\rangle$ and $\langle i_b|i_b\rangle = 1$. Thus $a\overline{a} + b\overline{b} = 1$. Then $\langle 0| |i_b\rangle\langle i_b| |0\rangle + \langle 1| |i_b\rangle\langle i_b| |1\rangle = \overline{a}a + \overline{b}b = 1$ meaning

$$tr_2(\rho') = \sum_i \lambda_i^2 |i_a\rangle\langle i_a|$$

and thus we can conclude $tr_2(\rho') = tr_2(\rho)$ as required.

4.33

We have from the circuit

$$|00\rangle \to \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \quad |01\rangle \to \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle)$$

$$|10\rangle \to \frac{1}{\sqrt{2}}(|01\rangle - |11\rangle) \quad |11\rangle \to \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle)$$

Now by inputting the bell states we then have

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \to \frac{1}{2}(|00\rangle + |10\rangle + |00\rangle - |10\rangle) = |00\rangle$$

$$\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \to \frac{1}{2}(|01\rangle + |11\rangle + |01\rangle - |11\rangle) = |01\rangle$$

$$\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \to \frac{1}{2}(|00\rangle + |10\rangle - |00\rangle) + |10\rangle) = |10\rangle$$

$$\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{1}{2}(|01\rangle + |11\rangle - |01\rangle + |11\rangle) = |11\rangle$$

Thus measurement of the computational basis is equivalent to measuring in the bell basis.

Because we have after a measurement, the state

$$\frac{M_m |\psi\rangle}{\sqrt{\langle\psi| M_m^\dagger M_m |\psi\rangle}}$$

So what we want is, when inputting the bell states, the measurements should take it to the same bell space This is true when $M_{00} = |\beta_{00}\rangle\langle\beta_{00}|$, $M_{01} = |\beta_{01}\rangle\langle\beta_{01}|$, $M_{10} = |\beta_{10}\rangle\langle\beta_{10}|$, and $M_{11} = |\beta_{11}\rangle\langle\beta_{1}|$ where β are the bell states. Since these are all projective measurements, we have their $POVM$ being the same since $M_m M_m^\dagger = E_m$.

4.34

We have after each gate

$$|0\psi_{in}\rangle \to \frac{1}{\sqrt{2}}(|0\psi_{in}\rangle + |1\psi_{in}\rangle) \to \frac{1}{\sqrt{2}}(|0\psi_{in}\rangle + |1(U\psi_{in})\rangle) \to$$

$$\frac{1}{\sqrt{2}}(|(H0)\psi_{in}\rangle + |(H1)(U\psi_{in})\rangle) = \frac{1}{2}(|0\psi_{in}\rangle + |1\psi_{in}\rangle + |0(U\psi_{in})\rangle - |1(U\psi_{in})\rangle)$$

Thus we would have when measuring $|0\rangle$

$$|\psi_{out}\rangle = (I+U)|\psi_{in}\rangle$$

and when measuring $|1\rangle$

$$|\psi_{out}\rangle = (I-U)|\psi_{in}\rangle$$

We also have for $|0\rangle\, U|\psi_{out}\rangle = U(I+U)|\psi_{in}\rangle = (U+U^2)|\psi_{in}\rangle = (U+I)|\psi_{in}\rangle = |\psi_{out}\rangle$ or $U|\psi_{out}\rangle\, U(I-U)|\psi_{in}\rangle = (U-U^2)|\psi_{in}\rangle = (U-I)|\psi_{in}\rangle = -|\psi_{out}\rangle$. Meaning $|\psi_{out}\rangle$ are eigenvectors in both cases and $|0\rangle$ corresponds with the eigenvalue 1, while $|1\rangle$ with the eigenvalue -1.

4.35

We have in the first circuit

$$|00\rangle \to |(P_0 0/\sqrt{\langle 0|\, P_0\, |0\rangle})0\rangle = |00\rangle$$
$$|01\rangle \to |(P_0 0/\sqrt{\langle 0|\, P_0\, |0\rangle})0\rangle = |01\rangle$$
$$|10\rangle \to |1(U0)\rangle \to |(P_1 1/\sqrt{\langle 1|\, P_1\, |1\rangle})(U0)\rangle = |1(U0)\rangle$$
$$|11\rangle \to |1(U1)\rangle \to |(P_1 1/\sqrt{\langle 1|\, P_1\, |1\rangle})(U1)\rangle = |1(U1)\rangle$$

