

1 Chapter 1 Solutions

1.1 Probabilistic classical algorithm

It is already shown that a deterministic classical computer would require $2^n/2 + 1$ queries.

Instead, if we use a probabilistic classical computer i.e, $f(x)$ is evaluated for randomly chosen x . With just one execution, we cannot determine whether $f(x)$ is a constant or a balanced function (atleast not with probability of error $\epsilon < 1/2$). If the second evaluation gives a different result than first, we can say with certainty that $f(x)$ is a balanced function. In the other case, the probability that we get same result twice in a row if the function was balanced would be $1/2$ for the first evaluation times $\frac{2^n/2-1}{2^n-1}$ for the second which is less than $1/2$ if:

$$\begin{aligned}\frac{1}{2} \times \frac{2^n/2-1}{2^n-1} &< \frac{1}{2} \\ 2^n - 2 &< 2(2^n - 1) \\ 2^n &< 2^{n+1} \\ n &< n + 1\end{aligned}\tag{1}$$

which is always true for all positive integer n . So if we get same evaluation twice, we can say that $f(x)$ is a constant function with a probability of error $\epsilon < 1/2$. Therefore, the best classical algorithm (probabilistic) will require 2 evaluations, irrespective of size of the input.

1.2 Explain how a device.

If a device, upon input of one of two non-orthogonal quantum states correctly identified the state, without collapsing. We can perform certain unitary transformation on an extra quantum state to create either of the quantum states, since we know its coefficients. Thus creating a clone of the input quantum state.

Conversely, if we have a device for cloning, we can in principle, generate multiple copies of the unknown quantum states and perform ensemble measurement to find its coefficients (hidden information - not accessible in single measurement) with enough precision to identify/distinguish them.

P1.1 Feynman-Gates Conversation

Bill Gates: Hi Richard, it's great to have the opportunity to chat with you about the future of computation

Richard Feynman: Hello Bill, it's an honor to be having this discussion with you. I'm excited to hear your thoughts on where you see technology heading in the near future.

Bill Gates: Well, I believe that we're on the cusp of a major breakthrough in artificial intelligence. We've already seen some incredible advancements in machine learning and natural language processing, but I think we're still only scratching the surface of what's possible. I believe that AI will become more and more integrated into our daily lives, and we'll see it being used in a wide variety of industries, from healthcare to transportation.

Richard Feynman: That's certainly an interesting perspective. I'm particularly intrigued by the potential of AI to revolutionize the field of medicine. With the ability to process vast amounts of data, AI has the potential to help us better understand and treat diseases, as well as improve patient outcomes.

Bill Gates: Absolutely. I think that AI will be particularly useful in the field of personalized medicine. By analyzing a patient's genetic data and medical history, AI will be able to help doctors make more accurate diagnoses and develop more effective treatment plans.

Richard Feynman: I also see great potential for AI in the field of quantum computing. As you know, traditional computing is based on binary digits (bits) which can be either 0 or 1. However, quantum computing uses quantum bits, or qubits, which can exist in multiple states simultaneously. This could potentially allow us to solve problems that are currently intractable using traditional computing methods.

Bill Gates: Yes, I agree. Quantum computing is still in its infancy, but I believe that we'll see some major breakthroughs in the near future. It has the potential to revolutionize fields like cryptography and drug discovery.

Richard Feynman: Another area where I think we'll see major advancements is in the field of robotics. With the development of more advanced sensors and machine learning algorithms, robots will be able to perform tasks that are currently too dangerous or difficult for humans.

Bill Gates: I agree. I think that we'll see robots becoming more and more integrated into our daily lives. For example, they could be used in manufacturing, construction, and even in our homes to assist with tasks like cleaning and cooking.

Richard Feynman: I also think that we'll see a lot of progress in the field of virtual reality and augmented reality. These technologies have the potential to change the way we interact with the world, and I believe that we'll see them being used in fields like education, entertainment, and even therapy.

Bill Gates: Yes, I think that VR and AR will have a huge impact on the way we experience the world. They'll allow us to explore new environments and interact with other people in ways that we never thought possible.

Richard Feynman: I think that technology is going to continue to change the world in ways that we can't even imagine. It's exciting to be alive during such a transformative time, and I look forward to seeing all of the advancements that are yet to come.

Bill Gates: I couldn't agree more. It's an exciting time to be alive, and I can't wait to see what the future holds for technology. Thank you for the interesting discussion, Richard.

Richard Feynman: Thank you, Bill. It was a pleasure to have this conversation with you

P1.2 Essay

Quantum computation and quantum information are relatively new fields of study that have the potential to revolutionize the way we think about and use computers. One of the most significant discoveries in these fields is the concept of quantum entanglement.

Quantum entanglement is a phenomenon where two or more quantum particles become linked in such a way that the state of one particle is dependent on the state of the other particle, even when the particles are separated by large distances. This means that if something happens to one particle, it will instantaneously affect the other particle, regardless of how far apart they are.

This strange behavior was first proposed by Albert Einstein, Boris Podolsky, and Nathan Rosen in 1935, but it was not until the 1980s that scientists were able to experimentally demonstrate quantum entanglement. Since then, scientists have been working to understand and harness the power of entanglement for use in quantum computing and quantum communication.

One of the most interesting applications of quantum entanglement is in quantum teleportation. This process, first proposed by physicist Charles Bennett in 1993, allows for the instant transfer of quantum information from one particle to another, without physically moving the particle. This is made possible by the phenomenon of entanglement, as the two particles become linked and can share information instantaneously.

Quantum teleportation has been demonstrated in a number of experiments, and it has the potential to revolutionize the way we think about communication. Instead of physically sending a particle or a piece of information, we could simply transfer the information instantaneously using entanglement. This could have a huge impact on fields like cryptography, as it would make it possible to transmit information securely and instantly, without the need for a physical connection.

Another potential application of entanglement is in quantum computing. In a classical computer, information is stored in bits, which can be either 0 or 1. However, in a quantum computer, information is stored in qubits, which can exist in multiple states simultaneously. This allows for the simultaneous

processing of multiple pieces of information, which could greatly speed up the time it takes to solve certain problems.

One of the most promising applications of quantum computing is in the field of cryptography. A quantum computer could be used to break today's encryption codes very fast and efficiently, making it a powerful tool in code breaking.

In conclusion, quantum entanglement is a fascinating phenomenon that has the potential to revolutionize the way we think about and use technology. From instant communication to quantum computing, the possibilities are truly endless. While there is still much research to be done in this field, it's clear that quantum entanglement will be an essential part of the future of technology.

2 Chapter 2 solutions

2.19 Pauli Matrices are unitary and Hermitian

We know the first Pauli matrix is the identity matrix, which is by definition unitary and hermitian:

$$\sigma_0^\dagger = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \sigma_0 \quad (2)$$

So, we have :

$$\sigma_0^\dagger \sigma_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I \quad (3)$$

Similarly for the other Pauli Matrices, we have

$$\sigma_1^\dagger = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \sigma_1 \quad (4)$$

So, we have :

$$\sigma_1^\dagger \sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I \quad (5)$$

For σ_2 , we have:

$$\sigma_2^\dagger = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = \sigma_2 \quad (6)$$

So, we have :

$$\sigma_2^\dagger \sigma_2 = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I \quad (7)$$

For σ_3 :

$$\sigma_3^\dagger = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \sigma_3 \quad (8)$$

So, we have :

$$\sigma_3^\dagger \sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I \quad (9)$$

Hence, all Pauli matrices are unitary and hermitian.

2.20 Basis Change

Given operator A , with two matrix representations A' and A'' , on a vector space V with two different orthonormal basis, $|v_i\rangle$ and $|w_i\rangle$. The relation between them:

$$\begin{aligned}
A'_{ij} &= \langle v_i | A | v_j \rangle \\
&\Rightarrow \sum_k \langle v_i | w_k \rangle \langle w_k | A | v_j \rangle \\
&\Rightarrow \sum_{k,l} \langle v_i | w_k \rangle \langle w_k | A | w_l \rangle \langle w_l | v_j \rangle \\
&\Rightarrow \sum_{k,l} \langle v_i | U | v_k \rangle \langle w_k | A | w_l \rangle \langle v_l | U^\dagger | v_j \rangle \\
&\Rightarrow \sum_{k,l} U_{ik} A''_{kl} U_{lj}^\dagger
\end{aligned}$$

where $U \equiv \sum_m |w_m\rangle \langle v_m|$

2.21 Spectral Decomposition

The spectral decomposition is an extremely useful representation theorem for normal operators. It states: Any normal operator M on a vector space V is diagonal with respect to some orthonormal basis for V . Conversely, any diagonalizable operator is normal.

We will solve this by the method of induction. We'll assume the $n = 1$ case is trivial. Now, let λ be an eigenvalue of M , P is the projector on to the λ eigenspace, and Q the projector onto the orthogonal component. Then,

$$M = (P + Q)M(P + Q)$$

$$M = PMP + QMP + PMQ + QMQ$$

Now, obviously $PMP = \lambda P$, $QMP = 0$, since M takes the P subspace onto itself.

Furthermore, we can take the Hermitian conjugate of both sides to show that:

$$0 = (QMP)^\dagger = PMQ$$

Showing that QMQ is normal is trivial, since $QMQ = (QMQ)^\dagger$. Since PMP is diagonal with respect to some vector space, and QMQ is normal, and thus diagonal with respect to another orthogonal vector space, $PMP + QMQ$ is diagonal with respect to some orthonormal basis for the total vector space.

Alternatively

Suppose M be hermitian. Then $M = M^\dagger$

$$M = IMI$$

$$M + (P + Q)M(P + Q)$$

$$M = PMP + QMP + PMQ + QMQ$$

Now, $PMP = \lambda P$, $QMP = 0$, $PMQ = PM^\dagger Q = (QMP)^* = 0$. Thus $M = PMP + QMQ$

Now, we need to prove QMQ is normal.

$$\begin{aligned} QMQ(QMQ)^\dagger &= QMQQM^\dagger Q \\ \implies QM^\dagger Q QMQ \\ \implies (QM^\dagger Q) QMQ \end{aligned}$$

Therefore QMQ is normal. By induction, QMQ is diagonal.

2.22 Two Eigenvectors of a Hermitian operator with different eigenvalues are necessarily orthogonal

Let us assume M be the hermitian operator and $|v_i\rangle$ are the eigenvectors of M with eigenvalues λ_i . Then

$$\langle v_i | M | v_j \rangle = \lambda_j \langle v_i | v_j \rangle$$

, Similarly

$$\langle v_i | M | v_j \rangle = \langle v_i | M^\dagger | v_j \rangle = \langle v_j | M | v_i \rangle^* = \lambda_i^* \langle v_j | v_i \rangle^* = \lambda_i^* \langle v_i | v_j \rangle = \lambda_i \langle v_j | v_i \rangle$$

Thus,

$$(\lambda_i - \lambda_j) \langle v_i | v_j \rangle = 0$$

If $\lambda_i \neq \lambda_j$, then $\langle v_i | v_j \rangle = 0$

2.23 Show that the eigenvalues of a projector P are all either 0 or 1

Let us assume P is the projector and $|\lambda\rangle$ are the eigenvectors of the projector, with eigen values λ . Since its a projector operator $P^2 = P$

$$P|\lambda\rangle = \lambda|\lambda\rangle \text{ and } P|\lambda\rangle = P^2|\lambda\rangle = \lambda P|\lambda\rangle = \lambda^2|\lambda\rangle$$

Therefore,

$$\lambda = \lambda^2$$

$$\lambda(\lambda - 1) = 0$$

$$\lambda = 0 \text{ or } 1$$

2.24 Hermiticity of positive operators

Suppose A be a positive operator, A can be decomposed as:

$$\begin{aligned} A &= \frac{A + A^\dagger}{2} + \iota \frac{A - A^\dagger}{2i} \\ &= B + \iota C \text{ where } B = \frac{A + A^\dagger}{2}, C = \frac{A - A^\dagger}{2i} \end{aligned}$$

Now the operators B and C are hermitian.

$$\begin{aligned} \langle v|A|v\rangle &= \langle v|B + \iota C|v\rangle \\ \implies &= \langle v|B|v\rangle + \iota \langle v|C|v\rangle \\ \implies &= \alpha + \iota\beta \text{ where } \alpha = \langle v|B|v\rangle, \beta = \langle v|C|v\rangle \end{aligned}$$

Since B and C are hermitian, $\alpha, \beta \in \mathbb{R}$. From definition of positive operator, β should be vanished because $\langle v|A|v\rangle$ is real. Hence $\beta = \langle v|C|v\rangle = 0$ for all $|v\rangle$, i.e $C = 0$.

Therefore $A = A^\dagger$.

2.25 For any operator A , $A^\dagger A$ is positive

$$\langle \psi|A^\dagger A|\psi\rangle = \|A|\psi\rangle\|^2 \geq 0 \forall |\psi\rangle$$

Thus $A^\dagger A$ is positive.

2.26 Tensor Product

Given $|\psi\rangle = \frac{(|0\rangle + |1\rangle)}{\sqrt{2}}$, We need to find the tensor products, i.e:

$$\begin{aligned} |\psi\rangle^{\otimes 2} &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \\ &= \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \end{aligned}$$

Similarly for $|\psi\rangle^{\otimes 3}$:

$$\begin{aligned} |\psi\rangle^{\otimes 3} &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle) \end{aligned}$$

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

2.27 Matrix representation of the tensor products of the Pauli operators

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

Similarly,

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

and, so for

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

In general, the tensor product is not commutable.

2.28 Show that the transpose, complex conjugation, and adjoint operations distribute over the tensor product

$$(A \otimes B)^* = \begin{bmatrix} A_{11}B & \dots & A_{1n}B \\ \vdots & \ddots & \vdots \\ A_{m1}B & \dots & A_{mn}B \end{bmatrix}^*$$

$$\begin{aligned}
&= \begin{bmatrix} A_{11}^* B^* & \dots & A_{1n}^* B^* \\ \vdots & \ddots & \vdots \\ A_{m1}^* B^* & \dots & A_{mn}^* B^* \end{bmatrix} \\
&= A^* \otimes B^*
\end{aligned}$$

Now, for $(A \otimes B)^T$

$$\begin{aligned}
(A \otimes B)^T &= \begin{bmatrix} A_{11}B & \dots & A_{1n}B \\ \vdots & \ddots & \vdots \\ A_{m1}B & \dots & A_{mn}B \end{bmatrix}^T \\
&= \begin{bmatrix} A_{11}B^T & \dots & A_{m1}B^T \\ \vdots & \ddots & \vdots \\ A_{1n}B^T & \dots & A_{mn}B^T \end{bmatrix} \\
&= \begin{bmatrix} A_{11}B^T & \dots & A_{1m}B^T \\ \vdots & \ddots & \vdots \\ A_{n1}B^T & \dots & A_{nm}B^T \end{bmatrix} \\
&= A^T \otimes B^T
\end{aligned}$$

and for $(A \otimes B)^\dagger$

$$\begin{aligned}
(A \otimes B)^\dagger &= ((A \otimes B)^*)^T \\
&= (A^* \otimes B^*)^T \\
&= (A^*)^T \otimes (B^*)^T \\
&= A^\dagger \otimes B^\dagger
\end{aligned}$$

2.29 Tensor product of two unitary operators is unitary.

Suppose U_1 and U_2 are unitary operators. Then

$$\begin{aligned}
(U_1 \otimes U_2)(U_1 \otimes U_2)^\dagger &= U_1 U_1^\dagger \otimes U_2 U_2^\dagger \\
&= I \otimes I
\end{aligned}$$

In a similar way:

$$(U_1 \otimes U_2)^\dagger (U_1 \otimes U_2) = I \otimes I$$

2.30 Tensor product of two Hermitian operators is Hermitian

Suppose A and B are Hermitian operators. Then

$$(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger = A \otimes B$$

Thus we can say that $A \otimes B$ is Hermitian.

2.31 Tensor product of two positive operators is positive.

Suppose A and B are two positive operators. Then

$$\langle \psi | \otimes \langle \psi | (A \otimes B) | \psi \rangle \otimes | \phi \rangle = \langle \psi | A | \psi \rangle \langle \phi | B | \phi \rangle$$

Since A and B are positive operators, we have $\langle \psi | A | \psi \rangle \geq 0$ and $\langle \phi | B | \phi \rangle \geq 0 \forall |\psi\rangle, |\phi\rangle$. Then their product will also be greater than zero i.e $\langle \psi | A | \psi \rangle \langle \phi | B | \phi \rangle \geq 0$. Thus $A \otimes B$ is positive if A and B are positive.

2.32 Tensor product of two projectors is a projector

Suppose P_1 and P_2 are projectors. Then

$$\begin{aligned} (P_1 \otimes P_2)^2 &= P_1^2 \otimes P_2^2 \\ &= P_1 \otimes P_2 \end{aligned}$$

Thus $P_1 \otimes P_2$ is also a projector.

2.33 Hadamard operator on one qubit may be written as

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

2.34 Square Root and Log of a Matrix

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

We need to find the eigen values and the eigen vectors, i.e

$$\begin{aligned} \det (A - \lambda I) &= (4 - \lambda)^2 - 3^2 \\ &= \lambda^2 - 8\lambda + 7 \\ &= (\lambda - 1)(\lambda - 7) \end{aligned}$$

The eigenvalues for the A matrix are $\lambda = 1, 7$. Corresponding eigenvectors are :

$$|\lambda = 1\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \text{ and } |\lambda = 7\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

Thus the A matrix can be written as :

$$A = 1|\lambda = 1\rangle\langle\lambda = 1| + 7|\lambda = 7\rangle\langle\lambda = 7|$$

Now, it's easier to apply the operations, hence:

$$\sqrt{A} = \sqrt{1}|\lambda = 1\rangle\langle\lambda = 1| + \sqrt{7}|\lambda = 7\rangle\langle\lambda = 7|$$

$$\begin{aligned} &= \frac{1}{2} \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} + \frac{\sqrt{7}}{2} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \\ &= \frac{1}{2} \begin{bmatrix} 1 + \sqrt{7} & -1 + \sqrt{7} \\ -1 + \sqrt{7} & 1 + \sqrt{7} \end{bmatrix} \end{aligned}$$

Similarly for logarithm,

$$\begin{aligned} \log(A) &= \log(1)|\lambda = 1\rangle\langle\lambda = 1| + \log(7)|\lambda = 7\rangle\langle\lambda = 7| \\ &= \frac{\log(7)}{2} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \end{aligned}$$

2.35 Exponent of Pauli Matrices

We know :

$$\vec{v} \cdot \vec{\sigma} = \sum_{i=1}^3 v_i \sigma_i$$

where σ_i is the i^{th} Pauli Matrix.

$$\begin{aligned} &= v_1 \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + v_2 \begin{bmatrix} 0 & -\iota \\ \iota & 0 \end{bmatrix} + v_3 \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \\ &= \begin{bmatrix} v_3 & v_1 - \iota v_2 \\ v_1 + \iota v_2 & -v_3 \end{bmatrix} \end{aligned}$$

Now, for the eigen values:

$$\det(\vec{v} \cdot \vec{\sigma} - \lambda I) = (v_3 - \lambda)(-v_3 - \lambda) - (v_1 - \iota v_2)(v_1 + \iota v_2)$$

$$\begin{aligned} &\lambda^2 - (v_1^2 + v_2^2 + v_3^2) \\ &= \lambda^2 - 1 \text{ (Since } |\vec{v}| = 1 \text{)} \end{aligned}$$

Eigenvalues are $\lambda = \pm 1$. We let the eigenvectors be $|\lambda_{\pm 1}\rangle$ with the eigen values ± 1 .

