Notes on Quantum Information

Apiros3

First Version : Mar 11, 2025
Last Update : Jan 29, 2025

Contents

1 Quantum States

1.1 Basic Definitions

Definition 1.1.1. *A (pure) state of a quantum bit,* ***qubit*** *is represented by a linear combination of* $|0\rangle$ *and* $|1\rangle$ *of the form,*

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \qquad \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1$$

. These linear combinations are called ***quantum superpositions****.*

So the states of a qubit are unit vectors in $\mathbb{C}^2$ over $\mathbb{C}$. In actual use, this is then an equivalence modulo global phase, where if $|\psi\rangle$ and $|\psi'\rangle$ are different states and

$$|\psi'\rangle = e^{i\gamma}|\psi\rangle$$

for some $\gamma \in [0, 2\pi)$, they represent the same phase.

Definition 1.1.2 (dirac Notation)**.** *Let*

$$\psi = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in \mathbb{C}^2 \tag{1}$$

Then, representing the standard basis vectors of $\mathbb{C}^2$ *as* $|0\rangle$ *and* $|1\rangle$*, we have the mapping,*

$$\psi = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

which has a natural correspondence to $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$*.*

Row vectors have a similar correspondence, where

$$\psi^\dagger = \begin{pmatrix} \overline{\alpha} & \overline{\beta} \end{pmatrix} = \overline{\alpha} \begin{pmatrix} 1 & 0 \end{pmatrix} + \overline{\beta} \begin{pmatrix} 0 & 1 \end{pmatrix}$$

has a correspondence with $\langle\psi| = \overline{\alpha}\langle 0| + \overline{\beta}\langle 1|$*.*

The scalar product between $|\psi\rangle$ and $\langle\psi'|$ is called a **bracket** and is denoted $\langle\psi|\psi'\rangle$ where

$$\langle\psi|\psi'\rangle := \psi^\dagger\psi' = \begin{pmatrix} \overline{\alpha} & \overline{\beta} \end{pmatrix} \begin{pmatrix} \alpha' \\ \beta' \end{pmatrix} = \overline{\alpha}\alpha' + \overline{\beta}\beta'$$

Using this, we can write

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

Definition 1.1.3 (Extended dirac Notation)**.** *We can extend our dirac notation from* $\mathbb{C}^2$ *to* $\mathbb{C}^d$ *for any* $d \in \mathbb{N}^+$*. We denote the standard basis for* $\mathbb{C}^d$ *using* $|0\rangle, \ldots, |d-1\rangle$ *and similarly for* $\langle i|$*. The natural correspondence follows. In particular,*

$$\langle\phi|\psi\rangle = \sum_{n=0}^{d-1} \overline{\phi}_n \psi_n$$

and the norm of $|\psi\rangle$ *is* $||\psi|| := \sqrt{\langle\psi|\psi\rangle}$*.*

We call the system with d perfectly distinguishable states a **qudit**, where states are of the form

$$|\psi\rangle = \psi_0|0\rangle + \dots \psi_{d-1}|d-1\rangle, \qquad \psi_0, \dots \psi_{d-1} \in \mathbb{C}, \sum_{n=0}^{d-1} |\psi_n|^2 = 1$$

and equivalence up to phrase.

In particular, there is a natural correspondence with a quantum system with $d < \infty$ perfectly distinguishable states is associated to the (Hilbert) vector space $\mathcal{H} = \mathbb{C}^d$.

Definition 1.1.4 (Basic Measurements: Born Rule)**.** *Basic measurements on a d-dimensional quantum system are represented by ON-basis in $\mathbb{C}^d$ up to global phases. Specifically, given a state $|\psi\rangle$, and ON-basis $\{|\psi_n\rangle \mid n = 0, \dots, d-1\}$,*

$$p_n = |\langle\psi_n|\psi\rangle|^2$$

If we obtain outcome n, then the state of the system immediately after the measurement is $|\psi_n\rangle$.

Proposition 1.1.5. *Suppose we have two ON-basis $\{|\psi_n\rangle \mid n = 0, \dots, d-1\}$ and $\{|\psi'_n\rangle \mid n = 0, \dots, d-1\}$ which are equal up to global phases. Then, the two basis assign the same probability for every possible state, and assign the same post-measurement state.*

Proof. Is immediate after substituting and rewriting both sides. □

Definition 1.1.6. *The standard basis $\{|n\rangle \mid n = 0, \dots d-1\}$ is called the **computation basis**. We define the **Fourier Basis** consisting of the **Fourier vectors** given by,*

$$|e_n\rangle := \frac{1}{\sqrt{d}} \sum_{m=0}^{d-1} \exp\left[\frac{2\pi i m n}{d}\right] |m\rangle, \qquad n = 0, \dots, d-1.$$

The fourier basis vectors are uniform superpositions of the vectors of the computational basis, where each $|e_n\rangle$ represented by the computational basis have the same coefficients on each basis vector.

Notation 1.1.7. Taking the fourier basis in $d = 2$, we write

$$|+\rangle := |e_0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$|-\rangle := |e_1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Remark 1.1.8. Every basic measurement has the same number of outcomes equal to the dimension of the system's Hilbert space, meaning we can only extract finite information.

Further, note that

$$||\psi||^2 = \sum_{n=0}^{d-1} |\psi_n|^2 = \sum_{n=0}^{d-1} |\langle n|\psi\rangle|^2 = \sum_{n=0}^{d-1} p_n = 1$$

Also, for any $n \in \{0, \dots, d-1\}$, $|\psi'\rangle = e^{i\gamma}|\psi\rangle$

$$|\langle\psi_n|\psi'\rangle|^2 = |e^{i\gamma}\langle\psi_n|\psi\rangle|^2 = |\langle\psi_n|\psi\rangle|^2$$

Specifically, global phases do not change probabilities.

In fact this condition is an if and only if. Suppose we have two states such that

$$|\langle\psi_n|\psi\rangle|^2 = |\langle\psi_n|\psi'\rangle|^2$$

for any choice of ON-basis $\{|\psi_n\rangle \mid n = 0, \dots, d-1\}$. Then, pick an ON-basis with vector $|\psi\rangle$. Then in particular, $|\langle\psi|\psi\rangle|^2 = |\langle\psi|\psi'\rangle|^2 = 1$. By CS inequality, $|\psi\rangle$ is a constant factor of $|\psi'\rangle$, and as they are both unit vectors, are phase apart.

1.2 Reversible Processes

Definition 1.2.1. *We say that $\mathcal{P}$ is a **reversible process** if there exists another process $\mathcal{P}'$ such that*

1. *applying $\mathcal{P}'$ after $\mathcal{P}$ brings the system back to the initial state*
2. *applying $\mathcal{P}$ after $\mathcal{P}'$ brings the system back to the initial state*

*In this case, we say that $\mathcal{P}'$ is the **inverse** of $\mathcal{P}$.*

The main idea of this subsection is that every unitary matrix represents a reversible process (Where a unitary matrix U is a matrix such that $U^\dagger U = I$).

Proposition 1.2.2. *Let $|\psi'\rangle = U|\psi\rangle$, where U is unitary. Then, $|||\psi'\rangle||^2 = |||\psi\rangle||^2$.*

Proof. Taking the complex conjugate on both sides, we have $\langle\psi'| = \langle\psi|U^\dagger$. Taking the product of both,

$$\begin{aligned} |||\psi'\rangle||^2 &= \langle\psi'|\psi'\rangle \\ &= |\psi\rangle U^\dagger U \langle\psi| \\ &= \langle\psi|\psi\rangle \\ &= |||\psi\rangle||^2 \end{aligned}$$

□

In particular, unit vectors are transformed into unit vectors after multiplication by unitary matricies. Thus, pure states are mapped into pure states. Note also that as matrix multiplication is a linear transformation, it can be thought of as mapping basis vectors by U.

Definition 1.2.3. *We define **Pauli Matrices** as*

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

We sometimes denote $\sigma_x, \sigma_y, \sigma_z$ as X, Y, Z respectively.

*Pauli X is called the **bit flip gate** as it flips the computational basis.*

*Pauli Z is called the **phase flip gate** as it flips the phase in front of $|1\rangle$ while leaving $|0\rangle$ unchanged. By flipping the phase, it flips $|+\rangle$ into $|-\rangle$ and vice versa.*

Proposition 1.2.4. *We have the following :*

1. *Pauli matrices are self-adjoint ($U^\dagger = U$)*
2. *$X^2 = Y^2 = Z^2 = I$*
3. *Pauli matrices are unitary*
4. *Distinct Pauli matrices anticommute: $U_1 U_2 = -U_2 U_1$.*

Proof. Immediate. One needs to work through (4). □

Pauli matrices give rise to a unitary matrix,

$$\boldsymbol{n}\cdot\boldsymbol{\sigma} := n_x\sigma_x + n_y\sigma_y + n_z\sigma_z = \begin{pmatrix} n_z & n_x - in_y \\ n_x + in_y & -n_z \end{pmatrix}$$

where $\boldsymbol{n} = \begin{pmatrix} n_x \\ n_y \\ n_z \end{pmatrix}$ is a unit vector in $\mathbb{R}^3$.

This is self-adjoint and unitary for any unit vector $\boldsymbol{n}$.

Remark 1.2.5. As usual, unitary matrices equal up to global phases are seen as equivalent, as there is no way to distinguish between the two processes.

Remark 1.2.6. Note the usual identities when dealing with unitary matrices:

- $U^\dagger U = I$
- $U^\dagger = U^{-1}$
- $UU^\dagger = I$

Definition 1.2.7 (Dirac Notation for Matrices)**.** *Using two vectors $|\alpha\rangle, |\beta\rangle$ in $\mathbb{C}^d$, writing*

$$|\alpha\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{d-1} \end{pmatrix} \qquad |\beta\rangle = \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{d-1} \end{pmatrix}$$

we write $|\alpha\rangle\langle\beta|$ to represent a d-by-d matrix. Specifically,

$$|\alpha\rangle\langle\beta| = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{d-1} \end{pmatrix} \begin{pmatrix} \overline{\beta}_0 & \overline{\beta}_1 & \cdots & \overline{\beta}_{d-1} \end{pmatrix} = \begin{pmatrix} \alpha_0\overline{\beta}_0 & \alpha_0\overline{\beta}_1 & \cdots \\ \alpha_1\overline{\beta}_0 & \alpha_1\overline{\beta}_1 & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix}$$

In particular, we have very natural identities with this notation.

