Notes on Quantum Information Processing

Edward Kim

September 16, 2020

1 Quantum Mechanics

1.1 Postulates of Quantum Mechanics

1.2 Density Matrices

Suppose we have an ensemble of states $\{|\psi_1\rangle, ..., |\psi_k\rangle\}$ in a statisitcal mixture in the sense that we know the distribution of the states. Let p_i denote the probability of selecting state $|\psi_i\rangle$ for $1 \leq i \leq k$ where $\sum_i p_i = 1$.

We wish to find a way to calculate the expected value of any observable A on this ensemble. Note that the linear superposition of these states in the form $\sum_{i=1}^k p_i |\psi_i\rangle$ is generally not the same as a statistical mixture of the individual states $|\psi_i\rangle$.

From Postulate three, we can calculate the probability that measuring with $A = \sum_i a_i P_i$ will yield outcome a_j:

$$p(j) = \sum_{i=1}^{k} p_i \langle\psi_i| P_j |\psi_i\rangle$$

Note that the $\langle\psi_i| P_j |\psi_i\rangle$ represent the probability of obtaining outcome a_j given the state vector is $|\psi_i\rangle$ as per postulate three. Thus, our expected value for the observable A would objects:

$$\langle A\rangle = \sum_{j=1}^{n} a_j p(j) = \sum_{j=1}^{n} a_i (\sum_{i=1}^{k} p_i \langle\psi_i| P_j |\psi_i\rangle) = \sum_{i=1}^{k} p_i \langle\psi_i| \sum_{i=1}^{n} a_j P_j |\psi_i\rangle = \sum_{i=1}^{k} p_i \langle\psi_i| A |\psi_i\rangle$$

Define the **density matrix** of the ensemble to be

$$\rho = \sum_{i=1}^{k} p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|$$

and $\langle A\rangle = Tr(\rho A)$. We verify this as follows:

$$Tr(\rho A) = \sum_{j=1}^{n} \langle j|\, \rho A \,|j\rangle = \sum_{j=1}^{n} \langle j|\, (\sum_{i=1}^{k} p_i \,|\psi_i\rangle \langle\psi_i|) A \,|j\rangle = \sum_{j=1}^{n}\sum_{i=1}^{k} p_i \langle j|\psi_i\rangle \langle\psi_i|\, A \,|j\rangle = \quad (1)$$

$$\sum_{i=1}^{k} p_i \langle\psi_i|\, A (\sum_{j=1}^{n} |j\rangle \langle j|) \,|\psi_i\rangle = \sum_{i=1}^{k} p_i \langle\psi_i|\, A \,|\psi_i\rangle = \langle A\rangle \quad (2)$$

where the next-to-last equality stems from the completeness criterion: $\sum_i |i\rangle \langle i| = I$. Thus, we have a method to describe expectation and probabilities in terms of operators rather than state vectors. Note that a pure state can be trivially described through the density matrix formalulation by $\rho = |\psi\rangle \langle\psi|$.

The density matrix has the following properties: Let $\{|i\rangle\}$ denote an orthogonal basis of our Hilbert space $\mathcal{H}$:

1. ρ **is Hermitian**: Let

   $$\rho_{ij} = \langle i|\, \rho \,|j\rangle = \sum_{m=1}^{k} p_m \langle i|\psi_m\rangle \langle\psi_m|j\rangle = \sum_{m=1}^{k} p_m c_i^{(m)} (c_j^{(m)})^*$$

   Thus,

   $$\rho_{ji}^* = \sum_{m=1}^{k} p_m (c_j^{(m)})^* c_i^{(m)} = \rho_{ij}$$

2. ρ **has unit trace** By our formula above:

   $$Tr(\rho) = \sum_{i=1}^{n} \rho_{ii} = \sum_{i=1}^{n}\sum_{m=1}^{k} p_m c_i^{(m)} (c_i^{(m)})^* = \sum_{m=1}^{k} p_m \sum_{i=1}^{n} |c_i^{(m)}|^2 = \sum_{m=1}^{k} p_m = 1$$

3. ρ **is non-negative**: Let $|\phi\rangle \in \mathcal{H}$. It suffices to prove that $\langle\phi| \rho |\phi\rangle \geq 0$.

Fromm property one above, we derive the following criteria for determining if a given density matrix ρ represents a mixed state or a pure state:

Theorem 1. *Given density matrix ρ, $Tr(\rho^2) = 1$ iff ρ represents a pure state. On the other hand, $Tr(\rho^2) < 1$ iff ρ represents a mixed state.*

Proof. □

1.2.1 How to prepare ρ

Suppose we have an ensemble of the form $\{p(i), |\psi_i\rangle\}$ where p refers to a distribution of probabilities over the indices $\{i\}$. We can classically prepare such a state by tossing a biased die obeying the distribution above, and preparing the corresponding state based on the outcome.

1.3 Composite Systems

We can use the density matrix formalism to express statistical measurements in subsystems in the following sense:

Let $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ be the *bipartite* separable system consisting of two subsystems expressed as Hilbert spaces $\mathcal{H}_1, \mathcal{H}_2$. By definition of the tensor product if $|\psi\rangle \in \mathcal{H}$, $|\psi\rangle$ has the form:

$$|\psi\rangle = \sum_{i,\alpha} c_i c_\alpha |i\rangle \otimes |\alpha\rangle = \sum_{i,\alpha} c_{i,\alpha} |i\rangle \otimes |\alpha\rangle$$

if we let $\{|i\rangle\}, \{|\alpha\rangle\}$ be sets of orthogonal basis vectors in $\mathcal{H}_1, \mathcal{H}_2$ respectively.