We know that $\vec{v} \cdot \vec{\sigma}$ is Hermitian, and hence diagonalizable. Then

$$\vec{v} \cdot \vec{\sigma} = |\lambda_1\rangle\langle\lambda_1| - |\lambda_{-1}\rangle\langle\lambda_{-1}|$$

Thus:

$$\begin{aligned} \exp \iota\theta \vec{v} \cdot \vec{\sigma} &= \exp \iota\theta |\lambda_1\rangle\langle\lambda_1| + \exp -\iota\theta |\lambda_{-1}\rangle\langle\lambda_{-1}| \\ &= (\cos \theta + \iota \sin \theta) |\lambda_1\rangle\langle\lambda_1| + (\cos \theta - \iota \sin \theta) |\lambda_{-1}\rangle\langle\lambda_{-1}| \\ &= \cos \theta |\lambda_1\rangle\langle\lambda_1| + |\lambda_{-1}\rangle\langle\lambda_{-1}| + \iota \sin \theta |\lambda_1\rangle\langle\lambda_1| - |\lambda_{-1}\rangle\langle\lambda_{-1}| \\ &= \cos \theta I + \iota \sin \theta \vec{v} \cdot \vec{\sigma} \end{aligned}$$

Since $\vec{v} \cdot \vec{\sigma}$ is Hermitian, $|\lambda_1\rangle$ and $|\lambda_{-1}\rangle$ are orthogonal. Thus

$$|\lambda_1\rangle\langle\lambda_1| + |\lambda_{-1}\rangle\langle\lambda_{-1}| = I$$

2.36 Pauli Matrices except I has a trace 0

For σ_1 :

$$\text{Tr}(\sigma_1) = \text{Tr} \left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right) = 0$$

For σ_2

$$\text{Tr}(\sigma_2) = \text{Tr} \left(\begin{bmatrix} 0 & -\iota \\ \iota & 0 \end{bmatrix} \right) = 0$$

For σ_3

$$\text{Tr}(\sigma_3) = \text{Tr} \left(\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \right) = 0$$

2.37 Cyclic Properties of Trace

$$\begin{aligned} \text{Tr}(AB) &= \sum_i \langle i|AB|i\rangle \\ &= \sum_i \langle i|AIB|i\rangle \\ &= \sum_i \langle i|A|j\rangle \langle j|B|i\rangle \\ &= \sum_i \langle j|B|i\rangle \langle i|A|j\rangle \\ &= \sum_j \langle j|BA|j\rangle \\ &= \text{Tr}(BA) \end{aligned}$$

2.38 Linearity of Trace

$$\begin{aligned}
\text{Tr}(A + B) &= \sum_i \langle i | A + B | i \rangle \\
&= \sum_i \langle i | A | i \rangle + \langle i | B | i \rangle \\
&= \sum_i \langle i | A | i \rangle + \sum_i \langle i | B | i \rangle \\
&= \text{Tr}(A) + \text{Tr}(B)
\end{aligned}$$

$$\begin{aligned}
\text{Tr}(zA) &= \sum_i \langle i | zA | i \rangle \\
&= \sum_i z \langle i | A | i \rangle \\
&= z \sum_i \langle i | A | i \rangle \\
&= z \text{Tr}(A)
\end{aligned}$$

2.39 Hilbert-Schmidt Inner Product on Operators

We have to show

$$(A, B) = \text{Tr}(A^\dagger B)$$

$$\begin{aligned}
\left(A, \sum_i \lambda_i B_i \right) &= \text{Tr} \left[A^\dagger \left(\sum_i \lambda_i B_i \right) \right] \\
&= \text{Tr}(A^\dagger \lambda_1 B_1) + \dots + \text{Tr}(A^\dagger \lambda_n B_n)
\end{aligned}$$

$$\lambda_1 \text{Tr}(A^\dagger B_1) + \dots + \lambda_n \text{Tr}(A^\dagger B_n)$$

$$\sum_i \lambda_i \text{Tr}(A^\dagger B_i)$$

and for

$$\begin{aligned}
(A, B)^* &= \left(\text{Tr}(A^\dagger B) \right)^* \\
&= \left(\sum_{i,j} \langle i | A^\dagger | j \rangle \langle j | B | i \rangle \right)^* \\
&= \sum_{i,j} \langle i | A^\dagger | j \rangle^* \langle j | B | i \rangle^*
\end{aligned}$$

$$\begin{aligned}
&= \sum_{i,j} \langle j|B|i\rangle^* \langle i|A^\dagger|j\rangle^* \\
&= \sum_{i,j} \langle i|B^\dagger|j\rangle \langle j|A|i\rangle \\
&= \sum_{i,j} \langle i|B^\dagger A|i\rangle \\
&= \text{Tr}(B^\dagger A) \\
&= (B, A)
\end{aligned}$$

and,

$$\begin{aligned}
(A, A) &= \text{Tr}(A^\dagger A) \\
&= \sum_i \langle i|A^\dagger A|i\rangle
\end{aligned}$$

Since $A^\dagger A$ is positive, $\langle i|A^\dagger A|i\rangle \geq 0 \forall |i\rangle$. Let a_i be the i^{th} column of A . If $\langle i|A^\dagger A|i\rangle = 0$, then

$$\langle i|A^\dagger A|i\rangle = a_i^\dagger a_i = \|a_i\|^2 = 0 \text{ iff } a_i = 0$$

Therefor $(A, A) = 0$ iff $A = 0$

ii). A linear transformation $T : V \rightarrow V$ where $\dim(V) = d$ can be represented as a $d \times d$ matrix. Since there are $d \times d = d^2$ matrices that are linearly independent, the dimension of L_V is d^2 .

2.40 Commutation relation for the Pauli Matrices

We have

$$[X, Y] = XY - YX$$

$$\begin{aligned}
[X, Y] &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -\iota \\ \iota & 0 \end{bmatrix} - \begin{bmatrix} 0 & -\iota \\ \iota & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\
&= \begin{bmatrix} \iota & 0 \\ 0 & -\iota \end{bmatrix} - \begin{bmatrix} -\iota & 0 \\ 0 & \iota \end{bmatrix} \\
&= \begin{bmatrix} 2\iota & 0 \\ 0 & -2\iota \end{bmatrix} \\
&= 2\iota Z
\end{aligned}$$

$$\begin{aligned}
[Y, Z] &= \begin{bmatrix} 0 & -\iota \\ \iota & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} - \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 0 & -\iota \\ \iota & 0 \end{bmatrix} \\
&= \begin{bmatrix} 0 & 2\iota \\ 2\iota & 0 \end{bmatrix} \\
&= 2\iota X
\end{aligned}$$

Similarly,

$$\begin{aligned}
[Z, X] &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} - \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \\
&= 2\iota \begin{bmatrix} 0 & -\iota \\ \iota & 0 \end{bmatrix} \\
&= 2\iota Y
\end{aligned}$$

2.41 Anti-Commutation relation for the Pauli Matrices

We have

$$\begin{aligned}
\{\sigma_1, \sigma_2\} &= \sigma_1 \sigma_2 + \sigma_2 \sigma_1 \\
&= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -\iota \\ \iota & 0 \end{bmatrix} + \begin{bmatrix} 0 & -\iota \\ \iota & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\
&= \begin{bmatrix} \iota & 0 \\ 0 & -\iota \end{bmatrix} + \begin{bmatrix} -\iota & 0 \\ 0 & \iota \end{bmatrix} \\
&= 0
\end{aligned}$$

Similarly,

$$\begin{aligned}
\{\sigma_2, \sigma_3\} &= \begin{bmatrix} 0 & -\iota \\ \iota & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} - \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 0 & -\iota \\ \iota & 0 \end{bmatrix} \\
&= 0
\end{aligned}$$

and,

$$\begin{aligned}
\{\sigma_3, \sigma_1\} &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} - \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \\
&= 0
\end{aligned}$$

and, we have

$$\begin{aligned}
\sigma_0^2 &= I^2 = I \\
\sigma_1^2 &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^2 = I \\
\sigma_2^2 &= \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}^2 = I \\
\sigma_3^2 &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}^2 = I
\end{aligned}$$

2.42 verify

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

2.43 Show $\sigma_j \sigma_k$

We know that $\{\sigma_j, \sigma_k\} = 2\delta_{jk}I$ using that

$$\begin{aligned}\sigma_j \sigma_k &= \frac{[\sigma_j, \sigma_k] + \{\sigma_j, \sigma_k\}}{2} \\ &= \frac{2\ell \sum_{i=1}^3 \epsilon_{jkl} \sigma_l + 2\delta_{jk}I}{2} \\ &= \delta_{jk}I + \ell \sum_{l=1}^3 \epsilon_{jkl} \sigma_l\end{aligned}$$

2.44 B must be zero

By Assumption, $[A, B] = 0$ and $\{A, B\} = 0$, then $AB = 0$. Since A is invertible, multiply by A^{-1} from left, then

$$A^{-1}AB = 0$$

$$IB = 0$$

$$B = 0$$

2.45 Verify

$$\begin{aligned}[A, B]^\dagger &= (AB - BA)^\dagger \\ &= B^\dagger A^\dagger - A^\dagger B^\dagger \\ &= [B^\dagger, A^\dagger]\end{aligned}$$

2.46 Verify

$$\begin{aligned}[A, B] &= AB - BA \\ &= -(BA - AB) \\ &= -[B, A]\end{aligned}$$

2.47 Verify

$$\begin{aligned}
(\iota[A, B])^\dagger &= \iota[A, B]^\dagger \\
&= \iota[B^\dagger, A^\dagger] \\
&= -\iota[B, A] \\
&= \iota[A, B]
\end{aligned}$$

2.48 Polar decomposition of P , U and H

Since P is positive, it is diagonalizable. Then $P = \sum_i \lambda_i |i\rangle\langle i|$, where $\lambda_i \geq 0$

$$J = \sqrt{P^\dagger P} = \sqrt{PP} = \sqrt{P^2} = \sum_i \sqrt{\lambda_i^2} |i\rangle\langle i| = \sum_i \lambda_i |i\rangle\langle i| = P$$

Therefore polar decomposition of P is $P = UP$ for all P . Thus $U = I$, then $P = P$

For the unitary U :

Suppose unitary U is decomposed by $U = WJ$ where W is unitary and J is positive, $J = \sqrt{U^\dagger U}$

$$J = \sqrt{U^\dagger U} = \sqrt{I} = I$$

Since unitary operators are invertible, $W = UJ^{-1} = UI^{-1} = UI = U$. Thus the polar decompositions of U is $U = U$

For the Hermitian H :

Suppose $H = UJ$

$$J = \sqrt{H^\dagger H} = \sqrt{HH} = \sqrt{H^2}$$

Thus $H = U\sqrt{H^2}$

In general $H \neq \sqrt{H^2}$ From spectral decomposition, $H = \sum_i \lambda_i |i\rangle\langle i|$, where $\lambda_i \in \mathbb{R}$

$$\sqrt{H^2} = \sqrt{\sum_i \lambda_i^2 |i\rangle\langle i|} = \sum_i \sqrt{\lambda_i^2} |i\rangle\langle i| = \sum_i |\lambda_i| |i\rangle\langle i| \neq H$$

2.49 Polar decomposition of Normal Matrix

Normal matrix is diagonalizable, $A = \sum_i \lambda_i |i\rangle\langle i|$

$$J = \sqrt{A^\dagger A} = \sum_i |\lambda_i| |i\rangle\langle i|$$

$$U = \sum_i |e_i\rangle\langle i|$$

$$A = UJ = \sum_i |\lambda_i| |e_i\rangle\langle i|$$

2.50 Left and Right Polar Decomposition

We have $A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ and so we have $A^\dagger A = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$

Characteristic equation of $A^\dagger A$ is $\det(A^\dagger A - \lambda I) = \lambda^2 - 3\lambda + 1 = 0$. Eigenvalues of $A^\dagger A$ are $\lambda_{\pm} = \frac{3 \pm \sqrt{5}}{2}$ and the associated eigenvectors are $|\lambda_{\pm}\rangle =$

$$\frac{1}{\sqrt{10 \mp 2\sqrt{5}}} \begin{bmatrix} 2 \\ -1 \pm \sqrt{5} \end{bmatrix}$$

$$A^\dagger A = \lambda_+ |\lambda_+\rangle \langle \lambda_+| + \lambda_- |\lambda_-\rangle \langle \lambda_-|$$

$$J = \sqrt{A^\dagger A} = \sqrt{\lambda_+} |\lambda_+\rangle \langle \lambda_+| + \sqrt{\lambda_-} |\lambda_-\rangle \langle \lambda_-|$$

Substituting all the values, you'll get:

$$J^{-1} = \frac{1}{\sqrt{\lambda_+}} |\lambda_+\rangle \langle \lambda_+| + \frac{1}{\sqrt{\lambda_-}} |\lambda_-\rangle \langle \lambda_-|$$

Which gives us $U = AJ^{-1}$

2.51 H is unitary

$$\begin{aligned} H^\dagger H &= \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \right)^\dagger \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \right) \\ &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \\ &= \frac{1}{2} \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = I \end{aligned}$$

2.52 H^2 is identity

$$\begin{aligned} H^\dagger &= \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \right)^\dagger \\ &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = H \end{aligned}$$

Thus

$$H^2 = I$$

2.53 Eigen values and eigen vectors of H

We have $\det(H - \lambda I) = \left(\frac{1}{\sqrt{2}} - \lambda\right)\left(\frac{-1}{\sqrt{2}} - \lambda\right) - \frac{1}{2}$

$$= \lambda^2 - \frac{1}{2} - \frac{1}{2}$$

$$= \lambda^2 - 1$$

Eigenvalues are $\lambda_{\pm} = \pm 1$ and associated eigenvectors are $|\lambda_{\pm}\rangle = \frac{1}{\sqrt{4 \mp 2\sqrt{2}}} \begin{bmatrix} 1 \\ -1 \pm \sqrt{2} \end{bmatrix}$

2.54 $\exp A \exp B = \exp A + B$

Since $[A, B] = 0$, A and B are simultaneously diagonalizable, $A = \sum_i a_i |i\rangle\langle i|$, and $B = \sum_i b_i |i\rangle\langle i|$.

So,

$$\begin{aligned} \exp A \exp B &= \left(\sum_i \exp a_i |i\rangle\langle i| \right) \left(\sum_j \exp b_j |j\rangle\langle j| \right) \\ &= \sum_{i,j} \exp a_i + b_j |i\rangle\langle i|j\rangle\langle j| \\ &= \sum_{i,j} \exp a_i + b_j |i\rangle\langle j| \delta_{i,j} \\ &= \sum_i \exp a_i + b_i |i\rangle\langle i| \\ &= \exp A + B \end{aligned}$$

2.55 $U(t_1, t_2)$ is unitary

$$\begin{aligned} H &= \sum_E E |E\rangle\langle E| \\ U(t_2 - t_1) U^\dagger(t_2 - t_1) &= \exp \frac{-iH(t_2 - t_1)}{\hbar} \exp \frac{iH(t_2 - t_1)}{\hbar} \\ &= \sum_{E, E'} \left(\exp \frac{-iE(t_2 - t_1)}{\hbar} |E\rangle\langle E| \right) \left(\exp \frac{-iE'(t_2 - t_1)}{\hbar} |E'\rangle\langle E'| \right) \\ &= \sum_E \exp 0 |E\rangle\langle E| \\ &= \sum_E |E\rangle\langle E| \\ &= I \end{aligned}$$

Similarly, $U^\dagger(t_2 - t_1) U(t_2 - t_1) = I$

2.56 Spectral Decomposition

$$U = \sum_i \lambda_i |\lambda_i\rangle\langle\lambda_i|$$

Now,

$$\log(U) = \sum_j \log(\lambda_j) |\lambda_j\rangle\langle\lambda_j| = \sum_j \iota \theta_j |\lambda_j\rangle\langle\lambda_j|$$

where $\theta_j = \arg(\lambda_j)$

$$K = \iota \log(U) = \sum_j \theta_j |\lambda_j\rangle\langle\lambda_j|$$

$$K^\dagger = (\iota \log U)^\dagger = \left(\sum_j \theta_j |\lambda_j\rangle\langle\lambda_j| \right)^\dagger = \sum_j \theta_j |\lambda_j\rangle\langle\lambda_j| = K$$

2.57 Cascaded Measurements are single measurements

We have

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

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

$$\begin{aligned} \frac{M_m |\phi\rangle}{\sqrt{\langle\phi|M_m^\dagger M_m|\phi\rangle}} &= \frac{M_m L_l |\psi\rangle}{\sqrt{\langle\phi|L_l^\dagger L_l|\phi\rangle}} = \frac{\sqrt{\langle\psi|L_l^\dagger L_l|\psi\rangle}}{\sqrt{\langle\psi|L_l^\dagger M_m^\dagger M_m L_l|\psi\rangle}} \\ &= \frac{M_m L_l |\psi\rangle}{\sqrt{\langle\psi|L_l^\dagger M_m^\dagger M_m L_l|\psi\rangle}} \\ &= \frac{N_{lm} |\psi\rangle}{\sqrt{\langle\psi|N_{lm}^\dagger N_{lm}|\psi\rangle}} \end{aligned}$$

2.58 Average Observed value of M

$$\langle M \rangle = \langle\psi|M|\psi\rangle = \langle\psi|m|\psi\rangle = m \langle\psi|\psi\rangle = m$$

$$\langle M^2 \rangle = \langle\psi|M^2|\psi\rangle = \langle\psi|m^2|\psi\rangle = m^2 \langle\psi|\psi\rangle = m^2$$

$$\text{deviation} = \langle M^2 \rangle - \langle M \rangle^2 = m^2 - m^2 = 0$$

2.59 Average and Standard Deviation of X

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

$$\langle X^2 \rangle = \langle 0|X^2|0 \rangle = \langle 0|X|1 \rangle = \langle 0|0 \rangle = 1$$

$$\text{standard deviation} = \sqrt{\langle X^2 \rangle - \langle X \rangle^2} = 1$$

2.60

$$\begin{aligned} \vec{v} \cdot \vec{\sigma} &= \sum_{i=1}^3 v_i \sigma_i \\ &= v_1 \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + v_2 \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} + v_3 \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \\ &= \begin{bmatrix} v_3 & v_1 - iv_2 \\ v_1 + iv_2 & -v_3 \end{bmatrix} \end{aligned}$$

$$\begin{aligned} \det(\vec{v} \cdot \vec{\sigma} - \lambda I) &= (v_3 - \lambda)(-v_3 - \lambda) - (v_1 - iv_2)(v_1 + iv_2) \\ &= \lambda^2 - (v_1^2 + v_2^2 + v_3^2) \\ &= \lambda^2 - 1 \quad (\because |\vec{v}| = 1) \end{aligned}$$

Eigenvalues are $\lambda = \pm 1$.

(i) if $\lambda = 1$

$$\begin{aligned} \vec{v} \cdot \vec{\sigma} - \lambda I &= \vec{v} \cdot \vec{\sigma} - I \\ &= \begin{bmatrix} v_3 - 1 & v_1 - iv_2 \\ v_1 + iv_2 & -v_3 - 1 \end{bmatrix} \end{aligned}$$

Normalized eigenvector is $|\lambda_1\rangle = \sqrt{\frac{1+v_3}{2}} \begin{bmatrix} 1 \\ \frac{1-v_3}{v_1-iv_2} \end{bmatrix}$.

$$\begin{aligned} \lambda_1 &= \frac{1+v_3}{2} \begin{bmatrix} 1 \\ \frac{1-v_3}{v_1-iv_2} \end{bmatrix} \begin{bmatrix} 1 & \frac{1-v_3}{v_1+iv_2} \end{bmatrix} = \frac{1+v_3}{2} \begin{bmatrix} 1 & \frac{v_1-iv_2}{1+v_3} \\ \frac{v_1+iv_2}{1+v_3} & \frac{1-v_3}{1+v_3} \end{bmatrix} \\ &= \frac{1}{2} \begin{bmatrix} 1+v_3 & v_1-iv_2 \\ v_1+iv_2 & 1-v_3 \end{bmatrix} = \frac{1}{2} \left(I + \begin{bmatrix} v_3 & v_1-iv_2 \\ v_1+iv_2 & -v_3 \end{bmatrix} \right) = \frac{1}{2} (I + \vec{v} \cdot \vec{\sigma}) \end{aligned}$$

(ii) If $\lambda = -1$.

$$\begin{aligned} \vec{v} \cdot \vec{\sigma} - \lambda I &= \vec{v} \cdot \vec{\sigma} + I \\ &= \begin{bmatrix} v_3 + 1 & v_1 - iv_2 \\ v_1 + iv_2 & -v_3 + 1 \end{bmatrix} \end{aligned}$$

Normalized eigenvalue is $|\lambda_{-1}\rangle = \sqrt{\frac{1-v_3}{2}} \begin{bmatrix} 1 \\ -\frac{1+v_3}{v_1-iv_2} \end{bmatrix}$.

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

This proof has a defect. The case $(v_1, v_2, v_3) = (0, 0, 1)$, second component of eigenstate, $\frac{1-v_3}{v_1-iv_2}$, diverges. So I implicitly assume $v_1 - iv_2 \neq 0$. Hence my proof is incomplete.

Since the exercise doesn't require explicit form of projector, we should prove the problem more abstractly. In order to prove, we use the following properties of $\vec{v} \cdot \vec{\sigma}$

- $\vec{v} \cdot \vec{\sigma}$ is Hermitian
- $(\vec{v} \cdot \vec{\sigma})^2 = I$ where \vec{v} is a real unit vector.

