Quantum Computing Study Sheet

Postulates of Quantum Mechanics

Postulate 1

Associated to any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the state space of the system. The system is completely described by its state vector, which is a unit vector in the system's state space. A coherent qubit is described by

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

with $\alpha, \beta \in \mathbb{C}$, which we call a *superposition* of the states $|0\rangle$ and $|1\rangle$. Also note $|\alpha|^2 + |\beta|^2 = 1$.

Postulate 2

The evolution of a closed quantum system is described by a unitary transformation. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U (meaning $U^\dagger = U^{-1}$) which depends only on the times t_1 and t_2,

$$|\psi'\rangle = U|\psi\rangle.$$

This postulate is equivalent to the statement that the time evolution of the state of a closed quantum is described by the Schrödinger equation.

Postulate 3

Quantum measurements are described by a collection of measurement operators $\{M_m\}$ such that:

- they act on the state space of the system being measured $|\psi\rangle$
- the index m corresponds to measurement outcome
- the probability of obtaining outcome m depends on the state of the system $|\psi\rangle$

Bloch sphere

While $|\psi\rangle$ is really 4-dimensional, we can collapse 2 of the dimensions by noting that global phase cannot be measured ($|\psi\rangle$ and $e^{i\varphi}|\psi\rangle$ are indistinguishable when we measure them), and $|\alpha|^2 + |\beta|^2 = 1$. Thus we can describe possible quantum states as being on the surface of a sphere parameterized by only 2 variables: φ and θ. This is the Bloch sphere representation of $|\psi\rangle$.

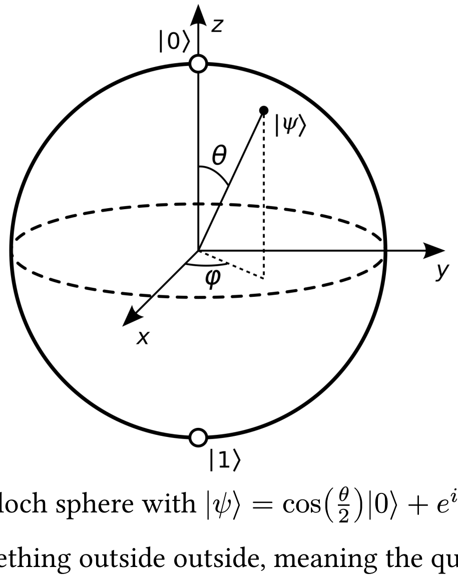


Figure 1: Bloch sphere with $|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle$.

Note that when a qubit interacts with something outside outside, meaning the quantum system becomes open rather than closed, these postulates do not apply. This is called decoherence.

Basis Vectors

We write out the basis vectors for each of the main bases with an explicit representation in the computational basis below:

Basis	+1 eigenstate	−1 eigenstate
Z	$\|0\rangle = \binom{1}{0}$	$\|1\rangle = \binom{0}{1}$
X	$\|+\rangle = \frac{1}{\sqrt{2}}\binom{1}{1}$	$\|-\rangle = \frac{1}{\sqrt{2}}\binom{1}{-1}$
Y	$\|+i\rangle = \frac{1}{\sqrt{2}}\binom{1}{i}$	$\|-i\rangle = \frac{1}{\sqrt{2}}\binom{1}{-i}$

Pauli Matrices

The following is all written in the computational basis. We can show that

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

form a basis of 2 × 2 Hermitian matrices. These matrices satisfy

$$[X, Y] = 2iZ; \quad [Y, Z] = 2iX; \quad [Z, X] = 2iY$$
$$\{\sigma_i, \sigma_j\} = 2\delta_{ij} I$$

where the commutator $[A, B] = AB - BA$ and the anti-commutator $\{A, B\} = AB + BA$. In particular, note $iX = YZ$.