By our definiton in the previous section, the density matrix for our pure state $|\psi\rangle$ will be:

$$\rho = |\psi\rangle \langle\psi| = \sum_{i,\alpha} \sum_{j,\beta} c_{i,\alpha} (c_{j,\beta})^* |i\rangle |\alpha\rangle \langle j| \langle\beta| = \sum_{(i,j),(\alpha,\beta)} \lambda_{(i,j),(\alpha,\beta)} |i\rangle \langle j| \otimes |\alpha\rangle \langle\beta|$$

Suppose we have an observable A_1 for subsystem $\mathcal{H}_1$, and we wish to find $\langle A_1 \rangle$ given $\mathcal{H}$. Let $A_1 \otimes I_2 : \mathcal{H} \to \mathcal{H}$ be the unique linear map induced by $A_1 : \mathcal{H}_1 \to \mathcal{H}_1$ and $I_2 : \mathcal{H}_2 \to \mathcal{H}_2$.

$$\langle A_1 \otimes I_2 \rangle = Tr(\rho(A_1 \otimes I_2)) = \sum_{i,\alpha} \langle i| \langle \alpha| \rho(A_1 \otimes I_2) |i\rangle |\alpha\rangle = \tag{3}$$

$$\sum_{i,\alpha} \langle i| \langle \alpha| [\sum_{(k,l),(\beta,\gamma)} \lambda_{(k,l),(\beta,\gamma)} |k\rangle \langle l| \otimes |\beta\rangle \langle \gamma|])(A_1 \otimes I_2) |i\rangle |\alpha\rangle = \tag{4}$$

$$\sum_{i} \langle i| \sum_{\alpha} \langle \alpha| (\sum_{(k,l),(\beta,\gamma)} \lambda_{(k,l),(\beta,\gamma)} |k\rangle \langle l| \otimes |\beta\rangle \langle \gamma|) |\alpha\rangle A_i |i\rangle = \sum_{i} \langle i| = \tag{5}$$

$$Tr_2(\rho) A_i |i\rangle = Tr(A_i Tr_b(\rho)) \tag{6}$$

where

$$\rho_1 = Tr_2(\rho) = \sum_{\alpha} \langle \alpha| \rho |\alpha\rangle$$

is the *partial trace* of density operator ρ. Note that these equalties follow directly from the bilinear property of the tensor product on Hilbert spaces $\mathcal{H}_1, \mathcal{H}_2$.

Similarly, for $\mathcal{H}_1$:

$$\rho_2 = Tr_1(\rho) = \sum_{i} \langle i| \rho |i\rangle$$

It can be directly checked that ρ_m for $m = 1, 2$ is indeed a density operator in that it is a Hermitian semi-definite operator with unit trace. We refer to the ρ_m as *local density operators* as they refer to density operators in respect to the individual subsystems.

The local density operators above can be seen as the quantim analogue of the marginal distribution defined in classical probability theory i.e if $p_{X,Y}(x, y)$ is a joint probability distribution over random variables X, Y, then the marginal distribution for X is $p_X(x) = \sum_y p_{X,Y}(x, y)$

1.4 Separable States

2 Qubits

A **qubit** $|\Psi\rangle$ is the linear combination of basis elements $|0\rangle$ and $|1\rangle$ interpreted as a superposition of $0, 1$:

$$|\Psi\rangle = \alpha |0\rangle + \beta |1\rangle , \quad \alpha, \beta \in \mathbb{C}$$

Taking n tensor products of $|0\rangle$,$|1\rangle$ yields entangled states of n-qubits:

$$\begin{gathered}
|0\rangle \otimes |0\rangle ... \otimes |0\rangle = |0....0\rangle \\
|0\rangle \otimes |0\rangle ... \otimes |1\rangle = |0....1\rangle \\
... \\
|1\rangle \otimes |1\rangle ... \otimes |1\rangle = |1....1\rangle
\end{gathered}$$

Let $\mathbb{C}^2$ be the 2 dimensional $\mathbb{C}$-vector space representing the space of superpostions of a single qubit. Then the n-qubit $\mathcal{H}_n$ can be represented as:

$$\mathcal{H}_n = (\mathbb{C}^2)^{\otimes n}$$

In other words, if $|\Psi\rangle \in \mathcal{H}_n$, then

$$|\Psi\rangle = \sum_{i=0}^{2^n-1} c_i |i\rangle \quad c_i \in \mathbb{C}$$

by definition of the n-tensor product of the two-dimensional complex vector space.

3 Quantum Gates

Quantum gates are esstentially unitary operators on Hilbert spaces. These unitary operators act on single qubits by rotating them along the Bloch sphere.

3.1 Hadamard Gates

There are many gates that do not have classical analogues. One example is the Hadamard gate $H : \mathbb{C}^2 \to \mathbb{C}^2$

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

which is represented as the matrix:

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

We can see from the definition that H takes a qubit and sends it to a superposition between $|0\rangle, |1\rangle$. H is unitary as $H^2 = I$:

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

We can directly calculate the effect the Hadamard gate has on n-qubits as such:

$$H^{\otimes n} |j_{n-1}...j_0\rangle = \frac{1}{\sqrt{2^n}} \bigotimes_{l=0}^{n-1} (|0\rangle + e^{i\pi j_l} |1\rangle)$$

where $j_i = \{0, 1\}$ for $0 \leq i \leq n - 1$.

It's worth mentioning that $H^{\otimes n}$ is a special case of the *Quantum Fourier Transform (QFT)* which is in turn a manifestation of the *Fourier Transform on Finite Abelian Groups.* In this case, our abelian group will be $\mathbb{Z}_2^n$.

$$F_{\mathbb{Z}_2^n} = \frac{1}{\sqrt{2^n}} \sum_{x,y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle \langle x| = H^{\otimes n} \tag{7}$$

These topics are covered in more detail in subsequent section. Consequently, an *equal* superposition where the probabilities for measuring a given n-qubit state are uniform:

$$H^{\otimes n} |0...0\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle$$

This superposition is instrumental in many quantum algorithms such as Grover's algorithm to extract useful information from oracles as it very roughly contains a "uniform" amount of information for every n-bit string. By this virtue, we can query all inputs to the oracle in tandem. However, we will still be left with a superposition even after the oracle query, so extracting this information is not simple to see at first.

