

PHY365 Final Exam Revision

Aditya K. Rao 1008307761

*University of Toronto**

(Dated: April 25, 2024)

CONTENTS		III. Problem Set Questions	12
I. Definitions	3	A. Problem Set One	12
A. Dirac Notation of Qubits in this Course	3	1. Question One: Eigenvalues and Properties of Pauli Matrices	12
B. Reading Circuit Diagrams	3	2. Question Two: Playing with Pauli Matrices	12
1. Unitary & Pauli Gates	3	3. Question Three: Verifying a Matrix is Unitary	13
2. Measurement Operations	3	B. Problem Set 2	13
3. Controlled Unitaries	3	1. Question One: Looking at the Bloch Sphere	13
4. Example: Quantum Teleportation	3	2. Question Two: Unitary Operations on the Bloch Sphere	13
II. Concepts	4	C. Problem Set 3	13
A. Fundamentals	4	1. Question One: Evaluating Concurrence	13
1. Single Qubit Gates	4	2. Question Two: The SWAP gate	14
2. Two Qubit Gates	4	D. Problem Set 4	14
B. Time Evolution	5	1. Question One: Proving Circuit Identities	14
1. Bell's Inequalities	5	2. Question Two: The Griffiths-Niu Theorem	14
2. Hidden variables and why they don't work	5	3. Question Three: Simplifying The Quantum Teleportation Circuit	15
C. Schmidt Decomposition Theorem	6	E. Problem Set 5	15
D. Teleportation & No Cloning Theorem	7	1. Question One: Introduction to Oracles	15
E. Quantum Fourier Transform	7	2. Question Two: Using Qubit to Store Binary	16
1. Binary Notation	7	F. Problem Set 6	16
2. Quantum Parallelism	7	1. Question One: Using the Discrete Fourier Transform	16
3. Discrete Fourier Transform	7	2. Question Two: Finding and Plotting Frequencies using the Discrete Fourier Transform	17
F. Algorithms	8	3. Question Three: The Quantum Fourier Transform	17
1. Deutsch-Jozsa Algorithm	8	G. Problem Set 7	17
2. Bernstein-Vazariani Algorithm	9	1. Question One: Generalizing Controlled Unitaries	17
3. Grover's Algorithm	9	2. Question Two: Generalizing Unitaries Analytically	17
4. Shor's Algorithm	9	H. Problem Set 8	17
G. Quantum Error Correction	9		
H. Error Correcting Codes	10		
I. Decoherence Free Spaces	10		
J. Quantum Key Distribution	10		
K. Device Physics	10		
1. DiVincenzo's Requirements for a Physical Quantum Computer	10		
2. Methods of Physical Implementation	10		
3. Temperature Bound	11		
4. Time Evolution	11		

* Date: April 25, 2024

1. Question One: Time Dependence in Quantum Information	18
2. Question Two: Solving the Equations of Motion for Quantum States	18
I. Extra Problems	18
1. Question One: Quantum Fourier Transform	18
2. Question Two: Quantum Fourier Transform	19
3. Question Three: Quantum Fourier Transform	19
4. Question Four: Quantum Fourier Transform	19
5. Question Five: Quantum Fourier Transform	19
IV. Midterm Questions	19
A. Midterm One	19
1. Question One: Unitaries in \mathbb{C}^2	19
2. Question Two: Tracing Circuits	19
B. Midterm Two	20
1. Question One	20
2. Question Two: Base 10 in Quantum States	20
V. Equations & Formulas	20
A. Concurrence and Schmidt Decomposition	20
1. Pauli Matrices	21
B. Fourier Transform	21
VI. Theorems	21
References	22

I. DEFINITIONS

A. Dirac Notation of Qubits in this Course

B. Reading Circuit Diagrams

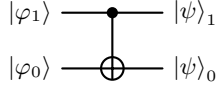


FIG. 1: Controlled not gate, the control is the black dot and the target is the \oplus . The $\oplus = \hat{X}$ by convention. The output is no longer necessarily a pure state.