Change of Basis

Note the change of basis from Z to X basis or X to Z basis is given by the Hadamard gate:

$$H = ([|0\rangle]_x \ \ [|1\rangle]_x) = ([|+\rangle]_z \ \ [|-\rangle]_z) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}_{x,z} = |+\rangle\langle 0| + |-\rangle\langle 1| = |0\rangle\langle +| + |1\rangle\langle -|$$

and the change of basis from the X basis to the Y basis is given by the phase gate:

$$S = \left([|+\rangle]_y \ \ |-\rangle_y\right) = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}_z = |+i\rangle\langle +| + |-i\rangle\langle -|$$

with the change of basis from Y to X being $S^{-1} = S^\dagger$ (since S is unitary but not Hermitian, unlike the Hadamard gate). Finally, a change of basis from Z to Y is given by composing the gates, i.e.,

$$SH = |+i\rangle\langle 0| + |-i\rangle\langle 1| = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} (1 \ \ 0) + \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix} (0 \ \ 1) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}_z$$

Element	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|+i\rangle$	$\|-i\rangle$
Z	$\|0\rangle$	$\|1\rangle$	$\frac{\|0\rangle+\|1\rangle}{\sqrt{2}}$	$\frac{\|0\rangle-\|1\rangle}{\sqrt{2}}$	$\frac{\|0\rangle+i\|1\rangle}{\sqrt{2}}$	$\frac{\|0\rangle-i\|1\rangle}{\sqrt{2}}$
X	$\frac{\|+\rangle+\|-\rangle}{\sqrt{2}}$	$\frac{\|+\rangle-\|-\rangle}{\sqrt{2}}$	$\|+\rangle$	$\|-\rangle$	$\frac{(1+i)\|+\rangle+(1-i)\|-\rangle}{2}$	$\frac{(1-i)\|+\rangle+(1+i)\|-\rangle}{2}$
Y	$\frac{\|+i\rangle+\|-i\rangle}{\sqrt{2}}$	$\frac{-i\|+i\rangle+i\|-i\rangle}{\sqrt{2}}$	$\frac{(1-i)\|+i\rangle+(1+i)\|-i\rangle}{2}$	$\frac{(1+i)\|+i\rangle+(1-i)\|-i\rangle}{2}$	$\|+i\rangle$	$\|-i\rangle$

Dirac Notation Decomposition

These matrices have the following representations in different bases:

Basis	Z	X	Y	I
Z	$\|0\rangle\langle 0\| - \|1\rangle\langle 1\|$	$\|1\rangle\langle 0\| + \|0\rangle\langle 1\|$	$i\|1\rangle\langle 0\| - i\|0\rangle\langle 1\|$	$\|0\rangle\langle 0\| + \|1\rangle\langle 1\|$
X	$\|+\rangle\langle -\| + \|-\rangle\langle +\|$	$\|+\rangle\langle +\| - \|-\rangle\langle -\|$		$\|+\rangle\langle +\| + \|-\rangle\langle -\|$
Y	$i\|+i\rangle\langle -i\| - i\|-i\rangle\langle +i\|$		$\|+i\rangle\langle +i\| - \|-i\rangle\langle -i\|$	$\|+i\rangle\langle +i\| + \|-i\rangle\langle -i\|$

and note the diagonal entires are simply the Spectral Decompositions, and can be used to derive the other entries in the row by simply writing basis vectors in the other bases.

Example calculation: Z in the X basis. We have

$$Z_x = I_{z\to x} Z_z I_{x\to z} = H_z Z_z H_z = X_z \Longrightarrow Z_x = |1\rangle_x \langle 0|_x + |0\rangle_x \langle 1|_x = |+\rangle\langle -| + |-\rangle\langle -|.$$