We can easily check above conditions.

$$\begin{aligned} (\vec{v} \cdot \vec{\sigma})^\dagger &= (v_1\sigma_1 + v_2\sigma_2 + v_3\sigma_3)^\dagger \\ &= v_1\sigma_1^\dagger + v_2\sigma_2^\dagger + v_3\sigma_3^\dagger \\ &= v_1\sigma_1 + v_2\sigma_2 + v_3\sigma_3 \quad (\because \text{Pauli matrices are Hermitian.}) \\ &= \vec{v} \cdot \vec{\sigma} \end{aligned}$$

$$\begin{aligned} (\vec{v} \cdot \vec{\sigma})^2 &= \sum_{j,k=1}^3 (v_j\sigma_j)(v_k\sigma_k) \\ &= \sum_{j,k=1}^3 v_jv_k\sigma_j\sigma_k \\ &= \sum_{j,k=1}^3 v_jv_k \left(\delta_{jk}I + i \sum_{l=1}^3 \epsilon_{jkl}\sigma_l \right) \quad (\because \text{eqn(2.78) page78}) \\ &= \sum_{j,k=1}^3 v_jv_k\delta_{jk}I + i \sum_{j,k,l=1}^3 \epsilon_{jkl}v_jv_k\sigma_l \\ &= \sum_{j=1}^3 v_j^2 I \\ &= I \quad \left(\because \sum_j v_j^2 = 1 \right) \end{aligned}$$

Suppose $|\lambda\rangle$ is an eigenstate of $\vec{v} \cdot \vec{\sigma}$ with eigenvalue λ . Then

$$\begin{aligned}\vec{v} \cdot \vec{\sigma} |\lambda\rangle &= \lambda |\lambda\rangle \\ (\vec{v} \cdot \vec{\sigma})^2 |\lambda\rangle &= \lambda^2 |\lambda\rangle\end{aligned}$$

On the other hand $(\vec{v} \cdot \vec{\sigma})^2 = I$,

$$\begin{aligned}(\vec{v} \cdot \vec{\sigma})^2 |\lambda\rangle &= I |\lambda\rangle = |\lambda\rangle \\ \therefore \lambda^2 |\lambda\rangle &= |\lambda\rangle.\end{aligned}$$

Thus $\lambda^2 = 1 \Rightarrow \lambda = \pm 1$. Therefore $\vec{v} \cdot \vec{\sigma}$ has eigenvalues ± 1 .

Let $|\lambda_1\rangle$ and $|\lambda_{-1}\rangle$ are eigenvectors with eigenvalues 1 and -1 , respectively. I will prove that $P_{\pm} = |\lambda_{\pm 1}\rangle$.

In order to prove above equation, all we have to do is prove following condition.

$$\langle \psi | (P_{\pm} - \lambda_{\pm 1}) | \psi \rangle = 0 \text{ for all } |\psi\rangle \in \mathbb{C}^2$$

Since $\vec{v} \cdot \vec{\sigma}$ is Hermitian, $|\lambda_1\rangle$ and $|\lambda_{-1}\rangle$ are orthonormal vector (\because Exercise 2.22). Let $|\psi\rangle \in \mathbb{C}^2$ be an arbitrary state. $|\psi\rangle$ can be written as

$$|\psi\rangle = \alpha |\lambda_1\rangle + \beta |\lambda_{-1}\rangle \quad (|\alpha|^2 + |\beta|^2 = 1, \alpha, \beta \in \mathbb{C}).$$

$$\begin{aligned}\langle \psi | (P_{\pm} - \lambda_{\pm}) | \psi \rangle &= \langle \psi | P_{\pm} | \psi \rangle - \langle \psi | \lambda_{\pm} \rangle \langle \lambda_{\pm} | \psi \rangle. \\ \langle \psi | P_{\pm} | \psi \rangle &= \langle \psi | \frac{1}{2} (I \pm \vec{v} \cdot \vec{\sigma}) | \psi \rangle \\ &= \frac{1}{2} \pm \frac{1}{2} \langle \psi | \vec{v} \cdot \vec{\sigma} | \psi \rangle \\ &= \frac{1}{2} \pm \frac{1}{2} (|\alpha|^2 - |\beta|^2) \\ &= \frac{1}{2} \pm \frac{1}{2} (2|\alpha|^2 - 1) \quad (\because |\alpha|^2 + |\beta|^2 = 1) \\ \langle \psi | \lambda_1 \rangle \langle \lambda_1 | \psi \rangle &= |\alpha|^2 \\ \langle \psi | \lambda_{-1} \rangle \langle \lambda_{-1} | \psi \rangle &= |\beta|^2 = 1 - |\alpha|^2\end{aligned}$$

Therefore $\langle \psi | (P_{\pm} - \lambda_{\pm 1}) | \psi \rangle = 0$ for all $|\psi\rangle \in \mathbb{C}^2$. Thus $P_{\pm} = \lambda_{\pm 1}$.

2.61 Calculate the Probability

$$\begin{aligned}\langle \lambda_1 | 0 \rangle \langle 0 | \lambda_1 \rangle &- \langle 0 | \lambda_1 \rangle \langle \lambda_1 | 0 \rangle \\ &= \langle 0 | \frac{1}{2} (I + \vec{v} \cdot \vec{\sigma}) | 0 \rangle \\ &= \frac{1}{2} (1 + v_3)\end{aligned}$$

and the state after measurement is

$$\begin{aligned}
\frac{|\lambda_1\rangle\langle\lambda_1|0\rangle}{\sqrt{\langle 0|\lambda_1\rangle\langle\lambda_1|0\rangle}} &= \frac{1}{\sqrt{\frac{1}{2}(1+v_3)}} \cdot \frac{1}{2} \begin{bmatrix} 1+v_3 \\ v_1+\iota v_2 \end{bmatrix} \\
&= \sqrt{\frac{1}{2}(1+v_3)} \cdot \begin{bmatrix} 1 \\ \frac{v_1+\iota v_2}{1+v_3} \end{bmatrix} \\
&= \sqrt{\frac{1+v_3}{2}} \begin{bmatrix} 1 \\ \frac{1-v_3}{v_1-\iota v_2} \end{bmatrix} \\
&= |\lambda_1\rangle
\end{aligned}$$

2.62 Projective Measurement

Let's assume M_m is a measurement operator. From the assumption, we have $E_m = M_m^\dagger M_m = M_m$, Then

$$\langle\psi|E_m|\psi\rangle = \langle\psi|M_m|\psi\rangle \geq 0 \quad \forall |\psi\rangle$$

Since M_m is a positive operator, M_m is Hermitian. Therefore,

$$E_m = M_m^\dagger M_m = M_m M_m = M_m^2 = M_m$$

Thus the measurement is a projective measurement.

2.63 Measurement Operators M_m

We have

$$\begin{aligned}
M_m^\dagger M_m &= \sqrt{E_m} U_m^\dagger U_m \sqrt{E_m} \\
&= \sqrt{E_m} I \sqrt{E_m} \\
&= E_m
\end{aligned}$$

Since E_m is POVM, for arbitrary unitary U , $M_m^\dagger M_m$ is a POVM

2.64 Construct a POVM

We can construct $|\psi'_j\rangle$ that is orthogonal to all states except $|\psi_j\rangle$. That is

$$|\psi'_j\rangle = |\psi_j\rangle - \sum_{k=1, k \neq j}^m \frac{\langle\psi_j|\psi_k\rangle|\psi_k\rangle}{||\psi_k||^2}$$

Then E_m is

$$E_m = A|\psi'_m\rangle\langle\psi'_m|$$

where A is chosen such that

$$E_{m+1} = I - \sum_{j=1}^m E_j$$

is positive.

2.65 Express the states in Composite system

The $|+\rangle$ and $|-\rangle$ states

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

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

2.66 Average Value

Let $|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$. Then,

$$\begin{aligned} E(X_1 Z_2) &= \langle \psi | X_1 Z_2 | \psi \rangle \\ &= \frac{1}{2} (\langle 00 | X_1 Z_2 | 00 \rangle + \langle 00 | X_1 Z_2 | 11 \rangle + \langle 11 | X_1 Z_2 | 00 \rangle + \langle 11 | X_1 Z_2 | 11 \rangle) \\ &= \frac{1}{2} (\langle 00 | 10 \rangle - \langle 00 | 01 \rangle + \langle 11 | 10 \rangle - \langle 11 | 01 \rangle) \\ &= 0 \end{aligned}$$

2.67 $V \approx$ Hilbert Space

Suppose W^\perp is the orthogonal complement of W . Then $V = W \oplus W^\perp$. Let $|w_i\rangle, |w'_j\rangle, |u'_j\rangle$ be orthonormal bases for $W, W^\perp, (\text{image}(U))^\perp$, respectively.

Define $U': V \rightarrow V$ as $U' = \sum_i u_i w_i + \sum_j u'_j w'_j$, where $|u_i\rangle = U |w_i\rangle$.

Now

$$\begin{aligned} (U')^\dagger U' &= \left(\sum_{i=1}^{\dim W} w_i u_i + \sum_{j=1}^{\dim W^\perp} w'_j u'_j \right) \left(\sum_i u_i w_i + \sum_j u'_j w'_j \right) \\ &= \sum_i w_i + \sum_j w'_j = I \end{aligned}$$

and

$$\begin{aligned} U'(U')^\dagger &= \left(\sum_i u_i w_i + \sum_j u'_j w'_j \right) \left(\sum_i w_i u_i + \sum_j w'_j u'_j \right) \\ &= \sum_i u_i + \sum_j u'_j = I. \end{aligned}$$

Thus U' is a unitary operator. Moreover, for all $|w\rangle \in W$,

$$\begin{aligned}
U'|w\rangle &= \left(\sum_i u_i w_i + \sum_j u'_j w'_j \right) |w\rangle \\
&= \sum_i |u_i\rangle \langle w_i|w\rangle + \sum_j |u'_j\rangle \langle w'_j|w\rangle \\
&= \sum_i |u_i\rangle \langle w_i|w\rangle \quad (\because |w'_j\rangle \perp |w\rangle) \\
&= \sum_i U|w_i\rangle \langle w_i|w\rangle \\
&= U|w\rangle.
\end{aligned}$$

Therefore U' is an extension of U .

2.68 $|\psi\rangle \neq |a\rangle|b\rangle$

Suppose one of the bell states:

$$|\psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$$

can be written as a product of single particle states

$$|a\rangle = \alpha_a|0\rangle + \beta_a|1\rangle$$

$$|b\rangle = \alpha_b|0\rangle + \beta_b|1\rangle$$

Then

$$|a\rangle|b\rangle = \alpha_a\alpha_b|00\rangle + \alpha_a\beta_b|01\rangle + \beta_a\alpha_b|10\rangle + \beta_a\beta_b|11\rangle$$

Comparing this with the bell state $|\psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ we have

$$\alpha_a\beta_b = 0$$

$$\beta_a\alpha_b = 0$$

This contradicts $|\psi\rangle = |a\rangle|b\rangle$. So $|\psi\rangle \neq |a\rangle|b\rangle$ for all single qubits states $|a\rangle$ and $|b\rangle$.

2.69 Bell Basis

We know the bell states are:

$$|\psi_1\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

$$|\psi_2\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ -1 \end{bmatrix}$$

$$|\psi_3\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

$$|\psi_4\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ -1 \\ 0 \end{bmatrix}$$

To form a basis, it must be linearly independent, Hence:

$$a_1 |\psi_1\rangle + a_2 |\psi_2\rangle + a_3 |\psi_3\rangle + a_4 |\psi_4\rangle = 0$$

$$\implies \frac{1}{\sqrt{2}} \begin{bmatrix} a_1 + a_2 \\ a_3 + a_4 \\ a_3 - a_4 \\ a_1 - a_2 \end{bmatrix} = 0$$

$$\implies a_1 = a_2 = a_3 = a_4 = 0$$

Thus $\{|\psi_i\rangle\}$ is a linearly independent basis.

Moreover $||\psi_i\rangle|| = 1$ and $\langle\psi_i|\psi_j\rangle = \delta_{ij}$ for $i, j = 1, 2, 3, 4$. Thus it forms an orthonormal basis.

2.70 Bell States

For any Bell state we have $\langle\psi_i|E \otimes I|\psi_i\rangle = \frac{1}{2}(\langle 0|E|0\rangle + \langle 1|E|1\rangle)$

Suppose Eve measures the qubit Alice sent by measurement operators M_m . The probability that Eve get result m is $p_i(m) = \langle\psi_i|M_m^\dagger M_m \otimes I|\psi_i\rangle$ Since $M_m^\dagger M_m$ is positive, $p_i(m)$ are same values for all $|\psi_i\rangle$. Thus Eve can't distinguish Bell states.

2.71 Mixed or Pure

We know from spectral decomposition

$$\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i|, \quad p_i \geq 0, \quad \sum_i p_i = 1$$

$$\begin{aligned} \rho^2 &= \sum_{i,j} p_i p_j |i\rangle \langle i| |j\rangle \langle j| \\ &= \sum_{i,j} p_i p_j |i\rangle \langle i| \delta_{ij} \end{aligned}$$

$$= \sum_i p_i^2 |i\rangle\langle i|$$

$$Tr(\rho^2) = Tr\left(\sum_i p_i^2 |i\rangle\langle i|\right) = \sum_i p_i^2 Tr(|i\rangle\langle i|) = \sum_i p_i^2 |i\rangle\langle i| = \sum_i p_i^2 \geq \sum_i p_i = 1$$

Suppose $Tr(\rho^2) = 1$. Then $\sum_i p_i^2 = 1$. Since $p_i^2 < p_i$ for $0 < p_i < 1$, only single p_i should be 1 and otherwise have to vanish. Therefore $\rho = |\psi_i\rangle\langle\psi_i|$. It is a pure state.

Conversely if ρ is pure, then $\rho = |\psi_i\rangle\langle\psi_i|$

$$Tr(\rho^2) = Tr(|\psi_i\rangle\langle\psi_i||\psi_i\rangle\langle\psi_i|) = Tr(|\psi_i\rangle\langle\psi_i|) = |\psi_i\rangle\langle\psi_i| = 1$$

2.72 Bloch Sphere

(1) Since density matrix is Hermitian, matrix representation is $\rho = \begin{bmatrix} a & b \\ b^* & d \end{bmatrix}$, $a, d \in \mathbb{R}$ and $b \in \mathbb{C}$ w.r.t. standard basis. Because ρ is density matrix, $(\rho) = a + d = 1$.

Define $a = (1 + r_3)/2$, $d = (1 - r_3)/2$ and $b = (r_1 - ir_2)/2$, ($r_i \in \mathbb{R}$).

In this case,

$$\rho = \begin{bmatrix} a & b \\ b^* & d \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 + r_3 & r_1 - ir_2 \\ r_1 + ir_2 & 1 - r_3 \end{bmatrix} = \frac{1}{2}(I + \vec{r} \cdot \vec{\sigma}).$$

Thus for arbitrary density matrix ρ can be written as $\rho = \frac{1}{2}(I + \vec{r} \cdot \vec{\sigma})$.

Next, we derive the condition that ρ is positive.

If ρ is positive, all eigenvalues of ρ should be non-negative.

$$\det(\rho - \lambda I) = (a - \lambda)(b - \lambda) - |b|^2 = \lambda^2 - (a + d)\lambda + ad - |b|^2 = 0$$

$$\begin{aligned} \lambda &= \frac{(a + d) \pm \sqrt{(a + d)^2 - 4(ad - |b|^2)}}{2} \\ &= \frac{1 \pm \sqrt{1 - 4\left(\frac{1-r_3^2}{4} - \frac{r_1^2+r_2^2}{4}\right)}}{2} \\ &= \frac{1 \pm \sqrt{1 - (1 - r_1^2 - r_2^2 - r_3^2)}}{2} = \frac{1 \pm \sqrt{|\vec{r}|^2}}{2} = \frac{1 \pm |\vec{r}|}{2} \end{aligned}$$

Since ρ is positive, $\frac{1-|\vec{r}|}{2} \geq 0 \rightarrow |\vec{r}| \leq 1$.

Therefore an arbitrary density matrix for a mixed state qubit is written as $\rho = \frac{1}{2}(I + \vec{r} \cdot \vec{\sigma})$.

(2)

$\rho = I/2 \rightarrow \vec{r} = 0$. Thus $\rho = I/2$ corresponds to the origin of Bloch sphere.

(3)

$$\begin{aligned}
\rho^2 &= \frac{1}{2}(I + \vec{r} \cdot \vec{\sigma}) \frac{1}{2}(I + \vec{r} \cdot \vec{\sigma}) \\
&= \frac{1}{4} \left[I + 2\vec{r} \cdot \vec{\sigma} + \sum_{j,k} r_j r_k \left(\delta_{jk} I + i \sum_{l=1}^3 \epsilon_{jkl} \sigma_l \right) \right] \\
&= \frac{1}{4} (I + 2\vec{r} \cdot \vec{\sigma} + |\vec{r}|^2 I) \\
(\rho^2) &= \frac{1}{4} (2 + 2|\vec{r}|^2)
\end{aligned}$$

If ρ is pure, then $(\rho^2) = 1$.

$$\begin{aligned}
1 &= (\rho^2) = \frac{1}{4} (2 + 2|\vec{r}|^2) \\
&\therefore |\vec{r}| = 1.
\end{aligned}$$

Conversely, if $|\vec{r}| = 1$, then $(\rho^2) = \frac{1}{4} (2 + 2|\vec{r}|^2) = 1$. Therefore ρ is pure.

2.73

Theorem 2.6

$$\rho = \sum_i p_i \psi_i = \sum_i \tilde{\psi}_i = \sum_j \tilde{\varphi}_j = \sum_j q_j \varphi_j \Leftrightarrow |\tilde{\psi}_i\rangle = \sum_j u_{ij} |\tilde{\varphi}_j\rangle$$

where u is unitary.

The transformation in theorem 2.6, $|\tilde{\psi}_i\rangle = \sum_j u_{ij} |\tilde{\varphi}_j\rangle$, corresponds to

$$[|\tilde{\psi}_1\rangle \cdots |\tilde{\psi}_k\rangle] = [|\tilde{\varphi}_1\rangle \cdots |\tilde{\varphi}_k\rangle] U^T$$

where $k = \text{rank}(\rho)$.

$$\sum_i \tilde{\psi}_i = [|\tilde{\psi}_1\rangle \cdots |\tilde{\psi}_k\rangle] \begin{bmatrix} \langle \tilde{\psi}_1 | \\ \vdots \\ \langle \tilde{\psi}_k | \end{bmatrix} \quad (10)$$

$$= [|\tilde{\varphi}_1\rangle \cdots |\tilde{\varphi}_k\rangle] U^T U^* \begin{bmatrix} \langle \tilde{\varphi}_1 | \\ \vdots \\ \langle \tilde{\varphi}_k | \end{bmatrix} \quad (11)$$

$$= [|\tilde{\varphi}_1\rangle \cdots |\tilde{\varphi}_k\rangle] \begin{bmatrix} \langle \tilde{\varphi}_1 | \\ \vdots \\ \langle \tilde{\varphi}_k | \end{bmatrix} \quad (12)$$

$$= \sum_j \tilde{\varphi}_j. \quad (13)$$

From spectral theorem, density matrix ρ is decomposed as $\rho = \sum_{k=1}^d \lambda_k k$ where $d = \dim \mathcal{H}$. Without loss of generality, we can assume $p_k > 0$ for $k = 1 \cdots l$ where $l = \text{rank}(\rho)$ and $p_k = 0$ for $k = l+1, \dots, d$. Thus $\rho = \sum_{k=1}^l p_k k = \sum_{k=1}^l \tilde{k}$, where $|\tilde{k}\rangle = \sqrt{\lambda_k} |k\rangle$.

Suppose $|\psi_i\rangle$ is a state in support ρ . Then

$$|\psi_i\rangle = \sum_{k=1}^l c_{ik} |k\rangle, \quad \sum_k |c_{ik}|^2 = 1.$$

Define $p_i = \frac{1}{\sum_k \frac{|c_{ik}|^2}{\lambda_k}}$ and $u_{ik} = \frac{\sqrt{p_i} c_{ik}}{\sqrt{\lambda_k}}$.

Now

$$\sum_k |u_{ik}|^2 = \sum_k \frac{p_i |c_{ik}|^2}{\lambda_k} = p_i \sum_k \frac{|c_{ik}|^2}{\lambda_k} = 1.$$

Next prepare an unitary operator¹ such that i th row of U is $[u_{i1} \cdots u_{ik} \cdots u_{il}]$.

¹By Gram-Schmidt procedure construct an orthonormal basis $\{\mathbf{u}_j\}$ (row vector) with $\mathbf{u}_i =$

Then we can define another ensemble such that

$$\left[|\tilde{\psi}_1\rangle \cdots |\tilde{\psi}_i\rangle \cdots |\tilde{\psi}_l\rangle \right] = \left[|\tilde{k}_1\rangle \cdots |\tilde{k}_l\rangle \right] U^T$$

where $|\tilde{\psi}_i\rangle = \sqrt{p_i} |\psi_i\rangle$. From theorem 2.6,

$$\rho = \sum_k \tilde{k} = \sum_k \tilde{\psi}_k.$$

Therefore we can obtain a minimal ensemble for ρ that contains $|\psi_i\rangle$.

Moreover since $\rho^{-1} = \sum_k \frac{1}{\lambda_k} k$,

$$\langle \psi_i | \rho^{-1} | \psi_i \rangle = \sum_k \frac{1}{\lambda_k} \langle \psi_i | k \rangle \langle k | \psi_i \rangle = \sum_k \frac{|c_{ik}|^2}{\lambda_k} = \frac{1}{p_i}.$$

Hence, $\frac{1}{\langle \psi_i | \rho^{-1} | \psi_i \rangle} = p_i$.

2.74

We know

$$\rho_{AB} = |a\rangle \langle a|_A \otimes |b\rangle \langle b|_B$$

$$\rho_A = \text{Tr}_B \rho_{AB} = |a\rangle \langle a| \text{Tr}(|b\rangle \langle b|) = |a\rangle \langle a|$$

$$\text{Tr}(\rho_A^2) = 1$$

Thus ρ_A is pure.