Proposition 1.2.8. *We have the identity,*

$$|\alpha\rangle\langle\beta||\psi\rangle = |\alpha\rangle\langle\beta|\psi\rangle = \langle\beta|\psi\rangle|\alpha\rangle$$

Proof. Immediate, either with matrix expansion or using the fact that $\langle\beta|\psi\rangle$ is a scalar in $\mathbb{C}$ (thus commutes). □

Proposition 1.2.9. *Given $|\alpha\rangle, |\beta\rangle, |\gamma\rangle, |\delta\rangle$ in $\mathbb{C}^d$, taking $A := |\alpha\rangle\langle\beta|$ and $B := |\gamma\rangle\langle\delta|$, $AB = \langle\beta|\gamma\rangle|\alpha\rangle\langle\delta|$.*

Proof. Immediate. □

Proposition 1.2.10. *Any matrix A can be written as a linear sum of matrices of the form $|\alpha_i\rangle\langle\beta_i|$.*

Proof. The standard basis for a matrix can be written by $|i\rangle\langle j|$. □

Proposition 1.2.11 (Adjoint Matrices with Dirac Notation)**.** *We have the following identities:*

1. *Given* $A = |\alpha\rangle\langle\beta|$, *we have* $A^\dagger = |\beta\rangle\langle\alpha|$

2. *Given a finite index* I, $A = \sum_{m\in I} c_m|\alpha_m\rangle\langle\beta_m|$, *we have* $A^\dagger = \sum_{m\in I} \bar{c}_m|\beta_m\rangle\langle\alpha_m|$

Proof. Immediate after expansion. □

Proposition 1.2.12. *Given any ON basis* $\{|\psi_m\rangle \mid m = 0, \ldots, d-1\}$,

$$\sum_{m=0}^{d-1} |\psi_m\rangle\langle\psi_m| = I_d$$

Proof. Noting that $|\psi_m\rangle\langle\psi_m||\psi_n\rangle = |\psi_m\rangle\delta_{mn}$, we can show that post-multiplying our matrix with any ψ keeps the vector unchanged. □

Proposition 1.2.13. *For any choice of ON-basis* $\{|\psi_m\rangle \mid m = 0, \ldots, d-1\}$ *and* $\{\delta_m \in \mathbb{R} \mid m = 0, \ldots, d-1\}$,

$$U = \sum_{m=0}^{d-1} e^{i\gamma_m}|\psi_m\rangle\langle\psi_m|$$

is unitary.

Proof. Expanding $U^\dagger U$,

$$\begin{aligned}
(\sum_{n=0}^{d-1} e^{-i\gamma_n}|\psi_n\rangle\langle\psi_n|)(\sum_{m=0}^{d-1} e^{i\gamma_m}|\psi_m\rangle\langle\psi_m|) &= \sum_{n=0}^{d-1}\sum_{m=0}^{d-1}(e^{-i\gamma_n}|\psi_n\rangle\langle\psi_n|)(e^{i\gamma_m}|\psi_m\rangle\langle\psi_m|) \\
&= \sum_{n=0}^{d-1}\sum_{m=0}^{d-1}(e^{i(\gamma_m-\gamma_n)}|\psi_n\rangle\langle\psi_n||\psi_m\rangle\langle\psi_m|) \\
&= \sum_{n=0}^{d-1}\sum_{m=0}^{d-1}(e^{i(\gamma_m-\gamma_n)}\delta_{nm}|\psi_n\rangle\langle\psi_m|) \\
&= \sum_{m=0}^{d-1}(|\psi_m\rangle\langle\psi_m|) = I
\end{aligned}$$

□

Remark 1.2.14. In fact, every unitary basis can be written in the above form, using the Spectral Theorem for unitary matrices in $\mathbb{C}$. Then, every vector $|\psi_m\rangle$ is an eigenvector of U with eigenvalue $e^{i\delta_m}$.

From a QI view, this means that reversible processes applied to $|\psi_m\rangle$ will be unchanged up to a global phase after the proceess.

Proposition 1.2.15. *Given two ON-basis* $\{|\psi_m\rangle \mid m = 0, \ldots, d-1\}$ *and* $\{|\phi_m\rangle \mid m = 0, \ldots, d-1\}$,

$$U = \sum_{m=0}^{d-1} |\psi_m\rangle\langle\phi_m|$$

is unitary. In fact, every unitary matrix can be written this way.

Proof. To show is unitary follows the same structure as Proposition 1.2.13. Given a unitary matrix U, fixing any ON basis $\{|\psi_m\rangle \mid m = 0, \ldots, d-1\}$, we have

$$U = UI = U(\sum_{m=0}^{d-1} |\psi_m\rangle\langle\psi_m|) = \sum_{m=0}^{d-1} U|\psi_m\rangle\langle\psi_m|$$

We show that $\{U|\psi_m\rangle \mid m = 0, \ldots, d-1\}$ is an ON-basis. This follows from

$$(U|\psi_m\rangle)^\dagger(U|\psi_n\rangle) = \langle\psi_m|U^\dagger U|\psi_n\rangle = \langle\psi_m|\psi_n\rangle = \delta_{mn}$$

□

Example 1.2.16. The matrix

$$F = \sum_{m=0}^{d-1} |e_m\rangle\langle m|$$

known as the **quantum Fourier Transform** is a reversible gate. This transforms the computational basis into the Fourier basis. In the specific case for qubits, this is known as the **Hadamard Gate**, denoted

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

Recalling the equation, $U|\phi_m\rangle = |\psi_m\rangle$. Consequently, we can use unitary matrices to change between matrices. Thus, we can reduce the problem of basic measurements to a measurement in the computational basis (by passing it through this change of basis).

Importantly, measurements are not reversible. However, we can gain knowledge about the state by utilizing reversible processes in between.

Example 1.2.17 (Elitzur-Vaidman Bomb Tester)**.** Suppose we set the initial state of our qubit into $|0\rangle$. Consider applying H twice onto this state, then measuring. as $H^2 = I$, we will always measure $|0\rangle$. However, if a measurement with the computational basis takes place in between the two applications, it transforms the qubit, giving a $1/2$ probability for measuring $|1\rangle$ after the second application. This way, we may be able to identify if a measurement took place in between.

To give a physical example, imagine a beamsplitter H that splits $|0\rangle$ into equal probabilities $|0\rangle$ and $|1\rangle$. Suppose there is a 50% probability there is an object along the path of $|0\rangle$ that will absorb this. If we combine the split light and pass it through another beamsplitter H, we will measure $|1\rangle$ only if there is an object along the path.

We can make this probability arbitrarily small. Consider the matrix,

$$U_n := \begin{pmatrix} \cos(\frac{\pi}{2n}) & -\sin(\frac{\pi}{2n}) \\ \sin(\frac{\pi}{2n}) & \cos(\frac{\pi}{2n}) \end{pmatrix}$$

Applying U_n to the intial state $|0\rangle$, we get

$$U_n|0\rangle = \cos\left(\frac{\pi}{2n}\right)|0\rangle + \sin\left(\frac{\pi}{2n}\right)|1\rangle$$

By simple trigonometry identities, after application k times, we get

$$(U_n)^k|0\rangle = \cos\left(\frac{k\pi}{2n}\right)|0\rangle + \sin\left(\frac{k\pi}{2n}\right)|1\rangle$$

Taking $k = n$, the final state of the photon after n iterations is $|1\rangle$. If the bomb is present, it will explode with probability $p(1) = |\langle 1|U_n|0\rangle|^2 = \left(\sin\frac{\pi}{2n}\right)^2$, we can make this value arbitrarily small by choosing suitably large n. If the bomb is present, it will remain on $|0\rangle$, with application always bring the state to $U_n|0\rangle$. After n iterations, the probability the bomb is unexploded and is on $|0\rangle$ is

$$(p_0)^n = \left[1 - \left(\sin\frac{\pi}{2n}\right)^2\right]^n \geq 1 - n\left(\sin\frac{\pi}{2n}\right)^2 \geq 1 - \frac{\pi^2}{4n}$$

Choosing n large enough, we can make this probability as close to 1 as we want.

The essential idea is the **quantum Zeno effect**, where frequent measurements by a fixed basis can "freeze" the change by time, locking the system to one of the states of the basis.

1.3 Composite System

Definition 1.3.1. *Given two Hilbert Spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ of dimensions d_A and d_B, the tensor product $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ is the space $\mathbb{C}^{d_A d_B}$ equipped with a map on vectors*

$$|\alpha\rangle = \begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_{d_A-1} \end{pmatrix} \qquad |\beta\rangle = \begin{pmatrix} \beta_0 \\ \vdots \\ \beta_{d_B-1} \end{pmatrix}$$

to their tensor product

$$|\alpha\rangle \otimes |\beta\rangle = \begin{pmatrix} \alpha_0\beta_0 \\ \vdots \\ \alpha_0\beta_{d_B-1} \\ \vdots \\ \alpha_{d_A-1}\beta_0 \\ \vdots \\ \alpha_{d_A-1}\beta_{d_B-1} \end{pmatrix}$$

As per qubits, we can give the computational basis as

$$\{|m\rangle \times |n\rangle \mid m = 0, \ldots, d_A - 1, n = 0, d_B - 1\}$$

and we can represent a composite quantum system with the linear combinations

$$|\Psi\rangle = \sum_{m=0}^{d_A-1} \sum_{n=0}^{d_B-1} \Psi_{mn}|m\rangle \otimes |n\rangle$$

where Ψ_{mn} satisfy $\sum_{m,n} |\Psi_{mn}|^2 = 1$.

Note the computational basis extracts exactly the coordinates described by the vector.

Definition 1.3.2. *Given $|\alpha\rangle \in \mathcal{H}_A$ and $|\beta\rangle \in \mathcal{H}_B$, $|a\rangle \otimes |b\rangle$ is called a **product state**.*

Definition 1.3.3. *A pure state $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is **entangled** if it is not a product state.*

Example 1.3.4. The state

$$|\Phi^+\rangle = \frac{|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle}{\sqrt{2}}$$

is an entangled state.

Definition 1.3.5. *Given $|\alpha\rangle \in \mathcal{H}_A$ and $|\beta\rangle \in \mathcal{H}_B$, $\langle\alpha| \otimes \langle\beta| = (|\alpha\rangle \otimes |\beta\rangle)^\dagger$. Products of this form are called* ***product bra****.*

Proposition 1.3.6. *For a valid choice of vectors $|\alpha\rangle, |\alpha'\rangle, |\beta\rangle, |\beta'\rangle$, we have*

$$(\langle\alpha| \otimes \langle\beta|)(|\alpha'\rangle \otimes |\beta'\rangle) = \langle\alpha|\alpha'\rangle\langle\beta|\beta'\rangle$$

Proposition 1.3.7. *Given ONB $\{|\alpha_m\rangle \mid m = 0, \ldots, d_A - 1\}$ and $\{|\beta_n\rangle \mid n = 0, \ldots, d_B - 1\}$, this induces a measurement on the composite system AB,*

$$\{|\alpha_m\rangle \otimes |\alpha_n\rangle \mid m = 0, \ldots, d_A - 1, n = 0, \ldots, d_B - 1\}$$

and this is an ONB.

Definition 1.3.8. *A measurement on the ONB $\{|\alpha_m\rangle \otimes |\beta_n\rangle\}$ is called the* ***product measurement****.*

Example 1.3.9. Not all valid measurements are product measurements. Suppose that A and B are qubits. Then the vectors

$$|\Phi^+\rangle := \frac{|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle}{\sqrt{2}}$$
$$|\Phi^-\rangle := \frac{|0\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle}{\sqrt{2}}$$
$$|\Psi^+\rangle := \frac{|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle}{\sqrt{2}}$$
$$|\Psi^-\rangle := \frac{|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle}{\sqrt{2}}$$

known as the **Bell Basis** is an ONB that is not a product measurement.