1. Unitary & Pauli Gates

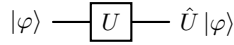


FIG. 2: Local unitary (substitute U for X , Y , Z , or H for the desired unitary)

a. Generic Unitary Gate

b. Pauli-X Gate

$$\hat{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{cases} \hat{X} |0\rangle = |1\rangle \\ \hat{X} |1\rangle = |0\rangle \end{cases}$$

c. Pauli-Z Gate

$$\hat{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{cases} \hat{Z} |0\rangle = |0\rangle \\ \hat{Z} |1\rangle = -|1\rangle \end{cases}$$

d. Pauli-Y Gate

$$\hat{Y} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{cases} \hat{Y} |0\rangle = i |1\rangle \\ \hat{Y} |1\rangle = |0\rangle \end{cases}$$

e. Hadamard Gate

$$\hat{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{cases} \hat{H} |0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \\ \hat{H} |1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \end{cases}$$

2. Measurement Operations

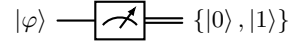


FIG. 3: Measurement operation. After the measurement the state collapses into a classical bit represented by the double wires.

$$\text{MEASUREMENT} = |0\rangle \langle 0| + |1\rangle \langle 1|$$

$$\text{CNOT} = |0\rangle \langle 0| \otimes \hat{I} + |1\rangle \langle 1| \otimes \hat{X} \begin{cases} \text{CNOT}(|00\rangle) = |00\rangle \\ \text{CNOT}(|10\rangle) = |11\rangle \\ \text{CNOT}(|01\rangle) = |01\rangle \\ \text{CNOT}(|11\rangle) = |10\rangle \end{cases} \quad (1)$$

3. Controlled Unitaries

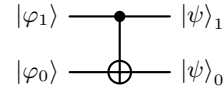


FIG. 4: Controlled not gate, the control is the black dot and the target is the \oplus . The $\oplus = \hat{X}$ by convention. The output is no longer necessarily a pure state.

$$\text{C}\hat{U} = |0\rangle \langle 0| \otimes \hat{I} + |1\rangle \langle 1| \otimes \hat{U} \begin{cases} \text{C}\hat{U}(|00\rangle) = |00\rangle \\ \text{C}\hat{U}(|10\rangle) = |01\rangle \\ \text{C}\hat{U}(|01\rangle) = |1\rangle \hat{U} |0\rangle \\ \text{C}\hat{U}(|11\rangle) = |1\rangle \hat{U} |1\rangle \end{cases} \quad (2)$$

4. Example: Quantum Teleportation

In order to more explicitly see the state teleportation, the mathematics will explicitly be shown at each key step. Each qubit can generally be referred to as \mathbb{Q}_n where n is the index of the qubit. Qubits are indexed from **bottom to top** in circuit diagrams and **right to left** in Dirac notation.

For clarity the state to be teleported is $|\varphi\rangle$ whereas the global state of the system is denoted with $|\psi_t\rangle$ where

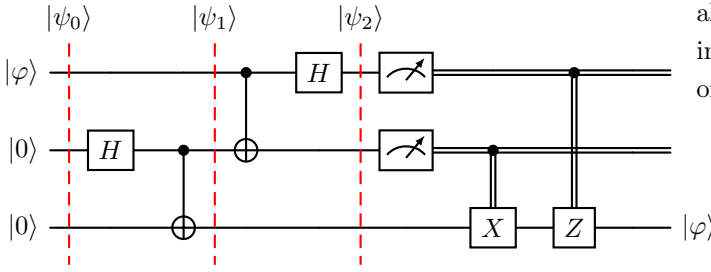


FIG. 5: Quantum teleportation circuit as described (with modification) in Neilson & Chuang [1]. The first Hadamard (\hat{H}) and CNOT gates describes the creation of a bell state.

t is the global state after some number of time steps. Generally, $|\varphi\rangle$ can be represented in (3).