3.2 CNOT Gates

Define the CNOT (Controlled-Not Gate) as the operator which takes a two-qubit system transforms as follows:

$$\begin{aligned}
|0\rangle\,|0\rangle &\mapsto |0\rangle\,|0\rangle \\
|0\rangle\,|1\rangle &\mapsto |0\rangle\,|1\rangle \\
|1\rangle\,|0\rangle &\mapsto |1\rangle\,|1\rangle \\
|1\rangle\,|1\rangle &\mapsto |1\rangle\,|0\rangle
\end{aligned}$$

The qubit on the bottom (target qubit) flips in respect to the value of the top qubit (control qubit). The corresponding matrix representation of $CNOT : \mathbb{C}^2 \to \mathbb{C}^2$ is:

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{8}$$

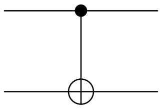

Figure 1: Matrix representaion of CNOT and its corresponding gate

We can extend this idea to create a set of *generalized* CNOT gates with the following matrices:

4 Quantum Algorithms

This section will simply be a catalogue of “classical” quantum algorithms and some of their properties. Many of these subsections will be based on the presentation given in [**?**].

4.1 Deutsch-Jozsa Algorithm

Let $f : \{0,1\} \to \{0,1\}$ be a boolean function with one-bit input. We would like to ascertain if f is either constant (both inputs have the same value) or balanced (inputs have different values). Through the classical perspective, one would have to query the function twice to determine the state of f as constant or balanced. However, we can leverage quantum mechanics so that f will only have to be queried once. The following circuit accomplishes this:

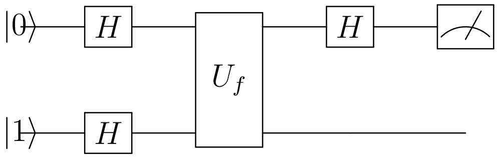

Figure 2: Deutsch-Jozsa circuit

where U_f is the map with the action: $|x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$. We calculate the action of the first two steps of the circuit above as follows:

$$|0\rangle|1\rangle \to \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) = \frac{1}{2}(|0\rangle(|f(0)\rangle - |1 \oplus f(0)\rangle) + |1\rangle(|f(1)\rangle - |1 \oplus f(1)\rangle)) = \tag{9}$$

$$\frac{1}{2}\sum_{x\in\{0,1\}} |x\rangle(|f(x)\rangle - |1 \oplus f(x)\rangle) = \tag{10}$$

$$\frac{1}{\sqrt{2}}\sum_{x\in\{0,1\}} (-1)^{f(x)}|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{11}$$

By ignoring the second register, we apply the Hadamard gate to the first register to get $|0\rangle$ up to a global phase if f is constant and $|1\rangle$ if f is balanced. Thus, if we measure the first register, we get the respective results with certainty.

In this algorithm, we only query the f-oracle once instead of twice as dictated by classical intuition. In fact, we can generalize this to a n-bit boolean function $f : \{0,1\}^n \to \{0,1\}$ where f is guaranteed to be either constant (all n-bit input strings map to the same value) or balanced (there are an equal number of bit strings mapping to both $0, 1$).

We apply $H^{\otimes(n+1)}$ to the first register of n-qubits and the second result register and another iteration of $H^{\otimes n}$ after applying the U_f gate accepting n-qubits:

$$|0...0\rangle |1\rangle \xrightarrow{H^{\otimes(n+1)}} \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \xrightarrow{U_f} \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad (12)$$

If we now discard the second result register and apply $H^{\otimes n}$ again to the first register, we yield:

$$\sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \xrightarrow{H^{\otimes n}} \begin{cases} e^{i\pi f(x)} |0...0\rangle \text{ if } f \text{ is constant} \\ |y\rangle, y \neq 0 \text{ if } f \text{ is balanced} \end{cases}$$

Thus, if we measure the first register, we measure with certainty $|0\rangle$ if f is constant and some other value if f is balanced as desired. Once again, this scheme only queries the f-oracle once.

4.2 Bernstein-Vazirani Algorithm

We can use the Deutsch-Jozsa circuit to reveal hidden traits for another special class of boolean functions. Let $f\{0,1\}^n \to \{0,1\}$ be of the following form:

$$f(x) = a \cdot x \oplus b \mod 2$$

where $\oplus$ refers to bitwise binary addition and $\cdot$ refers to the dot product i.e $x \cdot y = \sum_{i=1}^{n} x_i y_i \mod 2$. $a \in \{0,1\}^n$ and $b \in \{0,1\}$ are hidden, and we wish to find these constants. In the classical world, we would have to query the oracle $\mathcal{O}(n)$ times to find both constants a, b. By using the Deutsch-Jozsa circuit, we can drop this to $\mathcal{O}(1)$ queries. We use the exact circuit above and calculate the effect of the circuit:

$$|0...0\rangle\,|1\rangle \xrightarrow{H^{\otimes(n+1)}} \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle\,\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \xrightarrow{U_f} \tag{13}$$

$$\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle\,\frac{1}{\sqrt{2}}(|f(x)\rangle-|1\oplus f(x)\rangle) = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle\,\frac{1}{\sqrt{2}}(|a\cdot x\oplus b\rangle-|1\oplus(a\cdot x\oplus b)\rangle) = \tag{14}$$

$$\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^b\,|x\rangle\,\frac{1}{\sqrt{2}}(|a\cdot x\rangle-|1\oplus(a\cdot x)\rangle) = \frac{(-1)^b}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{a\cdot x}\,|x\rangle\,\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \tag{15}$$

We prove a lemma showing destructive interference for certain terms:

Lemma 1. *Let $z\in\{0,1\}^n$. Then*

$$\sum_{x=0}^{2^n-1}(-1)^{z\cdot x}=0$$

iff $z\neq 0$

Proof. We begin by expanding the form above:

$$\sum_{x=0}^{2^n-1}(-1)^{z\cdot x}=\sum_{x=0}^{2^n-1}\prod_{j=1}^{n}(-1)^{z_jx_j}=\sum_{x_n=0}^{1}\cdots\sum_{x_2=0}^{1}\sum_{x_1=0}^{1}\prod_{j=1}^{n}(-1)^{z_jx_j}$$

The last equality easily follows from the fact that we can rearrange the sum in the specific order imposed by the summation on the right.