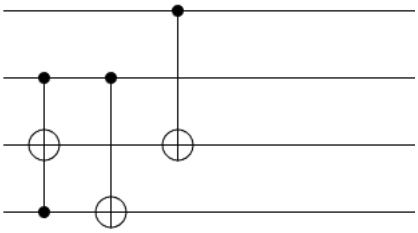
From the second circuit we have

$$|00\rangle \to |(P_0 0/\sqrt{\langle 0|\, P_0\, |0\rangle})0\rangle = |00\rangle$$
$$|01\rangle \to |(P_0 0/\sqrt{\langle 0|\, P_0\, |0\rangle})0\rangle = |01\rangle$$
$$|10\rangle \to |(P_1 1/\sqrt{\langle 1|\, P_1\, |1\rangle})0\rangle = |10\rangle \to |1(U0)\rangle$$
$$|11\rangle \to |(P_1 1/\sqrt{\langle 1|\, P_1\, |1\rangle})1\rangle = |11\rangle \to |1(U1)\rangle$$

and thus we can conclude that the two circuits are equivalent as required

4.36

consider the circuit



where the top two qubits represents x and the bottom two represents y. This circuit results in $|x, y\rangle \rightarrow |x, x + y \ mod \ 4\rangle$

4.40

We have

$$E(R_{\hat{n}}(\alpha), R_{\hat{n}}(\alpha + \beta)) = \max_{|\psi\rangle} |(R_{\hat{n}}(\alpha) - R_{\hat{n}}(\alpha + \beta)) |\psi\rangle |$$

The maximum difference occurs when we have a state that is perpendicular to the axis of rotation.

4.41

We have

$$|00\psi\rangle \xrightarrow{H,H} \frac{1}{\sqrt{2}}(|0(H0)\psi\rangle + |1(H0)\psi\rangle) = \frac{1}{2}(|00\psi\rangle + |01\psi\rangle + |10\psi\rangle + |11\psi\rangle) \xrightarrow{ccnot}$$

$$\frac{1}{2}(|00\psi\rangle + |01\psi\rangle + |10\psi\rangle + |11(X\psi)\rangle) \xrightarrow{S}$$

$$\frac{1}{2}(|00(S\psi)\rangle + |01(S\psi)\rangle + |10(S\psi)\rangle + |11(SX\psi)\rangle) \xrightarrow{ccnot}$$

$$\frac{1}{2}(|00(S\psi)\rangle + |01(S\psi)\rangle + |10(S\psi)\rangle + |11(XSX\psi)\rangle) \xrightarrow{H,H}$$

$$\frac{1}{2\sqrt{2}}(|0(H0)(S\psi)\rangle + |1(H0)(S\psi)\rangle + |0(H1)(S\psi)\rangle + |1(H1)(S\psi)\rangle +$$

$$|0(H0)(S\psi)\rangle - |1(H0)(S\psi)\rangle + |0(H1)(XSX\psi)\rangle - |1(H1)(XSX\psi)\rangle) =$$

$$\frac{1}{2\sqrt{2}}(2\,|0(H0)(S\psi)\rangle + |0(H1)(S\psi)\rangle + |1(H1)(S\psi)\rangle +$$

$$|0(H1)(XSX\psi)\rangle - |1(H1)(XSX\psi)\rangle) =$$

$$\frac{1}{4}(2\,|00(S\psi)\rangle + 2\,|01(S\psi)\rangle + |00(S\psi)\rangle - |01(S\psi)\rangle + |10(S\psi)\rangle - |11(S\psi)\rangle +$$

$$|00(XSX\psi)\rangle - |01(XSX\psi)\rangle - |10(XSX\psi)\rangle + |11(XSX\psi)\rangle) =$$

$$\frac{1}{4}(3\,|00(S\psi)\rangle + |01(S\psi)\rangle + |10(S\psi)\rangle - |11(S\psi)\rangle +$$

$$|00(XSX\psi)\rangle - |01(XSX\psi)\rangle - |10(XSX\psi)\rangle + |11(XSX\psi)\rangle) =$$

$$\frac{1}{4}(|00((3S + XSX)\psi)\rangle + |01((S - XSX)\psi)\rangle +$$

$$|10((S - XSX)\psi)\rangle + |11((XSX - S)\psi)\rangle)$$

Thus when both measurement outcomes are 0, we have $\frac{1}{4}(3S + XSX)$ being applied to the final qubit. But

$$\frac{1}{4}(3S + XSX) = \frac{1}{4}\left(3\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix} + \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\right) =$$

$$\frac{1}{4}\left(3\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix} + \begin{bmatrix}i & 0\\ 0 & 1\end{bmatrix}\right) = \frac{1}{4}\begin{bmatrix}3+i & 0\\ 0 & 1+3i\end{bmatrix} =$$

$$\frac{\sqrt{10}}{4}\begin{bmatrix}\frac{3}{\sqrt{10}} + i\frac{1}{\sqrt{10}} & 0\\ 0 & \frac{1}{\sqrt{10}} + i\frac{3}{\sqrt{10}}\end{bmatrix}$$

