

Quantum Mechanics, Information, and Computing

Evan Petrosky

Abstract

Recently, I have begun the project of typing out my handwritten quantum notes and worked exercises. This document is still a work-in-progress. When completed, it will contain a basic introduction to quantum mechanics, quantum information, and quantum computing. Please let me know if you notice any typos or have any comments! Last updated October 2025.

Contents

1	Introduction to Quantum Mechanics	2
1.1	State Vectors	2
1.2	Density Operators	2
1.2.1	Properties of Density Operators	3
1.2.2	Partial Trace	3
2	Quantum Information	4
2.1	Von Neumann Entropy	4
2.2	Other Useful Quantities	4
2.2.1	Relative Entropy	4
2.2.2	Quantum Conditional Entropy	4
2.2.3	Quantum Mutual Information	5
3	Some Basic Math Concepts	5
3.1	Inner Product	5
3.2	Group Theory Primer	5
3.3	Number Theory	5
4	Getting Started with Quantum Circuits	6
4.1	Basic Single Qubit Gates	6
4.2	Basic Two Qubit Gate: Controlled-NOT (CNOT)	6
4.3	Other Circuit Symbols	7
4.4	Hadamard Transform on n-qubits ($H^{\otimes n}$)	7
4.5	Quantum Fourier Transform (QFT)	8
4.6	Phase Estimation	8
5	Worked Examples	8
5.1	Problem 1: The No-Cloning Theorem	8
5.2	Problem 2: Measuring an Operator	10
5.3	Problem 3: The Toffoli (CCNOT) Gate	11
5.4	Problem 4: Deutsch-Jozsa (DJ) Algorithm	12
5.5	Problem 5: Bernstein-Vazirani Algorithm	12
6	References	13

1 Introduction to Quantum Mechanics

Quantum mechanics can be formulated in different ways. In this section, I recount the postulates of quantum mechanics using the language of both state vectors and density operators. In this section I follow the presentation in QCQI (see references list)

1.1 State Vectors

In this section, I focus on the postulates of quantum mechanics in the language of state vectors.

- **Postulate 1:** A system can be completely described by a unit vector (i.e. state vector) in its state space. A state space is a complex vector space with an inner product (i.e. Hilbert space) associated to any isolated physical system.
- **Postulate 2:** The evolution of a closed quantum system is described by a unitary transformation. If $|\psi\rangle$ is the state of a closed system at time t_1 and the state of the same closed system at t_2 is given by $|\psi'\rangle$ then we know that $|\psi'\rangle = U|\psi\rangle$ where U is some unitary transformation ($U^\dagger U = \mathbb{I}$).
- **Postulate 3:** Quantum measurements are described by a collection $\{M_m\}$ of measurement operators where m indicates the possible outcomes that may occur in the measurement and $\sum_m M_m^\dagger M_m = \mathbb{I}$ (ensures probabilities sum to one). Suppose that the system prior to measurement is in state $|\psi\rangle$. Then the probability of getting m is $p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle$ and the post-measurement state of the system is

$$|\psi_{new}\rangle = \frac{M_m |\psi\rangle}{\sqrt{\langle\psi| M_m^\dagger M_m |\psi\rangle}}. \quad (1)$$

One common example would be having our two measurement operators being the projectors onto the computational basis $M_0 = |0\rangle\langle 0|$ and $M_1 = |1\rangle\langle 1|$

- **Postulate 4:** The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. E.g. if we have a system of two qubits prepared in states $|\psi_1\rangle$ and $|\psi_2\rangle$ the total system state is $|\psi_1\rangle \otimes |\psi_2\rangle$.

Note that sometimes, the following will be said in lieu of postulate 2: The time evolution of the state of a closed quantum system is described by Schrodinger's equation

$$i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle \quad (2)$$

where $\hbar$ is Planck's constant and H is a hermitian operator known as the Hamiltonian. This is equivalent to postulate two above because the solution to Schrodinger's equation is

$$|\psi(t_2)\rangle = \exp\left(\frac{-iH(t_2 - t_1)}{\hbar}\right) \equiv U(t_1, t_2) |\psi(t_1)\rangle \quad (3)$$

where U is a unitary operator defined by the second equality. Any unitary operator can be expressed in the form $U = e^{iK}$ for some Hermitian operator K

1.2 Density Operators

Another way to formulate quantum mechanics is in terms of the density operator ρ . The density operator is a positive operator (i.e. $\langle\varphi|\rho|\varphi\rangle \geq 0$ for any φ) and satisfies $\text{tr}(\rho) = 1$. In terms of the state vector approach, the density operator can be written

$$\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i| \quad (4)$$

where $|\psi_i\rangle$ denote different quantum states and p_i is the probability of being in that state.