2.75 Reduced Density

Define $|\Phi_{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ and $|\Psi_{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$.

$$|\Phi_{\pm}\rangle \langle \Phi_{\pm}|_{AB} = \frac{1}{2}(|00\rangle \langle 00| \pm |00\rangle \langle 11| \pm |11\rangle \langle 00| + |11\rangle \langle 11|)$$

$$\text{Tr}_B(|\Phi_{\pm}\rangle \langle \Phi_{\pm}|_{AB}) = \frac{1}{2}(|0\rangle \langle 0| + |1\rangle \langle 1|) = \frac{I}{2}$$

$$|\Psi_{\pm}\rangle \langle \Psi_{\pm}| = \frac{1}{2}(|01\rangle \langle 01| \pm |01\rangle \langle 10| \pm |10\rangle \langle 01| + |10\rangle \langle 10|)$$

$$\text{Tr}_B(|\Psi_{\pm}\rangle \langle \Psi_{\pm}|) = \frac{1}{2}(|0\rangle \langle 0| + |1\rangle \langle 1|) = \frac{I}{2}$$

$[u_{i1} \cdots u_{ik} \cdots u_{il}]$. Then define unitary $U = \begin{bmatrix} \mathbf{u}_1 \\ \vdots \\ \mathbf{u}_i \\ \vdots \\ \mathbf{u}_l \end{bmatrix}$.

2.76 Extend Proof

Click https://en.wikipedia.org/wiki/Schmidt_decomposition#Proof to check the proof

2.77 ABC three components

$$\begin{aligned}
 |\psi\rangle &= |0\rangle |\Phi_+\rangle \\
 &= |0\rangle \left[\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \right] \\
 &= (\alpha |\phi_0\rangle + \beta |\phi_1\rangle) \left[\frac{1}{\sqrt{2}}(|\phi_0\phi_0\rangle + |\phi_1\phi_1\rangle) \right]
 \end{aligned}$$

where $|\phi_i\rangle$ are arbitrary orthonormal states and $\alpha, \beta \in \mathbb{C}$. We cannot vanish cross term. Therefore $|\psi\rangle$ cannot be written as $|\psi\rangle = \sum_i \lambda_i |i\rangle_A |i\rangle_B |i\rangle_C$.

2.78 Schmidt Number

Proof. First Part

If $|\psi\rangle$ is product, then there exist a state $|\phi_A\rangle$ for system A , and a state $|\phi_B\rangle$ for system B such that $|\psi\rangle = |\phi_A\rangle |\phi_B\rangle$.

Obviously, this Schmidt number is 1.

Conversely, if Schmidt number is 1, the state is written as $|\psi\rangle = |\phi_A\rangle |\phi_B\rangle$. Hence this is a product state. \square

Proof. Later part.

(\Rightarrow) Proved by exercise 2.74.

(\Leftarrow) Let a pure state be $|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle$. Then $\rho_A = Tr_B(|\psi\rangle \langle\psi|) = \sum_i \lambda_i^2 |i\rangle \langle i|$. If ρ_A is a pure state, then $\lambda_j = 1$ and otherwise 0 for some j . It follows that $|\psi_j\rangle = |j_A\rangle |j_B\rangle$. Thus $|\psi\rangle$ is a product state. \square

2.79 Schmidt Decomposition

Procedure of Schmidt decomposition.

Goal: $|\psi\rangle = \sum_i \sqrt{\lambda_i} |i_A\rangle |i_B\rangle$

- Diagonalize reduced density matrix $\rho_A = \sum_i \lambda_i |i_A\rangle \langle i_A|$.
- Derive $|i_B\rangle$, $|i_B\rangle = \frac{(I \otimes \langle i_A|) |\psi\rangle}{\sqrt{\lambda_i}}$
- Construct $|\psi\rangle$.

(i)

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \text{ This is already decomposed.}$$

(ii)

$$\frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2} = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) \otimes \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) = |\psi\rangle |\psi\rangle \text{ where } |\psi\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

(iii)

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{3}}(|00\rangle + |01\rangle + |10\rangle)$$

$$\rho_{AB} = \psi_{AB}$$

$$\rho_A = \text{Tr}_B(\rho_{AB}) = \frac{1}{3}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|)$$

$$\det(\rho_A - \lambda I) = \left(\frac{2}{3} - \lambda \right) \left(\frac{1}{3} - \lambda \right) - \frac{1}{9} = 0$$

$$\lambda^2 - \lambda + \frac{1}{9} = 0$$

$$\lambda = \frac{1 \pm \sqrt{5}/3}{2} = \frac{3 \pm \sqrt{5}}{6}$$

$$\text{Eigenvector with eigenvalue } \lambda_0 \equiv \frac{3 + \sqrt{5}}{6} \text{ is } |\lambda_0\rangle \equiv \frac{1}{\sqrt{\frac{5+\sqrt{5}}{2}}} \begin{bmatrix} \frac{1+\sqrt{5}}{2} \\ 1 \end{bmatrix}.$$

$$\text{Eigenvector with eigenvalue } \lambda_1 \equiv \frac{3 - \sqrt{5}}{6} \text{ is } |\lambda_1\rangle \equiv \frac{1}{\sqrt{\frac{5-\sqrt{5}}{2}}} \begin{bmatrix} \frac{1-\sqrt{5}}{2} \\ 1 \end{bmatrix}.$$

$$\rho_A = \lambda_0 |\lambda_0\rangle\langle \lambda_0| + \lambda_1 |\lambda_1\rangle\langle \lambda_1|.$$

$$|a_0\rangle \equiv \frac{(I \otimes \langle \lambda_0 |) |\psi\rangle}{\sqrt{\lambda_0}}$$

$$|a_1\rangle \equiv \frac{(I \otimes \langle \lambda_1 |) |\psi\rangle}{\sqrt{\lambda_1}}$$

Then

$$|\psi\rangle = \sum_{i=0}^1 \sqrt{\lambda_i} |a_i\rangle |\lambda_i\rangle.$$

Calculate $|a_i\rangle$

2.80 Schmidt Coefficient

Let $|\psi\rangle = \sum_i \lambda_i |\psi_i\rangle_A |\psi_i\rangle_B$ and $|\varphi\rangle = \sum_i \lambda_i |\varphi_i\rangle_A |\varphi_i\rangle_B$.
 Define $U = \sum_i |\psi_j\rangle \langle \varphi_j|_A$ and $V = \sum_j |\psi_j\rangle \langle \varphi_j|_B$.
 Then

$$\begin{aligned} (U \otimes V) |\varphi\rangle &= \sum_i \lambda_i U |\varphi_i\rangle_A V |\varphi_i\rangle_B \\ &= \sum_i \lambda_i |\psi_i\rangle_A |\psi_i\rangle_B \\ &= |\psi\rangle. \end{aligned}$$

2.81 Purification

Let the Schmidt decomposition of $|AR_1\rangle$ be $|AR_1\rangle = \sum_i \sqrt{p_i} |\psi_i^A\rangle |\psi_i^R\rangle$ and let $|AR_2\rangle = \sum_i \sqrt{q_i} |\phi_i^A\rangle |\phi_i^R\rangle$.
 Suppose ρ^A has orthonormal decomposition $\rho^A = \sum_i p_i |i\rangle \langle i|$.
 Since $|AR_1\rangle$ and $|AR_2\rangle$ are purifications of the ρ^A , we have

$$\begin{aligned} \text{Tr}_R(|AR_1\rangle \langle AR_1|) &= \text{Tr}_R(|AR_2\rangle \langle AR_2|) = \rho^A \\ \therefore \sum_i p_i |\psi_i^A\rangle \langle \psi_i^A| &= \sum_i q_i |\phi_i^A\rangle \langle \phi_i^A| = \sum_i \lambda_i |i\rangle \langle i|. \end{aligned}$$

The $|i\rangle$, $|\psi_i^A\rangle$, and $|\psi_i^R\rangle$ are orthonormal bases and they are eigenvectors of ρ^A . Hence without loss of generality, we can consider

$$\lambda_i = p_i = q_i \text{ and } |i\rangle = |\psi_i^A\rangle = |\phi_i^A\rangle.$$

Then

$$\begin{aligned} |AR_1\rangle &= \sum_i \lambda_i |i\rangle |\psi_i^R\rangle \\ |AR_2\rangle &= \sum_i \lambda_i |i\rangle |\phi_i^R\rangle \end{aligned}$$

Since $|AR_1\rangle$ and $|AR_2\rangle$ have same Schmidt numbers, there are two unitary operators U and V such that $|AR_1\rangle = (U \otimes V) |AR_2\rangle$ from exercise 2.80.

Suppose $U = I$ and $V = \sum_i |\psi_i^R\rangle \langle \phi_i^R|$. Then

$$\begin{aligned} \left(I \otimes \sum_j |\psi_j^R\rangle \langle \phi_j^R| \right) |AR_2\rangle &= \sum_i \lambda_i |i\rangle \left(\sum_j |\psi_j^R\rangle \langle \phi_j^R| |\phi_i^R\rangle \right) \\ &= \sum_i \lambda_i |i\rangle |\psi_i^R\rangle \\ &= |AR_1\rangle. \end{aligned}$$

Therefore there exists a unitary transformation U_R acting on system R such that $|AR_1\rangle = (I \otimes U_R) |AR_2\rangle$.

2.82

(1)

Let $|\psi\rangle = \sum_i \sqrt{p_i} |\psi_i\rangle |i\rangle$.

$$\begin{aligned} Tr_R(|\psi\rangle \langle\psi|) &= \sum_{i,j} \sqrt{p_i} \sqrt{p_j} |\psi_i\rangle \langle\psi_j| Tr_R(|i\rangle \langle j|) \\ &= \sum_{i,j} \sqrt{p_i} \sqrt{p_j} |\psi_i\rangle \langle\psi_j| \delta_{ij} \\ &= \sum_i p_i |\psi_i\rangle \langle\psi_i| = \rho. \end{aligned}$$

Thus $|\psi\rangle$ is a purification of ρ .

(2)

Define the projector P by $P = I \otimes |i\rangle \langle i|$. The probability we get the result i is

$$Tr[P|\psi\rangle \langle\psi|] = \langle\psi|P|\psi\rangle = \langle\psi|(I \otimes |i\rangle \langle i|)|\psi\rangle = p_i \langle\psi_i|\psi_i\rangle = p_i.$$

The post-measurement state is

$$\frac{P|\psi\rangle}{\sqrt{p_i}} = \frac{(I \otimes |i\rangle \langle i|)|\psi\rangle}{\sqrt{p_i}} = \frac{\sqrt{p_i} |\psi_i\rangle |i\rangle}{\sqrt{p_i}} = |\psi_i\rangle |i\rangle.$$

If we only focus on the state on system A ,

$$Tr_R(|\psi_i\rangle |i\rangle) = |\psi_i\rangle.$$

(3)

($\{|\psi_i\rangle\}$ is not necessary an orthonormal basis.)

Suppose $|AR\rangle$ is a purification of ρ and its Schmidt decomposition is $|AR\rangle = \sum_i \sqrt{\lambda_i} |\phi_i^A\rangle |\phi_i^R\rangle$.

From assumption

$$Tr_R(|AR\rangle \langle AR|) = \sum_i \lambda_i |\phi_i^A\rangle \langle\phi_i^A| = \sum_i p_i |\psi_i\rangle \langle\psi_i|.$$

By theorem 2.6, there exists a unitary matrix u_{ij} such that $\sqrt{\lambda_i} |\phi_i^A\rangle =$

$\sum_j u_{ij} \sqrt{p_j} |\psi_j\rangle$. Then

$$\begin{aligned}
|AR\rangle &= \sum_i \left(\sum_j u_{ij} \sqrt{p_j} |\psi_j\rangle \right) |\phi_i^R\rangle \\
&= \sum_j \sqrt{p_j} |\psi_j\rangle \otimes \left(\sum_i u_{ij} |\phi_i^R\rangle \right) \\
&= \sum_j \sqrt{p_j} |\psi_j\rangle |j\rangle \\
&= \sum_i \sqrt{p_i} |\psi_i\rangle |i\rangle
\end{aligned}$$

where $|i\rangle = \sum_k u_{ki} |\phi_k^R\rangle$.

About $|i\rangle$,

$$\begin{aligned}
\langle k|l\rangle &= \sum_{m,n} u_{mk}^* u_{nl} \langle \phi_m^R | \phi_n^R \rangle \\
&= \sum_{m,n} u_{mk}^* u_{nl} \delta_{mn} \\
&= \sum_m u_{mk}^* u_{ml} \\
&= \delta_{kl}, \quad (\because u_{ij} \text{ is unitary.})
\end{aligned}$$

which implies $|j\rangle$ is an orthonormal basis for system R .

Therefore if we measure system R w.r.t $|j\rangle$, we obtain j with probability p_j and post-measurement state for A is $|\psi_j\rangle$ from (2). Thus for any purification $|AR\rangle$, there exists an orthonormal basis $|i\rangle$ which satisfies the assertion.

2.1

From Exercise 2.35, $\vec{n} \cdot \vec{\sigma}$ is decomposed as

$$\vec{n} \cdot \vec{\sigma} = |\lambda_1\rangle \langle \lambda_1| - |\lambda_1\rangle \langle \lambda_{-1}|$$

where $|\lambda_{\pm 1}\rangle$ are eigenvector of $\vec{n} \cdot \vec{\sigma}$ with eigenvalues ± 1 .

Thus

$$\begin{aligned}
f(\theta \vec{n} \cdot \vec{\sigma}) &= f(\theta) |\lambda_1\rangle \langle \lambda_1| + f(-\theta) |\lambda_{-1}\rangle \langle \lambda_{-1}| \\
&= \left(\frac{f(\theta) + f(-\theta)}{2} + \frac{f(\theta) - f(-\theta)}{2} \right) |\lambda_1\rangle \langle \lambda_1| + \left(\frac{f(\theta) + f(-\theta)}{2} - \frac{f(\theta) - f(-\theta)}{2} \right) |\lambda_{-1}\rangle \langle \lambda_{-1}| \\
&= \frac{f(\theta) + f(-\theta)}{2} (|\lambda_1\rangle \langle \lambda_1| + |\lambda_{-1}\rangle \langle \lambda_{-1}|) + \frac{f(\theta) - f(-\theta)}{2} (|\lambda_1\rangle \langle \lambda_1| - |\lambda_{-1}\rangle \langle \lambda_{-1}|) \\
&= \frac{f(\theta) + f(-\theta)}{2} I + \frac{f(\theta) - f(-\theta)}{2} \vec{n} \cdot \vec{\sigma}
\end{aligned}$$

2.2

3 Chapter 3 solutions

3.1 Non-computable processes in Nature

Since we know that a Turing Machine only maps from non-negative to non-negative numbers, and if any process in nature is found to map between different sets of values then that process can't be run on a Turing Machine.

3.2 Turing numbers

Taking the input of the Turing Machine a_1, \dots, a_k and then give the Turing machine the value $p_1^{a_1} \times p_2^{a_2} \times \dots \times p_k^{a_k}$ with $p_1, p_2, p_3, \dots, p_k$ being the first k prime numbers, and thus all Turing machine with unique inputs will be given unique value identifiers since all numbers only have one kind of prime factorization.

3.3 Turing Machine to reverse a bit string

Our aim is to design a Turing Machine to reverse a binary string consisting of 0 and 1, we will call them a and b

- Move the last digit, replace x for a or x for b and move right to convert the corresponding B to a or b accordingly.
- Move left until the symbol left to x is reached.
- Perform Step 1 and Step 2 until B is reached while traversing left.
- Replace every x to B to make the cells empty since the reverse string is performed by the previous steps.

The transition diagram for the Turing machine looks like this

3.4 Turing Machine to add modulo 2

- Start in the initial state, with the tape head positioned over the leftmost digit of the first number.
- If the digit under the tape head is 0, move the tape head one position to the right and transition to the next state.
- If the digit under the tape head is 1, write a 0 at that position and move the tape head one position to the right.
- Repeat steps 2 and 3 until the tape head reaches the rightmost digit of the first number.
- Transition to the next state and move the tape head to the leftmost digit of the second number.
- Repeat steps 2-4 for the second number.

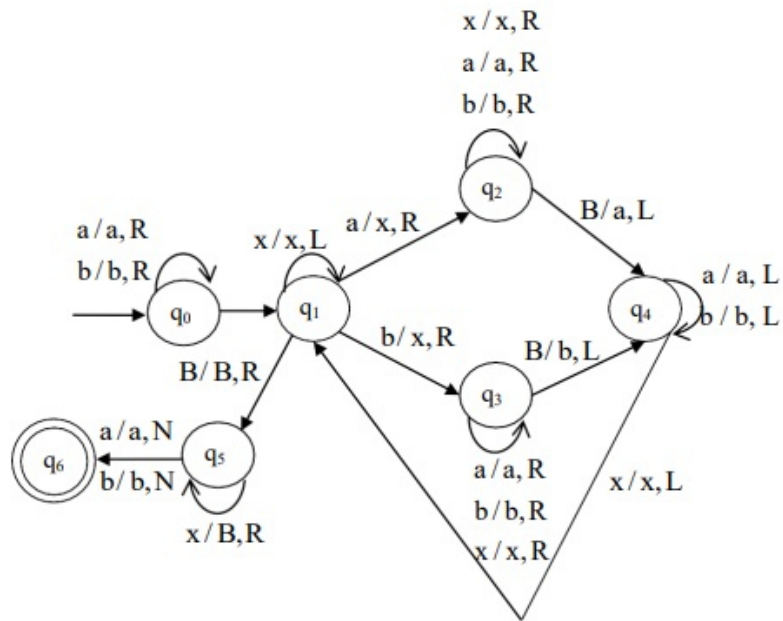


Figure 1: The Turing Machine for reverse string

- Move the tape head to the leftmost digit of the result and transition to the final state.

This Turing machine will add two binary numbers modulo 2, effectively performing a bitwise XOR operation on the input numbers.

3.5 Halting Problem with no inputs

The problem of determining whether a given Turing machine halts when the input to the machine is a blank tape is known as the halting problem. It was shown by Alan Turing in 1936 that there is no general algorithm that can determine whether an arbitrary Turing machine halts on a blank input.

The proof of this result relies on the concept of diagonalization, where a new machine is constructed that can determine whether any given machine halts on a blank input. If such an algorithm existed, then it could be encoded as a Turing machine, say H . It is possible to construct a new machine, say D , that takes as input the description of another machine M and runs both M and H on the blank tape. D compares the outputs of M and H for each machine it receives as input. If the outputs are different for any input machine M , D outputs "M does not halt." Otherwise, D outputs "M halts."

The problem is that D can be used to determine whether itself halts. If D halts, it will say "D halts." If D does not halt, it will say "D does not halt." This creates a contradiction, because D cannot simultaneously halt and not halt. Therefore, it is impossible for a machine to determine whether another machine halts on a blank input.

This proof was shown by Alan Turing in his paper "On computable numbers, with an application to the Entscheidungsproblem" in 1936, showing that the halting problem is undecidable.

Define $H2(M) = 0$ if the machine doesn't halt with blank input, 1 if the machine does halt with a blank input

We have the following algorithm

```

Turing(M)
Y = H2(M)
if y == 0
halt
else
'Loop Forever

```

Here if M is blank, then $H2(M) = 1$ only if $y = H2(M) = 0$, thus we form a contradiction, meaning this machine cannot read input M , which is blank, meaning there is no algorithm to solve $H2(M)$ for this particular machine.

3.6 Probabilistic halting problem

Define $Hp(x) = 0$ if probability machine x halts in input $x < 1/2$, 1 if probability $> 1/2$. We have the following algorithm:

```

    Turing(x)
Y = hp(x)
Y2 = flip an unbiased coin
if y==1 and y2 = heads
halt
Else
loop forever
End if

```

Here, assume $hp(x) = 1$ and thus corresponding probability $p > 1/2$. The probability program halts are $p \times 1/2 =$ at most $1/2$ since p is at most 1. Thus, this contradicts our original statement that $hp(x) = 1$, and thus there is no algorithm to correctly determine $hp(x)$ for this machine.

3.7 Halting oracle

Yes. Before, the problem was no algorithm existed to compute $HALT(x)$ for all x , but now that the black box exists that algorithm also exists, and since Turing machines can compute all algorithms, these Turing machines can compute this algorithm for all machines.

3.8 Universality of NAND

AND - input bit $[1, x_0, x_1]$. Apply NAND to x_0 and x_1 , then a NAND on $[1, \text{NAND}(x_0, x_1)]$
 NOT - NAND input bit x_0 and ancilla bit 1
 XOR - input $[1, x_0, x_1, 1, 1]$ NAND $[1, \text{NAND}[x_0, x_1], \text{NAND}[\text{NAND}[1, x_0] \text{NAND}[1, x_1]]]$

3.9 Prove that $f(n)$ is $O(g(n))$ iff $g(n)$ is $\Omega(f(n))$

$f(n)$ is $O(g(n)) \rightarrow f(n) \leq cg(n)$
 $g(n)$ is $\Omega(f(n)) \rightarrow cf(n) \leq g(n)$
 If $g(n)$ is $\Omega(f(n))$ then $cf(n) \leq g(n), f(n) \leq g(n)/c$
 And thus $f(n) \leq cg(n)$ and $f(n)$ is $O(g(n))$

Thus $g(n)$ is $\Theta(f(n))$ and $f(n)$ is $O(g(n))$

3.10 Suppose $g(n)$ is a polynomial of degree k

$$g(n) \text{ is } O(n^1) \longrightarrow g(n) \leq cn^1$$

$$g(n) = An^k + Bn^{k-1} + \dots + d \leq cn^1$$

Thus, because $An^k + Bn^{k-1} + \dots + d \leq n^{k+1} \leq n^{k+2}$ and we design c such that $An^k + Bn^{k-1} + \dots + d \leq cn^k$, thus $g(n)$ is $O(n^1)$.