Definition 1.3.10. *Given square matrices A and B, the* ***product matrix*** *$A \otimes B$ is the matrix defined by the relation*

$$(A \otimes B)(|\alpha\rangle \otimes |\beta\rangle) := A|\alpha\rangle \otimes B|\beta\rangle$$

for $|\alpha\rangle \in \mathcal{H}_A$ and $|\beta\rangle \in \mathcal{H}_B$.

Note that this defines the relation on every vector as

Example 1.3.11. The explicit representation, given $A = (a_{ij})$ and B can be seen as the block matrix

$$A \otimes B = \begin{pmatrix} a_{00}B & a_{01}B & \cdots & a_{0n}B \\ \vdots & & & \vdots \\ a_{n0}B & a_{n1}B & \cdots & a_{nn}B \end{pmatrix}$$

Proposition 1.3.12. *We note some properties about product matrices.*

- $(A \otimes B)(A' \otimes B') = AA' \otimes BB'$
- $(\langle\alpha| \otimes \langle\beta|)(A \otimes B)(|\alpha'\rangle \otimes |\beta'\rangle) = \langle\alpha|A|\alpha'\rangle\langle\beta|B|\beta'\rangle$ *for vectors $\alpha, \alpha' \in \mathcal{H}_A$ and $\beta, \beta' \in \mathcal{H}_B$.*
- $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$
- *If U_A and U_B are unitaries, then $U_A \otimes U_B$ is unitary.*

Remark 1.3.13. Measurements by unitary matrices evolve systems independently. That is,

$$(U_A \otimes U_B)(|\alpha\rangle \otimes |\beta\rangle) = U_A|\alpha\rangle \otimes U_B|\beta\rangle$$

Definition 1.3.14. *If a gate U_{AB} is not a product gate, we call it an **interaction gate**. If the gate transforms product states into entangled states, the gate is called an **entangling gate**.*

Example 1.3.15 (CNOT gate)**.** The controlled-NOT (CNOT) gate is defined as

$$\text{CNOT} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$

where X is the Pauli X matrix. Then we have that $\text{CNOT}^\dagger = \text{CNOT}$ and that CNOT is a unitary gate. The gate flips the second qubit if and only if the first qubit is $|1\rangle$.

When the first qubit is a Fourier basis, CNOT generates entanglement, sending

$$\text{CNOT}|\alpha\rangle \otimes |\beta\rangle = |(\beta = 0?\Phi : \Psi)^\alpha\rangle$$

where $\alpha \in \{+, -\}$ and $\beta \in \{0, 1\}$. In particular, this gives a way to measure with the Bell basis on Ψ, by passing it through the CNOT gate and then measuring on the product basis $\{|+\rangle|0\rangle, |+\rangle|1\rangle, |-\rangle|0\rangle, |-\rangle|1\rangle\}$. For instance,

$$p_{AB}(+, 0) = |\langle +| \otimes \langle 0|\text{CNOT}|\Psi\rangle|^2 = |\langle \Phi^+|\Psi\rangle|^2$$

noting that $\text{CNOT}^\dagger = \text{CNOT}$.

Proposition 1.3.16. *System composition is associative. We have,*

$$\mathcal{H}_A \otimes (\mathcal{H}_B \otimes \mathcal{H}_C) = \mathcal{H}_A \otimes \mathcal{H}_{BC} = \mathcal{H}_{ABC} = \mathcal{H}_{AB} \otimes \mathcal{H}_C = (\mathcal{H}_A \otimes \mathcal{H}_B) \otimes \mathcal{H}_C$$

because $\otimes$ is associative on vectors.

Example 1.3.17 (GHZ state)**.** An example of a three-qubit state where every system is entangled is

$$|\text{GHZ}\rangle = \frac{|0\rangle \otimes |0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle \otimes |1\rangle}{\sqrt{2}}$$

Remark 1.3.18. The notion of composing systems can be extended to an arbitrary number of systems. In any case, a generic pure state is written as a linear combination on the computational basis of each system, which of course grows exponentially with the number of systems.

1.4 Mixed States

Suppose we have a probability distribution about states themselves. Let ψ be in state $|\psi_i\rangle$ with probability p_i. Fix an ONB ϕ_i. We have that

$$\begin{aligned} P(\text{outcome } j) &= \sum_i p_i P(\text{outcome } j|\text{state is } i) \\ &= \sum_i p_i |\langle \phi_j|\psi_i\rangle|^2 \\ &= \sum_i p_i \langle \phi_j|\psi_i\rangle\langle \psi_i|\phi_j\rangle \\ &= \langle \phi_j| \left(\sum_i p_i |\psi_i\rangle\langle \psi_i| \right) |\phi_j\rangle \end{aligned}$$

We write $\rho = \sum_i p_i |\psi_i\rangle\langle \psi_i|$. Note that this is independent of the choice of basis ϕ_i.

Definition 1.4.1. *When ρ is nontrivial with multiple i such that p_i are nonzero, then we say that the state ρ is **mixed** with pure states ψ_i. We call ρ the **density matrix**, and can treat this as a state (to perform measurements on).*

Definition 1.4.2. *The set*

$$E = \{(|\psi_i\rangle, p_i) \mid i = 0, \ldots, k-1\}$$

*is called the **ensemble**. We can then say that ρ is the **average state** of the ensemble E.*

Following the above notation, we therefore have $p(n) = \langle\phi_n|\rho|\phi_n\rangle$. Consequently, ρ is positive semi-definite, with $\rho \geq 0$.

Proposition 1.4.3. *The function that transforms ensembles to density matrices is not injective. For instance, every ensemble of the form*

$$E = \left\{ \left(|\phi\rangle, \frac{1}{2} \right), \left(|\phi^\perp\rangle, \frac{1}{2} \right) \right\}$$

such that $\{|\phi\rangle, |\phi^\perp\rangle\}$ is a ONB has the same density matrix $\rho = I/2$ (e.g., computational basis and the fourier basis).

Proof. The density matrix is given by

$$\rho = \frac{1}{2}|\phi\rangle\langle\phi| + \frac{1}{2}|\phi^\perp\rangle\langle\phi^\perp| = I/2$$

The last equality follows from that

$$|\psi\rangle = \langle\phi|\psi\rangle|\phi\rangle + \langle\phi^\perp|\psi\rangle|\phi^\perp\rangle = (|\phi\rangle\langle\phi| + |\phi^\perp\rangle\langle\phi^\perp|)|\psi\rangle$$

□

Proposition 1.4.4. $\mathrm{Tr}(\rho) = 1$.

Proof. Follows from the fact that $\rho_{nn} = \langle n|\rho|n\rangle = p(n)$ on the computational basis. As the probability sum to 1, the trace must also. □

Lemma 1.4.5. *Let P be a positive $d \times d$ matrix. Then we have $P^\dagger = P$.*

Proof. Sketch. We use the fact that $\langle m|\rho|n\rangle$ can be written as a linear sum of $\langle n|\rho|n\rangle$ and $\langle m|\rho|m\rangle$. □

Corollary 1.4.6. *Given two density matrices ρ and σ that give the same probabilities for every basic measurement, $\rho = \sigma$.*

Proof. $\rho_{mn} = \langle m|\rho|n\rangle$ can be written as the sum of measurements on the computational basis. As these give identical results, so must the matrix. □

Theorem 1.4.7. *A positive $d \times d$ matrix such that $\mathrm{Tr}(\rho) = 1$ can be diagonalized as*

$$\rho = \sum_{i=0}^{d-1} \lambda_i |\psi_i\rangle\langle\psi_i|$$

where $|\psi_i\rangle$ form an ONB, $\lambda_i \geq 0$ and $\sum \lambda_i = 1$.

Remark 1.4.8. Note first that diagonalization is a consequence of the Spectral Theorem on $\mathbb{C}$, noting that $|\psi_i\rangle$ form an ON-eigenbasis. The eigenvalues being positive on a Hermitian matrix; $\lambda_i \geq 0$ is equivalent to the positivity of ρ. Finally, the λ_i summing to 1 is an immediate consequence of the trace of ρ being 1.

Consequently, we can take any such density matrix ρ and find an ensemble

$$E = \{(|\psi_i\rangle, \lambda_i) \mid i = 0, \ldots, d-1\}$$

such that ρ is the average state of this ensemble. That is, every mixture of pure states is described by a density matrix, and every density matrix describes some mixture of pure states.

Proposition 1.4.9. *If states $|\psi\rangle$ and $|\psi'\rangle$ differ only by a global state, they are represented by the same density matrix.*

Proof. Given $|\psi'\rangle = e^{i\gamma}|\psi\rangle$, we have

$$\rho' = |\psi'\rangle\langle\psi'| = (e^{i\gamma}|\psi\rangle)(e^{-i\gamma}|\psi\rangle) = |\psi\rangle\langle\psi| = \rho$$

□

Consequently, there is a bijective correspondence with the density matrix and the state of the system.

Proposition 1.4.10. *The rank of a density matrix ρ is equal to the number of mixed states represented by ρ.*

Lemma 1.4.11. *The following are equivalent*

- $\rho = |\psi\rangle\langle\psi|$ *for some unit vector* $|\psi\rangle$.
- $|\psi\rangle\rho\langle\psi|$ *for some unit vector* $|\psi\rangle$
- ρ *is a density matrix with* $\operatorname{rank}(\rho) = 1$
- ρ *is a density matrix and* $\rho^2 = \rho$.

Proof. Note that given an idempotent matrix, its eigenvalues are 1 or 0. By ρ to ensemble correspondence, we can see this has rank 1 (as the eigenvalues must sum to 1). □

Remark 1.4.12. A quantum system with d distinguishable states is associated to the HIlbert state $\mathbb{C}^d$, where states are represented with $d \times d$ matrices. The pure states are represented by density matrices of the form $\rho = |\psi\rangle\langle\psi|$ where $|\psi\rangle$ is a unit vector in $\mathbb{C}^d$.

We write $\mathrm{St}(\mathcal{H})$ for the set of quantum states (density matrices) on the Hilbert space $\mathcal{H}$. Note that by Corollary 1.4.6, density matrices have a well-defined map to (and from) the state of the system.

Lemma 1.4.13. *Every 2 by 2 density matrix can be decomposed as*

$$\rho = \frac{I + \mathbf{n} \cdot \boldsymbol{\sigma}}{2}$$

where $\mathbf{n} \in \mathbb{R}^3$ is a vector in the unit ball and σ is the usual Pauli matrices.

Proof. We show two methods, each with their own insights.