The density operator will be particularly useful for our circumstances because it provides a clear way to talk about quantum systems that are subsystems of larger systems.

The postulates of quantum mechanics can be rephrased in terms of the density operator.

- **Postulate 1:** An quantum system can be completely described by its density operator ρ acting on the state space. A state space is a complex vector space with an inner product (i.e. Hilbert space) associated to any isolated physical system. Suppose a system is in state ρ_i with probability p_i . Then the density operator is $\sum_i p_i \rho_i$.
- **Postulate 2:** The evolution of a closed quantum system is described by a unitary transformation. Suppose ρ is the state of the system at t_1 , ρ' is the state of the system at t_2 , and $U = U(t_1, t_2)$ is a unitary operator. The relation between these is given by

$$\rho' = U \rho U^\dagger \quad (5)$$

- **Postulate 3:** Quantum measurements are described by a collection $\{M_m\}$ of measurement operators where m indicates the possible outcomes that may occur in the measurement and $\sum_m M_m^\dagger M_m = \mathbb{I}$ (ensures probabilities sum to one). Suppose that the pre-measurement state of the system is described by ρ . The probability of result m is

$$p(m) = \text{tr}(M_m^\dagger M_m \rho) \quad (6)$$

and the final state ρ_f is given by

$$\rho_f = \frac{M_m \rho M_m^\dagger}{\text{tr}(M_m^\dagger M_m \rho)}. \quad (7)$$

- **Postulate 4:** The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. For example, if we have a composite system composed of two component systems the total state is $\rho = \rho_1 \otimes \rho_2$.

1.2.1 Properties of Density Operators

Here are some important facts about density operators:

- **Hermitian:** $\rho = \rho^\dagger$.
- **Positive Semidefinite:** $\langle \psi | \rho | \psi \rangle \geq 0$ for any state $|\psi\rangle$. All eigenvalues are non-negative.
- **Unit Trace:** $\text{Tr}(\rho) = 1$.
- **Decomposition:** Given ρ there exists an orthonormal basis $\{|p_a\rangle\}_{a=1}^d$ such that $\rho = \sum_a p_a |p_a\rangle \langle p_a|$ and $p_a \geq 0$ and $\sum_a p_a = 1$.
- **Measurement Probabilities:** If $\{\Lambda_k\}_{k=1}^K$ is a complete set of projectors (i.e. $\sum_i \Lambda_i = \mathbb{I}$) describing a set of measurement outcomes, the probability of outcome i is $\text{Tr}(\rho \Lambda_i)$.
- **Expectation Values:** The expectation value of an operator $\mathcal{O}$ is given by $\langle \mathcal{O} \rangle = \text{Tr}(\rho \mathcal{O})$.
- **Pure and Mixed States:** ρ represents a pure state if and only if only one p_a is non-zero and equal to 1 i.e. the state can be written $\rho = |\psi\rangle \langle \psi|$. This is equivalent to the condition $\text{Tr}(\rho^2) = 1$. A state is mixed if $\text{Tr}(\rho^2) < 1$.

1.2.2 Partial Trace

Consider a two part system denoted AB . The partial trace with respect to system B is the linear map $\text{Tr}_B : \mathcal{L}(\mathcal{H}_{AB}) \rightarrow \mathcal{L}(\mathcal{H}_A)$ whose action on an operator $\mathcal{O}_{AB}$ is given in terms of an orthonormal basis of $\mathcal{H}_B$ $\{|\mu\rangle_B\}$ by

$$\text{Tr}_B \mathcal{O}_{AB} = \sum_{\mu=1}^{d_b} {}_B \langle \mu | \mathcal{O}_{AB} | \mu \rangle_B. \quad (8)$$

In particular, this is used to define the reduced density operator:

$$\rho_A = \text{Tr}_B(\rho_{AB})$$

2 Quantum Information

2.1 Von Neumann Entropy

The Von Neumann entropy of a quantum state ρ is defined as:

$$S(\rho) = -\text{Tr}(\rho \log \rho)$$

Properties:

- $0 \leq S(\rho) \leq \log d$, where d is the dimension of the Hilbert space.
- $S(\rho) = 0$ if and only if ρ is a pure state.
- $S(\rho) = \log d$ achieved for the the maximally mixed state, $\rho = \frac{1}{d}I$.
- Let $|\psi\rangle_{AB} \in \mathcal{H}_{AB}$ be a pure state and $\rho_A = \text{Tr}_B |\psi\rangle_{AB} \langle \psi|$ and $\rho_B = \text{Tr}_A |\psi\rangle_{AB} \langle \psi|$. Then $S(\rho_A) = S(\rho_B)$.
- $S(\rho_A)$ and $S(\rho_B)$ are called *entanglement entropies*.
- $S(\rho_A) = S(\rho_B) = 0$ if and only if A and B are unentangled and $|\psi\rangle_{AB} = |\phi\rangle_A \otimes |\chi\rangle_B$
- $S(U\rho U^\dagger) = S(\rho)$ for any unitary operator U

Important inequalities obeyed by Von Neumann Entropies:

- Subadditivity: $S(\rho_{AB}) \leq S(\rho_A) + S(\rho_B)$. This means that the entropy of the whole system is less than or equal to the sum of the entropies of the smaller, component systems.
- Araki-Lieb: $|S(\rho_A) - S(\rho_B)| \leq S(\rho_{AB})$. This means that the difference in entropy of the smaller subsystems is less than or equal to the entropy of the combined system
- Strong Subadditivity: $S(\rho_{AB}) + S(\rho_{BC}) \geq S(\rho_{ABC}) + S(\rho_B)$

2.2 Other Useful Quantities

2.2.1 Relative Entropy

Let ρ, σ be density matrices on the same Hilbert Space. Relative entropy is defined via

$$D(\rho||\sigma) = \text{Tr}(\rho \log \rho) - \text{Tr}(\rho \log \sigma) \quad (9)$$

It has the following properties:

- Positive $D(\rho||\sigma) \geq 0$ with equality if and only if $\rho = \sigma$
- Pinsker's Inequality $D(\rho||\sigma) \geq \frac{1}{2\log 2} \|\rho - \sigma\|_1^2$ where $\|\mathcal{O}\|_1 \equiv \text{Tr}\sqrt{\mathcal{O}^\dagger \mathcal{O}}$. In this sense, relative entropy can be thought of as an upper bound on the distinguishability of two states.

2.2.2 Quantum Conditional Entropy

Let AB be a bipartate system. We define the quantum conditional entropy as

$$H(A|B) = S_{AB} - S_B. \quad (10)$$

Classically, we could interpret this as the remaining entropy once B is known i.e. what B still does not know. This can be less than zero in quantum theory.

2.2.3 Quantum Mutual Information

We define the mutual information as

$$I(A; B) = S(\rho_A) + S(\rho_B) - S(\rho_{AB}) \quad (11)$$

Note that we have the following equality

$$S(AB) = H(A|B) + I(A; B) + H(B|A). \quad (12)$$

The classical interpretation of the ingredients of this equation are as follows

- $S(AB)$ - Information content of the whole system
- $H(A|B)$ - What B doesn't know
- $I(A; B)$ - Shared information
- $H(B|A)$ - What A doesn't know.

3 Some Basic Math Concepts

3.1 Inner Product

Suppose we have two vector spaces V and W . Then the inner product on the tensor product $V \otimes W$ is

$$\left(\sum_i a_i |v_i\rangle \otimes |w_i\rangle, \sum_j b_j |v'_j\rangle \otimes |w'_j\rangle \right) \equiv \sum_{ij} a_i^* b_j \langle v_i | v'_j \rangle \langle w_i | w'_j \rangle \quad (13)$$

3.2 Group Theory Primer

A group is a nonempty set G with a binary group multiplication operation. It must have closure, associativity, an identity, and the existence of inverses.

The order of a finite group is the number of elements it contains. This is denoted $|G|$. A group is abelian if all its elements commute. A subgroup H of G is a subset of G that forms a group under the same group multiplication operation as G .

A set of elements $g_1, \dots, g_l$ of a group G is said to generate the group if every element of G can be written as a product of (possibly repeated) elements from the list $g_1, \dots, g_l$. This is denoted $G = \langle g_1, \dots, g_l \rangle$. If G has size $|G|$ then there exists a set of $\log |G|$ generators generating G .