Now suppose there exists $1\leq r\leq n$ such that $z_r=1$. From the form above, we derive that:

$$\sum_{x_n=0}^{1}\cdots\sum_{x_2=0}^{1}\sum_{x_1=0}^{1}\prod_{j=1}^{n}(-1)^{z_jx_j}=\sum_{x_n=0}^{1}\cdots\sum_{x_{r+1}=0}^{1}\sum_{x_{r-1}=0}^{1}\cdots\sum_{x_2=0}^{1}\sum_{x_1=0}^{1}\prod_{j=1,j\neq r}^{n}(-1)^{z_jx_j}((-1)^0+(-1)^1)=0$$

Note that from $\sum_{x=0}^{2^n-1}(-1)^{z\cdot x}\,|x\rangle=2^n\delta_{z,0}$, we have the converse as well. □

We cannot use this lemma directly on the form representing the first n-qubit register above as the sum involves constituent states $|x\rangle$ tied to the $(-1)^{z\cdot x}$. To fix this, we first apply $H^{\otimes n}$ on the first register:

$$\frac{(-1)^b}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{a\cdot x}|x\rangle \xrightarrow{H^{\otimes n}} \frac{(-1)^b}{2^n}\sum_{x=0}^{2^n-1}(-1)^{a\cdot x}\sum_{y=0}^{2^n-1}(-1)^{y\cdot x}|y\rangle = \tag{16}$$

$$\frac{(-1)^b}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}(-1)^{(a+y)\cdot x}|y\rangle \tag{17}$$

We now apply Lemma 1 to the first register above to find that it equals:

$$(-1)^b|a\rangle$$

Thus, by measuring the first register, we get the value of a off by some phase factor.

The main argument for the correctness of the algorithm stems from the destructive interference resulting from the operation of running an equal superposition of all 2^n possible bit-strings which can x take, then "merging" them together and letting destructive interference take its course.

4.3 Grover's Algorithm

Let X be an unstructured database of size N. We can simply think of X as an array with elements $\{1, ..., N\}$ not necessarily in sorted order. Classically, we would have to query the database $\mathcal{O}(N)$ times. However, Grover's algorithm shows that it is possible to leverage quantum phenomena to bring this down to $\mathcal{O}(\sqrt{N})$ queries.

For the sake of a simpler analysis, let $f : \{0,1\}^n \to \{0,1\}^n$ be a boolean function representing an unstructured database of size 2^n with a single marked element $w \in \{0,n\}^n$.

$$f(x) = \begin{cases} 1 \text{ if } x = w \\ 0 \text{ otherwise} \end{cases}$$

The crux of the algorithm comes from iterating a specially constructed unitary transformation G composed with the oracle query gate U_f.

$$G = H^{\otimes n}(-I + 2|0\rangle\langle 0|)H^{\otimes n}$$

Let us compute the action of G on $|x\rangle \in (\mathbb{C}^2)^{\otimes n}$ as follows: We first compute the below expression:

$$(-I + 2|0\rangle\langle 0|)H^{\otimes n}|x\rangle = (-I + 2|0\rangle\langle 0|))\frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1}(-1)^{y\cdot x}|y\rangle = \tag{18}$$

$$\frac{1}{\sqrt{2^n}}\big[-\sum_{y=0}^{2^n-1}(-1)^{y\cdot x}|y\rangle + 2|0\rangle\big] \tag{19}$$

Now we apply the last n-qubit Hadamard transform to yield the following:

$$\frac{1}{\sqrt{2^n}}H^{\otimes n}\big[-\sum_{y=0}^{2^n-1}(-1)^{y\cdot x}|y\rangle + 2|0\rangle\big] = \frac{1}{2^n}\big[-\sum_{z=0}^{2^n-1}\sum_{y=0}^{2^n-1}(-1)^{y\cdot(x+z)}|y\rangle + 2\sum_{z=0}^{2^n-1}|z\rangle\big] = \tag{20}$$

$$\frac{1}{2^n}(-2^n|x\rangle + 2|S\rangle) \tag{21}$$

where $|S\rangle = \sum_{z=0}^{2^n-1}|z\rangle$ refers to the equally-weighted superposition state of n-qubits. The second-to-last equality follows from reindexing the sum with y-indices instead of z-indices. Note that the Hadamard transform is an inverse of itself, giving us $-|x\rangle$ as the first term. Thus, we get that:

$$G|x\rangle = -|x\rangle + \frac{2}{2^n}|S\rangle$$

and we deduce the following $2^n \times 2^n$ matrix representation:

$$G = \begin{bmatrix} -1+\frac{2}{2^n} & \frac{2}{2^n} & \dots & \frac{2}{2^n} \\ \frac{2}{2^n} & -1+\frac{2}{2^n} & \dots & \frac{2}{2^n} \\ . & . & \dots & . \\ . & . & \dots & . \\ . & . & \dots & . \\ \frac{2}{2^n} & \frac{2}{2^n} & \dots & -1+\frac{2}{2^n} \end{bmatrix}$$

The iteration of GU_f has a geometric interpretation which we will now consider. Let $|S\rangle$ be the equally-weighted superposition and let $|x_0\rangle$ be the marked item:

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

Let θ be the angle between S and $x_0^{\perp} = \frac{1}{\sqrt{N-1}} \sum_{x \neq x_0} |x\rangle$. This gives us the following representation:

$$|S\rangle = \sin\theta x_0 + \cos\theta x_0^{\perp}$$

Note that

$$|S\rangle = \frac{1}{\sqrt{N}} \sum_{x \neq x_0} |x\rangle + \frac{1}{\sqrt{N}} |x_0\rangle = \sqrt{\frac{N-1}{N}} \left|x_0^{\perp}\right\rangle + \frac{1}{\sqrt{N}} |x_0\rangle$$

Thus,

$$\sin\theta = \langle x_0 | S\rangle = \frac{1}{\sqrt{N}}$$

implying that

$$\theta \approx \frac{1}{\sqrt{N}}$$

for sufficiently large N. We claim the following:

1. U_f corresponds to a reflection across hyperplane orthogonal to $|x_0\rangle$.
2. G corresponds to a reflection across hyperplane orthogonal to $|S\rangle$.