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (3)$$

Where $|0\rangle$ and $|1\rangle$ are the basis of the **spin-1/2** system. the initial global state $|\psi_0\rangle$ can hence be represented in (6). Note that the subscripts represent the qubit index.

$$|\psi_0\rangle = |\varphi\rangle_2 |0\rangle_1 |0\rangle_0 \text{ (Qubit index explicitly noted)} \quad (4)$$

$$= \alpha|0\rangle_2 |0\rangle_1 |0\rangle_0 + \beta|1\rangle_2 |0\rangle_1 |0\rangle_0 \quad (5)$$

$$= \alpha|000\rangle + \beta|100\rangle \quad (6)$$

Now induce a bell state [2] using a Hadamard gate and a *CNOT* gate (Controlled *X* gate). This can be seen in (11)

$$|\psi_1\rangle = \text{CNOT} \hat{H} \{\alpha|000\rangle + \beta|100\rangle\} \quad (7)$$

$$= \text{CNOT} \left\{ \frac{\alpha}{\sqrt{2}} |0\rangle (|0\rangle + |1\rangle) |0\rangle + \frac{\beta}{\sqrt{2}} |1\rangle (|0\rangle + |1\rangle) |0\rangle \right\} \quad (8)$$

$$= \frac{1}{\sqrt{2}} \text{CNOT} \{\alpha|000\rangle + \alpha|010\rangle + \beta|100\rangle + \beta|110\rangle\} \quad (9)$$

$$= \frac{1}{\sqrt{2}} (|0\rangle \langle 0| \otimes \hat{I} + |1\rangle \langle 1| \otimes \hat{X}) \{\alpha|000\rangle + \alpha|010\rangle + \beta|100\rangle + \beta|110\rangle\} \quad (10)$$

$$= \frac{1}{\sqrt{2}} \{\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle\} \quad (11)$$

Once a bell state has been prepared, \mathbb{Q}_0 can be separated an arbitrary distance from \mathbb{Q}_1 and \mathbb{Q}_2 . In order to actu-

ally teleport the state of $\mathbb{Q}_2 = |\varphi\rangle$ to \mathbb{Q}_0 , an additional interaction must be performed through local interactions on \mathbb{Q}_2 and \mathbb{Q}_1 . This is $|\psi_2\rangle$ and is calculated in (15).

$$|\psi_2\rangle = \frac{1}{\sqrt{2}} \hat{H} \text{CNOT} \{\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle\} \quad (12)$$

$$= \frac{1}{\sqrt{2}} \hat{H} \{\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle\} \quad (13)$$

$$= \frac{1}{2} \{\alpha(|0\rangle + |1\rangle) |00\rangle + \alpha(|0\rangle + |1\rangle) |11\rangle + \beta(|0\rangle - |1\rangle) |10\rangle + \beta(|0\rangle - |1\rangle) |01\rangle\} \quad (14)$$

$$= \frac{1}{2} \{\alpha|000\rangle + \alpha|100\rangle + \alpha|011\rangle + \alpha|111\rangle + \beta|010\rangle - \beta|110\rangle + \beta|001\rangle - \beta|101\rangle\} \quad (15)$$

At this point the teleportation is completed, this can be explicitly be seen through simple rearrangement in (17) rearranged. The final controlled measurements are meant as a ‘correction’ to flip and change signs to exactly obtain $|\varphi\rangle$.

$$|\psi_2\rangle = \frac{1}{2} \{ |00\rangle (\alpha|0\rangle + \beta|1\rangle) + |10\rangle (\alpha|0\rangle - \beta|1\rangle) + |01\rangle (\alpha|1\rangle + \beta|0\rangle) + |11\rangle (\alpha|1\rangle - \beta|0\rangle) \} \quad (16)$$

$$= \frac{1}{2} \{ |00\rangle (|\varphi\rangle) + |10\rangle (\hat{Z}|\varphi\rangle) + |01\rangle (\hat{X}|\varphi\rangle) + |11\rangle (\hat{X}\hat{Z}|\varphi\rangle) \} \quad (17)$$

$$= \frac{1}{2} \{ |0\rangle_2 |0\rangle_1 (|\varphi\rangle_0) + |1\rangle_2 |0\rangle_1 (\hat{Z}|\varphi\rangle_0) + |0\rangle_2 |1\rangle_1 (\hat{X}|\varphi\rangle_0) + |1\rangle_2 |1\rangle_1 (\hat{X}\hat{Z}|\varphi\rangle_0) \} \quad (18)$$