The Clifford group is generated by H , S , and $CNOT$. The Gottesman–Knill theorem tells us that quantum circuits that consist only of Clifford gates can be efficiently simulated by a classical computer.

3.3 Number Theory

Here are some relevant number theory facts and definitions:

- **The Integers:** Recall that the integers are positive and negative whole numbers and zero $\{\dots, -2, -1, 0, 1, 2, \dots\}$. We say that d divides n when there exists $k \in \mathbb{Z}$ such that $n = kd$
- **Modular Arithmetic:** This is the arithmetic of remainders. For positive integers x, n , we can write $x = kn + r$, where k is a non-negative integer and $r \in \{0, 1, \dots, n-1\}$ is the remainder. We write this as $x \equiv r \pmod{n}$.
- **Fundamental Theorem of Arithmetic:** Let a be any integer greater than 1. Then a has a prime factorization of the form:

$$a = P_1^{a_1} P_2^{a_2} \dots P_n^{a_n} \quad (14)$$

where $P_1, \dots, P_n$ are distinct prime numbers and $a_1, \dots, a_n$ are positive integers. This prime factorization is unique up to the order of the factors.

- **Greatest Common Divisor (GCD):** The GCD of two integers a and b , denoted $\gcd(a, b)$, is the largest integer that divides both a and b . If $\gcd(a, b) = 1$, a and b are said to be coprime.
- **Multiplicative Inverse:** Let n be an integer greater than 1. An integer a has a multiplicative inverse modulo n (i.e. there exists a b such that $ab = 1 \pmod{n}$) if and only if $\gcd(a, n) = 1$.
- **Euclid's Algorithm:** A method for finding the GCD of two integers. It uses the following theorem: Let a and b be integers and let r be the remainder when a is divided by b . Then, provided $r \neq 0$, $\gcd(a, b) = \gcd(b, r)$.
- **Order Finding:** Suppose N is a positive integer coprime to x (i.e. $\gcd(x, N) = 1$) where $1 \leq x \leq N$. The order of x modulo N is the smallest positive integer r such that $x^r = 1 \pmod{N}$. The order finding problem is to determine r given x and N ($\text{ord}_N(x) = r \iff x^r = 1 \pmod{N}$). Order finding and factoring are closely related.

4 Getting Started with Quantum Circuits

4.1 Basic Single Qubit Gates

Computational Basis: $|0\rangle \leftrightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle \leftrightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Gate	Symbol	Matrix Representation	Notes
Hadamard	H	$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	$H^2 = \mathbb{I}$, $H = \frac{X+Z}{\sqrt{2}}$
Pauli-X	X	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	"Spin Flip", $X^2 = \mathbb{I}$
Pauli-Y	Y	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	$Y^2 = \mathbb{I}$
Pauli-Z	Z	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	Flips sign of $ 1\rangle$, $Z^2 = \mathbb{I}$
Phase	S	$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$	$S^2 = Z$
$\pi/8$ Gate	T	$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$	$T^2 = S$

Useful Identities: $HZH = X$, $HYH = -Y$, $XYX = -Y$

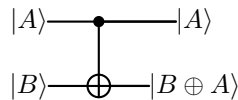
4.2 Basic Two Qubit Gate: Controlled-NOT (CNOT)

The first qubit is the control, the second is the target.

Matrix Representation:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad (15)$$

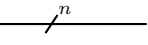
Circuit Diagram (top qubit is control, bottom is target):



Summary of Functionality:

- Does nothing to control
- If control = $|0\rangle$, it does nothing to the target.
- If control = $|1\rangle$, it flips the target.

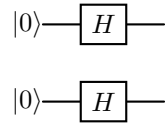
4.3 Other Circuit Symbols

- Measurement:  (i.e. projection onto $|0\rangle$ and $|1\rangle$)
- Qubit:  (can think of time as running left to right)
- Classical Bit: 
- n qubits: 

4.4 Hadamard Transform on n-qubits ($H^{\otimes n}$)

This refers to n Hadamard gates acting in parallel on n qubits.

For example, consider the case $n = 2$ with two qubits initialized in state $|0\rangle$.



produces

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \quad (16)$$

Generalizing, for action on n qubits initialized in $|0\rangle$ we have

$$H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$$

where x runs over all possible combos of strings of 1's and 0's of length n . We see that, starting from all states in $|0\rangle$, the Hadamard transform produces an equal superposition of all computational basis states.