So by setting $Ae^{i\theta/2} = \frac{3}{\sqrt{10}} + i\frac{1}{\sqrt{10}}$ and $Ae^{-i\theta/2} = \frac{1}{\sqrt{10}} + i\frac{3}{\sqrt{10}}$. Then

$$A^2 = \left(\frac{3}{\sqrt{10}} + i\frac{1}{\sqrt{10}}\right)\left(\frac{1}{\sqrt{10}} + i\frac{3}{\sqrt{10}}\right) = \frac{3}{10} + i - \frac{3}{10} = i = \left(\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right)^2$$

Therefore

$$A = \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}} = e^{i\pi/4}$$

making $e^{i\theta/2} = e^{-i\pi/4}(\frac{3}{\sqrt{10}} + i\frac{1}{\sqrt{10}})$ and $e^{-i\theta/2} = e^{-i\pi/4}(\frac{1}{\sqrt{10}} + i\frac{3}{\sqrt{10}})$. Thus we have

$$\frac{1}{4}(3S + XSX) = \frac{\sqrt{10}e^{i\pi/4}}{4}\begin{bmatrix}e^{-i\pi/4}\left(\frac{3}{\sqrt{10}} + i\frac{1}{\sqrt{10}}\right) & 0\\ 0 & e^{-i\pi/4}\left(\frac{1}{\sqrt{10}} + i\frac{3}{\sqrt{10}}\right)\end{bmatrix}$$

which is indeed $R_z(\theta)$ with a global phase shift. We also have

$$e^{i\theta} = \frac{\frac{3}{\sqrt{10}} + i\frac{1}{\sqrt{10}}}{\frac{1}{\sqrt{10}} + i\frac{3}{\sqrt{10}}} = \frac{\frac{3}{\sqrt{10}} + i\frac{1}{\sqrt{10}}}{\frac{1}{\sqrt{10}} + i\frac{3}{\sqrt{10}}}\left(\frac{\frac{1}{\sqrt{10}} - i\frac{3}{\sqrt{10}}}{\frac{1}{\sqrt{10}} - i\frac{3}{\sqrt{10}}}\right) = \frac{3}{10} + \frac{i}{10} - \frac{9i}{10} + \frac{3}{10} = \frac{3}{5} + \frac{4}{5}i$$

Thus $\cos(\theta) = 3/5$ as required. In the other cases we have $\pm(S - XSX)$ applied to the final qubit. Since

$$S - XSX = \begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix} - \begin{bmatrix}i & 0\\ 0 & 1\end{bmatrix} = -iZ$$

we have an application of Z with global phase shift. The probability of both measurements being 0 is

$$\frac{1}{16}\langle 00(\sqrt{10}e^{i\pi/4}R_z(\theta)\psi)|00(\sqrt{10}e^{i\pi/4}R_z(\theta)\psi)\rangle =$$

$$\frac{10}{16}\langle 00(R_z(\theta)\psi)|00(R_z(\theta)\psi)\rangle = \frac{5}{8}$$

as required

If the resulting measurements is not 00, we can apply a Z gate to the final qubit in order to get the final qubit back to its initial state. Then we can apply the circuit again in order to try and obtain 00. More and more applications of this procedure will result in higher probability of achieving $R_z(\theta)$ since the probability of $R_z(\theta)$ is $1 - (\frac{3}{8})^n$, where n is the number of times the circuit is applied. Thus as $n \to \infty$, the probability of the desired gate goes to 1.