These two operations rotate generic unit vector $|\Psi\rangle$ by 2θ. To see this, imagine a generic unit vector $|\Psi\rangle$ some angle θ_0 from $x_0^{\perp}$ on the two-dimensional plane spanned by $|x_0\rangle$ and $\left|x_0^{\perp}\right\rangle$. Assume that we orient our plane such that we visualize $\left|x_0^{\perp}\right\rangle$ as our horizontal axis and $|x_0\rangle$ as our vertical axis. Reflecting across the axis $\left|x_0^{\perp}\right\rangle$ rotates our $|\Psi\rangle$ $2\theta_0$ clockwise, giving position $-\theta_0$. Then reflecting it across axis $|S\rangle$ rotates it by $2(\theta_0+\theta)$, giving the angle $2(\theta_0 + \theta) - \theta_0 = \theta_0 + 2\theta$.

Since $\theta \approx \frac{1}{\sqrt{N}}$ is close to zero for sufficiently large N, it suffices to rotate our equally-weighted superposition $|S\rangle$ around $\frac{\pi}{2}$ to become close to $|x_0\rangle$ as $\left|x_0^{\perp}\right\rangle, |x_0\rangle$ are orthogonal to each other. We thus solve the following:

$$2k\theta \approx \frac{\pi}{2} \implies k = \frac{\sqrt{N}\pi}{4}$$

This gives us that we need about $\mathcal{O}(\sqrt{N})$ iterations to give us a state when measured gives us the desired index with high probability. As each iteration queries the oracle a constant number of times, it follows that we need $\mathcal{O}(\sqrt{N})$ queries.

4.4 Quantum Fourier Transform

We now investigate the quantum analogue of the discrete Fourier transform as follows: For an n-qubit system, we define the *Quantum Fourier Transform*:

$$F = \frac{1}{\sqrt{2^n}} \sum_{x,y=0}^{2^n-1} \zeta^{xy} \left| y \right\rangle \left\langle x \right|$$

where $\zeta = e^{2\pi i/2^n}$. This operation is unitary as we can directly check:

$$F^\dagger F = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} \zeta^{xy-xy} \left| x \right\rangle \left\langle x \right| = \sum_{x=0}^{2^n-1} \left| x \right\rangle \left\langle x \right| = I$$

We can explictly express the action of F on a basis vector $x \in (\mathbb{C}^2)^{\otimes n}$

$$\begin{aligned}
F\left|x\right\rangle &= \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} \zeta^{xy} \left|y\right\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{y_0=0}^{1} \sum_{y_2=0}^{1} \cdots \sum_{y_{n-1}=0}^{1} \zeta^{x(\sum_{j=1}^{n} y_j 2^j)} \left|y_{n-1}\right\rangle \dots \left|y_0\right\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{y_0=0}^{1} \sum_{y_1=0}^{1} \cdots \sum_{y_{n-1}=0}^{1} \prod_{j=0}^{n-1} \zeta^{xy_j 2^j} \left|y_{n-1}\right\rangle \dots \left|y_0\right\rangle \\
&= \frac{1}{\sqrt{2^n}} \bigotimes_{i=0}^{n-1} \sum_{y_i=0}^{1} \zeta^{xy_i 2^i} \left|y_i\right\rangle \\
&= \frac{1}{\sqrt{2^n}} \bigotimes_{i=0}^{n-1} \left|0\right\rangle + \zeta^{x2^i} \left|1\right\rangle \\
&= \frac{1}{\sqrt{2^n}} \bigotimes_{i=1}^{n-1} \left|0\right\rangle + \zeta^{\sum_{k=0}^{n-1} x_k 2^{k+i}} \left|1\right\rangle \\
&= \frac{1}{\sqrt{2^n}} \bigotimes_{i=0}^{n-1} \left|0\right\rangle + e^{2\pi i(x_{n-1}2^{i-1}+x_{n-2}2^{i-2}+\dots+x_0 2^{i-n}))} \left|1\right\rangle \\
&= \frac{1}{\sqrt{2^n}} \bigotimes_{i=0}^{n-1} \left|0\right\rangle + e^{2\pi i(x_{n-i-1}2^{-1}+x_{n-i-2}2^{-2}+\dots+x_0 2^{i-n})} \left|1\right\rangle \\
&= \frac{1}{\sqrt{2^n}} \bigotimes_{i=0}^{n-1} \left|0\right\rangle + e^{2\pi i[0.x_{n-i-1}\dots x_1 x_0]} \left|1\right\rangle
\end{aligned}$$

The last equality follows from the fact that any bit shift past $n-1-k$ times will result in an even power of $e^{2\pi i}$ which will always be equal to one. where

$$P_i = \begin{bmatrix} 1 & 0 \\ 0 & \zeta^{2^i} \end{bmatrix}$$

is the phase shift gate rotating ζ^{2^i} Note that

$$e^{2\pi i(x_{n-1-i}2^{-1})} = e^{\pi i x_{n-1-i}} = \begin{cases} 0 \text{ if } x_{n-1-i} = 0 \\ -1 \text{ if } x_{n-1-i} = 1 \end{cases}$$

Thus, $|0\rangle + e^{2\pi i(x_{n-1-i}2^{-1})}\,|1\rangle$ can be realized through a Hadamard transform on each $|x_{n_1-i}\rangle$, $0 \le i \le n-1$. Now from this expression, we can construct the quantum circuit implementing the Quantum Fourier Transform for a basis vector x in Figure 3.