What about if we apply the Hadamard Transform on an arbitrary n -qubit initial state?

First, we note that for a single basis state, you can succinctly write the action of the Hadamard as

$$H |x\rangle = \frac{1}{\sqrt{2}} \sum_Z (-1)^{x \cdot Z} |Z\rangle \quad (17)$$

where $Z = 0, 1$.

Explicitly, we have

$$x = 0 \quad H |0\rangle = \frac{1}{\sqrt{2}} \sum_Z (-1)^0 |Z\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad (18)$$

$$x = 1 \quad H |1\rangle = \frac{1}{\sqrt{2}} \sum_Z (-1)^Z |Z\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad (19)$$

This means that for an arbitrary input state $|x\rangle \in \{0,1\}^n$ (can be inferred from above using linearity)

$$H^{\otimes n} |x_1, \dots, x_n\rangle = \frac{1}{\sqrt{2^n}} \sum_{z_1, \dots, z_n} (-1)^{x_1 z_1 + \dots + x_n z_n} |z_1, \dots, z_n\rangle \equiv \frac{1}{\sqrt{2^n}} \sum_z (-1)^{x \cdot z} |z\rangle \quad (20)$$

where $x \cdot z$ is the bitwise inner product, modulo 2.

Note: We will be using modular arithmetic. For example $2 = 5 = 8 = 11 \pmod{3}$ because the remainder for all of these numbers divided by 3 is 2. We will use $\oplus$ to denote modulo 2 addition.

4.5 Quantum Fourier Transform (QFT)

We begin by introducing some notation. Consider a n qubit system. Let $N = 2^n$. Our basis to describe the system is $j \in (0, \dots, N-1) \in \{0, 1\}^n$. We can represent $|j\rangle$ using binary representation $j = j_1 j_2 \dots j_n$ which is interpreted to mean $j = j_1 2^{n-1} + j_2 2^{n-2} + \dots + j_n 2^0$.

We can also just binary decimals $0.j_1 j_2 \dots j_n$ to mean $\frac{1}{2}j_1 + \frac{1}{4}j_2 + \dots + \frac{1}{2^{n-1}}j_n$.

The QFT¹ is a unitary transformation on n qubits that maps a computational basis state $|j\rangle$ to a superposition of all basis states. For an $N = 2^n$ dimensional space:

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

The QFT can also be written in the following product representation

$$\text{QFT } |j_1 \dots j_n\rangle = \frac{1}{2^{n/2}} (|0\rangle + e^{2\pi i 0.j_n} |1\rangle) (|0\rangle + e^{2\pi i 0.j_{n-1} j_n} |1\rangle) \dots (|0\rangle + e^{2\pi i 0.j_1 \dots j_n} |1\rangle)$$

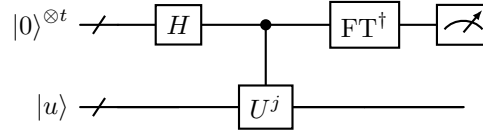
where we have used the binary decimals defined above.

4.6 Phase Estimation

Given a unitary operator U with an eigenvector $|u\rangle$ and corresponding eigenvalue $e^{2\pi i \varphi}$, the quantum phase estimation algorithm finds an estimate of the phase φ .

We assume that we have a black box which can perform a controlled U^{2^j} and prepares state $|u\rangle$.

Here is a schematic of a circuit that solves this problem:



The procedure is as follows

1. Initialize the state to $|0\rangle |u\rangle$.
2. Apply Hadamard gates to the first qubits: $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle |u\rangle$.
3. Apply a series of controlled- U^{2^k} operations for $k = 0, \dots, t-1$. The final state is $\frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} e^{2\pi i j \varphi} |j\rangle |u\rangle = |\tilde{\varphi}\rangle |u\rangle$.
4. Apply the inverse QFT to the first register and measure to get an estimate of φ .

5 Worked Examples

In this section, I work through some illustrative examples.

5.1 Problem 1: The No-Cloning Theorem

(Adapted from D. Stanford and F. Larsen)

¹For fellow particle physicists - for these notes QFT will predominantly mean Quantum Fourier Transform NOT Quantum Field Theory.