(Qubit indices explicitly noted)

II. CONCEPTS

A. Fundamentals

1. Single Qubit Gates

2. Two Qubit Gates

One can try applying unitaries to create entanglement but this won’t work. this is because **localized operations** don’t change entanglement. Instead one has to use a *two qubit gate*.

B. Time Evolution*1. Bell's Inequalities*

Consider a state

$$|\beta_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\Phi_+\rangle$$

Notice that if you measure \mathbb{Q}_1 , **instantaneously**, \mathbb{Q}_2 collapses on the same state as the outcome of the measurement of \mathbb{Q}_1 . The idea of instantaneous influence may violate the principle of special relativity (*Einstein-Podolsky-Rosen Paradox* [3]).

States such as these are known as **Bell States** and are **maximally entangled**. There are 4-bell states

$$\begin{aligned} |\beta_0\rangle &= |\Phi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ |\beta_1\rangle &= |\Psi_-\rangle = \frac{i}{\sqrt{2}}(|01\rangle + |10\rangle) = I \otimes \sigma_1 |\beta_0\rangle \\ |\beta_2\rangle &= |\Psi_+\rangle = \frac{-1}{\sqrt{2}}(|01\rangle - |10\rangle) = I \otimes \sigma_2 |\beta_0\rangle \\ |\beta_3\rangle &= |\Phi_-\rangle = \frac{i}{\sqrt{2}}(|00\rangle - |11\rangle) = I \otimes \sigma_3 |\beta_0\rangle \end{aligned}$$

Together these form an orthonormal basis known as the **bell basis** or the **singlet basis** (or some other permutation). An example state in this basis can be seen below

$$\begin{aligned} |\psi\rangle &= A |\beta_0\rangle + B |\beta_1\rangle + C |\beta_2\rangle + D |\beta_3\rangle \\ &= \frac{A+Di}{\sqrt{2}} |00\rangle + \frac{iB-C}{\sqrt{2}} |10\rangle + \dots \end{aligned}$$

Now we can see $\alpha = \frac{A+Di}{\sqrt{2}}$ and so on. Using (25), one can obtain the concurrence as:

$$\begin{aligned} C &= 2|\alpha\delta - \gamma\beta| \\ &= 2\left|\frac{1}{2}(A+iD)(A-iD) - \frac{1}{2}(iB-C)(iB+C)\right| \\ &= |A^2 + B^2 + C^2 + D^2| \end{aligned}$$

Theorem II.1. The Fundamental Theorem of En-

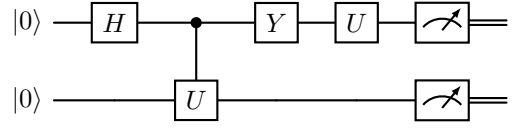


FIG. 6: Measurement Operations and Bell's inequalities

tanglement

$$\begin{aligned} (I \otimes U) |\beta_2\rangle &= -\frac{1}{\sqrt{2}}(|0\rangle \otimes (b|0\rangle + a^*|1\rangle) \\ &\quad - |1\rangle \otimes (a|0\rangle - b^*|1\rangle)) \\ &= -(U^\dagger \otimes I) |\beta_2\rangle \\ \therefore (U \otimes U) |\beta_2\rangle &= -|\beta_2\rangle \end{aligned}$$

A unitary applied to \mathbb{Q}_0 in a maximally entangled (in singlet basis) pair is equivalent to applying a related [4] unitary to \mathbb{Q}_1 of the pair