Partial Rotation Quantum Gates

In addition to the Pauli gates and change of basis gates listed above, we can do a partial rotation in a given direction via

$$X(\theta) \equiv \exp\left(-i\frac{\theta}{2}\sigma_x\right) = \cos\left(-\frac{\theta}{2}\right)I + i\sin\left(-\frac{\theta}{2}\right)\sigma_x = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -i\sin\left(\frac{\theta}{2}\right) \\ -i\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix}.$$

$$Y(\alpha) \equiv \exp\left(-i\frac{\alpha}{2}\sigma_y\right) = \cos\left(-\frac{\alpha}{2}\right)I + i\sin\left(-\frac{\alpha}{2}\right)\sigma_y = \begin{pmatrix} \cos\left(\frac{\alpha}{2}\right) & -\sin\left(\frac{\alpha}{2}\right) \\ \sin\left(\frac{\alpha}{2}\right) & \cos\left(\frac{\alpha}{2}\right) \end{pmatrix}$$

$$Z(\beta) \equiv \exp\left(-i\frac{\beta}{2}\sigma_z\right) = \begin{pmatrix} e^{-i\frac{\beta}{2}} & 0 \\ 0 & e^{i\frac{\beta}{2}} \end{pmatrix}.$$

These can be used to create a “generalized Hadamard” as in HW 4 #4 according to Office Hours: $Y(\alpha)X(\beta)$.

Two Qubit Gates

Some typical 2 qubit gates are:

$$\text{CNOT} = \text{CX} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$

$$\text{CZ} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z$$

$$\text{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = |00\rangle\langle 00| + |10\rangle\langle 01| + |01\rangle\langle 10| + |11\rangle\langle 11|.$$

Eigendecomposition

For a Hermitian operator A, the Spectral Theorem tells us we can write $f(A) = Q^\dagger f(\Lambda) Q = \sum_\lambda f(\lambda)|v\rangle\langle v|$ for a unitary Q and and unit eigenvectors v.

For example,

$$e^{\theta Z} = e^{\theta}|0\rangle\langle 0| + e^{-\theta}|1\rangle\langle 1| = \begin{pmatrix} e^{\theta} & 0 \\ 0 & e^{-\theta} \end{pmatrix}.$$

Schrödinger Equation

The Schrödinger equation is given by

$$i\hbar \frac{d}{dt}|\psi(t)\rangle = \hat{H}|\psi(t)\rangle.$$

If $\hat{H}$ is independent of time, $|\psi(t)\rangle$ can be solved by separation of variables. The result is given by

$$|\psi(t)\rangle = \exp\left(-\frac{it}{\hbar}\hat{H}\right)|\psi(0)\rangle.$$

Using an eigendecomposition for the Hamiltonian, we can write

$$\exp\left(-\frac{it}{\hbar}\hat{H}\right) = \exp\left(-\frac{it}{\hbar}\lambda_1\right)|v_1\rangle\langle v_1| + \exp\left(-\frac{it}{\hbar}\lambda_2\right)|v_2\rangle\langle v_2|.$$

If $\hat{H}$ is dependent on time, $|\psi(t)\rangle$ can be solved by solving the two ODEs, $\alpha(t)$ and $\beta(t)$, where $|\psi(t)\rangle = \begin{pmatrix}\alpha(t)\\ \beta(t)\end{pmatrix}$.

Mathematics of Quantum Measurements

According to Postulate 3, we have that the probability of $|\psi\rangle$ being in outcome m is

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$$

and once measured the state becomes

$$|\varphi\rangle = \frac{M_m|\psi\rangle}{\sqrt{p(m)}}.$$

Note that a set of measurement operators must satisfy a completeness condition due to being a probability mass function:

$$\sum_m M_m^\dagger M_m = I \Longleftrightarrow \sum_m p(m) = \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle = 1.$$

Projective Measurements

A projective measurement is a special type of measurement given by an observable M. An observable is a Hermitian operator M on the state space being observed. It has a spectral decomposition

$$M = \sum_m m P_m$$

where P_m is the projector onto the eigenspace of the eigenvalue m, i.e. $P_m = |v_m\rangle\langle v_m|$.