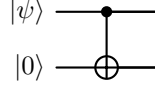
a) CNOT cloning for basis states

Consider a qubit in state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Show that for U equal to the CNOT operator (with first qubit as control and the second qubit as the target),

$$U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle \quad (21)$$

for both $|\psi\rangle = |0\rangle$ and $|\psi\rangle = |1\rangle$.

The circuit can be represented pictorially as:



- **Case 1:** $|\psi\rangle = |0\rangle$

The CNOT does not act on the second qubit, and the final state is $|0\rangle \otimes |0\rangle = |\psi\rangle \otimes |\psi\rangle$.

- **Case 2:** $|\psi\rangle = |1\rangle$

The CNOT does act on the second qubit, and the final state is $|1\rangle \otimes |1\rangle = |\psi\rangle \otimes |\psi\rangle$.

For a general state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$:

$$\begin{aligned} U_{\text{CNOT}}(|\psi\rangle \otimes |0\rangle) &= U_{\text{CNOT}}[\alpha|00\rangle + \beta|10\rangle] \\ &= \alpha|00\rangle + \beta|11\rangle \end{aligned}$$

But $|\psi\rangle \otimes |\psi\rangle = \alpha^2|00\rangle + \alpha\beta|01\rangle + \beta\alpha|10\rangle + \beta^2|11\rangle$. These are only equal if $\alpha = 1, \beta = 0$ OR $\beta = 1, \alpha = 0$. We will explore this more in the following part of the problem.

b) General Proof of the No-Cloning Theorem

Show that no linear operator U can accomplish this task for arbitrary $|\psi\rangle$ i.e. that no linear operator can copy a general unknown wavefunction $|\psi\rangle$ into two copies of itself $|\psi\rangle \otimes |\psi\rangle$ i.e. prove the no-cloning theorem. (the following proof follows that of QCQI)

Suppose that there was such an operator. That is, we had a unitary operator U that can clone any arbitrary quantum state $|\psi\rangle$ and $|\phi\rangle$ from a pure, normalized state $|s\rangle$. Let's take the inner product of these two equations. Remember that $U^\dagger U = \mathbb{I}$ by unitarity.

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle \quad (22)$$

$$U(|\phi\rangle \otimes |s\rangle) = |\phi\rangle \otimes |\phi\rangle \quad (23)$$

Taking the inner product of these two equations:

- LHS: $\langle\phi| \langle s| U^\dagger U |\psi\rangle |s\rangle = \langle\phi|\psi\rangle \langle s|s\rangle = \langle\phi|\psi\rangle$
- RHS: $(\langle\phi| \langle\phi|)(|\psi\rangle |\psi\rangle) = \langle\phi|\psi\rangle \langle\phi|\psi\rangle = (\langle\phi|\psi\rangle)^2$

Equating them gives $\langle\phi|\psi\rangle = (\langle\phi|\psi\rangle)^2$, which has two solutions:

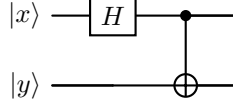
1. $\langle\phi|\psi\rangle = 1 \implies |\phi\rangle = |\psi\rangle$
2. $\langle\phi|\psi\rangle = 0 \implies |\phi\rangle \perp |\psi\rangle$

This means that a general quantum cloning device can only clone states which are orthogonal to each other. No linear, unitary operator can copy a generic wavefunction into two copies of itself.

c) Circuit to create a Bell state

Draw a quantum circuit that transforms a “baseline” state $|00\rangle$ into the maximally entangled state $|MAX\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Sometimes $|MAX\rangle$ is denoted β_{00} . It is one of 4 “bell states”. They can be created by the following circuit.



which produces final state $|\beta_{xy}\rangle$

Explicitly, for initial state $|00\rangle$ we have

$$|00\rangle \xrightarrow{H \otimes \mathbb{I}} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |MAX\rangle$$

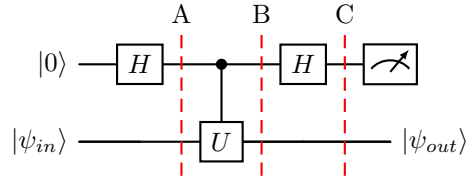
The other three bell states can be produced by the same circuit but with initial states $|01\rangle, |10\rangle, |11\rangle$

5.2 Problem 2: Measuring an Operator

(Problem adapted from QCQI and F. Larsen)

Consider a single-qubit operator U with eigenvalues ± 1 . The operator is both unitary and hermitian so it's both an observable and quantum gate. Unitarity + Hermiticity means $U^\dagger U = U^2 = \mathbb{I}$. We seek to measure the observable U yielding a result that indicates one of the two eigenvalues as well as leaving a post measurement state which is the corresponding eigenvector.