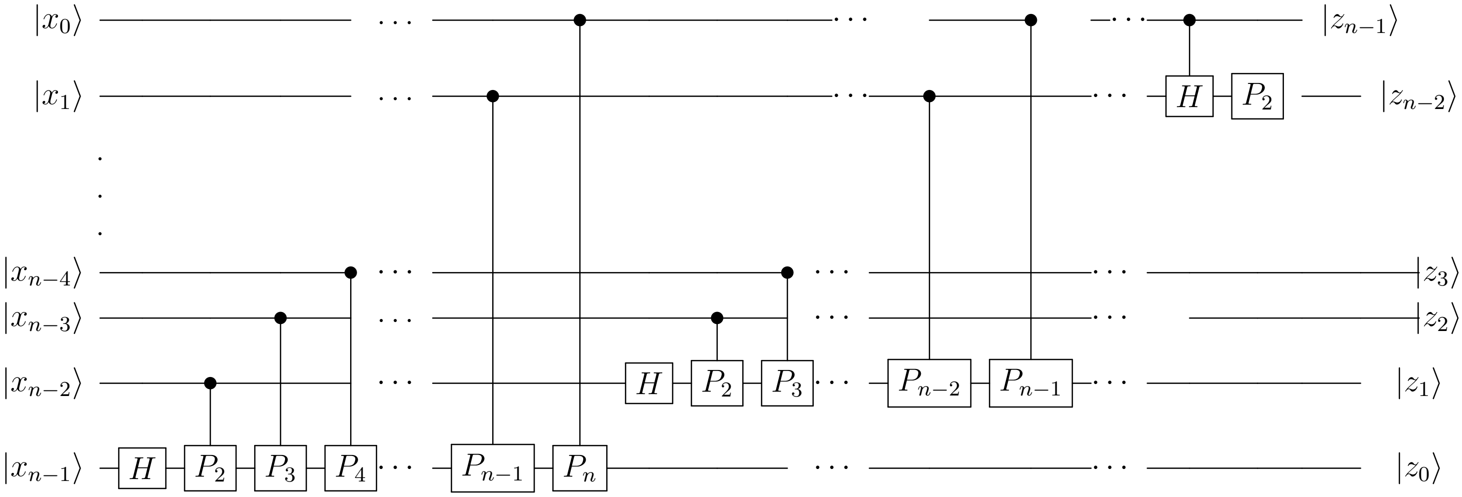

Figure 3: Quantum circuit realizing the QFT

4.5 Phase Estimation

The setup of the phase estimation problem is the following: one is given an unitary operator U and a state $|\phi\rangle$ promised to be an eigenvector of U such that

$$U\,|\phi\rangle = e^{i\phi}\,|\phi\rangle \tag{22}$$

We wish to determine an n-bit estimate of ϕ. The quantum circuit which achieves this is as below: We first prepare the initial quantum state as the uniform superposition:

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

applying the operator

$$\sum_{x=0}^{2^n-1}|x\rangle\langle x| \otimes U^x \tag{23}$$

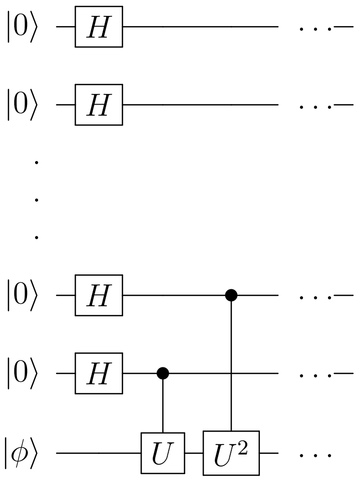

Figure 4: Phase Estimation Circuit

to the initial state gives way to:

$$\sum_{x=0}^{2^n-1} e^{i\phi x} |x\rangle \otimes |\phi\rangle$$

Equivalently this state can be written as:

$$\sum_{x=0}^{2^n-1} e^{\frac{\phi}{2\pi}[2\pi i x]} |x\rangle \otimes |\phi\rangle \tag{24}$$

Suppose that $\phi/2\pi$ terminates after at most n-bits or if $\frac{\phi}{2\pi} = y/2^n$ for some $y \in \mathbb{Z}_{2^n}$. Then $\phi = \frac{2\pi y}{2^n}$. Substituting this in the expression above and applying the inverse QFT to the first n registers will result in the state $|y\rangle \otimes \phi$. Therefore, measuring on the first register will give us the exact value of y.

(Todo: think about the general case)

5 The Hidden Subgroup Problem and its Applications

The Hidden Subgroup Problem (HSP) can be phrased by first introducing the following oracle: Suppose I have a finite group G along with a function $f : G \to S$ with some finite set

S. Furthermore, a guarantee is given that f is constant on cosets of some *hidden subgroup* $H < N$:

$$f(x) = f(y) \text{ iff } x^{-1}y \in H$$

We wish to determine H through a generator representation by quering the oracle preferrably as little as needed. Determining such a subgroup is important in studying Quantum algorithms to algebraic problems. This section will focus on one such application where this problem naturally appears: **Shor's Algorithm** for finding the discrete logarithm.

5.1 Shor's Algorithm: Discrete Logarithm

First, we set the stage. Suppose that I have a finite cyclic group $G = \langle g \rangle$. To simplify the presentation, let us assume that the order of G is known beforehand. In general, we do not know the period of an arbitrary cyclic group. Furthermore, let us assume that $x \neq g$ as this can be checked in constant time.