2. Hidden variables and why they don't work

Recall §IB2, however, instead of 0 and 1, let's measure -1 and 1 to create this definition we must redefine an operator as such:

$$\begin{aligned} \hat{a} \text{ (operator)} &= \vec{a} \cdot \hat{\sigma} \\ &= a_x \hat{X} + a_y \hat{Y} + a_z \hat{Z} \\ &= \begin{bmatrix} a_z & a_x - ia_y \\ a_x - ia_y & -a_z \end{bmatrix} \end{aligned}$$

where \vec{a} is a **vector**, $\hat{\sigma}$ are the Pauli operators, and \hat{a} is an operator. This gives us the eigenvalues -1 and 1 as desired for these measurements. Define the average of \vec{a} as \bar{a} to obtain the following:

$$\begin{aligned} \bar{a} &= \int a(\lambda) p(\lambda) d\lambda \\ &= \langle \hat{a} | \hat{a} \rangle = \text{Quantum Prediction} \end{aligned}$$

Let us consider some hidden-variable theory. For the hidden variable theory to be true, there must be something about it which avoids Bell's inequalities.

One can "test" this with Bell's inequalities as follows. Consider a circuit as in figure 6.

Where \mathbb{Q}_0 U is $\frac{\hat{a}}{b}$ and \mathbb{Q}_1 U is $\frac{\hat{a}}{b}$. Using the idea of a hidden variable, one can obtain the following

$$\mathcal{S} = \{a(\lambda) + b(\lambda)\}c(\lambda) + a(\lambda) - b(\lambda)d(\lambda)$$

Therefore this implies

$$\begin{aligned} a(\lambda) = b(x) &\implies \mathcal{S} = 2ac = \pm 2 \\ a(\lambda) = -b(x) &\implies \mathcal{S} = \pm 2ac = \pm 2 \end{aligned}$$

The hidden variable theory states that these averages must be able to be predicted using quantum mechanics. That is to say \overline{ac} (and others) must be the same as the Q.M. averages.

$$\begin{aligned} \overline{ac} &= \langle \beta_2 | \hat{a} \otimes \hat{c} | \beta_2 \rangle \langle \beta_2 | \hat{a} \otimes \hat{c} | \beta_2 \rangle \\ &= \det\{c\} \left\langle \beta_2 \hat{a} \hat{c}^\dagger \otimes \hat{I} | \beta_2 \right| \beta_2 \hat{a} \hat{c}^\dagger \otimes \hat{I} | \beta_2 \rangle \\ &= \dots \\ &= -1(\vec{a} \cdot \vec{c}) \end{aligned}$$

Subbing this back into the average value of \mathcal{S}

$$\begin{aligned} |\overline{\mathcal{S}}| &= |\vec{a} \cdot \vec{c} + \vec{b} \cdot \vec{c} + \vec{a} \cdot \vec{d} - \vec{b} \cdot \vec{d}| \\ \implies \vec{a} &= (1, 0, 0) \\ \vec{b} &= (0, 0, 1) \\ \vec{c} &= \frac{1}{\sqrt{2}}(-1, 0, 1) \\ \vec{d} &= \frac{1}{\sqrt{2}}(-1, 0, 1) \end{aligned}$$

This states that \mathcal{S} **cannot be more than 2**. Otherwise there is no **local** hidden variable description of the phenomena.

C. Schmidt Decomposition Theorem

Theorem II.2. *Schmidt Decomposition Theorem*

Any two qubits state $|\psi\rangle$ can be Schmidt decomposed into

$$|\psi\rangle = U_A \otimes U_B (\lambda_0 |00\rangle + \lambda_1 |11\rangle)$$

Where λ_0, λ_1 are the “Schmidt numbers.” If **the concurrence is 1** then the Schmidt numbers are always $\lambda_1 = \lambda_2 = \frac{1}{\sqrt{2}}$. We can always apply local basis changes

to either of those 2 qubits and have the same 2 local unitaries.