We will show that the following quantum circuit solves this problem



The state evolution is as follows:

Initial: $|0\rangle \otimes |\psi_{in}\rangle$

At (A): $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |\psi_{in}\rangle = \frac{1}{\sqrt{2}}(|0\psi_{in}\rangle + |1\psi_{in}\rangle)$

At (B): $\frac{1}{\sqrt{2}}(|0\rangle \otimes |\psi_{in}\rangle + |1\rangle \otimes U|\psi_{in}\rangle)$

At (C): $\frac{1}{2}((|0\rangle + |1\rangle)|\psi_{in}\rangle + (|0\rangle - |1\rangle)U|\psi_{in}\rangle) = \frac{1}{2}(|0\rangle(|\psi_{in}\rangle + U|\psi_{in}\rangle) + |1\rangle(|\psi_{in}\rangle - U|\psi_{in}\rangle))$

Now, we measure the control qubit.

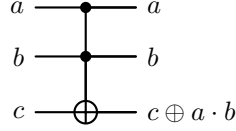
- **If we measure $|0\rangle$:** The post-measurement state is $|\psi_{out}\rangle = (U + \mathbb{I})|\psi_{in}\rangle$. Applying U shows that this is an eigenvector with eigenvalue $+1$.
- **If we measure $|1\rangle$:** The post-measurement state is $|\psi_{out}\rangle = (U - \mathbb{I})|\psi_{in}\rangle$. Applying U shows that this is an eigenvector with eigenvalue -1 .

Thus, circuit achieves the desired task.

5.3 Problem 3: The Toffoli (CCNOT) Gate

(Problem adapted from D. Stanford and F. Larsen)

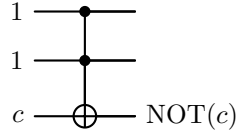
In this example, we will work with the Toffoli gate. The Toffoli gate flips the target bit c if and only if the control bits a and b are both 1. Pictorially, we can represent the Toffoli gate as



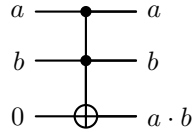
Three of the standard logical operations on a classical computer are NOT, AND, and COPY (FANOUT). In this example, we will show that the Toffoli gate can simulate these gates. We will show how to encode the classical input bit(s) into the three qubits that are inputs to the Toffoli quantum gate, and how to read the classical output bit(s) from the three outputs of the Toffoli gate.

a) Simulating Classical Gates

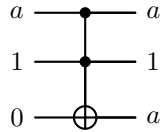
- **NOT Gate:** Classically, transforms a single classical bit into the other possible value. Set controls $a = 1, b = 1$. The target c becomes $c \oplus 1 = \text{NOT}(c)$.



- **AND Gate:** Classically, takes two input bits, a and b and transforms into a single output with value 1 if $a = b = 1$ or 0 otherwise. Set target $c = 0$. The third output wire will be $a \cdot b$.



- **COPY (FANOUT) Gate:** Classically, this takes a single bit a and transforms it into two output bits that both take the value a . Set control $b = 1$ and target $c = 0$. The first and third wires will both output a .



b) Toffoli Gate Decomposition and Matrix Form

The Toffoli gate can be represented as an 8×8 matrix.

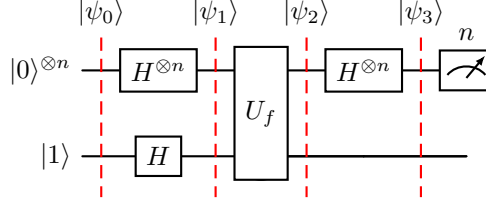
$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \quad (24)$$

It can also be decomposed in terms of standard gates such as H , T , and $CNOT$.

5.4 Problem 4: Deutsch-Jozsa (DJ) Algorithm

Problem: Suppose we have a black box $f(x) : \{0, 1\}^{\otimes n} \rightarrow \{0, 1\}$ and we know that $f(x)$ is either (1) constant or (2) balanced with $f(x) = 0, 1$ with a 50-50 split. Determine with certainty whether $f(x)$ is in case (1) or case (2).