Now we define a function $f : \mathbb{Z}_N \times \mathbb{Z}_N \to G$:

$$f(\alpha, \beta) = g^{\alpha \log_g x + \beta} \tag{25}$$

This is simply $f(\alpha, \beta) = x^\alpha g^\beta$. From this form, the function f is seen to be efficiently computable since computing f only requires modular exponentiation and multiplication in G.

We are interested in the following subgroup H:

$$\begin{aligned} H &= \{(\alpha, \beta) \in \mathbb{Z}_N \times \mathbb{Z}_N \mid \alpha \log_g x + \beta = 0\} \\ &= \{(0,0), (1, -\log_g x), (2, -2\log_g x), \ldots, (N-1, -(N-1)\log_g x)\} \end{aligned}$$

Observe that f is constant on H. In fact, f is constant on the cosets of H as well.

$$(0, \delta) + H = \{(r, \delta - r\log_g x) \mid r \in \mathbb{Z}_N\} = \{(\alpha, \beta) \in \mathbb{Z}_N \times \mathbb{Z}_N \mid \alpha \log_g x + \beta = \delta\} \tag{26}$$

for $\delta \in \mathbb{Z}_N$. To see that the $(0, \delta)$ form a complete set of representatives of every coset $(\gamma, \delta) + H$, $\gamma, \delta \in \mathbb{Z}_N$, use Lagrange's theorem to show that $(\mathbb{Z}_N \times \mathbb{Z}_N : H) = N$. If we let $R = \{(0, \delta) \mid \delta \in \mathbb{Z}_N\}$ be set of alleged coset representatives, it suffices to show that

$(0,\delta) \not\sim (0,\sigma)$ for $\delta \neq \sigma$. However, this easily seen through the definition of H above. Finally, by the string of equalities shown in (26), f is constant on the cosets of H.

The observations above will guide the construction of the algorithm as follows: We initialize an uniform superposition over all $(\alpha,\beta) \in \mathbb{Z}_N \times \mathbb{Z}_N$ and induce the action of $f(\alpha,\beta)$ on the state:

$$\frac{1}{N}\sum_{\alpha,\beta} |\alpha,\beta\rangle \xrightarrow{f} \frac{1}{N}\sum_{\alpha,\beta} |\alpha,\beta,f(\alpha,\beta)\rangle \tag{27}$$

We now measure the third register to receive a value $f(\alpha,\beta)$ for some α,β. This will collapse the superposition to those consistent with the result, namely the elements contained in a coset of H:

$$\frac{1}{\sqrt{N}}\sum_{\alpha} \left|\alpha,\delta-\alpha\log_g x\right\rangle \quad \delta \in \mathbb{Z}_N \tag{28}$$

We now perform the Quantum Fourier Transform over $\mathbb{Z}_N \times \mathbb{Z}_N$ to yield the expression below:

$$\begin{aligned} \frac{1}{\sqrt{N}}\sum_{\alpha} \left|\alpha,\delta-\alpha\log_g x\right\rangle \xrightarrow{QFT} & \frac{1}{N^{3/2}}\sum_{\alpha}\Big(\sum_{\sigma}\zeta_N^{\alpha\sigma}\left|\sigma\right\rangle\Big)\otimes\Big(\sum_{\theta}\zeta_N^{\delta\log_g x\theta}\left|\theta\right\rangle\Big) = \\ & \frac{1}{N^{3/2}}\sum_{\alpha,\sigma,\theta}\zeta_N^{\alpha\sigma+(\delta-\alpha\log_g x)\theta}\left|\sigma,\theta\right\rangle \end{aligned} \tag{29}$$

By rearranging some terms, we arrive at the following form:

$$\frac{1}{N^{3/2}}\sum_{\sigma,\theta}\zeta_N^{\delta\theta}\sum_{\alpha}\zeta_N^{\alpha(\sigma-\log_g x\theta)}\left|\sigma,\theta\right\rangle. \tag{30}$$

By the identity concerning geometric sums of roots of unity:

$$\sum_{\alpha}\zeta_N^{\alpha\gamma} = N\delta_{0,\gamma}$$

So, the final form will be

$$\frac{1}{\sqrt{N}}\sum_{\sigma}\zeta_N^{\delta\theta}\left|\theta\log_g x,\theta\right\rangle$$

By measuring this state, we will receive one of the $(\theta\log_g x,\theta)$ with uniform probability. If θ has a multiplicative inverse, i.e is relatively prime to N, we can simply multiply $\theta\log_g x$ on the left to reveal the discrete logarithm. If not, we repeat the experiment until we find such a θ as it turns out that $\phi(N)/N = \Omega(1/\log\log N)$.

Remark 1. *The QFT transform above roughly transfers the information encoded into the states to the phases. By the identity above, certain phases will engage in destructive interference, leaving the useful information to be measured. This technique is known as* **Fourier Sampling**. *We will touch Fourier Sampling in an upcoming section.*

5.2 Shor's Algorithm: Period Finding

A similar vein of thought can be applied to the Period Finding Problem.

5.3 On the Abelian HSP

We can define a general form for the QFT over an arbitrary *finite abelian* group G. From what we know from the representation theory of finite groups, there are exactly $|G|$ irreducible representations of degree one over G. Let $\hat{G} = \{\chi_y\}_{1\leq y\leq |G|}$ be all such characters of their corresponding irreducible representations. As a minor abuse of notation, we will identify $\hat{G}$ as the indices y of the characters rather than the characters themselves. The QFT over G is defined appears:

$$F_G = \frac{1}{\sqrt{|G|}} \sum_{x\in G} \sum_{\chi_y \in \hat{G}} \chi_y(x) \left|y\right\rangle \left\langle x\right| \tag{31}$$

where we recall that a character is a function $\chi_y : G \to \mathbb{C}$ such that

$$\chi_y(x) = \mathrm{T}r(\rho_y(x))$$

where $\rho_y : G \to GL(V_y)$ is the irreducible representation indiced by y. Furthermore, each irreducible representation is of dimension one as G is abelian. Thus, for $y \in \hat{G}$ and $r, q \in G$, $\rho_{q+r} = \rho_q \rho_r$ will simply be a multiplication of scalars and

$$\chi_y(r + q) = \chi_y(r)\chi_y(q) \tag{32}$$

Recall that the HSP involves a function $f : G \to S$ to some finite set such that

$$f(x) = f(y) \text{ iff } x^{-1}y \in H \quad \forall x, y \in G$$

for some hidden subgroup H. We use a similar idea found in Shor's algorithm to ascertain generators of H with high probability.