From (25), it is known that if $C = 0$ the state must hence be separable. Therefore, we can represent a state as

$$\begin{aligned} |\psi'\rangle &= (U \otimes I) |\psi\rangle = \begin{bmatrix} \alpha' \\ \beta' \\ \gamma' \\ \delta' \end{bmatrix} \\ &= \begin{bmatrix} aI & bI \\ -b^*I & a^*I \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix} \end{aligned}$$

Therefore, any bipartite state can be written as

$$|\psi\rangle = (U_A \otimes U_B)(\lambda_0 |00\rangle + \lambda_1 |11\rangle) \quad (19)$$

Where λ_0 and λ_1 are real numbers. The relation between λ_0 and λ_1 is outlined in (20).

$$\lambda_0^2 + \lambda_1^2 = 1 \quad (20)$$

From (20) and (25), one can find both λ_0 and λ_1 .

$$\begin{aligned} \lambda_0^2 + \left(\frac{C}{2\lambda_0}\right)^2 &= 1 \\ \implies \lambda_0^4 - \lambda_0^2 + \left(\frac{C}{2}\right)^2 &= 0 \end{aligned}$$

Therefore, one can find λ_0 as

$$\lambda_0 = \frac{1 \pm \sqrt{1 - C^2}}{2} \quad (21)$$

Notice that for a *maximally entangled state*[5]. This can be more easily be visualized in figure 7 which has a maxima at (0.5, 0.5) implying the state is maximally entangled when $\lambda_0 = 0.5$.

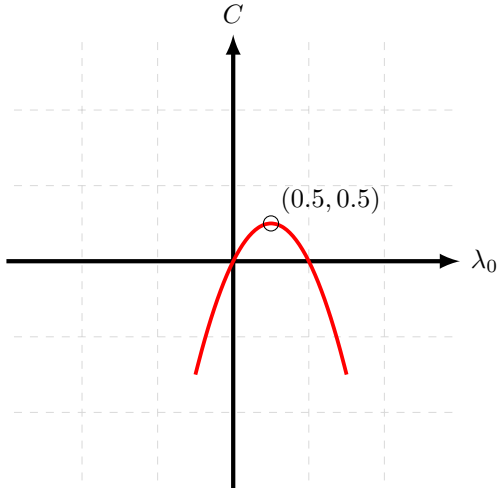


FIG. 7: Variation of concurrence C of a quantum system with changing λ_0

D. Teleportation & No Cloning Theorem

E. Quantum Fourier Transform

1. Binary Notation

First notice, one can represent a base 10 numbers in binary as follows:

$$\begin{aligned} 7_{10} &= 7 \text{ base 10} \\ &= 0111_2 \text{ base 2} \end{aligned}$$

Therefore an L qubit state can be represented as

$$L - \text{qubit state: } |x\rangle = |x_{L-1}\rangle \otimes |x_{L-2}\rangle \otimes \cdots \otimes |x_1\rangle \otimes |x_0\rangle$$

2. Quantum Parallelism

Say one wants to evaluate function $f(x)$. In order for $f(x)$ to be a valid unitary it must be **bijective**. In order to evaluate a *unitary*, you must use **two** registers.

$$\begin{aligned} |x\rangle & \text{ (L-qubits)} \\ |y\rangle & \text{ (M-qubits) : } M \leq L \\ & \longrightarrow U_f |x\rangle |y\rangle \\ & = |x\rangle |y \oplus f(x)\rangle \end{aligned}$$

Note that this \oplus is known as *bit-wise addition modulo two* that is to say

$$\begin{aligned} 0 \oplus 0 &= 0 \\ 1 \oplus 0 &= 1 \\ 0 \oplus 1 &= 1 \\ 1 \oplus 1 &= 0 \\ 1011 \oplus 0110 &= 10001 \end{aligned}$$

Therefore, one can evaluate a unitary U_f as

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

Since $f(x)$ always evaluates to 0 or 1.