3.11 Show that $\log(n)$ is $O(n^k)$ for any $k > 0$

$\log n \leq cn^k$, $n \leq c10^{n^k}$, so we design c^k such that $n \leq c \times 10^{n^k}$ for all $k > 0$

3.12 $n^{\log n}$ is super polynomial

From 3.10, we proved $\log n \geq k$ for sufficiently large n , thus $g(n) = n^k$ is in $O(n^{\log n})$. However, $\log n$ is not $\leq k$ for large n , so $g(n) = n^k$ is never in $O(n^k)$

3.13 $n^{\log n}$ is sub-exponential

c^n is $\Omega(n^{\log n})$, check graphically for sufficiently large n .
Since c^n is $\Omega(n^{\log n})$, $n^{\log n}$ can't be in $\Omega(c^n)$.

3.14 Suppose $e(n)$ is $O(f(n))$ and $g(n)$ is $O(h(n))$

$$e(n) \text{ is } O(f(n)) \rightarrow e(n) \leq cf(n)$$

$$g(n) \text{ is } O(h(n)) \rightarrow g(n) \leq c2 \times h(n)$$

$$e(n) \times g(n) \leq c \times c2 \times f(n) \times h(n) = c3 \times f(n) \times h(n)$$

3.15 Lower bound for compare and swap based sorts

After 1 swapping, there is only 2^1 ordering such that the swapping puts the whole thing in order. After 2 swapping, there are 2^2 orderings that were two swapping away from being sorted. After k swappings, it follows that 2^k initial orderings are now sorted.

$$2^n \log n = 2^{\log n^n = n^n} \geq n!$$

Thus, the lower bound on sorting is $n \log n$. You can see that asymptotic notations have the important effect of allowing us to find how efficient a particular algorithm can be on a process, but it doesn't necessarily tell us HOW to make such an algorithm, but it gives us an idea of how efficient the most efficient algorithm can be.

3.16 Hard to compute function exist

There exist Boolean functions on n inputs which require at least $2^n / \log(n)$ logic gates to compute. One such example is the function known as the "n-input majority function."

The majority function, denoted as $MAJ_n(x_1, x_2, \dots, x_n)$, is a Boolean function that takes n binary inputs and outputs 1 if and only if more than $n/2$ of the inputs are 1. The function can be computed by creating n AND gates, one for each input, and $n - 1$ OR gates to combine the outputs of the AND

gates. In the worst case, where all inputs are 1, the number of gates required is $(n - 1) + (n - 1) = 2n - 2 = 2^n / \log(n)$ gates.

Another example is the "n-input parity function," which is a Boolean function that takes n binary inputs and outputs 1 if and only if the number of 1s in the inputs is odd. The function can be computed by creating n XOR gates, one for each input, and then $n - 1$ XOR gates to combine the outputs of the previous XOR gates. In the worst-case scenario, the number of gates required is $(n - 1) + (n - 1) = 2n - 2 = 2^n / \log(n)$ gates.

This shows that there are Boolean functions that require at least $2^n / \log(n)$ logic gates to compute, and that is a lower bound for the complexity of some Boolean functions.

3.17 Prove that a polynomial-time algorithm for finding the factors of a number m exists iff the factoring decision problem is in P

If this problem is in P , then a Turing machine exists for identifying if a value is a factor of a number m and less than L , and thus setting $L = m$ we have the factoring algorithm that can thus be done efficiently. If this problem isn't in P , the factoring obviously can't be done efficiently since if for any L it is inefficient then $L = m$ is definitely inefficient.

3.18 Prove that if $coNP \neq NP$, then $P \neq NP$

P is a subset of $CoNP$ so if $CoNP$ does not equal NP , there are some problems in P and $CoNP$, and the rest of the problems in P and NP , and thus there are some problems in P that are in $CoNP$ but not NP and thus P does not equal NP .

3.19 The REACHABILITY problem

Start at the first vertex, try to get to the 2nd. At most n vertices exist to visit, so its $O(n)$ (algorithm would make sure not to visit a vertex more than once). Then use Reachability algorithm to form the following $O(n^2)$ algorithm:
 For i through all vertices
 For j through all vertices
 Test Reachability(vertex(i), vertex(j))
 End j
 End i

3.20 Euler's Theorem

Euler's theorem is based on the following idea: If you visit a node, you can go on a new edge you haven't gone before, because the vertex has an even amount of incident edges so if a node is visited and then left, 2 edges have been traversed and used. Thus if you go through all nodes you will always have a new edge

to move through for every node until there are no more edges left to visit, at which point you are back at the original node and have completed the cycle.

The procedure then would be to start at a node, go to all other nodes until you have reached back to the original node and there are no new edges to visit.

3.21 Transitive property of reduction

Since $L1 \rightarrow L2$ exists, there exists function $R(x)$ that gives a string in language $L2$ iff x is in $L1$. Since $L2 \rightarrow L3$ exists, there exists a function $R2(x_2)$ that gives a string in $L3$ iff x_2 is in $L2$. Thus, with $R(x) + R2(R(x))$ (polynomial time overhead), we reduce $L1$ to $L3$.

3.22 L is complete

Since all other problems can be reduced to L , and L can be reduced to L' , all other problems can be reduced to L' .

3.23 SAT is NP-complete problem

SAT (Satisfiability) is a problem of determining whether a given Boolean formula, in conjunctive normal form (CNF) has a satisfying assignment.

First, to show that SAT is in NP, we need to show that a solution to the problem can be verified in polynomial time. Given a Boolean formula in CNF and an assignment, we can check in polynomial time if the assignment satisfies the formula, by checking each clause of the formula. If all the clauses are true for the given assignment, then the assignment is a satisfying assignment, otherwise not. Since the size of the input does not affect the time complexity of the verification, this means that SAT is in NP.

Next, to show that SAT is NP-complete, we need to show that there exists a reduction from an arbitrary problem in NP to SAT. One such problem is known as CSAT (Circuit SAT), which is the problem of determining whether a given Boolean circuit has a satisfying assignment.

To show that CSAT reduces to SAT, we can construct a Boolean formula in CNF that represents the given Boolean circuit. Each gate in the circuit can be represented by a clause in the CNF formula, and each input to the circuit can be represented by a variable in the formula. We can then use the variables to represent the inputs and the clauses to represent the gates, such that the Boolean formula in CNF is satisfied if and only if the circuit has a satisfying assignment.

Since CSAT is in NP and it is possible to reduce it to SAT, it implies that SAT is NP-complete. This means that SAT is at least as hard as any problem in NP, and that any problem in NP can be reduced to SAT in polynomial time.

3.25 PSPACE subset EXP

With $lm^{p(n)}$ different states, all problems in PSPACE can be solved by going through all possible states in $lm^{p(n)}$ time, or exponential time. Thus PSPACE is a subset of EXP

3.26 L subset P

If you can solve a problem in L , then you can solve the problem by going through around $c \times \log(n)$ spaces, thus you can solve it in time $c \times \log(n)$, which is polynomial. Thus L is a subset of P .

3.27 Approximation algorithm for VERTEX COVER

In this algorithm, at worst the min vector span is made up of all the alpha's and none of the Beta's, in which case at worst this algorithm calculates the a vector span that is $2 \times$ the space of the min vector span.

3.29 Fredkin gate is self inverse

A Fredkin gate is a reversible gate that acts on three qubits, and it is also known as a Controlled-SWAP gate. The Fredkin gate is defined as:

$$\begin{aligned} |x\rangle|y\rangle|z\rangle &\rightarrow |x\rangle|y\rangle|z\rangle \text{ if } x = 0 \\ |x\rangle|y\rangle|z\rangle &\rightarrow |x\rangle|z\rangle|y\rangle \text{ if } x = 1 \end{aligned}$$

Where $|x\rangle$, $|y\rangle$ and $|z\rangle$ are the input qubits and $-x\rangle$, $-y\rangle$, $-z\rangle$ are the output qubits. The qubit x is the control qubit, and the qubits y and z are the target qubits.

Now, let's consider applying two consecutive Fredkin gates, where the first one acts on qubits $-x\rangle$, $-y\rangle$, $-z\rangle$ and the second one acts on qubits $-x\rangle$, $-z\rangle$, $-w\rangle$.

If $x = 0$, the first Fredkin gate doesn't change the state of the qubits and the second Fredkin gate also don't change the state of the qubits, and the output state is $-x\rangle-y\rangle-z\rangle-w\rangle$ which is the same as the input state $-x\rangle-y\rangle-z\rangle-w\rangle$

If $x = 1$, the first Fredkin gate swaps the qubits $-y\rangle$ and $-z\rangle$, and the second Fredkin gate swaps the qubits $-z\rangle$ and $-w\rangle$. The net effect is that the qubits $-y\rangle$ and $-w\rangle$ are swapped and the output state is $-x\rangle-w\rangle-z\rangle-y\rangle$ which is the same as the input state $-x\rangle-y\rangle-z\rangle-w\rangle$

Therefore, applying two consecutive Fredkin gates gives the same outputs as inputs

3.32 From fredkin to toffoli

The Toffoli gate, also known as the Controlled-Controlled-NOT gate, is a reversible gate that acts on three qubits. The Toffoli gate is defined as:

$$|x\rangle|y\rangle|z\rangle \rightarrow |x\rangle|y\rangle|z\rangle \text{ if } x = 0 \text{ and } y = 0$$

$$|x\rangle|y\rangle|z\rangle \rightarrow |x\rangle|y\rangle|z \oplus 1\rangle \text{ if } x = 0 \text{ and } y = 1$$

where $|x\rangle$, $|y\rangle$, and $|z\rangle$ are the input qubits and $|x\rangle$, $|y\rangle$, $|z\rangle$ are the output qubits. The qubits x and y are the control qubits, and the qubit z is the target qubit.

The smallest number of Fredkin gates needed to simulate a Toffoli gate is 3. To simulate a Toffoli gate with three Fredkin gates, we can use a technique called 'controlled-SWAP-controlled-SWAP', where the first two Fredkin gates act on $|x\rangle$, $|y\rangle$, $|z\rangle$ and the third Fredkin gate acts on $|x\rangle$, $|y\rangle$, $|t\rangle$ where $|t\rangle$ is an auxiliary qubit.

On the other hand, Toffoli gate is a more powerful gate than Fredkin gate and it can simulate Fredkin gate, but it requires 2 Toffoli gates to simulate 1 Fredkin gate. To simulate a Fredkin gate with two Toffoli gates, we can use a technique called "controlled-controlled-NOT-controlled-NOT" where the first Toffoli gate is applied on $|x\rangle$, $|y\rangle$, $|t1\rangle$ where $|t1\rangle$ is an auxiliary qubit, and the second Toffoli gate is applied on $|x\rangle$, $|t1\rangle$, $|z\rangle$

It's important to note that while it's possible to simulate a Toffoli gate using Fredkin gates, or vice versa, it's not always the most efficient way to perform the operation, as the number of gates required for the simulation is higher than using the native gate.

4 Chapter 4 solutions

4.1 Find the points on the Bloch Sphere which corresponds to normalized eigenvectors of different Pauli Matrices

Eigenvectors for the Pauli-x matrix:

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

,

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

Eigenvectors for the Pauli-y matrix:

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix}$$

,

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

Eigenvectors for the Pauli-z matrix:

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

,

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

So we see that the eigenvectors are the different “poles” of the Bloch sphere.

4.2 Show that

$$\exp \iota Ax = \cos(x)I + \iota \sin(x)A$$

Use the Taylor development of the exponential function and simplify using the property $A^2 = I$.

$$e^{iAx} = \sum_{k=0}^{\infty} \frac{(iAx)^k}{k!} = \sum_{k=0, \text{even } k}^{\infty} \frac{(ix)^k}{k!} A^k + \sum_{k=0, \text{odd } k}^{\infty} \frac{(ix)^k}{k!} A^k = \sum_{k=0, \text{even } k}^{\infty} \frac{(ix)^k}{k!} I + \sum_{k=0, \text{odd } k}^{\infty} \frac{(ix)^k}{k!} A.$$

or

First, write out the identities in Taylor’s Series for $\sin x$ and $\cos x$ as well as e^x .

$$\sin x = x - x^3/(3!) + x^5/(5!) \dots$$

$$\cos x = 1 - x^2/(2!) + x^4/(4!) \dots$$

$$e^x = 1 + x + x^2/(2!) + x^3/(3!) + x^4/(4!)...$$

Usually, to prove Euler's Formula you multiply e^x by i , in this case, we will multiply e^x by i .

And we will end with e^{ix} thus it will be equal to...

$$1 + (-ix) + (-ix)^2/(2!) + (-ix)^3/(3!) + (-ix)^4/(4!)...$$

Expand...

$$1 - ix - x^2/(2!) - ix^3/(3!) + x^4/(4!)...$$

Factorise it

$$(1 - x^2/(2!) + x^4/(4!)...) - i(x - x^3/(3!) + x^5/(5!)...)$$

And the first part of the equation is equal to $\cos x$ and the second part to $\sin x$, now we can replace them.

$$(\cos x) - i(\sin x)$$

Hence:

$$e^{(-ix)} = \cos x - i \sin x$$

4.3 Show that up to a global phase, the $\pi/8$ gate satisfies $T = R_z(\pi/4)$

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

And

$$\begin{aligned} R_z\left(\frac{\pi}{4}\right) &= \cos\left(\frac{\pi}{8}\right)I - i\sin\left(\frac{\pi}{8}\right)Z \\ &= \begin{bmatrix} \cos\left(\frac{\pi}{8}\right) - i\sin\left(\frac{\pi}{8}\right) & 0 \\ 0 & \cos\left(\frac{\pi}{8}\right) + i\sin\left(\frac{\pi}{8}\right) \end{bmatrix} \\ &= \begin{bmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{bmatrix} \\ &= e^{-i\frac{\pi}{8}} \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix} \end{aligned}$$

This equals T times a global phase shift.

4.4 Express the Hadamard gate as a product of R_x and R_z rotations

Analyzing what the Hadamard gate does the eigenvectors of the Pauli X, Y, and Z matrices, we see that:

$-z; +\rangle$ to $-x; +\rangle$, $-z; -\rangle$ to $-x; -\rangle$, and $-y; +\rangle$ to $-y; -\rangle$.

Thus, geometrically, we see that the Hadamard is the equivalent of a $\pi/2$ rotation about the y-axis followed by a π rotation about the x-axis. Thus,

$$H = R_x(\pi)R_y\left(\frac{\pi}{2}\right)e^{i\phi}$$

To find the constant, we can multiply out the x and y rotation matrices, arriving at

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

We can now take out

$$-i\frac{\sqrt{2}}{2}$$

to arrive at the matrix

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

. Thus the constant is $-i$ and ϕ is $3 \times \pi/2$.

4.5 Prove that $n \cdot \sigma = I$

Let $Q = n \cdot \vec{\sigma}$ Since all pauli matrices are hermitian we know that Q is also hermitian. This means we can use the spectral decomposition theorem to show that these matrices are diagonalizable. In exercise 2.60, we find that Q has eigenvalues $+1, -1$. Thus,

$$Q = |q_1\rangle\langle q_1| - |q_2\rangle\langle q_2|$$

where

$$|q_1\rangle$$

and

$$|q_2\rangle$$

form an orthonormal basis. Squaring we get,

$$Q^2 = |q_1\rangle\langle q_1| + |q_2\rangle\langle q_2| = I$$

Where the last line follows from the completeness relation.

4.6 Bloch Sphere interpretation of rotation

The first step to proving this is that $R_x(\alpha)$, $R_y(\alpha)$, $R_z(\alpha)$ rotate a state around the x, y, and z axis of the bloch vector. Let's start with the z-axis. To prove this we start with the bloch-angle representation of a qubit,

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi} \sin(\theta/2)|1\rangle$$

Multiplying this with $R_z(\alpha)$ to get,

$$\begin{aligned} & (\cos(\alpha/2)I - i \sin(\alpha/2)Z)(\cos(\theta/2)|0\rangle + e^{i\phi} \sin(\theta/2)|1\rangle) \\ &= \cos(\frac{\theta}{2}) \left[\cos(\frac{\alpha}{2}) - i \sin(\frac{\alpha}{2}) \right] |0\rangle + e^{i\phi} \sin(\frac{\theta}{2}) \left[\cos(\frac{\alpha}{2}) + i \sin(\frac{\alpha}{2}) \right] |1\rangle \\ &= \cos(\frac{\theta}{2}) e^{-i\alpha/2} |0\rangle + e^{i\phi} \sin(\theta/2) e^{i\alpha/2} |1\rangle \\ &= \cos(\frac{\theta}{2}) |0\rangle + e^{i(\phi+\alpha)} \sin(\frac{\theta}{2}) |1\rangle \end{aligned}$$

Which means that the state is indeed rotated by α around the z-axis. We can do a similar process with $R_y(\alpha)$ and $R_z(\alpha)$. Now, we need to show that $R_n(\alpha)$ indeed rotates a bloch vector by α around the (n_x, n_y, n_z) axis. To do this, we can construct such a rotation with just rotations around the 3 axes and show that this indeed equals $R_n(\alpha)$. Consider the following diagram:

Note that the angles θ and ϕ are referring to the angles that the bloch vector (n_x, n_y, n_z) are making, not the qubit itself. Now, to perform a rotation $R_n(\alpha)$ we follow the following procedure: 1. Rotation around Z by $\frac{\pi}{2} - \phi$ 2. Rotation around X by θ 3. Rotation around Z by α 4. Rotation around X by $-\theta$ 5. Rotation around Z by $\phi - \frac{\pi}{2}$

So we need to show that this procedure is equivalent to $R_n(\alpha)$. We know that:

$$R_n(\alpha) \equiv \cos(\frac{\theta}{2})I - i \sin(\frac{\theta}{2})(n_x X + n_y Y + n_z Z)$$

And we must show that this equals our rotation procedure which can be written like so:

$$\begin{aligned} & \left[\cos\left(\frac{\pi/2 - \phi}{2}\right) I + i \sin\left(\frac{\pi/2 - \phi}{2}\right) Z \right] \left[\cos\left(\frac{\theta}{2}\right) I + i \sin\left(\frac{\theta}{2}\right) X \right] \\ & \left[\cos\left(\frac{\alpha}{2}\right) I - i \sin\left(\frac{\alpha}{2}\right) Z \right] \left[\cos\left(\frac{\theta}{2}\right) I - i \sin\left(\frac{\theta}{2}\right) X \right] \left[\cos\left(\frac{\pi/2 - \phi}{2}\right) I - i \sin\left(\frac{\pi/2 - \phi}{2}\right) Z \right] \end{aligned}$$

While it seems tedious to multiply out, we can make the process easier by first multiplying the middle three rotational terms.

$$\left[\cos\left(\frac{\theta}{2}\right) I + i \sin\left(\frac{\theta}{2}\right) X \right] \left[\cos\left(\frac{\alpha}{2}\right) I - i \sin\left(\frac{\alpha}{2}\right) Z \right]$$