(i) Note first that every $|\psi\rangle$ can be written as $|\psi\rangle = \cos(\frac{\theta}{2})|0\rangle + e^{i\phi}\sin(\frac{\theta}{2})|1\rangle$. Then we have

$$\rho_\psi = |\psi\rangle\langle\psi| = \begin{pmatrix} \cos^2(\frac{\theta}{2}) & e^{i\phi}\cos(\frac{\theta}{2})\sin(\frac{\theta}{2}) \\ -e^{i\phi}\cos(\frac{\theta}{2})\sin(\frac{\theta}{2}) & \sin^2(\frac{\theta}{2}) \end{pmatrix}$$

We can rewrite this as

$$\rho_\psi = \frac{1}{2}(I + \sin(\theta)\cos(\phi)X + \sin(\theta)\sin(\phi)Y + \cos(\theta)Z)$$

Thus $\rho_\psi = (I + \mathbf{n}\cdot\boldsymbol{\sigma})/2$ with

$$\mathbf{n} = \begin{pmatrix} \sin(\theta)\cos(\phi) \\ \sin(\theta)\sin(\phi) \\ \cos(\theta) \end{pmatrix}$$

Now, a generic density matrix is written as

$$\rho = \sum p_i|\psi_i\rangle\langle\psi_i| = \sum p_i\frac{1}{2}(I + \mathbf{n}_i\boldsymbol{\sigma}) = \frac{1}{2}\left(I + \left(\sum p_i\mathbf{n}_i\right)\sigma\right)$$

By the triangle inequality, we have $||\sum p_i\mathbf{n}_i|| \leq 1$. The generic vector lands ρ into a unique point in D^3.

(ii) The matrices I, X, Y, Z form a basis for the Hermitian matrices. Thus, we can write

$$\rho = \alpha_0 I + \alpha_1 X + \alpha_2 Y + \alpha_3 Z$$

We apply trace,

$$\begin{aligned} \mathrm{Tr}(\rho) &= 1 = 2\alpha_0 \\ \mathrm{Tr}(X\rho) &= 2\alpha_1 \\ \mathrm{Tr}(Y\rho) &= 2\alpha_2 \\ \mathrm{Tr}(Z\rho) &= 2\alpha_3 \end{aligned}$$

Noting that $\mathrm{Tr}(\sigma_i\sigma_j) = \delta_{ij}$. This gives a straightforward representation,

$$\rho = \frac{1}{2}(I + \mathrm{Tr}(X\rho) + \mathrm{Tr}(Y\rho) + \mathrm{Tr}(Z\rho))$$

□

2 Qubit Bijection with the 2-sphere

2.1 Bloch Sphere

We can remove ambiguity about phase shifts by giving a bijection between pure states up to phase shifts and the Block Sphere.

Suppose first we are given a unit vector $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. We can write the coefficients in polar form, with

$$\alpha = |\alpha|e^{i\gamma} \qquad \beta = |\beta|e^{i\delta}$$

for some suitable γ, δ. Using the condition that $|\alpha|^2 + |\beta|^2 = 1$, we can write these as,

$$|\alpha| = \cos\frac{\theta}{2} \qquad |\beta| = \sin\frac{\theta}{2}$$

Note the condition that $\theta \in [0, \pi]$ for them to both be non-negative. Consequently,

$$|\psi\rangle = e^{i\gamma}\left[\cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\phi}|1\rangle\right]$$

where $\phi = \delta - \gamma$. We can remove the global phase, obtaining

$$|\psi'\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\phi}|1\rangle$$

We finally remove the case $\theta = 0$ and $\theta = \pi$ separately as for these θ we get the same state for any ϕ. This gives,

$$\{\cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\phi}|1\rangle \mid \theta \in (0, \pi), \phi \in [0, 2\pi)\} \cup \{|0\rangle, |1\rangle\}$$

This gives a natural map to the unit sphere via

$$\cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\phi}|1\rangle \mapsto \begin{pmatrix}\sin\theta\ \cos\phi\\ \sin\theta\ \sin\phi\\ \cos\theta\end{pmatrix}$$

It also maps $|0\rangle$ to $(0\ 0\ 1)^T$ and $|1\rangle$ to $(0\ 0\ -1)^T$

Intuitively the z coordinate on the sphere corresponds to the magnitude on $|0\rangle$ and $|1\rangle$, where ϕ corresponds to the phase coefficient on $|1\rangle$. Quotienting by global phase, there is a correspondence between circles to circles between the dimensions of $\mathbb{C}^2$. Parameterizing on this circle, we get a 2-sphere.

When we use the unit sphere to represent qubit states, we call this the **Bloch Sphere**. The vector it maps to is called the **Bloch vector**.

2.1.1 Bloch Sphere by Pauli Matrices

Proposition 2.1.1. *We can obtain the bloch vector of a unit vector in $\mathbb{C}^2$ via the map*

$$\psi \mapsto \begin{pmatrix}\langle\psi|X|\psi\rangle\\ \langle\psi|Y|\psi\rangle\\ \langle\psi|Z|\psi\rangle\end{pmatrix}$$

where X, Y, Z are the Pauli Matrices.

Proof. Follows via simple computation. □

Proposition 2.1.2. *Define measurements by ON-basis $\mathbf{B}_x = \{|+\rangle, |-\rangle\}$, $\mathbf{B}_y = \{|+i\rangle, |-i\rangle\}$, $\mathbf{B}_z = \{|0\rangle, |1\rangle\}$ where $|+i\rangle := (|0\rangle + i|1\rangle)/\sqrt{2}, |-i\rangle := (|0\rangle - i|1\rangle)/\sqrt{2}$. Then,*

1. *$X = |+\rangle\langle+| - |-\rangle\langle-|$, $Y = |+i\rangle\langle+i| - |-i\rangle\langle-i|$, $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$*
2. *$|\psi\rangle X\langle\psi| = |\langle+|\psi\rangle|^2 - |\langle-|\psi\rangle|^2$, $|\psi\rangle Y\langle\psi| = |\langle+i|\psi\rangle|^2 - |\langle-i|\psi\rangle|^2$, $|\psi\rangle Z\langle\psi| = |\langle 0|\psi\rangle|^2 - |\langle 1|\psi\rangle|^2$*

Proof. Follows by simple expansion. □

As a corollary, it follows from this that if two qubits give the same probabilities for the measurements on the bases $\mathbf{B}_x, \mathbf{B}_y, \mathbf{B}_z$, they have the same Bloch vector, implying they correspond to the same pure state.

2.1.2 Measuring probabilities

Proposition 2.1.3. *Given two vectors in $\mathbb{C}^2$, we have the relation*

$$|\langle\psi|\psi'\rangle|^2 = \frac{1+\mathbf{r}\cdot\mathbf{r}'}{2}$$

where $\mathbf{r}$ and $\mathbf{r}'$ correspond to Bloch vectors from $|\psi\rangle$ and $|\psi'\rangle$ respectively.

Proof. Follows from writing the unit vectors in the canonical trigonometric form, then taking the norm by carefully expanding. □

Consequently, two vectors are othogonal if and only if $\mathbf{r}\cdot\mathbf{r}' = -1$. Note that this is only possible if and only if the two Bloch vectors are at antipodes (follows from the CS-inequality). To go to antipodes, we map $\theta \mapsto \pi - \theta$ and $\phi \mapsto \psi + \pi$.

2.1.3 Reversible procesess = rotations

Proposition 2.1.4. *Every two-by-two unitary matrix can be parametrized as*

$$U = e^{i\gamma}\left(\cos\frac{\alpha}{2}I - i\sin\frac{\alpha}{2}\boldsymbol{n}\cdot\boldsymbol{\sigma}\right)$$

where $\gamma \in [0, 2\pi), \alpha \in [0, \pi)$. In fact every matrix of this form is unitary.

Proof. Using Proposition 1.2.13, we can write

$$U = e^{i\lambda_0}|\psi_0\rangle\langle\psi_0| + e^{i\lambda_1}|\psi_1\rangle\langle\psi_1|$$

for real numbers λ_0, λ_1 and orthonormal vectors $|\psi_0\rangle$ and $|\psi_1\rangle$. Writing $\gamma = (\lambda_0+\lambda_1)/2$, $\alpha = \lambda_1 - \lambda_0$,

$$\begin{aligned} U &= e^{i\gamma}(e^{-i\alpha/2}|\psi_0\rangle\langle\psi_1| + e^{i\alpha/2}|\psi_1\rangle\langle\psi_1|) \\ &= e^{i\gamma}\left[\cos\frac{\alpha}{2}\left(|\psi_0\rangle\langle\psi_0| + |\psi_1\rangle\langle\psi_1|\right) - i\sin\frac{\alpha}{2}\left(|\psi_0\rangle\langle\psi_0| - |\psi_1\rangle\langle\psi_1|\right)\right] \\ &= e^{i\gamma}\left(\cos\frac{\alpha}{2}I - i\sin\frac{\alpha}{2}A\right) \end{aligned}$$

Where $A = |\psi_0\rangle\langle\psi_0| - |\psi_1\rangle\langle\psi_1|$. It suffices to show this can be written as $\boldsymbol{n}\cdot\boldsymbol{\sigma}$ for some $\boldsymbol{n}$. Writing $|\psi_0\rangle$ canonically, noting that $|\psi_1\rangle$ is on the opposite point of the Bloch sphere, expansion shows this is satisfied with $\boldsymbol{n} = (\sin\theta\cos\phi \;\; \sin\theta\sin\phi \;\; \cos\theta)^T$. □

A quick check shows that every matrix of this form is indeed unitary. We use the fact that $\boldsymbol{n}\cdot\boldsymbol{\sigma}$ is unitary.

Consequently, by removing global phase, we can write general reversible processes by

$$U_{\alpha,\boldsymbol{n}} = \cos\frac{\alpha}{2}I - i\sin\frac{\alpha}{2}\boldsymbol{n}\cdot\boldsymbol{\sigma}$$

The matrix $U_{\alpha,\boldsymbol{n}}$ corresponds to the rotation by an angle α by the axis $\boldsymbol{n}$.

The proof for the above statement follows in three steps.

1. Show that the map $|\phi\rangle \mapsto U_{\alpha,\boldsymbol{n}}|\phi\rangle$ as represented on the Bloch sphere corresponds to a map $\mathbf{r} \mapsto O\mathbf{r}$ where O is an orthogonal (3 by 3) matrix.

2. Show that $\boldsymbol{n}$ is unchanged by multiplication by O

3. O acts as a rotation in the plane orthogonal to $\boldsymbol{n}$

As a remark, note that 2-by-2 unitary matrices has a correspondence with rotations on the Bloch sphere. Reversible processes on the Bloch sphere are more expressive (such as reflections about a plane or inversions) but in general, this does not correspond to reversible processes on qubits.

Also note that this bijection to Bloch spheres do not match intuitions about directions in the physical sense, we only refer to the idea that qubits quotiented by global phases map bijectively to the bloch sphere via Pauli Matrices.

Finally, in higher dimensions, d-dimensional pure states correspond to a subset of points of a $d^2 - 1$ ball. There are some points which do not correspond to pure states, and the bijection is a nice consequence we have with $d = 2$ (and trivially for $d = 1$).