Note that this definition implies projective measurements satisfy completeness, orthogonality ($M_m M_{m'} = \delta_{m,m'} M_m$), and Hermiticity.

Note since projective measurements are idempotent, the probability of $|\psi\rangle$ being in the state of eigenvalue m simplifies to $p(m) = \langle\psi|P_m|\psi\rangle$.

Identities

Some key identities are:

$$\begin{aligned}
&A = |\psi\rangle\langle\phi| \to A^\dagger = |\phi\rangle\langle\psi| \\
&(AB|\psi\rangle)^\dagger = \langle\psi|B^\dagger A^\dagger \\
&(A+B)^\dagger = A^\dagger + B^\dagger \\
&\operatorname{tr}(A \otimes B) = \operatorname{tr}(A)\operatorname{tr}(B) \\
&(f \otimes g)(u \otimes w) = f(u) \otimes g(w) \text{ for } f : U \to V \text{ and } g : W \to Z \\
&\operatorname{tr}_B([|a_1\rangle\langle a_1| \otimes |b_1\rangle\langle b_1|]) \equiv |a_1\rangle\langle a_1| \operatorname{tr}(|b_1\rangle\langle b_1|)
\end{aligned}$$

Key Theorems

Real Spectral Theorem

Any Hermitian operator M on a vector space V is diagonal with respect to some orthonormal basis for V and has real eigenvalues.

Simultaneous Diagonalization Theorem

Suppose A and B are Hermitian operators. Then $[A, B] = 0 \Longleftrightarrow \exists$ an orthonormal basis such that A and B are diagonal wrt that basis.

Observable Exponential

Let $\mathbf{v} \in \mathbb{R}^3$ be a real unit vector and let $\theta \in \mathbb{R}$. Then

$$\exp(i\theta\mathbf{v} \cdot \boldsymbol{\sigma}) = \cos(\theta)I + i\sin(\theta)\mathbf{v} \cdot \boldsymbol{\sigma}$$

No Cloning Theorem

It is impossible to create an independent and identical copy of an arbitrary unknown quantum state. This follows from the fact that given two states $|\psi\rangle$ and $|\varphi\rangle$, we can show that a unitary “cloning” operator implies $\langle\psi|\varphi\rangle \in \{0, 1\}$, meaning we can only copy states if they are the same or orthogonal.

Density Matrix Representation

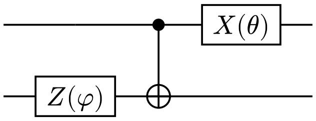
An arbitrary density matrix for a mixed state qubit may be written as

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

where $\mathbf{r}$ is a real three-dimensional vector such that $\|\mathbf{r}\| \leq 1$.

Quantum Circuits

Given a quantum circuit such as



with initial state $|\psi\rangle = \frac{1}{\sqrt{5}}(|01\rangle + 2|10\rangle)$, we start on the left and apply each unitary in succession as follows:

$$|\psi'\rangle = U_3U_2U_1|\psi\rangle$$

where

$$\begin{aligned} U_1 &= I \otimes Z(\varphi) = I \otimes \exp\left(-i\frac{\varphi}{2}\sigma_z\right) \\ U_2 &= \text{CNOT} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X \\ U_3 &= X(\theta) \otimes I = \exp\left(-i\frac{\theta}{2}\sigma_x\right) \otimes I. \end{aligned}$$

Note that a 50:50 beamsplitter is realized by a Hadamard gate.

Quantum Zeno Effect

In order to get predictable quantum states, we can repeatedly measure a state after a short time interval, collapsing it back to its initial state with high probability. If we have some small rotation

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

then the probability of measuring 0 for all time goes to 1 as $n \to \infty$.