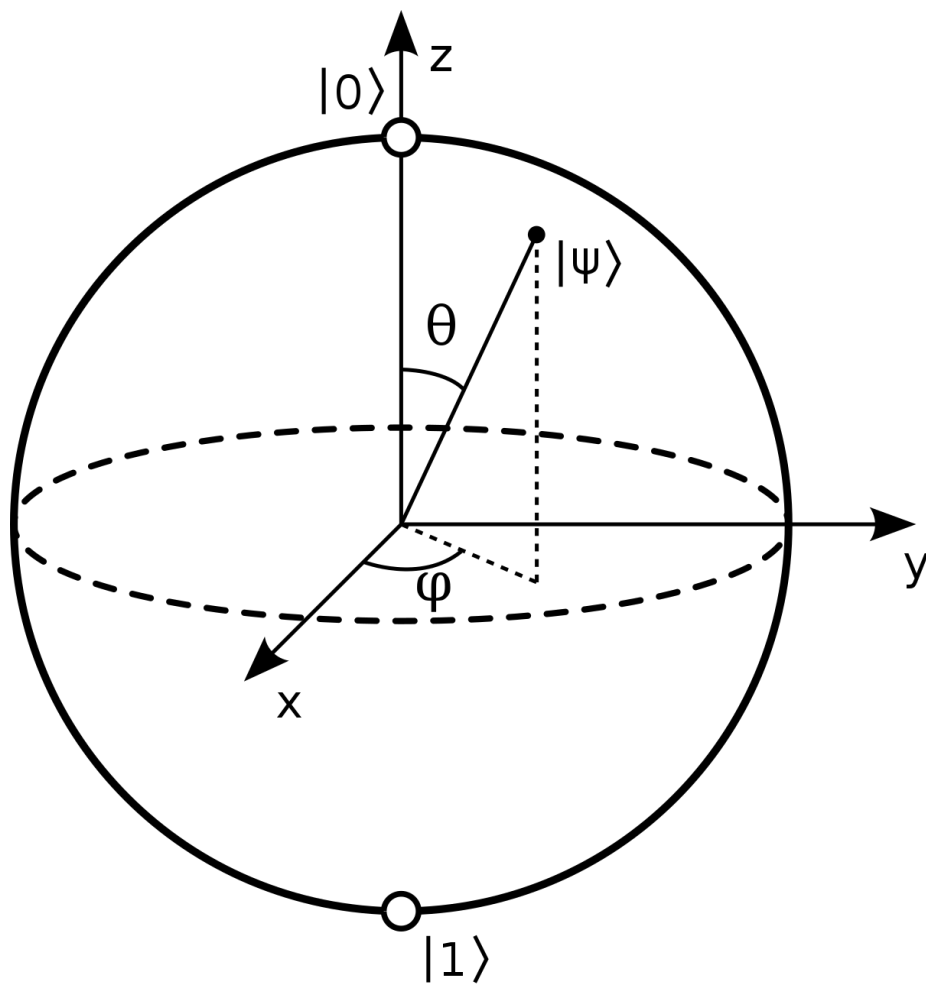


Figure 2: The Bloch Sphere

$$\left[\cos\left(\frac{\theta}{2}\right) I - i \sin\left(\frac{\theta}{2}\right) X \right] = \cos\left(\frac{\alpha}{2}\right) I - i \sin\left(\frac{\alpha}{2}\right) n_z Z - i \sin\left(\frac{\alpha}{2}\right) \sqrt{n_y^2 + n_x^2} Y$$

Now we multiply this with the first and last terms of our rotation procedure like so:

$$\left[\cos\left(\frac{\pi/2 - \varphi}{2}\right) I + i \sin\left(\frac{\pi/2 - \varphi}{2}\right) Z \right] \left[\cos\left(\frac{\alpha}{2}\right) I - i \sin\left(\frac{\alpha}{2}\right) n_z Z - i \sin\left(\frac{\alpha}{2}\right) (n_y^2 + n_x^2) Y \right] \left[\cos\left(\frac{\pi/2 - \varphi}{2}\right) I - i \sin\left(\frac{\pi/2 - \varphi}{2}\right) Z \right]$$

Simplifying this out we get,

$$\begin{aligned} \cos\left(\frac{\alpha}{2}\right) I - i \sin\left(\frac{\alpha}{2}\right) n_z Z - i \sin\left(\frac{\alpha}{2}\right) \sqrt{n_y^2 + n_x^2} \left(\frac{n_y}{\sqrt{n_x^2 + n_y^2}} Y + \frac{n_x}{\sqrt{n_x^2 + n_y^2}} X \right) \\ = \cos\left(\frac{\alpha}{2}\right) I - i \sin\left(\frac{\alpha}{2}\right) (n_x X + n_y Y + n_z Z) \end{aligned}$$

And we have proven that

$$R_n(\alpha)$$

indeed is equivalent to a rotation of

$$\alpha$$

radians around the

$$(n_x, n_y, n_z)$$

axis.

4.7 Show that $XYX = -Y$

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

For the second part,

$$\begin{aligned} XR_y(\theta)X &= X \left(\cos\left(\frac{\theta}{2}\right) I - i \sin\left(\frac{\theta}{2}\right) Y \right) X \\ &= \cos\left(\frac{\theta}{2}\right) X^2 - i \sin\left(\frac{\theta}{2}\right) XYX \\ &= \cos\left(\frac{\theta}{2}\right) I + i \sin\left(\frac{\theta}{2}\right) Y = R_y(-\theta) \end{aligned}$$

4.8 An arbitrary single qubit unitary operator can be written as
 $U \exp i\alpha R_N(\theta)$

1.

$$U = e^{i\alpha} R_n(\theta) = e^{i\alpha} e^{-i(\frac{\theta}{2})(n \cdot \sigma)}$$

Considering the adjoint,

$$\begin{aligned} U^\dagger &= (e^{i\alpha})^\dagger (e^{-i(\frac{\theta}{2})(n \cdot \sigma)})^\dagger \\ &= e^{-i\alpha} e^{i(\frac{\theta}{2})(n \cdot \sigma)} \end{aligned}$$

Thus,

$$UU^\dagger = I$$

2.

$$H = R_x(\pi) R_y(\frac{\pi}{2}) e^{i\frac{3\pi}{2}} = e^{-i(\frac{\pi}{2})(\frac{X+Y}{2})}$$

Thus, $\alpha = \frac{3\pi}{2}, \theta = \pi, n = 1, \frac{1}{2}, 0$

3.

$$\begin{aligned} S &= R_x(0) R_y(0) R_z(\frac{\pi}{2}) e^{i*0} \\ &= e^{(-i)(0)(X/2)} e^{(-i)(0)(Y/2)} e^{(-i)(\pi/2)(Z/2)} \\ &= e^{(-i)(\frac{\pi}{2})(0X+0Y+(\frac{\pi}{2})Z)} \end{aligned}$$

Thus, $\theta = \frac{\pi} 2, \alpha = 0, n = 0, 0, \frac{1}{2}$

4.9 Explain why any single qubit unitary operator may be written in different form

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

$$U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$U^\dagger = \begin{bmatrix} a^* & c^* \\ b^* & d^* \end{bmatrix}$$

$$\begin{aligned} UU^\dagger &= \begin{bmatrix} aa^* + bb^* & (a^i + b^j) \cdot (c^{*i} + d^{*j}) \\ (c^i + d^j) \cdot (a^{*i} + b^{*j}) & cc^* + dd^* \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{aligned}$$

This means that the rows/columns are orthonormal with each other and each row/column is normal. Now we can consider U in form 4.12. Here the rows are normal because

$$aa^* + bb^* = e^{i(a-b/2-\delta/2)} e^{-i(a-b/2-\delta/2)} \cos(\frac{\gamma}{2})^2 + e^{i(a-b/2+\delta/2)} e^{-i(a-b/2+\delta/2)} \sin(\frac{\gamma}{2})^2$$

$$= e^0 \sin(\frac{\gamma}{2})^2 + e^0 \cos(\frac{\gamma}{2})^2 = 1$$

We can use a similar process to show that the rows are orthonormal and that the columns follow the same rules.

4.12 Give A,B,C and α for the Hadamard gate.

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

We know, from equation 4.12, that:

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

So we need to find the α, β, δ , and γ values that give H. Playing around, we realize its best to take care of the $1/\sqrt{2}$ part by giving gamma the value of $\pi/2$. Now we have to focus on the $e^i \dots$ part. Again, just looking at it, it isn't too hard to see that, if we set $\beta = 0$, we just need to find a good definition of alpha and sigma values. We realize $\alpha = \pi/2$ and $\sigma = \pi/2$ works. Now, according to theorem 4.1, we have:

$$H = e^{i\pi/2} R_z(0) R_y(\pi/2) R_z(\pi/2)$$

From the proof of the theorem, we say that we just need to define

$$A = R_z(0) R_y(\pi/4)$$

,

$$B = R_y(-\gamma/2) R_z(-(\sigma + \beta)/2)$$

, and

$$C = R_z(\pi/4)$$

, and

$$\alpha = \pi/2$$

.

4.13 Circuit identities

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

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

4.14 Show that $HTH = R_x(\pi/4)$

$$\begin{aligned}
HTH &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \\
&= \begin{bmatrix} \frac{1}{2} + \frac{1}{2}e^{i\pi/4} & \frac{1}{2} - \frac{1}{2}e^{i\pi/4} \\ \frac{1}{2} - \frac{1}{2}e^{i\pi/4} & \frac{1}{2} + \frac{1}{2}e^{i\pi/4} \end{bmatrix}
\end{aligned}$$

Our goal in the end is to get a matrix that looks like:

$$R_x\left(\frac{\pi}{4}\right) = \begin{bmatrix} \cos\left(\frac{\pi}{8}\right) & -i\sin\left(\frac{\pi}{8}\right) \\ -i\sin\left(\frac{\pi}{8}\right) & \cos\left(\frac{\pi}{8}\right) \end{bmatrix}$$

This leads us to take out a global phase of

$$e^{i\pi/8}$$

$$\begin{aligned}
HTH &= e^{i\pi/8} \begin{bmatrix} \frac{1}{2}e^{-i\pi/8} + \frac{1}{2}e^{i\pi/8} & \frac{1}{2}e^{-i\pi/8} - \frac{1}{2}e^{i\pi/8} \\ \frac{1}{2}e^{-i\pi/8} - \frac{1}{2}e^{i\pi/8} & \frac{1}{2}e^{-i\pi/8} + \frac{1}{2}e^{i\pi/8} \end{bmatrix} \\
&= e^{i\pi/8} \begin{bmatrix} \cos\left(\frac{\pi}{8}\right) & -i\sin\left(\frac{\pi}{8}\right) \\ -i\sin\left(\frac{\pi}{8}\right) & \cos\left(\frac{\pi}{8}\right) \end{bmatrix}
\end{aligned}$$

4.16 Matrix representation of multi-qubit gates

To build the matrix we have to see what the effect of the circuit is on the different computational basis states. For the state $|00\rangle = [10][10] = [1000]$, the circuit changes it to $|0\rangle|+\rangle = [1/\sqrt{2}][1/\sqrt{2}][00]$. For the state $|01\rangle = [10][01] = [0100]$, the circuit changes the state to $|0\rangle|-\rangle = [1/\sqrt{2}][1/\sqrt{2}][00]$. For the state $|10\rangle = [01][10] = [0010]$, the circuit changes the state to $|1\rangle|+\rangle = [001/\sqrt{2}][1/\sqrt{2}][00]$. For the state $|11\rangle = [01][01] = [0001]$, the circuit changes the state to $|1\rangle|-\rangle = [001/\sqrt{2}][1/\sqrt{2}][00]$. Thus, using these results, we can build the following matrix:

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

Using the same process, for the next circuit we get:

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

4.17 Building CNOT from controlled-Z gates

To construct a CNOT gate from one controlled Z gate, we can use the following circuit:

Apply a Hadamard gate to the first qubit (control qubit) Apply a Controlled-Z gate with the first qubit as control and the second qubit as target. Apply a Hadamard gate to the first qubit (control qubit) The matrix operation of a CNOT gate with the first qubit as the control qubit and the second qubit as the target qubit is given by:

$$\text{CNOT} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

The matrix operation of a controlled Z gate with the control qubit as the first qubit and the target qubit as the second qubit is given by:

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

The matrix operation of a Hadamard gate on a single qubit is given by:

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

To find the matrix operation of the circuit described, we need to find the matrix product of the individual gates in the order they appear in the circuit.

The matrix operation of the circuit is:

$$\text{CNOT} = H \cdot \text{CZ} \cdot H$$

You can use matrix multiplication to find the final matrix representation of the CNOT gate:

As you can see, the matrix representation of the CNOT gate is identical to the one obtained by directly applying a CNOT gate, which means that the circuit constructed using one Controlled-Z gate and two Hadamard gates indeed implements a CNOT gate.

4.18 Show that

For both circuits, their effect on the computational basis states are the same: for $|00\rangle = [1000]$, both don't change it, for $|01\rangle = [0100]$, both don't change it, for $|10\rangle = [0010]$, both don't change it, and finally for $|11\rangle = [0001]$, both change this to $[000 - 1]$. Thus, both circuits' corresponding matrix is:

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

Thus, the two circuits are equal.

4.19 CNOT action on density matrices

When a unitary operator is applied to a density operator, it has the effect: Up Thus, apply $[\text{CNOT}(1 \rightarrow 2)]^\dagger \text{CNOT}(1 \rightarrow 2)$, we get:

$$\begin{bmatrix} p_{11} & p_{12} & p_{14} & p_{13} \\ p_{21} & p_{22} & p_{24} & p_{23} \\ p_{41} & p_{42} & p_{44} & p_{43} \\ p_{31} & p_{32} & p_{34} & p_{33} \end{bmatrix}$$

4.20 CNOT Basis transformations

Representing the operators (H1 tensor H2) with the matrix

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

and the operator CNOT($2 \rightarrow 1$) as

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

(based off how it changes the computational basis states), we then multiply matrix (H1 tensor H2) CNOT($2 \rightarrow 1$) (H1 tensor H2) to get the matrix

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

which is the matrix of the operator CNOT($1 \rightarrow 2$). Thus, applying two hadamards, CNOT($2 \rightarrow 1$), and again two hadamards is the same as applying CNOT($1 \rightarrow 2$). Now, let's say that instead of the computational basis, we are in the $|+\rangle |-\rangle$ basis. Lets say the first qubit is the control qubit, and the second is the target. This is the same as the circuit

(H1 tensor H2) CNOT($2 \rightarrow 1$) (H1 tensor H2)

and with this circuit we get $|0\rangle |0\rangle \text{CNOT}(2 \rightarrow 1) = |0\rangle |0\rangle$ (H1 tensor H2) $= |+\rangle |+\rangle$. Using the same process for input qubits $|-\rangle |+\rangle, |+\rangle |-\rangle$, and $|-\rangle |-\rangle$, we get the following formulas:

$$\begin{aligned} |+\rangle |+\rangle &\longrightarrow |+\rangle |+\rangle \\ |-\rangle |+\rangle &\longrightarrow |-\rangle |+\rangle \\ |+\rangle |-\rangle &\longrightarrow |-\rangle |-\rangle \\ |-\rangle |-\rangle &\longrightarrow |+\rangle |-\rangle \end{aligned}$$

We notice that it seems that, even though the first qubit is the control and the second is the target, the roles are flipped! Thus, the roles of control and target are ambiguous when qubits are not in the computational basis, or the classical bit basis. You can also tell from the circuit that this flipping of roles happens, because the circuit essentially says that CNOT($2 \rightarrow 1$), when hadamard on both sides, is the same as CNOT($1 \rightarrow 2$), so with any states that can be turned into the computational basis states upon being "hadamarded" (and inversely be turned back) can have CNOT($1 \rightarrow 2$) = CNOT($2 \rightarrow 1$). These states are the $|+\rangle, |-\rangle$ states.

4.21 Verify

Lets go through all cases: $1, 1, q \rightarrow 1, 1,$

$$V(q) \rightarrow 1, 0,$$

$$V(q)- > 1, 0,$$

$$V(q)- > 1, 1,$$

$$V(q)- > 1, 1,$$

$$V^2(q) = U(q)$$

$$1, 0, q- > 1, 0, q- > 1, 1, q- > 1, 1, V_{adjoint}(q)- > 1, 0, V_{adjoint}(q)- > 1, 1, V V_{adjoint}(q) = q \ 0, 1, q- > 0, 1, V(q)- > 0, 1, V(q)- > 0, 1, V_{adjoint} V(q)- > 0, 1, q- > 0, 1, q \ 0, 0, q- > 0, 0, q- > 0, 0, q- > 0, 0, q- > 0, 0, q- > 0, 0, q$$

Thus, the figure does indeed implement the a C2(U) circuit.

4.25

1. Three toffoli gates with the last two bits switching at each gate

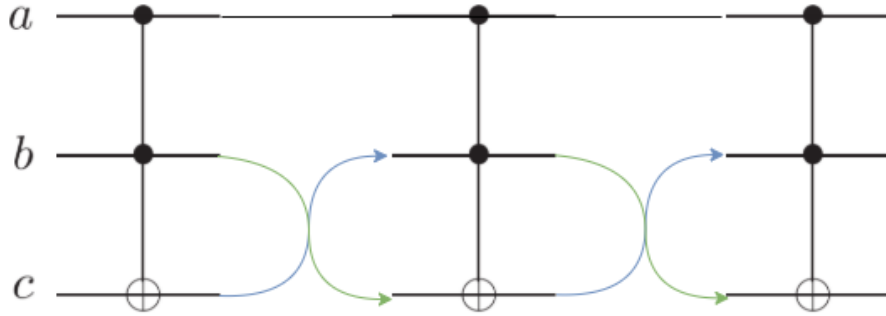


Figure 3: 4.25 : Three toffoli gates with the last two bits switching at each gate

2. We can replace the first and the last toffoli gate like:

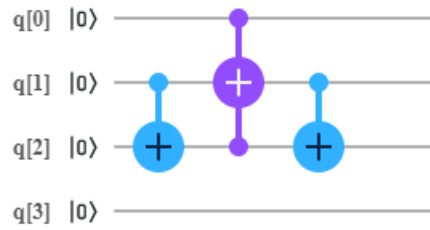


Figure 4: 4.25 : We can replace the first and the last toffoli gate like

4.26 Show that the circuit

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

$$R_y(\pi/4) = \begin{bmatrix} \cos(\pi/8) & -\sin(\pi/8) \\ \sin(\pi/8) & \cos(\pi/8) \end{bmatrix}$$

$$R_y(-\pi/4) = \begin{bmatrix} \cos(\pi/8) & \sin(\pi/8) \\ -\sin(\pi/8) & \cos(\pi/8) \end{bmatrix}$$

We can consider each of the different transformations for the four possible computational basis states of the first two qubits. 1.

$$|00\rangle$$

results in

$$\begin{aligned} R_y(\pi/4)R_y(\pi/4)R_y(-\pi/4)R_y(-\pi/4) \\ = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{aligned}$$

2.

$$|01\rangle$$

results in

$$\begin{aligned} R_y(\pi/4)XR_y(\pi/4)R_y(-\pi/4)XR_y(-\pi/4) \\ = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{aligned}$$

3.

$$|10\rangle$$

results in

$$\begin{aligned} R_y(\pi/4)R_y(\pi/4)XR_y(-\pi/4)R_y(-\pi/4) \\ = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \end{aligned}$$

4.

$$|11\rangle$$

results in

$$\begin{aligned} R_y(\pi/4)XR_y(\pi/4)XR_y(-\pi/4)XR_y(-\pi/4) \\ = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \end{aligned}$$

Which makes sense. You only want to invert the bit when both bits “a” and “b” are 1.

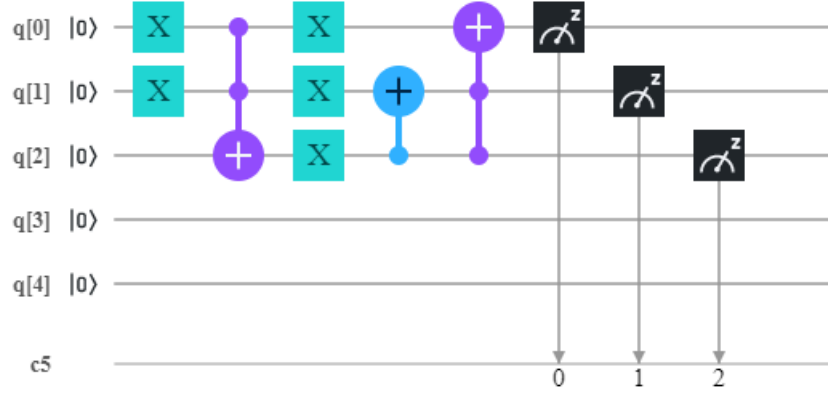


Figure 5:

4.27 Using CNOT construct the gate

The gate implements the following changes to the computational basis states:

$$\begin{aligned}
 |000\rangle &\rightarrow |000\rangle \\
 |001\rangle &\rightarrow |111\rangle \\
 |010\rangle &\rightarrow |001\rangle \\
 |011\rangle &\rightarrow |010\rangle \\
 |100\rangle &\rightarrow |011\rangle \\
 |101\rangle &\rightarrow |100\rangle \\
 |110\rangle &\rightarrow |101\rangle \\
 |111\rangle &\rightarrow |110\rangle
 \end{aligned}$$

The circuit will be like:

$$\begin{aligned}
 &CNOT_{q[0], q[1]} \\
 &CNOT_{q[1], q[2]} \\
 &Toffoli_{q[0], q[1], q[2]} \\
 &CNOT_{q[1], q[2]} \\
 &CNOT_{q[0], q[1]}
 \end{aligned}$$

This circuit uses CNOT gates to flip the states of the second and third qubits based on the state of the first qubit, and a Toffoli gate to flip the state of the third qubit based on the states of the first and second qubits. The order of the CNOT and Toffoli gates, as well as the qubits they act on, are chosen so that the overall circuit performs the desired transformations

4.32 Density Matrix

Given that outcome i occurs, the state of the quantum system is:

Thus, if a measurement occurs there is a $p(0)$ chance that outcome 0 occurs and a $p(1)$ chance that outcome 1 occurs. This means that the state will be:

$$\rho' = p(0) \frac{P_0 \rho P_0}{p(0)} + p(1) \frac{P_1 \rho P_1}{p(1)} = P_0 \rho P_0 + P_1 \rho P_1$$

Now for the second part of the question.

$$\begin{aligned} \rho &= \sum_i p_i |\psi_a\rangle\langle\psi_a| |\psi_b\rangle\langle\psi_b| \\ \text{tr}_b(\rho) &= \sum_i p_i \text{tr}_b(|\psi_a\rangle\langle\psi_a| |\psi_b\rangle\langle\psi_b|) \\ &= \sum_i p_i \text{tr}_b(|\psi_a\rangle\langle\psi_a| \otimes |\psi_b\rangle\langle\psi_b|) \\ &= \sum_i p_i (|\psi_a\rangle\langle\psi_a|) \langle\psi_b|\psi_b\rangle \end{aligned}$$

Finding the trace of the post-measurement (but not post-observation) state,

$$\begin{aligned} \text{tr}_b(\rho') &= \sum_i p_i \text{tr}_b(P_0 |\psi_a\rangle\langle\psi_a| |\psi_b\rangle\langle\psi_b| P_0) + \text{tr}_b(P_1 |\psi_a\rangle\langle\psi_a| |\psi_b\rangle\langle\psi_b| P_1) \\ \text{tr}_b(\rho') &= \sum_i p_i \text{tr}_b(|\psi_a\rangle\langle\psi_a| \otimes P_0 |\psi_b\rangle\langle\psi_b| P_0) + \text{tr}_b(|\psi_a\rangle\langle\psi_a| \otimes P_1 |\psi_b\rangle\langle\psi_b| P_1) \\ \text{tr}_b(\rho') &= \sum_i p_i (|\psi_a\rangle\langle\psi_a|) (\langle\psi_b| P_0 |\psi_b\rangle + \langle\psi_b| P_1 |\psi_b\rangle) \\ \text{tr}_b(\rho') &= \sum_i p_i (|\psi_a\rangle\langle\psi_a|) (\langle\psi_b| (P_0 + P_1) |\psi_b\rangle) \end{aligned}$$

But by the completeness relation we know that, thus

$$\text{tr}_b(\rho') = \text{tr}_b(\rho)$$

4.33 Measurement in the Bell Basis

We know that,

$$|00\rangle = \frac{|B_{00}\rangle + |B_{10}\rangle}{\sqrt{2}}$$

If you put the $|00\rangle$ through the circuit, we get $\frac{|00\rangle + |10\rangle}{\sqrt{2}}$ as the result. This means that for $|00\rangle$, the circuit is indeed measuring it with respect to the Bell states. We can confirm that this holds for the other three computational basis states. Now we must show that the measurement is being performed with the

projectors onto the Bell states as corresponding POVM elements. To do so, once again consider the computational basis state $|00\rangle$.