3 System Properties

3.1 Quantum Steering

Consider systems prepared independently measured independently give independent measurements. Speficially,

$$\begin{aligned} p_{AB}(m,n) &= |(\langle\alpha_m| \otimes \langle\beta_n|)(|\alpha\rangle \otimes |\beta\rangle)|^2 \\ &= |\langle\alpha_m|\alpha\rangle\langle\beta_m|\beta\rangle|^2 \\ &= p_A(m)p_B(n) \end{aligned}$$

This condition fails when the state is entangled. For instance, measuring with $\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\}$ on $|\Phi^+\rangle$, we get $p_{AB}(0,1) = p_{AB}(1,0) = 0$ and $p_{AB}(1,1) = p_{AB}(0,0) = 1/2$, whereas the marginal distributions are

$$p_A(m) := \sum_n p_{AB}(m,n) = 1/2, \qquad p_B(n) := \sum_m p_{AB}(m,n) = 1/2$$

Importantly, if Alice measures before Bob, the conditional probability on Bob's measurement shows that Bob's state is exactly what Alice observed. For instance in the case Alice measures 0, we have

$$p_{B|A}(n|0) := \frac{p_{AB}(0,n)}{p_A(0)}$$

so $p_{B|A}(0|0) = 1$, thus in particular, the state of B is $|0\rangle$ up to global phase.

In a similar fashion, measuring on the fourier basis, we get

$$p_{AB}(+,+) = p_{AB}(-,-) = 1/2 \qquad p_{AB}(+,-) = p_{AB}(-,+) = 0$$

And by the same arguement, measurement by Alice will make Bob's system jump to $|+\rangle$ or $|-\rangle$ based on Alice's measurement.

Consequently, Alice's choice of measurement can 'steer' Bob's system. In particular, Alice can steer Bob's system to be one of the basis states

$$\begin{aligned} |0,\theta\rangle &:= \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle \\ |1,\theta\rangle &:= \sin\frac{\theta}{2}|0\rangle - \cos\frac{\theta}{2}|1\rangle \end{aligned}$$

for every possible $\theta \in [0,\pi)$

Theorem 3.1.1 (No Signaling Theorem)**.** *Given a compositive system $A \otimes B$, the probability distribution p_B is independent of the choice of ONB of A for any pure state Ψ.*

Proof. Let $\{|\alpha_m\rangle \mid 0, \ldots, d_A - 1\}$ and $\{|\beta_m\rangle \mid 0, \ldots, d_B - 1\}$ be the ONB for systems A and B. Suppose now we have a state $|\Psi\rangle$ in a composite system AB. Then,

$$\begin{aligned} p_{AB}(m,n) &= |\langle\alpha_m| \otimes \langle\beta_n||\Psi\rangle|^2 \\ &= [\langle\Psi||\alpha_m\rangle \otimes |\beta_n\rangle]\,[\langle\alpha_m| \otimes \langle\beta_n||\Psi\rangle] \\ &= \langle\Psi|\,[(|\alpha_m\rangle \otimes |\beta_n\rangle)(\langle\alpha_m| \otimes \langle\beta_n|)]\,|\Psi\rangle \\ &= \langle\Psi|(|\alpha_m\rangle\langle\alpha_m| \otimes |\beta_n\rangle\langle\beta_n|)|\Psi\rangle \end{aligned}$$

Thus,

$$\begin{aligned} p_B(n) &= \sum_{m=0}^{d_A-1} p_{AB}(m,n) \\ &= \sum_{m=0}^{d_A-1} \langle\Psi|(|\alpha_m\rangle\langle\alpha_m| \otimes |\beta_n\rangle\langle\beta_n|)|\Psi\rangle \\ &= \langle\Psi|\left[(\sum_{m=0}^{d_A-1} |\alpha_m\rangle\langle\alpha_m|) \otimes |\beta_n\rangle\langle\beta_n|\right]|\Psi\rangle \\ &= \langle\Psi|(I_A \otimes |\beta_n\rangle\langle\beta_n|)|\Psi\rangle \end{aligned}$$

□

Remark 3.1.2. Extending this to mixed states, decomposition of ρ into its pure states shows this is the case for mixed states as well. Thus, we can calculate probabilities on one system by taking the computational basis. That is,

$$\begin{aligned} p_A(m) &= \sum_{n=0}^{d_B-1} (\langle\alpha_m| \otimes \langle n|)\rho_{AB}(|\alpha_m\rangle \otimes |n\rangle) \\ &= \sum_{n=0}^{d_B-1} \langle\alpha_m|(I_A \otimes \langle n|)\rho_{AB}(I_A \otimes |n\rangle)|\alpha_m\rangle \\ &= \langle\alpha_m|\left\{\sum_{n=0}^{d_B-1} (I_A \otimes \langle n|)\rho_{AB}(I_A \otimes |n\rangle)\right\}|\alpha_m\rangle \\ &= \langle\alpha_m|\mathrm{Tr}_B[\rho_A B]|\alpha_m\rangle \end{aligned}$$

where $\mathrm{Tr}_B[\rho_A B] := \sum_{n=0}^{d_B-1}(I_A \otimes \langle n|)\rho_{AB}(I_A \otimes |n\rangle)$. Thus, we have $p_A(m) = \langle\alpha_m|\rho_A|\alpha_m\rangle$ where $\rho_A = \mathrm{Tr}_B(\rho_{AB})$. We call $\mathrm{Tr}_B(\rho_{AB})$ the **partial trace** of the matrix ρ_{AB} over the system B. Note that the probability measure ensures that ρ is positive semi-definite and that the trace is 1. We call ρ_A, ρ_B to be **marginal states**.

Remark 3.1.3. Note that in general, $\rho_{AB} \neq \rho_A \otimes \rho_B$. When this is the case, systems A and B are uncorrelated.

Theorem 3.1.4 (Dense Coding Protocol)**.** *Two qubits in the Bell state plus the communication of 1 qubit yielxs two bits of classical information. That is,*

$$1 \text{ ebit} + 1 \text{ qubit} \succeq 2 \text{ bits}$$

(where 1 ebit denotes the basic unit of entanglement represented by two qubits in a Bell state, and the 1 qubit is shorthand for denoting the communication, and the $\succeq$ means the resource on the right can be obtained by those on the left).

Proof. Suppose Alice has access to a qubit A and Bob has access to a qubit B. The composite system AB is initially set to Φ^+. Alice encodes two bits by acting on A based on the encoding via

$$U_{00} = I, \quad U_{01} = X, \quad U_{10} = Z, \quad U_{11} = ZX$$

Alice then sends qubit A to Bob. Bob measures AB in the Bell basis. The outcome of Bob's measurement can be used to extract Alice's message. This works without error as the transformation $U_{ij} \otimes I_B$ sends Φ^+ to exactly the Bell basis. □

3.2 Quantum Circuit Model

We consider a a quantum computer, where bits are replaced by qubits and boolean functions are replaced by a finite set of unitary gates. The stadard choice of measurement at the output state is the computational basis. The initial state of every qubit is fixed to the state $|0\rangle$. The standard model of quantum computation then allows gates H, T, CNOT, where H is the Hadamard gate, $T = \cos\frac{\pi}{8} I - i \sin\frac{\pi}{8} Z$.

Definition 3.2.1. *Let $|\psi\rangle \in \mathbb{C}^d$ and $|\psi'\rangle \in \mathbb{C}^d$ be two unit vectors. We say that the corresponding pure states are ϵ-**close** if there exists a global phase $e^{i\gamma}$ such that*

$$|| \ |\psi'\rangle - e^{i\gamma}|\psi\rangle \ || < \epsilon$$

Note that this relation is symmetric, as the length of the vector $|\psi'\rangle - e^{i\gamma}|\psi\rangle$ equals the length of the vector $|\psi\rangle - e^{-i\gamma}|\psi'\rangle$.

The idea is that pure states corresponding to vectors $|\psi\rangle$ and $|\psi'\rangle$ give approximately the same probabilities for every possible measurement.

Proposition 3.2.2. *Let $\{|\alpha_n\rangle\}$ be an arbitrary ONB. If pure states $|\psi\rangle$ and $|\psi'\rangle$ are ϵ-close, we have $p(n) := |\langle\alpha_n|\psi\rangle|^2$ and $p'(n) := |\langle\alpha_n|\psi'\rangle|^2$ satisfy the condition*

$$|p'(n) - p(n)| < 2\epsilon + \epsilon^2$$

for every $n \in \{0, \ldots, d-1\}$.

Definition 3.2.3. *Two unitary $d \times d$ matrices U and U' are ϵ-close if for any $\psi \in \mathbb{C}^d$, we have that $U'|\psi\rangle$ and $U|\psi\rangle$ are ϵ-close. We then say that U ϵ-approximates U' or that U' ϵ-approximates U.*

Definition 3.2.4. *Let F be a finite set of unitary matrices, each matrix acting on a finite number of qubits. We say that F is a **universal for quantum computation** if for every integer $n \in \mathbb{N}$ and for every positive constant $\epsilon > 0$, every n-qubit unitary gate U can be ϵ-approximated by an n-qubit unitary gate U_ϵ corresponding to a quantum circuit built entirely from gates in F.*

Suppose that we want to prepare n qubits in the state $|\Psi\rangle$. In general, there exists a unitary gate U that generates Ψ from the initial state

$$|\Psi_0\rangle = \underbrace{|0\rangle \otimes \cdots \otimes |0\rangle}_{n \text{ times}}$$

Such that $|\Psi\rangle = U|\Psi_0\rangle$. We can ϵ-approximate U with a unitary gate U_ϵ built from elementary gates. Using U_ϵ, we write $|\Psi_\epsilon\rangle := U_\epsilon(\Psi_0)$, and note that $|\Psi_\epsilon\rangle$ and $|\Psi\rangle$ are epsilon apart.

Suppose now that we want to measure on a basis $\{|\Psi_x\rangle\}$, where $x = (x_1, \ldots, x_n)$, is a string of n bits that labels the 2^n possible outcomes of measurement. The only measurement that can be performed directly is the measurement in the computational basis, consisting of vectors

$$|x\rangle = |x_1\rangle \otimes \cdots \otimes |x_n\rangle$$

To implement measurement on the basis $\{\Psi_x\}$, we transform the basis into the computational basis via

$$U := \sum_x |x\rangle\langle\Psi_x|$$

Thus, $\langle x|U = \langle\Psi_x|$ for and $x \in \{0, \ldots, 2^n - 1\}$. Then we can ϵ-approximate U with another unitary gate U_ϵ corresponding to a sequence of elementary gates. We can apply the unitary gate U_ϵ to the n qubits and measure in the computational basis such that

$$p_\epsilon(x) := |\langle x|U_\epsilon|\Psi\rangle|^2$$

where the desired measurement is

$$p(e) := |\langle\Psi_x|\Psi\rangle|^2 = |\langle x|U|\Psi\rangle|^2$$

Now noting that $U|\Psi\rangle$ and $U_\epsilon|\Psi\rangle$ are epsilon close,we can see as a consequence of the previous proposition that

$$|p_\epsilon(x) - p(x)| < 2\epsilon + \epsilon^2$$

3.2.1 Creating Universal Gate Sets

Theorem 3.2.5. *The set $F = \{H, T, \text{CNOT}\}$ is a universal gate set.*

Theorem 3.2.6. *Let U_2 be a two-qubit entangling gate (that transforms some product state into an entangled state). Then every n-qubit gate can be decomposed exactly into a circuit consisting only of single qubit gates and the gate U_2.*

From the above theorem, we can exactly implement an arbitrary n-qubit gates if we can generate entanglemenet from product states and perform all single qubit gates. Implementing approximate n-qubit gates then is reduced to a problem of choosing an entangling gate and a way to approximately implement all single qubit gates. Thus it suffices to find a way to approximate arbitrary single-qubit gates with sequences of gates in a finite set. Noting that single-qubit gates are rotations about the Bloch sphere, the problem reduces to approximate every rotation using a finite number of rotations. Rotations can be decomposed into a rotation about the z-axis and x-axis. To approximate rotation about these axis is straightforward, by choosing a rotation about each axis by some irrational angle, say $\alpha = \sqrt{2}\pi$. This generates a dense set of angles in the interval $[0, 2\pi)$. Explicitly, gates of the form

$$U_{\phi,z} = \cos\frac{\phi}{2} - i\sin\frac{\phi}{2}Z$$

can be approximated by a gate of the form $U_\epsilon = U_{\alpha,z}^{n_\epsilon}$, where $\alpha = \sqrt{2}\pi$ and n_ϵ is a suitable integer.