Observables

An observable O is a physical property that can be measured. They are self-adjoint operators that assign values to outcomes of measurements, corresponding with eigenvalues of the operator. The expectaton of an observable represents the expected values of the measurement, which is a weighted sum of the probability of getting different measurements $p(m)$ multiplied by the value of each measurement $c(m) \in \mathbb{R}$

$$\mathbb{E}(O) = \langle \hat{O} \rangle = \sum_m c(m) \langle \psi | M_m^\dagger M | \psi \rangle = \langle \psi | \sum_m c_m M_m^\dagger M_m | \psi \rangle = \langle \psi | \hat{O} | \psi \rangle = \operatorname{tr}\Big(|\psi\rangle\langle\psi| \hat{O} \Big).$$

Note from probability theory, the standard deviation of an observable is given by $\sigma = \sqrt{\mathbb{E}(O^2) - \mathbb{E}(O)^2}$.

Notice $|\psi\rangle\langle\psi|$ is a measurement operator in the ψ basis.

Partial Trace

We can describe a subsystem of a joined quantum system using partial trace. For example, suppose we have physical systems A and B, whose state is described by a density operator ρ^{AB}. The reduced density operator is defined by

$$\rho^A \equiv \operatorname{tr}_B\left(\rho^{AB}\right)$$

where tr_B is a map of operators known as the partial trace over system B. This is defined by

$$\operatorname{tr}_B([|a_1\rangle\langle a_1| \otimes |b_1\rangle\langle b_1|]) \equiv |a_1\rangle\langle a_1| \operatorname{tr}(|b_1\rangle\langle b_1|)$$

where a_1, a_2 are vectors in the state space of A and b_1, b_2 are vectors in the state space of B. Notice $\operatorname{tr}(|b_1\rangle\langle b_2|) = \langle b_2 | b_1 \rangle$.

For example, if $\rho^{AB} = \rho \otimes \sigma$, then $\rho^A = \operatorname{tr}_B(\rho \otimes \sigma) = \rho \operatorname{tr}(\sigma) = \rho$, and similarly $\rho^B = \sigma$.

Given a pure Bell state, the corresponding density operator in the computational basis is

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

meaning if we trace out the second qubit,

$$\begin{aligned} \rho^1 &= \operatorname{tr}_2(\rho) \\ &= \frac{\operatorname{tr}_2(|00\rangle\langle 00|) + \operatorname{tr}_2(|11\rangle\langle 00|) + \operatorname{tr}_2(|00\rangle\langle 11|) + \operatorname{tr}_2(|11\rangle\langle 11|)}{2} \\ &= \frac{|0\rangle\langle 0|\langle 0|0\rangle + |1\rangle\langle 0|\langle 0|1\rangle + |0\rangle\langle 1|\langle 1|0\rangle + |1\rangle\langle 1|\langle 1|1\rangle}{2} \\ &= \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \frac{I}{2}. \end{aligned}$$

Environments

An arbitrary open quantum system can be described as an interaction between the system of interest and an environment, which together form a closed quantum system. Suppose we have a system in state ρ and sent it through a box coupled to an environment. Assume that the system-environment state is a product state, $\rho \otimes \rho_{\text{env}}$.

In this case the effect of the environment can be evaluated by tracing out the environmental system

$$\mathcal{E}(\rho) = \operatorname{tr}_{\text{env}}\left[U(\rho \otimes \rho_{\text{env}}) U^\dagger \right]$$

giving us the reduced state of the system alone, since the system no longer interacts with the environment after the transformation U.