5 The Quantum Fourier Transform and its Applications

5.1

We have

$$U = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} e^{2\pi ijk/N} |k\rangle \langle j|$$

and

$$U^\dagger = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} e^{-2\pi ijk/N} |j\rangle \langle k|$$

This means

$$U^\dagger U = \left(\frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} e^{-2\pi ijk/N} |j\rangle \langle k| \right) \left(\frac{1}{\sqrt{N}} \sum_{h=0}^{N-1} \sum_{p=0}^{N-1} e^{2\pi ihp/N} |p\rangle \langle h| \right) =$$

$$\frac{1}{N} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} \left(\sum_{h=0}^{N-1} \sum_{p=0}^{N-1} e^{-2\pi ijk/N} e^{2\pi ihp/N} |j\rangle \langle k| |p\rangle \langle h| \right) =$$

$$\frac{1}{N} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} \sum_{h=0}^{N-1} e^{-2\pi ijk/N} e^{2\pi ihk/N} |j\rangle \langle h|$$

Since we have when $j \neq h$

$$\sum_{k=0}^{N-1} e^{-2\pi ijk/N} e^{2\pi ihk/N} |j\rangle \langle h| = 0$$

and 1 when $j = k$, we end up with $U^\dagger U = I$ as required

5.2

We have

$$|0...0\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i * 0 * k/N} |k\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle$$

5.3

Since we need 2^n output, and each output is of the form $y_k = \sum_{n=0}^{2^n-1} a_n * b_n$, each output needs 2^n multiplication operations and 2^n addition operations. So each y_k requires $2 * 2^n$ operations. Since we need 2^n output of this form, we will need $2^n * 2 * 2^n = 2 * 2^{2n}$ operations which is $\Theta(2^n)$ arithmetic operations as required.

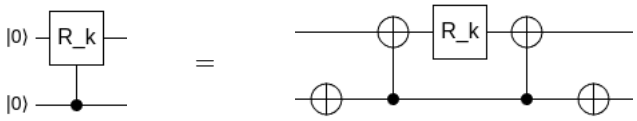
We have

$$\sum_{j=0}^{2^n-1} x_j |j\rangle \rightarrow \sum_{j=0}^{2^n-1} x_j \frac{1}{2^{n/2}} \otimes_{l=1}^{n} \left[|0\rangle + e^{2\pi ij2^{-l}} |1\rangle \right] = \sum_{k=0}^{2^n-1} y_k |k\rangle$$

We can recursively solve for all y_k by summing all components with $j_n = 0$ and all components with $j_n = 1$ then tensoring with the necessary component. This can be done recursively for each sum component. Since each level will require 2^n addition operations due to there being 2^n elements, and there being $\log(2^n) = n$ levels of the recursion, we will need $n2^n$ operations. The tensoring operations that are done on each level will require at most $2 * 2^n$ operations which with $log(2^n)$ levels means an additional $2n * 2^n$ operations. This totals $n2^n(1 + 2) = 3n2^n$ total operations, making it $\Theta(n2^n)$ as required.

5.4

A controlled R_x gate can be implemented as



as one can see by inputting the computational basis

6 Physical Realization

7.1

We have

$$a^\dagger a = \frac{1}{\sqrt{2m\hbar\omega}}(m\omega x - ip)\frac{1}{\sqrt{2m\hbar\omega}}(m\omega x + ip) =$$

$$\frac{1}{2m\hbar\omega}(m^2\omega^2x^2 - im\omega px + im\omega xp + p^2) =$$

$$\frac{1}{2m\hbar\omega}(m^2\omega^2x^2 + im\omega(xp - px) + p^2) =$$

$$\frac{1}{2m\hbar\omega}(m^2\omega^2x^2 + im\omega(i\hbar) + p^2) = \frac{1}{2m\hbar\omega}(m^2\omega^2x^2 - m\omega\hbar + p^2) =$$

$$\frac{1}{\hbar\omega}\left(\frac{m\omega^2x^2}{2} + \frac{p^2}{2m}\right) - \frac{1}{2} = \frac{H}{\hbar\omega} - \frac{1}{2}$$

as required

7.2

We have

$$aa^\dagger = \frac{1}{\sqrt{2m\hbar\omega}}(m\omega x + ip)\frac{1}{\sqrt{2m\hbar\omega}}(m\omega x - ip) =$$

$$\frac{1}{2m\hbar\omega}(m^2\omega^2x^2 + im\omega(px - xp) + p^2) = \frac{1}{2m\hbar\omega}(m^2\omega^2x^2 + m\omega\hbar + p^2)$$

So

$$[a, a^\dagger] = aa^\dagger - a^\dagger a = \frac{1}{2m\hbar\omega}\left((m\omega x)^2 + m\omega\hbar + p^2 - (m\omega x)^2 + m\omega\hbar - p^2)\right) = 1$$