Generally, we have

Proposition 3.2.7. *Let $t \in \mathbb{R}$ be an irrational number and let $n \in \mathbb{R}^3$ be a direction in space. Then for every $\epsilon > 0$, every rotation around the axis $\mathbf{n}$ can be ϵ-approximated by the rotation of $\alpha = t\pi$ around $\mathbf{n}$ for a finite number of times.*

Remark 3.2.8. The above gives a recipe for constructing universal gate sets:

- Choose a two-qubit entangling gate
- Choose a finite set of single-qubit gates that generate rotations of irrational angles (not a rational multiple of π) around two distinct axes.

Then for example, the set $\{\text{CNOT}, U_{\sqrt{2}\pi,x}, U_{\sqrt{2}\pi,z}\}$ is universal.

Note that the set $\{\text{CNOT}, H, T\}$ is not of this shape, but is enough as matrices HT and TH are rotations of irrational angles around two distinct axes.

3.2.2 Classical in Quantum

We can implement a classical computer on a quantum computer by noting that it is enough to implement a NAND gate, thus enough to implement the NOT and AND gate. The NOT gate is immediate, as we can simply apply Pauli gate X.

To implement AND, consider the Toffoli gate,

$$\texttt{TOFFOLI}|x\rangle \otimes |y\rangle \otimes |z\rangle = |x\rangle \otimes |y\rangle \otimes |z \oplus \texttt{AND}(x, y)\rangle$$

where $\oplus$ is the sum modulo 2 and $\texttt{AND}(x, y)$ is the result of the `AND` gate when inputs bits are x and y. Taking the third qubit state to be in state $|0\rangle$, then measuring on the computational basis gives $\texttt{AND}(x, y)$.

3.2.3 Complexity

Definition 3.2.9. *The **complexity** of an n-qubit unitary gate U is the minimum number of elementary gates needed to ϵ-approximate U. We write the complexity as $C(U, \epsilon)$.*

Theorem 3.2.10 (Solovey-Kitaev Theorem)**.** *For a fixed number of qubits, the complexity grows as $(\log \frac{1}{\epsilon})^c$ for some $c \in [0, 2]$.*

Note this does not say anything about scaling with n, and we know there are n-qubit matrices that require an exponential number of elementary gates.

Theorem 3.2.11. *Define the Fourier gate to be*

$$F := \sum_{x=0}^{2^n-1} |e_x\rangle\langle x|$$

The complexity of the n-qubit Fourier gate is $O(n^2)$.

Example 3.2.12. For the following examples we fix $\epsilon = 0$.

- The Pauli gate Z can be expressed as $T^4 = -iZ$, which is equal to Z up to global phase. Of course, this is due to the fact Z is a rotation about the z-axis by π and T is a rotation by $\pi/4$.
- From $T^8 = -I$, we have $T^\dagger = -T^7$, so the inverse of T has complexity at most 7.

Proposition 3.2.13. *The `TOFFOLI` gate can be implemented without error with 21 elementary gates from $\{$`CNOT`$, H, T\}$. In particular, every classical computation that uses the `AND` gate k times and the `NOT` gate l times can be implemented with a quantum computer that uses $21k + l$ gates.*

The above shows that any quantum computer can implement a classical computation by at most $c \leq 21$ times in complexity compared to the classical complexity.

Definition 3.2.14. *The **complexity** of a quantum state with the standard model of computation is equal to the minimum number of elementary operations needed to prepare that state (or to implement that measurement).*

Example 3.2.15. We outline some basic examples:

- The bell state can be written as

$$|\Phi^+\rangle = \texttt{CNOT}_{12}(H_1 \otimes I_2)|0\rangle \otimes |0\rangle$$

  We have 2 initializations, a Hadamard gate and a CNOT gate for a total of 4 elementary operations.

- The GHZ state can be decomposed as

$$|\texttt{GHZ}\rangle = (I_1 \otimes \texttt{CNOT}_{23})(\texttt{CNOT}_{12} \otimes I_3)(H_1 \otimes I_2 \otimes I_3)|0\rangle \otimes |0\rangle \otimes |0\rangle$$

  Thus the complexity of generating the GHZ state is at most 6.

- The n-qubit Fourier state $|e_0\rangle$ is a uniform superposition of all vectors in the computational basis

$$|e_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$$

  where $|x\rangle = |x_1\rangle \otimes \cdots \otimes |x_n\rangle$ where $x_1, \ldots, x_n$ are the binary expansion of x. Now,

$$\begin{aligned} |e_0\rangle &= \frac{1}{\sqrt{2^n}} \sum_{x_1=0,1} \cdots \sum_{x_n=0,1} |x_1\rangle \otimes \cdots \otimes |x_n\rangle \\ &= \frac{1}{\sqrt{2^n}} \left(\sum_{x_1=0,1} |x_1\rangle \right) \otimes \cdots \otimes \left(\sum_{x_n=0,1} |x_1\rangle \right) \\ &= \underbrace{|+\rangle \otimes \cdots \otimes |+\rangle}_{n \text{ times}} \end{aligned}$$

  We thus have

$$|e_0\rangle = (H_1 \otimes \cdots \otimes H_n)(|0\rangle \otimes \cdots \otimes |0\rangle)$$

  Thus the Fourier state $|e_0\rangle$ has complexity at most $2n$.

- To measure n qubits in the Fourier basis, we can use the Fourier gate

$$\langle e_x| = \langle x|F^\dagger$$

  A measurement in the Fourier basis can thus be implemented by first performing the $F^\dagger$ gate and then measuring each qubit in the computational basis. F can be realised by $O(n^2)$ gates from $\{\texttt{CNOT}, H, T\}$, so $F^\dagger$ can be made by the dagger of these sets. Now,

$$\begin{aligned} \texttt{CNOT}^\dagger &= \texttt{CNOT} \\ H^\dagger &= H \\ T^\dagger &= -T^7 \end{aligned}$$

  Thus $F^\dagger$ has complexity at most 7 times that of F. $F^\dagger$ thus has complexity $O(n^2)$. Implementing the n-qubit measurements have n complexity, thus the complexity for this measurement is $O(n^2)$.

4 Games

4.1 Query Complexity

Consider a game with Alice and a referee. The referee picks a function $f : \{0, \ldots, M-1\} \to \{0, \ldots, N-1\}$, which is promised to have exactly one property from some finite set of alternatives. To discover the property, Alice asks a question q to the referee, who will return an answer $a = \mathcal{B}_f(q)$, using a black box function $\mathcal{B}_f$. The goal is to discover the property with the minimum number of questions.

Definition 4.1.1. *The black box $\mathcal{B}_f$ is an **oracle** for f. One use of an oracle is called a **query**, and the minimum number of queries needed to solve a given problem is called the **query complexity**.*

The query complexity depends on the oracle. An oracle that gives useless information will have infinite query complexity, where an oracle that tells the answer has a query complexity of 1. Classically, a reasonable oracle is therefore the function itself.

In the quantum case, we use a unitary gate thta can map inputs of a computational basis state $|x\rangle \in \mathcal{H}_A$ to $|f(x)\rangle \in \mathcal{H}_B$.

Definition 4.1.2. *Let $f : \{0, \ldots, M-1\} \to \{0, \ldots, N-1\}$ be any function. The **quantum oracle** for the function f is the unitary gate U_f acting on $\mathcal{C}^m \otimes \mathcal{C}^n$ defined by*

$$U_f(|x\rangle \otimes |y\rangle) := |x\rangle \otimes |y \oplus f(x)\rangle$$

where $\oplus$ is a binary operator that gives the sum modulo N.

Importantly, U_f is unitary (as it is a reversible process) and we have $U_f^\dagger(|x\rangle \otimes |y\rangle) = |x\rangle \otimes |y \ominus f(x)\rangle$ (where $\ominus$ is subtraction modulo N).

Example 4.1.3. The identify function on $\{0, 1\}$'s quantum oracle is the CNOT gate.

Remark 4.1.4. The quantum oracle U_f is at least as powerful as the classical oracle f. This follows from the fact that

$$U_f(|x\rangle \otimes |0\rangle) = |x\rangle \otimes |f(x)\rangle$$

and thus $f(x)$ can be determined by measuring system B in the computational basis. This is infact strict, as preparing system A in the Fourier basis state

$$|e_0\rangle = \frac{\sum_{x=0}^{M-1} |x\rangle}{\sqrt{M}}$$

and taking system B to $|0\rangle$, we have

$$U_f(|e_0\rangle \otimes |0\rangle) = \frac{\sum_{x=0}^{M-1} U_f|x\rangle}{\sqrt{M}} = \frac{\sum_{x=0}^{M-1} |x\rangle \otimes |f(x)\rangle}{\sqrt{M}}$$

Importantly, this state contains some global information about the values on the function f.

Definition 4.1.5. *The **reduced oracle** on $f : \{0, \ldots, M-1\} \to \{0, \ldots, N-1\}$ is a gate that depends only on the input register A, defined as*

$$V_f := \sum_{x=0}^{M-1} \omega^{f(x)} |x\rangle\langle x|$$

with $\omega := e^{\frac{-2\pi i}{N}}$.

Theorem 4.1.6. *Given a system B in the fourier state $|e_1\rangle$, the system A is transformed by the gate V_f. That is,*

$$U_f(|\alpha\rangle \otimes |e_1\rangle) = (V_f|\alpha\rangle) \otimes |e_1\rangle$$

Example 4.1.7. Suppose that f is a boolean function. Then we have $N = 2$ and $e^{-2\pi i/N} = -1$. Thus, we have

$$V_f = \sum_{x=0}^{M-1} (-1)^{f(x)} |x\rangle\langle x|$$

Thus, we have

$$V_f|x\rangle = \begin{cases} |x\rangle & \text{if } f(x) = 0 \\ -|x\rangle & \text{if } f(x) = 1 \end{cases}$$

4.1.1 Deutsch-Jozsa Game

The referee picks a Boolean function $f : \{0, \ldots, M-1\} \to \{0, 1\}$ with M even. f is either constant or balanced (number of x such that $f(x) = 0$ is equal to the number of x such that $f(x) = 1$). We want to find the query complexity. Note that in the classical case, the worst case complexity is $M/2 + 1$.