In the special case where ρ and $|0\rangle$ go through a CNOT we have

$$\begin{aligned}
\mathcal{E}(\rho) &= \operatorname{tr}_{\text{env}}\left[U(\rho \otimes \rho_{\text{env}})U^\dagger\right] \\
&= \operatorname{tr}_{\text{env}}\left[\text{CNOT }(\rho \otimes \rho_{\text{env}})\text{CNOT}^\dagger\right] \\
&= \operatorname{tr}_{\text{env}}[(P_0 \otimes I + P_1 \otimes X)(\rho \otimes |0\rangle\langle 0|)(P_0 \otimes I + P_1 \otimes X)] \\
&= \operatorname{tr}_{\text{env}}[(P_0 \otimes |0\rangle + P_1 \otimes |1\rangle)(\rho \otimes I)(P_0 \otimes \langle 0| + P_1 \otimes \langle 1|)] \\
&= \operatorname{tr}_{\text{env}}[(P_0\rho P_0 \otimes |0\rangle\langle 0|) + (P_1\rho P_1 \otimes |1\rangle\langle 1|) + (P_0\rho P_1 \otimes |0\rangle\langle 1|) + (P_1\rho P_0 \otimes |1\rangle\langle 0|)] \\
&= P_0\rho P_0\langle 0|0\rangle + P_1\rho P_1\langle 1|1\rangle + P_0\rho P_1\langle 0|1\rangle + P_1\rho P_0\langle 1|0\rangle \\
&= P_0\rho P_0 + P_1\rho P_1
\end{aligned}$$

If they go through a CY gate,

$$\begin{aligned}
\mathcal{E}(\rho) &= \operatorname{tr}_{\text{env}}\left[U(\rho \otimes \rho_{\text{env}})U^\dagger\right] \\
&= \operatorname{tr}_{\text{env}}\left[CY(\rho \otimes \rho_{\text{env}})(CY)^\dagger\right] \\
&= \operatorname{tr}_{\text{env}}[(P_0 \otimes I + P_1 \otimes Y)(\rho \otimes |0\rangle\langle 0|)(P_0 \otimes I + P_1 \otimes Y)] \\
&= \operatorname{tr}_{\text{env}}[(P_0 \otimes I + P_1 \otimes (i|1\rangle\langle 0| - i|0\rangle\langle 1|))(\rho \otimes |0\rangle\langle 0|)(P_0 \otimes I + P_1 \otimes (i|1\rangle\langle 0| - i|0\rangle\langle 1|))] \\
&= \operatorname{tr}_{\text{env}}[(P_0 \otimes |0\rangle + P_1 \otimes (i|1\rangle))(\rho \otimes I)(P_0 \otimes \langle 0| + P_1 \otimes (-i\langle 1|))] \\
&= \operatorname{tr}_{\text{env}}[P_0\rho P_0 \otimes |0\rangle\langle 0| + P_1\rho P_1 \otimes |0\rangle\langle 0|] \\
&= P_0\rho P_0 + P_1\rho P_1
\end{aligned}$$

Operator Sum Representation

We can generalize this by introducing an orthonormal basis $|e_k\rangle$ for the state space of the environment, with $\rho_{\text{env}} = |e_0\rangle\langle e_0|$. There is no loss of generality associated with making this state pure, since if it is mixed, we can introduce an intermediary system purifying the state. Thus we can rewrite this

$$\begin{aligned}
\mathcal{E}(\rho) &= \operatorname{tr}_{\text{env}}\left[U(\rho \otimes \rho_{\text{env}})U^\dagger\right] \\
&= \sum_k \langle I \otimes e_k|U[\rho \otimes |e_0\rangle\langle e_0|]U^\dagger|I \otimes e_k\rangle \\
&= \sum_k \langle I \otimes e_k|U(I \otimes |e_0\rangle)\rho(I \otimes \langle e_0|)U^\dagger|I \otimes e_k\rangle \\
&= \sum_k E_k\rho E_k^\dagger
\end{aligned}$$

where $E_k \equiv \langle I \otimes e_k|U|I \otimes e_0\rangle$ is an operator on the state space of the principal system.

Quantum Algorithms

Deutsch’s Algorithm

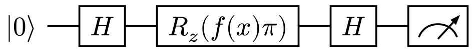
Suppose you are given a function $f : \{0, 1\} \to \{0, 1\}$ as a black box. You are promised that f is either of two cases:

1. CONST: f is constant, meaning $f(0) = f(1)$
2. BAL: f is balanced, meaning $f(0) \neq f(1)$.

The problem is to determine which of these two cases we have, using f as few times as possible.