If the Bell state of the projectors are the corresponding POVM elements, then the state of $|00\rangle$ after a measurement in the Bell basis would be either

$$\left(\frac{P_{00}|\psi\rangle}{\sqrt{p(00)}} \right)$$

or

$$\left(\frac{P_{10}|\psi\rangle}{\sqrt{p(10)}} \right)$$

Re-normalizing this, we see that the projector tells us the state will be either

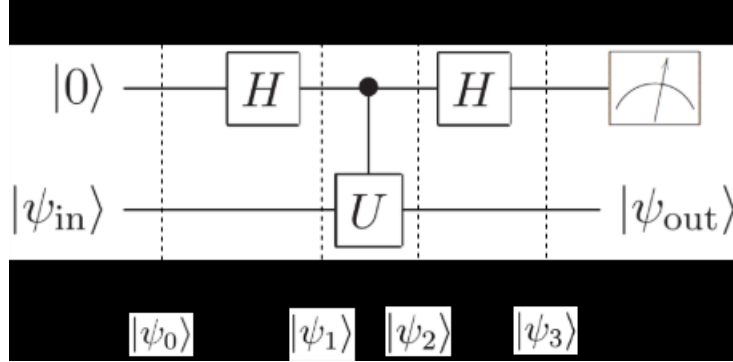
$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

or

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

, which are exactly the Bell states our circuit predicts. One can go through similar work for the other computational basis states to ensure that the problem statement is indeed correct.

4.34 Measuring an Operator



$$|\psi_0\rangle = |0\rangle|\psi_{in}\rangle$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle|\psi_{in}\rangle + |1\rangle|\psi_{in}\rangle)$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle|\psi_{in}\rangle + |1\rangle U|\psi_{in}\rangle)$$

$$\begin{aligned}
|\psi_3\rangle &= \frac{1}{2} [(|0\rangle + |1\rangle)|\psi_{in}\rangle + (|0\rangle - |1\rangle)U|\psi_{in}\rangle] \\
&= \frac{1}{2} [|0\rangle(I + U)|\psi_{in}\rangle + |1\rangle(I - U)|\psi_{in}\rangle]
\end{aligned}$$

So if the measurement gives us 0 (representing the +1 eigenvalue), we have the corresponding eigenvector to be

$$(I + U)|\psi\rangle$$

. This is indeed true, since

$$U(I + U)|\psi\rangle = (U + I)|\psi\rangle$$

, since U is both hermitian and unitary.

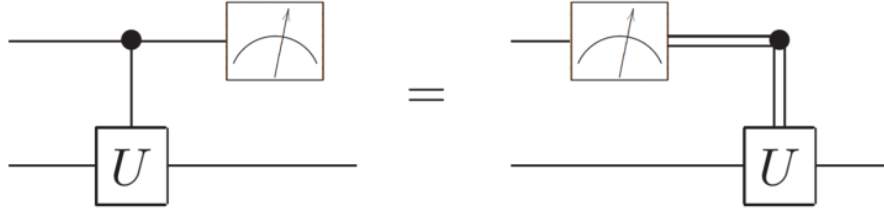
If the measurement gives us a 1 (representing the -1 eigenvalue), we have

$$U(I - U)|\psi\rangle = -1(I - U)|\psi\rangle$$

. Thus, we have showed that the circuit implements a measurement of U.

4.35 Measurement commutes with controls

The figure:



Considering the circuit on the left first, we have:

$$|\psi_0\rangle = (a|0\rangle + b|1\rangle)(c|0\rangle + d|1\rangle)$$

$$|\psi_0\rangle = (ac|0\rangle|0\rangle + ad|0\rangle|1\rangle + bc|1\rangle|0\rangle + bd|1\rangle|1\rangle)$$

$$|\psi_1\rangle = (ac|0\rangle|0\rangle + ad|0\rangle|1\rangle + (bc)U|1\rangle|0\rangle + (bd)U|1\rangle|1\rangle)$$

After measurement, the state of the 2nd qubit becomes

$$a(c|0\rangle + d|1\rangle) + b(cU|0\rangle + dU|1\rangle)$$

Considering the circuit on the right, if the first qubit is

$$|0\rangle$$

then the second qubit is

$$c|0\rangle + d|1\rangle$$

. Likewise, if the first qubit is

$$|1\rangle$$

, then the second qubit is

$$cU|0\rangle + dU|1\rangle$$

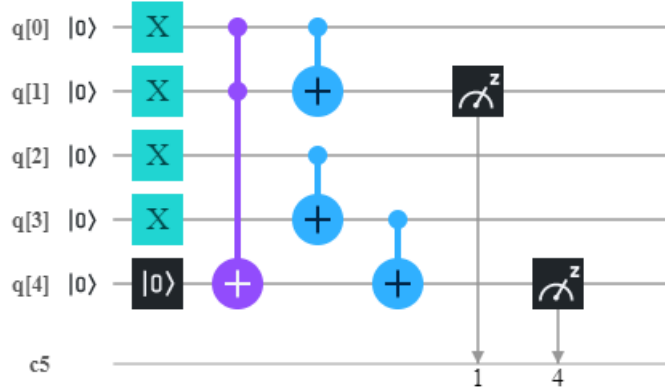
. Thus, combining the two facts, we get

$$a(c|0\rangle + d|1\rangle) + b(cU|0\rangle + dU|1\rangle)$$

and both circuits are equivalent.

4.36 Construct a Quantum Circuit

In this figure, q[0] is the first qubit of the first number, q[1] is the first qubit of the 2nd number, q[2] is the 2nd qubit of the first number, and q[3] is the 2nd qubit of the 2nd number. Note that the pauli-x matrices in the beginning are just to define the initial values of the 2 numbers.



4.37 Provide a decomposition

Using the process in the lesson we initially get,

$$U_3U_2U_1U = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & i\frac{\sqrt{2}}{2} & 0 & -i\frac{\sqrt{2}}{2} \\ 0 & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$U_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \\ 0 & 0 & 1 & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \end{bmatrix}$$

$$U_2 = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & 1 & 0 & 0 \\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$U_3 = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \end{bmatrix}$$

This means that

$$U_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -i\frac{\sqrt{2}}{2} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 1 \\ 0 & i\frac{\sqrt{2}}{2} & \frac{1}{\sqrt{2}} & 0 \end{bmatrix}$$

Except, this matrix isn't a two-level unitary matrix. We can still decompose it into two-level unitary matrices, with a similar process such that

$$V_2 V_1 U_4 = I$$

$$V_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & i\frac{\sqrt{2}}{2} & 0 & -i\frac{\sqrt{2}}{2} \\ 0 & 0 & 1 & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \end{bmatrix}$$

$$U_4 = V_1^\dagger V_2^\dagger$$

$$U_4 U_3 U_2 U_1 U = I$$

$$V_1^\dagger V_2^\dagger U_3 U_2 U_1 U = I$$

Thus, the final two-level unitary decomposition is

$$U = U_1^\dagger U_2^\dagger U_3^\dagger V_2 V_1$$

4.39 Find a Quantum Circuit

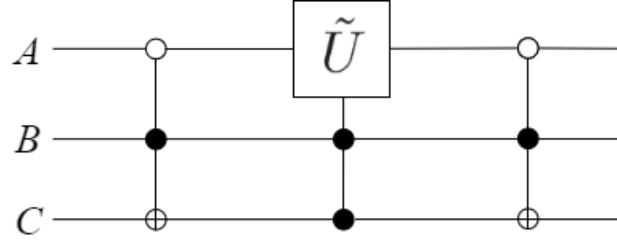
In this two-level unitary matrix, it only acts on the vector components

$$|010\rangle$$

to

$$|111\rangle$$

. The corresponding circuit is shown above.



4.40 Arbitrary α and β

$$E(R_n(\alpha), R_n(\alpha+\beta)) = ||(R_n(\alpha) - R_n(\alpha+\beta))|\psi\rangle|| = \sqrt{\langle\psi|(R_n(\alpha) - R_n(\alpha+\beta))^\dagger(R_n(\alpha) - R_n(\alpha+\beta))|\psi\rangle}$$

$$R_n(\alpha) \equiv \exp(-i\alpha^n \cdot \sigma/2) = \cos(\frac{\alpha}{2})I - i\sin(\frac{\alpha}{2})(n_xX + n_yY + n_zZ)$$

To simplify the calculations, use the following substitutions:

$$d = \cos(\frac{\alpha}{2}) - \cos(\frac{\alpha+\beta}{2})$$

$$f = \sin(\frac{\alpha}{2}) - \sin(\frac{\alpha+\beta}{2})$$

$$(R_n(\alpha) - R_n(\alpha+\beta))^\dagger(R_n(\alpha) - R_n(\alpha+\beta)) = (dI - if(n_xX + n_yY + n_zZ))(dI + if(n_xX + n_yY + n_zZ)) = (d^2I + if(n_xX + n_yY + n_zZ)^2)$$

So now we know that the desired value is

$$\langle\psi|(d^2I + if(n_xX + n_yY + n_zZ)^2)|\psi\rangle = d^2 + \langle\psi|f(n_xX + n_yY + n_zZ)^2|\psi\rangle$$

Now remember that

$$\langle\psi|AA|\psi\rangle = ||A|\psi\rangle||^2$$

. So in order to calculate

$$\langle\psi|f(n_xX + n_yY + n_zZ)^2|\psi\rangle$$

, we just have to find

$$||(n_xX + n_yY + n_zZ)|\psi\rangle||$$

(remember that f and ni are real, and X, Y, and Z are Hermitian). Letting

$$|\psi\rangle = [ab]$$

$$(n_x X + n_y Y + n_z Z)|\psi\rangle = [(n_x b - n_y bi + n_z a)(n_x a + n_y ai - n_z b)]$$

So the magnitude of this vector equals:

$$|n_x b - n_y bi + n_z a|^2 + |n_x a + n_y ai - n_z b|^2 = |(n_x b + n_z a) - (n_y b)i|^2 + |(n_x a - n_z b) + (n_y a)i|^2$$

Expanding out, and using

$$a^2 + b^2 = 1$$

and

$$n_x^2 + n_y^2 + n_z^2 = 1$$

, we find that the magnitude of the above vector is 1. Thus,

$$\langle\psi|f(n_x X + n_y Y + n_z Z)^2|\psi\rangle$$

is equal to

$$f^2$$

. Thus we have,

$$|(R_{\hat{n}}(\alpha) - R_{\hat{n}}(\alpha + \beta))|\psi\rangle| = \sqrt{d^2 + f^2}$$

$$\begin{aligned} & \sqrt{\left[\cos\left(\frac{\alpha}{2}\right) - \cos\left(\frac{\alpha + \beta}{2}\right) \right]^2 \left[\sin\left(\frac{\alpha}{2}\right) - \sin\left(\frac{\alpha + \beta}{2}\right) \right]^2} \\ &= \sqrt{2 - 2 \left(\cos\left(\frac{\alpha}{2}\right) \cos\left(\frac{\alpha + \beta}{2}\right) - \sin\left(\frac{\alpha}{2}\right) \sin\left(\frac{\alpha + \beta}{2}\right) \right)} \end{aligned}$$

Remember that,

$$\cos\left(\frac{\alpha + \beta}{2} - \frac{\alpha}{2}\right) = \cos\left(\frac{\alpha}{2}\right) \cos\left(\frac{\alpha + \beta}{2}\right) - \sin\left(\frac{\alpha}{2}\right) \sin\left(\frac{\alpha + \beta}{2}\right)$$

Thus, we get a final answer of

$$\sqrt{2 - 2\cos\left(\frac{\beta}{2}\right)}$$

, which is equal to the

$$|1 - \exp(i\beta/2)|$$

in the problem statement.

4.41 Construction showing the circuit

Considering the diagram in the question

$$\begin{aligned}
|\psi_0\rangle &= |0\rangle|0\rangle|\psi\rangle \\
|\psi_1\rangle &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)|\psi\rangle \\
|\psi_2\rangle &= \frac{1}{2}(|00\rangle S|\psi\rangle + |01\rangle S|\psi\rangle + |10\rangle S|\psi\rangle + |11\rangle X S X|\psi\rangle) \\
|\psi_3\rangle &= \frac{1}{4}(|00\rangle(3S + X S X)|\psi\rangle + |01\rangle(S - X S X)|\psi\rangle + |10\rangle(-S - X S X)|\psi\rangle + |11\rangle(-S + X S X)|\psi\rangle)
\end{aligned}$$

Considering the

$$|00\rangle$$

term, the matrix in front of it can be written as:

$$\begin{aligned}
&\frac{\sqrt{10}}{e^{\frac{i\pi}{4}}} \begin{bmatrix} e^{i(\alpha - \frac{\pi}{4})} & 0 \\ 0 & e^{i(\frac{\pi}{4} - \alpha)} \end{bmatrix} \\
& , \\
&\sin(\alpha) = \frac{1}{\sqrt{10}} \\
& , \\
&\cos(\alpha) = \frac{3}{\sqrt{10}} \\
& , \\
&p(|00\rangle) = \left| \frac{\sqrt{10}}{4e^{i\frac{\pi}{4}}} \right|^2 = 5/8
\end{aligned}$$

With some basic trigonometry, we can prove that this matrix is indeed the rotation around the z-axis by theta.

4.42 Irrationality of θ

(1) If θ is a rational multiple of 2π ($\theta = 2\pi k$), then there must exist an integer m such that mk is an integer and thus,

$$e^{i(2\pi mk)} = 1$$

And so,

$$\begin{aligned}
e^{i(2\pi mk)} &= \frac{(3 + 4i)^m}{5^m} = 1 \\
& , \\
&(3 + 4i)^m = 5^m
\end{aligned}$$

(2) To show this equivalence, all we need to show is that

$$(3 + 4i)^2 \equiv 3 + 4i \pmod{4}$$

, and since m is an integer, the rest follows. Expanding out, we see that this equation is true. This means that $(3+4i)$ cannot be a multiple of 5, and thus can never equal

$$5^m$$

4.43 Use the result of the previous exercise

Because θ is an irrational multiple of 2π , we can use equation 4.76 and show that any single qubit gate in the form $R_z(\alpha)$ can be represented within an error of $\frac{\epsilon}{3}$. Now, we will show that

$$HR_z(\alpha)H = R_x(\alpha)$$

$$\begin{aligned} R_z(\alpha) &= \cos\left(\frac{\alpha}{2}\right)I - i\sin\left(\frac{\alpha}{2}\right)(Z) \\ HR_z(\alpha)H &= H \left[\cos\left(\frac{\alpha}{2}\right)I - i\sin\left(\frac{\alpha}{2}\right)(Z) \right] H \\ &= \cos\left(\frac{\alpha}{2}\right)I - i\sin\left(\frac{\alpha}{2}\right)HZH \end{aligned}$$

. Remember that $H^2 = I$, and that $HZH = X$, so:

$$HR_z(\alpha)H = \cos\left(\frac{\alpha}{2}\right)I - i\sin\left(\frac{\alpha}{2}\right)X = R_x(\alpha)$$

Following the same logic from page 197 (10th anniversary edition), we can approximate any n gate quantum circuit.

4.44 Show the three qubit gate

$$i = e^{i\frac{\pi}{2}}$$

is just a global phase factor, so the work is the same as the exercise above.

4.45 U is unitary

The statement is easy to see if you write out the H, S, CNOT, and Toffoli Matrices

$$\begin{aligned} H &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \\ S &= \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \\ CNOT &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \end{aligned}$$

(Toffoli gate has similar structure as CNOT Gate)

Inspecting these matrices, it's clear that all four satisfy the conditions stated in the problem. Now we just need to show that any unitary transform constructed by these four gates satisfies the conditions. Any transform can be constructed by using the tensor product or matrix multiplication operation between these four matrices and the identity matrix (which also satisfies the problem's properties). When we multiply or tensor product, it is clear that all elements remain complex integers and the only scalar coefficient will be in the form:

$$\left(\frac{1}{\sqrt{2}}\right)^k = 2^{-k/2}$$

4.46 Exponential complexity growth of quantum systems

$$\rho = \sum_i p_i |\psi_n\rangle \dots |\psi_1\rangle \otimes \langle \psi_n| \dots \langle \psi_1|$$

Each $|\psi_i\rangle$ has dimension 2, so $|\psi_n\rangle \dots |\psi_1\rangle$ has dimension 2^n , and the matrix ρ has dimension $2^n \times 2^n$. Since it's normalized, the matrix requires $4^n - 1$ independent real numbers to describe it.

4.47 Prove the following

To prove this, all we have to show is that

$$e^{A+B} = e^A e^B \text{ if } AB = BA$$

. To do this, we use

$$\begin{aligned} e^X &= \sum_{i=0}^{\infty} \frac{x^i}{i!} \\ e^A e^B &= \left(\frac{I}{0!} + \frac{A^1}{1!} + \frac{A^2}{2!} \dots\right) \left(\frac{I}{0!} + \frac{B^1}{1!} + \frac{B^2}{2!} \dots\right) \\ e^{A+B} &= \left(\frac{I}{0!} + \frac{(A+B)^1}{1!} + \frac{(A+B)^2}{2!} \dots\right) \end{aligned}$$

The n th term in the e^{A+B} expansion is $\frac{(A+B)^n}{n!}$, and if $AB = BA$ is true, we can use the binomial theorem

$$\frac{(A+B)^n}{n!} = \sum_{i=0}^n \frac{1}{i!(n-i)!} A^i B^{n-i} = \sum_{i=0}^n \left(\frac{A^i}{i!}\right) \left(\frac{B^{n-i}}{(n-i)!}\right)$$

This right hand side is precisely what you get when expanding $e^A e^B$. In this expansion there is precisely one

$$\left(\frac{A^i}{i!}\right) \left(\frac{B^{n-i}}{(n-i)!}\right)$$

for a specific n and i . To complete this question, we need to show that the term

$$\left(\frac{A^i}{i!}\right) \left(\frac{B^{n-i}}{(n-i)!}\right)$$

does not repeat for each n . However, this is obvious that for two different n_1 and n_2 that term cannot repeat, and we are done.

4.48 Restriction of H_k

$$c \binom{n}{c} \leq n^c$$

which is a polynomial in n .