Consider the following algorithm

- Prepare the Fourier state $|e_0\rangle = \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle$
- Apply the reduced oracle V_f. Measure the output on the Fourier basis.
- If the measurement outcome is $k = 0$, declare f is constant. Otherwise, declare f is balanced.

To see why the algorithm works, note that when we apply the orcale to $|e_0\rangle$. Then we have

$$\begin{aligned} V_f|e_0\rangle &= \frac{\sum_x V_f|x\rangle}{\sqrt{M}} \\ &= \frac{\sum_x (-1)^{f(x)|x\rangle}}{\sqrt{M}} \\ &= \frac{(\sum_{x:f(x)=0} |x\rangle) - (\sum_{x:f(x)=1} |x\rangle)}{\sqrt{M}} \end{aligned}$$

If the function is balanced, the probability of outcome $k = 0$ is

$$\begin{aligned} p(0) &= |\langle e_0|V_f|e_0\rangle|^2 \\ &= \left| \frac{(\sum_{x:f(x)=0} \langle e_0|x\rangle) - (\sum_{x:f(x)=1} \langle e_0|x\rangle)}{\sqrt{M}} \right|^2 \\ &= \left| \frac{(\sum_{x:f(x)=0} 1) - (\sum_{x:f(x)=1} 1)}{M} \right| = 0 \end{aligned}$$

where the last equality follows from the fact that f is balanced, and $\langle e_0|x\rangle = \frac{1}{\sqrt{M}}$. If the function is constant, we have

$$V_f|e_0\rangle = |e_0\rangle$$

if $f(x) = 0$, and $-|e_0\rangle$ if $f(x) = -1$. In either case,

$$\begin{aligned} p(0) &= ||e_0\rangle V_f \langle e_0||^2 \\ &= |\langle e_0|e_0\rangle|^2 = 1 \end{aligned}$$

Thus the query complexity is 1. The idea is that V_f gives information about the global state, at the cost of losing knowledge about the local state.

4.1.2 Grover's Algorithm

Given $S << N$ such that $f(x) = 1$ for S unique values and 0 otherwise, we want a search algorithm that finds an x such that $f(x) = 1$. The classical solution has complexity $\Theta(n)$. We give a quantum search algorithm with query complexity $\Theta(\sqrt{n})$.

The steps are as follows:

- Prepare the system in the Fourier basis state $|e_0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$.
- Apply the reduced oracle V_f
- Apply the gate $W := 2|e_0\rangle\langle e_0| - I$
- Repeat the application for K times, where K is the closest integer to $\frac{\pi}{4}\sqrt{\frac{N}{S}} - \frac{1}{2}$

We first separate $|e_0\rangle$ into components that give solutions and those that don't. Explicitly,

$$|e_0\rangle = \frac{\sum |x\rangle}{\sqrt{N}} = \sqrt{\frac{N-S}{N}}|\phi_0\rangle + \sqrt{\frac{S}{N}}|\phi_1\rangle$$

where $|\phi_0\rangle = \frac{1}{\sqrt{N-S}} \left(\sum_{x:f(x)=0} |x\rangle \right)$ and $|\phi_1\rangle := \frac{1}{\sqrt{S}} \left(\sum_{x:f(x)=1} \right)$. We set $\cos(\theta) := \sqrt{1 - \frac{S}{N}}$ and $\sin(\theta) := \sqrt{\frac{S}{N}}$, we can write

$$|e_0\rangle = \cos(\theta)|\phi_0\rangle + \sin(\theta)|\phi_1\rangle$$

Thus, we can view $|\phi_0\rangle$ and $|\phi_1\rangle$ as unit vectors in the direction of x and y axis. Then, with view to this, we can write

$$|e_0\rangle \equiv \begin{pmatrix} \cos(\theta) \\ \sin(\theta) \end{pmatrix}$$

Applying the gate V_f, on the computational basis, we have

$$V_f|x\rangle := \begin{cases} -|x\rangle & \text{if } f(x) = 1 \\ |x\rangle & \text{if } f(x) = 0 \end{cases}$$

In particular, we have $V_f \begin{pmatrix} \cos(\theta) \\ \sin(\theta) \end{pmatrix} = \begin{pmatrix} \cos(\theta) \\ -\sin(\theta) \end{pmatrix}$, a reflection about the x axis.

Applying W to the orthonormal set $|e_0\rangle, |e_0^\perp\rangle$, we have

$$W|e_0\rangle = 2|e_0\rangle\langle e_0|e_0\rangle - |e_0\rangle = |e_0\rangle$$

and

$$W|e_0^\perp\rangle = 2|e_0\rangle\langle e_0|e_0^\perp\rangle - |e_0^\perp\rangle = -|e_0^\perp\rangle$$

Thus this gives a reflection about $|e_0\rangle$. In particular, an application of WV_f corresponds to a rotation of $|e_0\rangle$ by 2θ.

Generally, writing $G_f := WV_f$, we have

$$G_f^K|e_0\rangle = \cos[(2K+1)\theta]|\phi_0\rangle + \sin[(2K+1)\theta]|\phi_1\rangle$$

as we start from θ and rotate by 2θ. Measuring the probability in the computational basis, if x is a solution, we have

$$\begin{aligned} p(x) &= |\langle x|G_f^K|e_0\rangle|^2 \\ &= |\cos[(2K+1)\theta]\langle x|\phi_0\rangle + \sin[(2K+1)\theta]\langle x|\phi_1\rangle|^2 \\ &= \frac{(\sin[(2K+1)\theta]^2)}{S} \end{aligned}$$

The probability, the measurement outcome of a solution is

$$p_{\text{sol}} = \sum_{x:f(x)=1} p(x) = \sin^2[(2K+1)\theta]$$

The probability is close to 1 when $(2K+1)\theta$ is close to $\pi/2$, or equivalently when K is close to $\frac{\pi}{4\theta} - \frac{1}{2}$, so we can do well by taking the closest integer to it. The difference between $\pi/2$ and $(2K+1)\theta$ is at most θ, so we can write

$$(2K+1)\theta = \frac{\pi}{2} + \delta$$

for $|\delta| \leq \theta$. We can lower bound the probability for a solution as

$$\begin{aligned} p_{\text{sol}} &= \sin^2[(2K+1)\theta] \\ &= \sin^2\left[\left(\frac{\pi}{2} + \delta\right)\right] \\ &= \cos^2\delta \geq \cos^2\theta = 1 - \frac{S}{N} \end{aligned}$$

With the last inequality a consequence of $|\delta| \leq \theta$ and θ is small.

As S is small compared to N, we can approximate

$$\theta \approx \sin\theta = \sqrt{\frac{S}{N}}$$

Thus the number of repetitions is given approximately by

$$K \approx \frac{\pi}{4}\sqrt{\frac{N}{S}} - \frac{1}{2}$$

Thus, the query complexity is $\Theta(\sqrt{N})$.

Notably, the probability of finding the solution is not 1. However, fixing an ϵ, we can always be correct with probability at least $1-\epsilon$, noting that $(\frac{S}{N})^t \leq \epsilon$ taking large enough t.

4.2 CHSH Game

The CHSH game goes as follows.

- Alice and Bob can decide a strategy before the game
- The game master chooses $a = 0, 1$ and $b = 0, 1$ randomly each with probability $p(a, b) = 1/4$.
- Alice and bob each answer 1 bit, x and y respectively.
- Alice and Bob score 1 point if $x \oplus y = a \cdot b$ and lose one point otherwise.

The payoff can be written as

$$\omega(x, y|a, b) = (-1)^{x+y+a\cdot b}$$

with the expected payoff as

$$\omega = \frac{1}{4}\sum_{a,b}\sum_{x,y}(-1)^{x+y+ab}p(x, y|a, b)$$

where the probability distribution describes the **strategy** adopted by Alice and Bob. The idea is that the probability distribution accessible in the classical world is a strict subset of that which is accessible in the quantum world.

Given deterministic strategies, we have strategies $x = f(a)$ and $y = g(b)$. Then,

$$p(x, y|a, b) = \begin{cases} 1 & \text{if } x = f(a) \text{ and } y = g(b) \\ 0 & \text{otherwise} \end{cases}$$

Thus, the expected payoff is

$$\omega = \frac{1}{4}\sum_{a,b}\sum_{x,y}(-1)^{x+y+ab}p(x, y|a, b) = \frac{1}{4}\sum_{a,b}(-1)^{f(a)+g(b)+ab}$$

By a quick case analysis, $\omega_{\max} = 1/2$. This is achieved for example when $x = 0$ and $y = 0$ always.

Given probabilistic strategies, we first set a probability distribution λ, and generate such that Alice gives x at random with probability $p_A(x|a, \lambda)$ and Bob gives y at random with $p_B(y|b, \lambda)$. Then,

$$p_{AB}(x, y|a, b) = \sum_{\lambda} p_A(x|a, \lambda)p_B(y|b, \lambda)p(\lambda)$$

Thus,

$$\omega = \sum_{\lambda} p(\lambda)\left[\frac{1}{4}\sum_{a,b}\sum_{x,y}(-1)^{x+y+ab}p_A(x|a, \lambda)p_B(y|b, \lambda)\right]$$

We can show that $\omega \leq \frac{1}{2}$ (idea sketch, considering how we can maximize the inner equation at each variable, the strategy becomes fixing values, which reduces to the previous case).

Consider the following strategy:

- Prepare a bell state $|\Phi^+\rangle$, and split them between Alice and Bob
- If the question is a, Alice measures on basis $\{|0, \theta_a\rangle, |1, \theta_a\rangle\}$ with $\theta_0 = 0$ and $\theta_1 = \frac{\pi}{2}$. The outcome measure is her answer.

- If the question is b, Bob measures on basis $\{|0,\tau_b\rangle, |1,\tau_b\rangle\}$ with $\tau_0 = \frac{\pi}{4}$ and $\tau_1 = -\frac{\pi}{4}$. The outcome measure is he answer.