Classically we can just use 2 queries to figure this out, i.e., just evaluate $f(0)$ and $f(1)$.

To solve this in quantum computing we need only 1 query: just use the Mach Zehnder interferometer



where

$$R_z(f(x)\pi) = \begin{pmatrix} (-1)^{f(0)} & 0 \\ 0 & (-1)^{f(1)} \end{pmatrix} = \begin{pmatrix} e^{i\pi f(0)} & 0 \\ 0 & e^{i\pi f(1)} \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi(f(1)-f(0))} \end{pmatrix}$$

where the equivalence is by a global phase. Then the evolution of the state is given by

$$\begin{aligned} HR_zH|0\rangle &= HR_z\frac{|0\rangle + |1\rangle}{\sqrt{2}} \\ &= H\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}} \\ &= \frac{(-1)^{f(0)}|+\rangle + (-1)^{f(1)}|-\rangle}{\sqrt{2}} \\ &= \frac{(-1)^{f(0)}\frac{|0\rangle+|1\rangle}{\sqrt{2}}}{\sqrt{2}} + \frac{(-1)^{f(1)}\frac{|0\rangle-|1\rangle}{\sqrt{2}}}{\sqrt{2}} \\ &= \frac{|0\rangle\left((-1)^{f(0)} + (-1)^{f(1)}\right)}{2} + \frac{|1\rangle\left((-1)^{f(0)} - (-1)^{f(1)}\right)}{2} \\ &\equiv \begin{cases} |0\rangle & f(0) = f(1) \\ |1\rangle & f(0) \neq f(1) \end{cases} \end{aligned}$$

up to a global phase.

Calculation Shortcuts

Trigonometry Identities

$$\begin{aligned} \sin(2\theta) &= 2\sin(\theta)\cos(\theta) \\ \cos(2\theta) &= \cos^2(\theta) - \sin^2(\theta) \\ &= 2\cos^2(\theta) - 1 \\ &= 1 - 2\sin^2(\theta) \\ \tan(2\theta) &= \frac{2\tan(\theta)}{1 - \tan^2(\theta)} \end{aligned}$$

$$\cos(\theta) = \frac{e^{i\theta} + e^{i\theta}}{2}, \quad \sin(\theta) = \frac{e^{i\theta} - e^{i\theta}}{2i}$$

Generalized Pure State

Let $|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle$ then we have that the density matrix ρ, for $|\psi\rangle$, is given by

$$\begin{aligned} \rho &= |\psi\rangle\langle\psi| \\ &= \left(\cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle\right)\left(\cos\left(\frac{\theta}{2}\right)\langle 0| + e^{-i\varphi}\sin\left(\frac{\theta}{2}\right)\langle 1|\right) \\ &= \cos^2\left(\frac{\theta}{2}\right)|0\rangle\langle 0| + \sin^2\left(\frac{\theta}{2}\right)|1\rangle\langle 1| + \cos\left(\frac{\theta}{2}\right)\sin\left(\frac{\theta}{2}\right)\left(e^{i\varphi}|1\rangle\langle 0| + e^{-i\varphi}|0\rangle\langle 1|\right) \\ &= \cos^2\left(\frac{\theta}{2}\right)|0\rangle\langle 0| + \sin^2\left(\frac{\theta}{2}\right)|1\rangle\langle 1| + \frac{\sin(\theta)}{2}\left(e^{i\varphi}|1\rangle\langle 0| + e^{-i\varphi}|0\rangle\langle 1|\right) \\ &= \begin{pmatrix} \cos^2\left(\frac{\theta}{2}\right) & \frac{e^{-i\varphi}}{2}\sin\left(\frac{\theta}{2}\right) \\ \frac{e^{i\varphi}}{2}\sin\left(\frac{\theta}{2}\right) & \sin^2\left(\frac{\theta}{2}\right) \end{pmatrix}. \end{aligned}$$