Take a uniform superposition over G and apply the action of our function on the state

$$\frac{1}{\sqrt{G}}\sum_{x\in G}|x\rangle \xrightarrow{f} \frac{1}{\sqrt{G}}\sum_{x\in G}|x, f(x)\rangle \tag{33}$$

By measuring on the second register, we collapse the state to a uniform superposition over elements of a left coset $x+H$:

$$|x+H\rangle = \frac{1}{\sqrt{H}}\sum_{h\in G}|x+h\rangle \tag{34}$$

for some $x \in G$. This is deemed as a *coset state of* H. Since we sample for this coset over the uniform superpostion, we have the mixed state

$$\rho = \frac{1}{|G|}\sum_{x\in G}|x+H\rangle\langle x+H| \tag{35}$$

Now apply the QFT transform over G to this state

$$\begin{aligned}
|\widehat{x+H}\rangle &= F_G\,|x+H\rangle \\
&= \frac{1}{\sqrt{|G||H|}}\sum_{y\in\hat{G}}\sum_{h\in H}\chi_y(x+h)\,|y\rangle \\
&= \sqrt{\frac{|H|}{|G|}}\sum_{y\in\hat{G}}\chi_y(x)\big[\frac{1}{|H|}\sum_{h\in H}\chi_y(h)\big]\,|y\rangle \\
&= \sqrt{\frac{|H|}{|G|}}\sum_{y\in\hat{G}}\chi_y(x)\chi_y(H)\,|y\rangle
\end{aligned} \tag{36}$$

where $\chi_y(H) = \frac{1}{|H|}\sum_{h\in H}\chi_y(h)$. Note that $\chi_y(x+h)$ separates into factors $\chi_y(x)\chi_y(h)$ by (32). By orthogonality relations between irreducible characters, we know orthogonality

$$\frac{1}{|H|}\sum_{h\in H}\chi_y(h) = \frac{1}{|H|}\sum_{h\in H}\chi_y(h)\chi_{y'}(h) = \delta_{y,y'}$$

where we take y' to be the trivial representation of H. Thus, we can express the form above as

$$|\widehat{x+H}\rangle = \sqrt{\frac{|H|}{|G|}} \sum_{\substack{y\in\hat{G} \\ \chi_y(H)=1}} \chi_y(x)\,|y\rangle \tag{37}$$

By the mixed state in (35), our mixed state after applying the QFT will be

$$\begin{aligned} \hat{\rho} = \frac{1}{|G|}\sum_{x\in G} |\widehat{x+H}\rangle\langle\widehat{x+H}| &= \frac{|H|}{|G|^2} \sum_{\substack{\chi_y(H)=1 \\ \chi_r(H)=1}} \sum_{x\in G} \chi_y(x)\chi_r(x)^*\,|y\rangle\,\langle r| \\ &= \frac{|H|}{|G|} \sum_{\chi_y(H)=1} |y\rangle\,\langle y| \end{aligned} \tag{38}$$

The last equality follows once again from the orthogonality relations between irreducible characters. The state $\hat{\rho}$ suggests that it is a classical uniform distribution over the characters taking value one on H. Thus, measuring on this state will yield such a character. The method which will progressively crave out H will be to take intersections of the sets of G which are trivial on the χ_y:

$$C_y = \{x \in G \mid \chi_y(x) = 1\}$$

C_y can be seen as the kernel of χ_y which makes sense as $\chi_y : G \to \mathbb{C}^\times$ is a group homomorphism in this particular case.

6 Fourier Analysis over Nonabelian Finite Groups

Let G be a finite group (non necessarily abelian). Let $\mathbb{C}[G]$ the *group algebra* of G over $\mathbb{C}$ i.e the $\mathbb{C}$-algebra with elements of the form:

$$f = \sum_g a_g \cdot g$$

with addition done with the group elements as indices and multiplication adhering to the binary operation on G. The general *Fourier Transform over* G is a unitary transformation $F_G : \mathbb{C}[G] \to \bigoplus_{y\in\hat{G}} \mathbb{C}^{n_y} \otimes \mathbb{C}^{n_y}$ with following action on basis vectors $x \in G$

$$|\hat{x}\rangle = F_G\,|x\rangle = \frac{1}{\sqrt{|G|}} \sum_{y\in\hat{G}} n_y\,|y, \rho_y(x)\rangle \tag{39}$$

where $\hat{G}$ indices of the set of irreducible representation of G, n_i is the dimension of the i^{th} irreducible representation, and

$$|\rho_y(x)\rangle = \sum_{1 \leq q,r \leq n_y} \frac{\rho_y(x)_{q,r}}{\sqrt{n_y}} |q\rangle \otimes |r\rangle \tag{40}$$

By summing over all such basis vectors, we get the operator

$$F_G = \sum_{x \in G} |\hat{x}\rangle \langle x|$$

Observe we arrive at the form encountered in the previous section when we assume G is abelian as $\chi_y(x) = \mathrm{Tr}(\rho_y(x)) = \rho_y(x)_{1,1} = \lambda_y \in \mathbb{C}$. Thus, $|\rho_y(x)\rangle = \lambda_y$ so simplifying will yield the desired form (31). Finally, F_G is verified to be a unitary transformation as

$$\langle \hat{z} | \hat{y} \rangle \tag{41}$$