We therefore have

$$p_{AB}(x,y|a,b) = |\langle x,\theta_a| \otimes \langle y,\tau_b||\Phi^+\rangle|^2$$

Thus,

$$\begin{aligned}
\omega &= \frac{1}{4}\sum_{a,b}\sum_{x,y}(-1)^{x+y+ab}|\langle x,\theta_a| \otimes \langle y,\tau_b||\Phi^+\rangle|^2 \\
&= \frac{1}{4}\sum_{a,b}\sum_{x,y}(-1)^{x+y+ab}\langle\Phi^+|(|x,\theta_a\rangle\langle x,\theta_a| \otimes |y,\tau_b\rangle\langle y,\tau_b|)|\Phi^+\rangle \\
&= \frac{1}{4}(-1)^{ab}\sum_{a,b}\langle\Phi^+|\left(\sum_x(-1)^x|x,\theta_a\rangle\langle x,\theta_a|\right)\left(\sum_y(-1)^y|y,\tau_b\rangle\langle y,\tau_b|\right)|\Phi^+\rangle
\end{aligned}$$

Now we use the relation

$$\sum_x(-1)^x|x,\theta\rangle\langle x,\theta| = \mathbf{m}\cdot\boldsymbol{\sigma}$$

where $\mathbf{m} := \begin{pmatrix}\sin\theta\\0\\\cos\theta\end{pmatrix}$

Expanding,

$$\begin{aligned}
\omega &= \frac{1}{8}\sum_{a,b}(-1)^{ab}\left(\sum_k\langle k|\otimes\langle k|\right)(\mathbf{m}_a\cdot\boldsymbol{\sigma}\otimes\mathbf{n}_b\cdot\boldsymbol{\sigma})\left(\sum_l\langle l|\otimes\langle l|\right) \\
&= \frac{1}{8}\sum_{a,b}\sum_{k,l}(-1)^{ab}\langle k|(\mathbf{m}_a\cdot\boldsymbol{\sigma})|l\rangle\langle k|(\mathbf{n}_a\cdot\boldsymbol{\sigma})|l\rangle \\
&= \frac{1}{8}\sum_{a,b}\sum_{k,l}(-1)^{ab}\langle k|(\mathbf{m}_a\cdot\boldsymbol{\sigma})|l\rangle\langle l|(\mathbf{n}_a\cdot\boldsymbol{\sigma})^T|k\rangle \\
&= \frac{1}{8}\sum_{a,b}\mathrm{Tr}\left[(\mathbf{m}_a\cdot\boldsymbol{\sigma})(\mathbf{n}_a\cdot\boldsymbol{\sigma})^T\right] \\
&= \frac{1}{8}\sum_{a,b}\mathrm{Tr}\left[(\mathbf{m}_a\cdot\boldsymbol{\sigma})(\mathbf{n}_a\cdot\boldsymbol{\sigma})\right]
\end{aligned}$$

Now, note that

$$\mathrm{Tr}[(\mathbf{m}\cdot\boldsymbol{\sigma})(\mathbf{n}\cdot\boldsymbol{\sigma})] = 2\mathbf{m}\cdot\mathbf{n}$$

Thus,

$$\begin{aligned}
\omega &= \frac{1}{4}\sum_{a,b}(-1)^{ab}\mathbf{m}\cdot\mathbf{n} \\
&= \frac{1}{4}\sum_{a,b}(-1)^{ab}(\sin\theta_a\sin\tau_b + \cos\theta_a\cos\tau_b) \\
&= \frac{1}{4}\sum_{a,b}(-1)^{ab}\cos(\theta_a-\tau_b) \\
&= \frac{1}{4}\left[\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}-\left(-\frac{1}{\sqrt{2}}\right)\right] = \frac{1}{\sqrt{2}}
\end{aligned}$$

4.3 GHZ Game

Alice, Bob, Charlie play the following game.

- Players can discuss strategies beforehand
- Referee asks a question, represented by a bit to each player. The constraint is that the referee asks 0 to everyone, or only to one player
- Players answer a bit a, b, c
- if the referee asked 0 to everyone, they win if $a \oplus b \oplus c = 0$
- if the referee asked 0 to one player, they win if $a \oplus b \oplus c = 1$.

In the classical case the three can not always win, but quantum methods give a strategy they can always win with. Consider the following

- Prepare three qubits in the GHZ gate, and separate each to themselves.
- If the question is zero, measure on the basis

$$|\phi_0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} |\phi_1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

  If the question is one, measure on

$$|\psi_0\rangle = \frac{|0\rangle + i|1\rangle}{\sqrt{2}} |\psi_1\rangle = \frac{|0\rangle - i|1\rangle}{\sqrt{2}}$$

- the outcome of the measurement is the answer of the player

if the question asked is $(0, 0, 0)$, we have

$$p_{ABC}(m, n, l|0, 0, 0) = |\langle \phi_m| \otimes \langle \phi_n| \otimes \langle l||\text{GHZ}\rangle|^2$$

Noting that $|\phi_m\rangle = \frac{|0\rangle + (-1)^m |1\rangle}{\sqrt{2}}$, we have

$$\begin{aligned} & p_{ABC}(m, n, l|0, 0, 0) \\ &= \left| \left(\frac{\langle 0| + (-1)^m \langle 1|}{\sqrt{2}} \otimes \frac{\langle 0| + (-1)^n \langle 1|}{\sqrt{2}} \otimes \frac{\langle 0| + (-1)^l \langle 1|}{\sqrt{2}} \right) \left(\frac{|0\rangle \otimes |0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle \otimes |1\rangle}{\sqrt{2}} \right) \right| \\ &= \left| \frac{1 + (-1)^{m+n+l}}{4} \right| \end{aligned}$$

In particular, the probability is 0 whenever $m \oplus n \oplus l = 1$. Thus the players never lose (their answer xors to 0).

In the other case, we write

$$|\psi_n\rangle = \frac{|0\rangle + i(-1)^n |1\rangle}{\sqrt{2}}$$

Then we can similarly calculate

$$p_{ABC}(m, n, l|0, 1, 1) = \left| \frac{1 - (-1)^{m+n+l}}{4} \right|$$

The probability is zero whenever $m \oplus n \oplus l = 0$, thus the probability of losing is 0. Noting that other cases are symmetric, the probability to win becomes 1.

4.4 Shor's Algorithm

We are given an f that is strongly periodic. That is, f is periodic and if two inputs satisfy $f(x) = f(y)$, the difference between x and y is a multiple of the period.

In our case, we know that the period is smaller than some fixed d. The general Shor's Algorithm determines the period in $\Theta(1)$. We consider a weaker case where d is known to be a multiple of the period. Thus, given that the period is t, we can write $d = Mt$ for some constant M.

The simplified Shor's Algorithm outputs a multiple of d/t, such that we get $n = j\frac{d}{t}$ for $j \in [0, t)$, chosen random with probability $1/t$. Using the algorithm twice, this gives two integers of the form

$$n_1 = j_1\frac{d}{t} \qquad n_2 = j_2\frac{d}{t}$$

Given j_1, j_2 coprime, we can find d/t by simply taking the gcd of n_1 and n_2. This is enough information to obtain t, as $t = d/\gcd(n_1, n_2)$. Moreover, the probability that two numbers are coprime has a fixed lower bound of $6/\frac{\pi}{2}$, thus we can find the period with high probability in constant time. To find these random multiples of d/t, consider the following

- Prepare system A in the Fourier state $|e_0\rangle$ and B in the computational state $|0\rangle$.
- Apply U_f
- Measure B in the computational basis.
- Measure A in the Fourier basis.

Let us analyze the above. At the start, we have a composite system AB which is in the state

$$|e_0\rangle \otimes |0\rangle = \frac{1}{\sqrt{d}}\sum_{x=0}^{d-1}|x\rangle \otimes |0\rangle$$

Applying U_f, we get

$$|\Psi\rangle := U_f\frac{1}{\sqrt{d}}\sum_{x=0}^{d-1}|x\rangle \otimes |0\rangle = \frac{1}{\sqrt{d}}\sum_{x=0}^{d-1}|x\rangle \otimes |f(x)\rangle$$

Noting that f is periodic with t, the sum over x can be split based on this period as

$$\begin{aligned}
|\Phi\rangle &= \frac{1}{\sqrt{d}}\sum_{m=0}^{M-1}\sum_{x=0}^{t-1}|x+mt\rangle \otimes |f(x+mt)\rangle \\
&= \frac{1}{\sqrt{d}}\sum_{m=0}^{M-1}\sum_{x=0}^{t-1}|x+mt\rangle \otimes |f(x)\rangle \\
&= \frac{1}{\sqrt{t}}\sum_{x=0}^{t-1}\left(\frac{1}{\sqrt{M}}\sum_{m=0}^{M-1}|x+mt\rangle\right) \otimes |f(x)\rangle
\end{aligned}$$

By strong periodicity, every $f(x)$ in the sum now is distinct. We write $|\phi_x\rangle = \frac{1}{\sqrt{M}}\sum_{m=0}^{M-1}|x+mt\rangle$. Measuring on the computational basis, we obtain the value $y = f(x)$ for some unknown x, steering the state of system to $|\phi_x\rangle$. Measuring A in the Fourier basis, we have

$$p_A(n|x) = |\langle e_n|\phi_x\rangle|^2$$

Now note that

$$\langle x|e_n\rangle = \langle x|\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1} e^{\frac{2\pi ink}{d}}|k\rangle \tag{2}$$

$$= \frac{1}{\sqrt{d}} e^{\frac{2\pi inx}{d}} \tag{3}$$

Now,

$$\begin{aligned}
\langle \phi_x|e_n\rangle &= \left(\frac{1}{\sqrt{M}}\sum_{m=0}^{M-1}\langle x+mt|\right)|e_n\rangle \\
&= \frac{1}{\sqrt{M}}\sum_{m=0}^{M-1}\langle x+mt|e_n\rangle \\
&= \frac{1}{\sqrt{Md}}\sum_{m=0}^{M-1} e^{\frac{2\pi i(x+mt)n}{d}} \\
&= \frac{1}{\sqrt{Md}} e^{\frac{2\pi ixn}{d}}\sum_{m=0}^{M-1} e^{\frac{2\pi imtn}{d}} \\
&= \frac{1}{\sqrt{Md}} e^{\frac{2\pi ixn}{d}}\sum_{m=0}^{M-1} e^{\frac{2\pi imn}{M}}
\end{aligned}$$

Now note that

$$\sum_{m=0}^{M-1} e^{\frac{2\pi imn}{M}} = \begin{cases} M & n \text{ is a multiple of } M \\ 0 & \text{otherwise} \end{cases}$$

Thus we have

$$p_A(n|x) = |\langle \phi_x|e_n\rangle|^2 = \begin{cases} \frac{1}{t} & n \text{ is a multiple of } M \\ 0 & \text{otherwise} \end{cases}$$

In particular, the outcome of the Fourier measurement must be a multiple of M.

5 Identities

- $H = |+\rangle\langle 0| + |-\rangle\langle 1|$
- Pauli matrices minus is on right column.
- Control-unitary gate (of the form $U = \sum |\alpha_x\rangle\langle\alpha_x| \otimes U_x$) (input retainment on the first, application on the second)
- For any U, $(\langle x| \otimes \langle y|)U^\dagger U(|x'\rangle \otimes |y'\rangle) = \delta_{xx'}\delta_{yy'}$ implies that U is a unitary gate.
- Locality: When two spatially separated systems are measured at the same time, the choice of measurement system does not affect the outcome of the measurement performed on the other system.
- The matcies I, X, Y, Z form a $\mathbb{C}$ on the 2 by 2 Hermitian matrices. Now, Taking trace on ρ and $\sigma_i\rho$, we can extract exact values (in particular, the coordinate corresponding to σ_i is attained by $\frac{1}{2}\mathrm{Tr}(\sigma_i\rho)$).