7.3

We have

$$[H, a] = Ha - aH = \hbar\omega\left(a^\dagger aa + \frac{a}{2} - aa^\dagger a - \frac{a}{2}\right) = \hbar\omega\left(a^\dagger aa - aa^\dagger a\right)$$

$$\hbar\omega\left(a^\dagger a - aa^\dagger\right)a = -\hbar\omega a$$

Since $|\psi\rangle$ has energy $E \geq n\hbar\omega$. We then have $Ha^n|\psi\rangle = Haa^{n-1}|\psi\rangle = ([H, a] + aH)a^{n-1}|\psi\rangle = ([H, a] + aH)a^{n-1}|\psi\rangle = ([H, a] + aH)a^{n-1}|\psi\rangle = (-\hbar\omega a + aH)a^{n-1}|\psi\rangle = -\hbar\omega a^n|\psi\rangle + aHa^{n-1}|\psi\rangle$. But we can reapply H to a^{n-1} in the same way and get another $-\hbar\omega a^n|\psi\rangle$ term until we have n of it and H gets applied to $|\psi\rangle$ resulting in a $E|\psi\rangle$ term. Thus we have $(E - n\hbar\omega)a^n|\psi\rangle$.

7.4

Consider the base case $n = 0$, we then have

$$|0\rangle = \frac{(a^\dagger)^0}{\sqrt{0!}}|0\rangle = |0\rangle$$

proving the base case. Now suppose for some $n \geq 0$, we have

$$|n\rangle = \frac{(a^\dagger)^n}{\sqrt{n!}} |0\rangle$$

Since

$$a^\dagger |n\rangle = \sqrt{n+1}\,|n+1\rangle \quad \text{we have} \quad \frac{a^\dagger}{\sqrt{n+1}} |n\rangle = |n+1\rangle$$

But

$$\frac{a^\dagger}{\sqrt{n+1}} |n\rangle = \frac{(a^\dagger)^{n+1}}{\sqrt{(n+1)!}} |0\rangle$$

by inductive hypothesis and so

$$|n+1\rangle = \frac{(a^\dagger)^{n+1}}{\sqrt{(n+1)!}} |0\rangle$$

as required

7.5

We have $a^\dagger a |n\rangle = a^\dagger \sqrt{n}\,|n-1\rangle = \sqrt{n} a^\dagger |n-1\rangle = \sqrt{n}\sqrt{n}\,|n\rangle = n\,|n\rangle$ as required.

7.6

We have

$$a|\alpha\rangle = a\left(e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle\right) = e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}a|n\rangle =$$

$$e^{-|\alpha|^2/2}\left(a|0\rangle + \sum_{n=1}^{\infty}\frac{\alpha^n}{\sqrt{n!}}a|n\rangle\right) = e^{-|\alpha|^2/2}\sum_{n=1}^{\infty}\frac{\alpha^n}{\sqrt{n!}}a|n\rangle =$$

$$e^{-|\alpha|^2/2}\sum_{n=1}^{\infty}\frac{\alpha^n}{\sqrt{n!}}\sqrt{n}|n-1\rangle = e^{-|\alpha|^2/2}\sum_{n=1}^{\infty}\frac{\alpha^n}{\sqrt{(n-1)!}}|n-1\rangle =$$

$$\frac{1}{\alpha}e^{-|\alpha|^2/2}\sum_{n=1}^{\infty}\frac{\alpha^{n-1}}{\sqrt{(n-1)!}}|n-1\rangle = \frac{1}{\alpha}e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{(n)!}}|n\rangle = \frac{1}{\alpha}|\alpha\rangle$$

as required

7.7

We have $|\psi_{in}\rangle = c_0|01\rangle + c_1|10\rangle$. Then after going through the circuit shown, we have $|\psi_{out}\rangle = c_0 e^{i\pi}|01\rangle + c_1|10\rangle = c_0 e^{i\pi}|01\rangle + c_1|10\rangle = -c_0|01\rangle + c_1|10\rangle$ From the matrix we have

$$\begin{bmatrix} e^{i\pi} & 0 \\ 0 & 1 \end{bmatrix} |\psi_i n\rangle = \begin{bmatrix} e^{i\pi} & 0 \\ 0 & 1 \end{bmatrix} (c_0|01\rangle + c_1|10\rangle) = -c_0|01\rangle + c_1|10\rangle)$$