This problem is solved by the following circuit:



Let's see how this works by tracking the evolution of the state vectors throughout the circuit. The first two steps are as follows:

- $|\psi_0\rangle = |0\rangle^{\otimes n} |1\rangle$
- $|\psi_1\rangle = \sum_{x \in \{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$

Now, we evaluate the black box. $U_f |a, b\rangle \rightarrow |a, b \oplus f(x)\rangle$. In this case, $a \sim \sum_{x \in \{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}}$ and $b \sim \frac{|0\rangle - |1\rangle}{\sqrt{2}}$. We can think about evaluating this separately for each $|x\rangle$. There are two possibilities.

- If $f(x) = 0 \implies b \rightarrow b$
- If $f(x) = 1 \implies b \rightarrow b \oplus 1 = -b$

We can write this as

$$|\psi_2\rangle = \sum_{x \in \{0,1\}^n} \frac{(-1)^{f(x)} |x\rangle}{\sqrt{2^n}} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \quad (25)$$

The final step is to evaluate the final set of n Hadamards. This acts on each n qubit basis state $|x\rangle$ in the sum.

$$|\psi_3\rangle = \sum_z \sum_x \frac{(-1)^{x \cdot z + f(x)} |z\rangle}{2^n} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \quad (26)$$

In the DJ algorithm, one observes the top qubits. By projecting onto $|0\rangle^{\otimes n}$ you pick out the $z = 0$ state with amplitude $\frac{1}{2^n} \sum_x (-1)^{f(x)}$. Depending on what we measure, we can solve our initial problem.

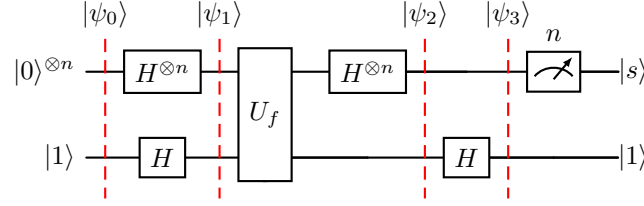
Explicitly,

- If $f = \text{constant}$ this means that all 2^n terms in the sum contribute either ± 1 so the final amplitude is $\frac{\pm 2^n}{2^n} = \pm 1$. This in turn means that all other amplitudes will be zero and our observation will yield 0s for all the qubits in the upper line.
- Alternatively, if $f = \text{balanced}$ then the amplitude projecting onto $|0\rangle^{\otimes n}$ will be zero and a measurement must yield a nonzero result for at least one qubit in the top register.

5.5 Problem 5: Bernstein-Vazirani Algorithm

Problem: We have a function f that maps a set of n qubits to one qubit $f(x) : \{0, 1\}^{\otimes n} \rightarrow \{0, 1\}$. The function takes the form $f(x) = s \cdot x \pmod{2}$. $s \in \{0, 1\}^{\otimes n}$ is unknown. We want to find a quantum circuit that finds s with a single call to the U_f gate.

We can use the DJ algorithm above as inspiration. The following circuit solves this problem



It is basically the DJ circuit plus an extra Hadamard on the bottom qubit.

Let's see how this works. From the DJ algorithm above, we know that

$$|\psi_2\rangle = \sum_z \sum_x \frac{(-1)^{x \cdot (z+s)}}{2^n} |z\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \quad (27)$$

where I have taken Eq. 26 and substituted in $f(x) = x \cdot s$.

Now, we apply a $H^{-1} = H$ to the bottom qubit state to simplify. We have

$$|\psi_3\rangle = \sum_z \sum_x \frac{(-1)^{x \cdot (z+s)}}{2^n} |z\rangle |1\rangle \quad (28)$$

Let's now perform the sum over x . For this sum $(z+s)$ is constant. If $z+s=0$, then the sum over x is 1. Instead if $z+s \neq 0$ then the sum over x will yield zero because the number of $+1$ and -1 contributions will cancel out. Therefore, the only nonzero contribution to the above sum is when $z \oplus s = 0 \implies z = s$. This means we can write

$$|\psi_3\rangle = |s\rangle |1\rangle. \quad (29)$$

By making a measurement in the computational basis of the top n qubits we can figure out $|s\rangle$.

6 References

These notes are based primarily on the following references:

- Quantum Computation and Quantum Information (10th Anniversary Edition) by Nielsen and Chuang (QCQI)
- Lecture notes by F. Larsen and D. Stanford
- Quantum Information for Particle Theorists by Lykken