4.49 Baker–Campbell–Hausdorff formula

Proving equation 4.103:

$$e^{i(A+B)\delta t} = e^{iA\delta t} e^{iB\delta t} + O(\delta t^2)$$

Start similarly to the proof of Trotter Formula.

$$\begin{aligned} e^{i(A+B)\delta t} &= I + \frac{i(A+B)\delta t}{1} + \frac{[i(A+B)]^2 \delta t^2}{2!} + O(\delta t^3) \\ e^{iA\delta t} e^{iB\delta t} &= \left(I + \frac{iA\delta t}{1} + \frac{(iA)^2 \delta t^2}{2!} + O(\delta t^3)\right) \left(I + \frac{iB\delta t}{1} + \frac{(iB)^2 \delta t^2}{2!} + O(\delta t^3)\right) \\ &= I + \frac{[i(A+B)]\delta t}{1} + \frac{((iA)^2 + (iB)^2)}{2!} + (iA)(iB)\delta t^2 + O(\delta t^3) \end{aligned}$$

In order for this to equal

$$e^{i(A+B)\delta t}$$

, we need to add the

$$O(\delta t^2)$$

term, and we are done.

Proving equation 4.104:

$$\begin{aligned} e^{iA\delta t/2} e^{iB\delta t} e^{iA\delta t/2} &= \left(I + \frac{iA\delta t}{2} + \frac{1}{2!} \left(\frac{iA\delta t}{2}\right)^2 + O(\delta t^3)\right) \left(I + iB\delta t + \frac{1}{2!} (iB\delta t)^2 + O(\delta t^3)\right) \\ &\quad \left(I + \frac{iA\delta t}{2} + \frac{1}{2!} \left(\frac{iA\delta t}{2}\right)^2 + O(\delta t^3)\right) \\ &= I + i(A+B)\delta t + \frac{(iA+iB)^2 \delta t^2}{2} + O(\delta t^3) \end{aligned}$$

Proving equation 4.105:

4.50

Part A): The key is to use equation 4.104, and generalize it with multiple variables.

$$\begin{aligned} e^{i(A+B)\Delta t} &= e^{iA\Delta t/2} e^{iB\Delta t} e^{iA\Delta t/2} + O(\Delta t^3) \\ e^{i(C+(A+B))\Delta t} &= e^{iC\Delta t/2} e^{i(A+B)\Delta t} e^{iC\Delta t/2} + O(\Delta t^3) \\ &= e^{iC\Delta t/2} e^{iA\Delta t/2} e^{iB\Delta t} e^{iA\Delta t/2} e^{iC\Delta t/2} + O(\Delta t^3) \end{aligned}$$

Thus,

$$e^{-2iH\Delta t} = e^{-i(2H_1+\dots+2H_L)\Delta t} = e^{-iH_1\Delta t} \dots e^{-iH_{L-1}\Delta t} e^{-2iH_L\Delta t} e^{-iH_{L-1}\Delta t} \dots e^{-iH_1\Delta t}$$

But by exercise 4.47,

$$e^{-2iH_L\Delta t} = e^{-iH_L\Delta t} e^{-iH_L\Delta t}$$

And we are done.

Part B):

$$E(U_{\Delta t}, e^{-2iH\Delta t}) = \max ||(U - V)|\psi\rangle|| = O(\Delta t^3)$$

By equation 4.63,

$$E(U_{\Delta t}^m, e^{-2miH\Delta t}) = mO(\Delta t^3)$$

By definition of big O,

$$O(\Delta t^3) = \alpha \Delta t^3$$

, so we are done.

5 Chapter 5 solutions

5.1 Transformation is Unitary

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

$$\langle j' | U^\dagger U | j \rangle = \frac{1}{N} \sum_{k=0}^{N-1} e^{2\pi i (j-j') k / N}$$

Case 1: $\Delta j = j - j' = 0 \implies P = 1$

Case 2: $\Delta j = j - j' \neq 0$

$$\frac{1}{N} \sum_{k=0}^{N-1} r^k \quad (r = e^{2\pi i \Delta j / N})$$

$$\frac{1 - r^N}{1 - r} = \frac{1 - e^{2\pi i \Delta j}}{1 - r} = 0$$

$(\Delta j \in \mathbb{Z})$

$$U^\dagger U = 1$$

5.2 Compute the Fourier Transform

$$U|00\dots 0\rangle = \frac{1}{\sqrt{2^n}} \sum_{i_1, \dots, i_n} |i_1 \dots i_n\rangle$$

5.4 Give a Decomposition

The controlled R_k gate, where k is an integer, can be decomposed into a sequence of single qubit gates and CNOT gates. One way to decompose it is as follows:

- Apply a Hadamard gate (H) to the control qubit.
- Apply a R_k gate to the target qubit.
- Apply a CNOT gate with the control qubit as the control and the target qubit as the target.
- Apply a R_k gate to the target qubit.
- Apply a CNOT gate with the control qubit as the control and the target qubit as the target.
- Apply a Hadamard gate (H) to the control qubit.

This decomposition is based on the fact that the controlled R_k gate can be written as a product of a controlled-U gate and a single-qubit rotation gate U , where $U = e^{(ik\pi/2^n)}$, and n is the number of qubits of the register.

5.5 Give a quantum circuit

The inverse quantum Fourier transform (IQFT) is the inverse operation of the quantum Fourier transform (QFT). It can be implemented using a circuit of Hadamard gates followed by controlled-phase gates. The circuit for an n -qubit register is given by:

- For $i = n - 1$ to 0 , apply a Hadamard gate (H) to the i -th qubit.
- For $i = 1$ to $n - 1$, apply controlled-phase gates with the i -th qubit as the control and the j -th qubit as the target, where j ranges from $i + 1$ to $n - 1$. The controlled-phase gate is defined as a CNOT gate followed by a single-qubit rotation gate R_k , where $k = 2^{(j-i)}$ and $R_k = e^{(ik\pi/2^n)}$

The mathematical foundation behind this circuit is the following:

The QFT is defined as:

$$QFT|x\rangle = 1/\sqrt{(2^n)} * \text{Summation } (i = 0 \text{ to } 2^{n-1}) e^{(2\pi i * x / 2^n)} |i\rangle$$

The IQFT is the inverse operation of QFT, so it is defined as:

$$IQFT|x\rangle = 1/\sqrt{(2^n)} * \text{Summation } (i = 0 \text{ to } 2^n - 1) e^{(-2\pi i * x / 2^n)} |i\rangle$$

So, the circuit implements the IQFT by applying the inverse of the operations that the QFT applies. The Hadamard gate is its own inverse, and the controlled-phase gates are inverted by conjugating the angles of the rotations.

So, the circuit applies the inverse of the QFT operation, which is the IQFT.

5.6 Approximate Quantum Fourier Transform

Since $E(U_1 U_2, V_1 V_2) \leq E(U_1, V_1) + E(U_2, V_2)$ the error accumulates linearly and FFT circuit contains $O(n^2)$ controlled - R_k gates

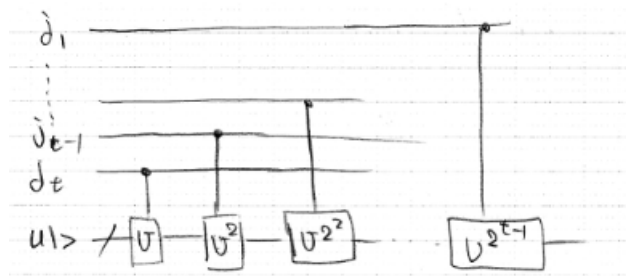
$$E(U, V) \approx O(n^2) \times \Delta \approx O\left(\frac{n^2}{p(n)}\right)$$

5.7 Additional insight into the circuit

$$|j\rangle = |j_1 \dots j_t\rangle$$

Total number of U operations is

$$= 2^0 \times j_t + 2^1 j_{t-1} + 2^2 j_{t-2} + \dots + 2^{t-1} j_1 = j$$



5.8 Phase Estimation

Solution attached as an image

5.9 U be a unitary transform

Considering the case of $t = 1$ in the phase estimation μ

$$\mu|0\rangle \otimes |u\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i \phi} |1\rangle \right) \otimes |u\rangle$$

For,

$$|\phi\rangle = \alpha_+ |\mu_+\rangle + \alpha_- |\mu_-\rangle$$

$$\begin{aligned} \mu|0\rangle \otimes |\phi\rangle &= \frac{\alpha_+}{\sqrt{2}} \left(|0\rangle + |1\rangle \right) \otimes |\mu_+\rangle \\ &+ \frac{\alpha_-}{\sqrt{2}} \left(|0\rangle - |1\rangle \right) \otimes |\mu_-\rangle \end{aligned}$$

$$\begin{aligned} (H \otimes 1) \cdot \mu(|0\rangle \otimes |\phi\rangle) &= \alpha_+ |0\rangle \otimes |\mu_+\rangle \\ &+ \alpha_- |1\rangle \otimes |\mu_-\rangle \end{aligned}$$

This is exactly the same circuit as in Ex 4.34

5.10 Show that the order of $x = 5$ modulo $N = 21$ is 6

$$5^2 = 4 \pmod{21}$$

$$5^3 = 20 \pmod{21}$$

$$5^4 = 100 = 16 \pmod{21}$$

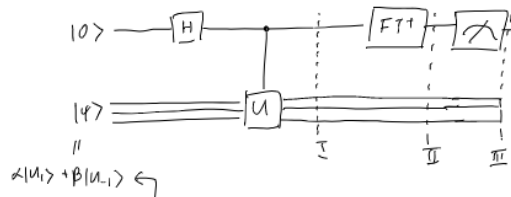
$$5^5 = 80 = 19 \pmod{21}$$

$$5^6 = 85 = 1 \pmod{21}$$

Exercise 5.8

Eigenvalues: $\begin{cases} 1 \rightarrow \text{associated eval: } u_1 \rightarrow \text{Phase } \phi_{u_1} = 0 \\ e^{2\pi i \phi_{u_1}} \end{cases}$
 $\begin{cases} -1 \rightarrow \text{associated eval: } u_{-1} \rightarrow \phi_{u_{-1}} = \frac{1}{2} = 0.1 \text{ (in binary)} \end{cases}$

The following circuit implements this:



Unlike in phase estimation algo
ancilla not guaranteed to be an
eigenstate

Intuition: what happens here is a superposition of what happens in regular
phase estimation.

$$\begin{aligned} \text{I): } & \alpha \left[\frac{1}{2} (|0\rangle + e^{2\pi i \phi_{u_1}} |1\rangle) |u_1\rangle \right] + \beta \left[\frac{1}{2} (|0\rangle + e^{2\pi i \phi_{u_{-1}}} |1\rangle) |u_{-1}\rangle \right] \\ &= \alpha \left[\frac{1}{2} (|0\rangle + e^{2\pi i 0/2} |1\rangle) |u_1\rangle \right] + \beta \left[\frac{1}{2} (|0\rangle + e^{2\pi i 1/2} |1\rangle) |u_{-1}\rangle \right] \\ &= \alpha \left(\frac{1}{2} \sum_{k=0}^1 e^{2\pi i 0 k/2} |k\rangle \right) |u_1\rangle + \beta \left(\frac{1}{2} \sum_{k=0}^1 e^{2\pi i 1 k/2} |k\rangle \right) |u_{-1}\rangle \end{aligned}$$

$$\text{II) } \alpha |0\rangle |u_1\rangle + \beta |1\rangle |u_{-1}\rangle$$

III) Measurement projects 1st register onto basis states: $\{|0\rangle, |1\rangle\}$.

Resulting state is $|0\rangle |u_1\rangle$ w prob $|\alpha|^2 \rightarrow$ measurement outcome 0,
 $|1\rangle |u_{-1}\rangle$ w prob $|\beta|^2 \rightarrow$ " " " "

Figure 6: Solution to Exercise 5.8

5.11 Show that the order of x satisfies $r \leq N$

$\phi(n)$: Euler function $x^{\phi(n)} = 1 \pmod{N}$

$$r \leq \phi(n) < N$$

5.12 Show that U is unitary

It is sufficient to show that $\tilde{U}^\dagger U = 1$

$$U \sim \begin{pmatrix} \tilde{U} & 0 \\ 0 & 1 \end{pmatrix} \begin{matrix} 0 \\ \vdots \\ p-1 \\ p \\ \vdots \\ 2^L-1 \end{matrix}$$

$$0 \leq y, y' \leq N-1$$

$$\langle y' | U^\dagger U | y \rangle = \langle xy' | xy \rangle$$

$$\text{if } xy' = xy \pmod{N}$$

$$\implies y^\dagger = y \pmod{N}$$

x is co-prime to N , so

$$U^\dagger U = 1$$

5.13 Prove 5.44

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{2\pi i s k / r} |u_s\rangle$$

$$\frac{1}{r} \sum_{s, k'=0}^{r-1} e^{\frac{-2\pi i s (k' - k)}{r}} |x^{k'} \bmod N\rangle$$

Now,

$$\sum_{s=0}^{r-1} e^{\frac{-2\pi i s (k' - k)}{r}} = r \text{ (for } k' = k)$$

$$= \frac{1 - e^{-2\pi i r (k' - k)/r}}{1 - e^{-2\pi i (k' - k)/r}} = 0$$

for $k' \neq k$

$$\Phi = \sum_{k'=0}^{r-1} \delta_{kk'} |x^{k'} \bmod N\rangle = |x^k \bmod N\rangle$$

5.15

The least common multiple (LCM) of two positive integers x and y is the smallest positive integer that is a multiple of both x and y . The greatest common divisor (GCD) of x and y is the largest positive integer that divides both x and y without leaving a remainder.

We can use the property that the product of the LCM and GCD of two integers is equal to the product of the integers themselves:

$$LCM(x, y) \times GCD(x, y) = x \times y$$

By dividing both sides of the equation by $GCD(x, y)$, we can find that:

$$LCM(x, y) = (x \times y) / GCD(x, y)$$

The GCD of two integers can be computed using the Euclidean algorithm in $O(L)$ operations, where L is the number of bits in the larger of the two integers. Therefore, computing the LCM of two L -bit integers using the formula above takes $O(L)$ operations for the GCD calculation and $O(1)$ operations for the division, for a total of $O(L)$ operations.

It should be $O(L^2)$ instead of $O(L)$

5.20

Using the cyclicity:

$$f(l) = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{-2\pi i l x / N} f(x)$$

$$\frac{1}{\sqrt{N}} \sum_{k=0}^{m-1} \sum_{x=0}^{r-1} e^{-2\pi i l (kr+x) / mr} f(x)$$

Now,

$$\sum_{k=0}^{m-1} e^{-2\pi i l k r / mr} = m \cdot \alpha e \cdot mn$$

$$= \frac{\sqrt{N}}{r} \sum_{x=0}^{r-1} e^{-2\pi i l x / N} f(x) \alpha e \frac{N}{r} \times x$$

Especially for $N = r$

$$f(l) = \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{-2\pi i l x / r} f(x)$$

5.21 Period finding and phase estimation

$$\begin{aligned}
(1) \quad U_y |\hat{f}(l)\rangle &= \frac{1}{\sqrt{n}} \sum_{x=0}^{n-1} e^{-2\pi i l x / n} |f(x+y)\rangle \\
&= \frac{1}{\sqrt{n}} e^{2\pi i l y / n} \sum_{x=y}^{n-1+y} e^{-2\pi i l x / n} |f(x)\rangle \\
&= e^{2\pi i l y / n} \frac{1}{\sqrt{n}} \sum_{x=0}^{n-1} e^{-2\pi i l x / n} |f(x)\rangle \\
&\quad \left(\because g(x) = e^{-2\pi i l x / n} |f(x)\rangle \text{ is cyclic} \right. \\
&\quad \left. g(x+1) = g(x) \right) \\
&= e^{2\pi i l y / n} |\hat{f}(l)\rangle \\
\therefore |\hat{f}(l)\rangle &\text{ is an eigen state with } \mathcal{G}_l = \frac{2\pi y}{n} \\
(2) \quad \text{Now } |f(x_0)\rangle &= \frac{1}{n} \sum_{l=0}^{n-1} e^{2\pi i l x_0 / n} |\hat{f}(l)\rangle \\
&= \sum_{l=0}^{n-1} \alpha_l |\hat{f}(l)\rangle \quad (|\alpha_l|^2 = \frac{1}{n}) \\
\therefore \text{By setting } |u\rangle &= |f(x_0)\rangle \text{ in the second register} \\
&\text{of the phase estimator, the result of the "Black} \\
&\text{box" is:} \\
\sum_{l=0}^{n-1} \alpha_l \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} e^{2\pi i j \mathcal{G}_l} |j\rangle |\hat{f}(l)\rangle &\rightarrow \sum_{l=0}^{n-1} \alpha_l |\tilde{\mathcal{G}}_l\rangle |\hat{f}(l)\rangle \\
&\quad \text{Inverse FT.} \quad //
\end{aligned}$$

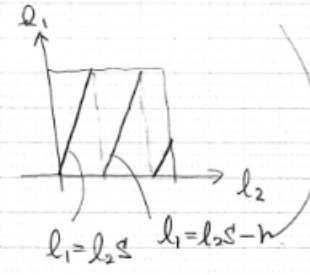
Figure 7: 5.21 solution

5.22

$$\begin{aligned}
 & \left. \begin{aligned} f(x_1, x_2) &= f(x_1 + l, x_2 - ls) & \text{--- } \textcircled{D} \\ f(x_1, x_2) &= f(x_1, x_2 + w) & \text{--- } \textcircled{E} \quad (\because a^w = 1) \end{aligned} \right\} \\
 & \text{Setting } l = -x_1 \text{ in } \textcircled{D}, \quad f(x_1, x_2) = f(0, x_2 + x_1 s) \\
 & \therefore |\hat{f}(l_1, l_2)\rangle = \frac{1}{N} \sum_{x_1=0}^{r-1} \sum_{x_2=0}^{r-1} e^{-2\pi i(l_1 x_1 + l_2 x_2)/N} |f(x_1, x_2)\rangle \\
 & = \frac{1}{N} \sum_{x_1=0}^{r-1} \sum_{j=x_1 s}^{x_1 s + (r-1)} e^{-2\pi i(l_1 x_1 + l_2 j - l_2 x_1 s)/N} |f(0, j)\rangle \underbrace{|f(0, x_2 + x_1 s)\rangle}_{(j = x_2 + x_1 s)} \\
 & = \frac{1}{N} \underbrace{\sum_{x_1=0}^{r-1} e^{-2\pi i(l_1 - l_2 s)x_1/N}}_{\text{"}} \sum_{j=x_1 s}^{x_1 s + (r-1)} e^{-2\pi i l_2 j/N} |f(0, j)\rangle \\
 & \quad N \times \delta_{l_1 - l_2 s, r\mathbb{Z}} \quad \underbrace{\sum_{j=0}^{r-1}}_{\substack{\downarrow \\ \text{cyclic for } j \rightarrow j+w}} \quad (\because \text{cyclic for } j \rightarrow j+w) \\
 & = \sum_{j=0}^{r-1} e^{-2\pi i l_2 j/N} |f(0, j)\rangle \times \delta_{l_1 - l_2 s, r\mathbb{Z}} //
 \end{aligned}$$

Figure 8: 5.22 solution

5.23

$$\begin{aligned}
& \frac{1}{h} \sum_{l_1=0}^{h-1} \sum_{l_2=0}^{h-1} e^{-2\pi i(l_1 x_1 + l_2 x_2)/h} |\hat{f}(l_1, l_2)\rangle \\
&= \frac{1}{h} \sum_{l_1, l_2} e^{-2\pi i(l_1 x_1 + l_2 x_2)/h} \sum_{j=0}^{h-1} e^{-2\pi i l_2 j/h} |f(0, j)\rangle \\
&= \frac{1}{h} \sum_{l_2=0}^{h-1} \sum_{j=0}^{h-1} e^{-2\pi i \{ (l_2 s + \cancel{p\mathbb{Z}}) x_1 + l_2 x_2 - l_2 j \}/h} |f(0, j)\rangle \\
&\quad \left(\begin{array}{l} \because \text{there is a single } l_1 \\ \text{that satisfies the condition} \\ l_1 - l_2 s = p\mathbb{Z} \end{array} \right)
\end{aligned}$$


$$\begin{aligned}
&= \frac{1}{h} \sum_{j=0}^{h-1} \sum_{l_2=0}^{h-1} e^{-2\pi i l_2 (s x_1 + x_2 - j)/h} |f(0, j)\rangle \\
&= \sum_{j=0}^{h-1} |f(0, j)\rangle \times \delta_{s x_1 + x_2 - j, p\mathbb{Z}} \\
&= |f(0, s x_1 + x_2 + p\mathbb{Z})\rangle = |f(x_1, x_2)\rangle
\end{aligned}$$

Figure 9: 5.23 solution

6 Chapter 8 solutions

8.1 The density operator of the initial state is written by $k b \psi$ and final form is written by $U k b \psi U^\dagger$.

Thus time development of $\rho = k b \psi$ can be written by $\mathcal{E}(\rho) = U \rho U^\dagger$.

8.2 From eqn (2.147) (on page 100),

$$\rho_m = \frac{M_m \rho M_m^\dagger}{(M_m^\dagger M_m \rho)} = \frac{M_m \rho M_m^\dagger}{(M_m \rho M_m^\dagger)} = \frac{\mathcal{E}_m(\rho)}{\mathcal{E}_m(\rho)}.$$

And from eqn (2.143) (on page 99), $p(m) = \text{Tr}(M_m^\dagger M_m \rho) = \text{Tr}(M_m \rho M_m^\dagger) =$

$$Tr\mathcal{E}_m(\rho).$$