Now to implement Quantum Parallelism one can do the following:

$$\begin{aligned} H|0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ (H \otimes H)|00\rangle &= \frac{1}{2}(|0\rangle + |1\rangle)(\cdots) \\ &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \\ \implies H^{\otimes L}|0\rangle_L &= \frac{1}{2^{\frac{L}{2}}} \sum_{x=0}^{2^L-1} |x\rangle = |a11\rangle_L \end{aligned}$$

Therefore, if we had the H applied to all states in the argument register, we'd have

$$\begin{aligned} (H^{\otimes L} \otimes I^{\otimes M})|0\rangle_L \otimes |0\rangle_M & \text{ first ket is the argument} \\ & = |a11\rangle_L \otimes |0\rangle_M \\ \implies U_f |a11\rangle_L \otimes |0\rangle_M & = \frac{1}{2^{\frac{L}{2}}} \sum_{x=0}^{2^L-1} |x\rangle |f(x)\rangle \end{aligned}$$

3. Discrete Fourier Transform

First, note that *any function that is periodic can be written as a sum of sines and cosines*. That is to say:

$$\begin{aligned} f(t) &= \int_{-\infty}^{\infty} \tilde{f}(v) \exp(-2\pi i v t) dv \\ \tilde{f}(v) &= \int_{-\infty}^{\infty} f(t) \exp(2\pi i v t) dt \end{aligned}$$

Any statement that has a finite amount of energy can be written in such a manner. *However*, when you do this on a computer, you cannot due infinitesimal calculations. So how is this done for a discrete case? Instead of functions, *strings* are used, that is to say, *sets of data* $\{f(t_0), f(t_1), f(t_2), \dots\}$. These will be a sample of the data points of the function at different points, t_0, t_1, \dots . This can be listed as follows:

$$\tilde{f}_l = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp\left(\frac{2\pi i k l}{N} f_k\right)$$

An example using the DFT is as follows. Say some function, f_k as period 2, and we evaluate \tilde{f}_l using $N = 7$ points, $\eta = \exp(2\pi i l/N)$.

$$\tilde{f}_l = \frac{1}{\sqrt{7}}(f_0 + f_1\eta + f_2\eta^2 + f_3\eta^3 + f_4\eta^4 + f_5\eta^5 + f_6\eta^6)$$

From this, we know that

$$\begin{aligned} f_6 &= f_4 = f_2 = f_0 \\ f_5 &= f_3 = f_1 \end{aligned}$$

Therefore, it follows that

$$\begin{aligned} \tilde{f}_l &= \frac{1}{\sqrt{7}}(f_0 + f_1\eta + f_0\eta^2 + f_1\eta^3 + f_0\eta^4 + f_1\eta^5 + f_0\eta^6) \\ &= \frac{1}{\sqrt{7}}(f_0(1 + \eta^2 + \eta^4) + f_1\eta(1 + \eta^2 + \eta^4) + f_0\eta^6) \\ &= \frac{1}{\sqrt{7}}(1 + \eta^2 + \eta^4)(f_0 + f_1\eta) + \frac{f_0\eta^6}{\sqrt{7}} \end{aligned}$$

For arbitrary $N > 7$, $\{f_0, f_1, \dots, f_{N-1}\}$. For some period P we'd have

$$\begin{aligned} &f_0, f_1, \dots, f_{P-1}, f_P, f_{P+1}, \\ &\dots, f_{2P-1}, f_{2P}, \dots, f_{3P-1}, f_{3P+1}, \dots, f_N \\ &\text{grouping these up} \\ &(f_0, f_1, \dots, f_{P-1}), (f_P, f_{P+1}, \\ &\dots, f_{2P-1}), \\ &(f_{2P}, \\ &\dots, f_{3P-1}), (f_{3P+1}, \dots, f_N) \end{aligned}$$

Where each of these groupings represents one period of the target function. Writing this out in the DFT summation:

$$\tilde{f}_l = \frac{1}{\sqrt{N}} \left(\sum_{k=0}^{P-1} f_k \eta^k \right) \left(\sum_{r=0}^{q-1} \eta^{Pr} \right) + \tilde{f}_l^{\text{end}} \quad (22)$$

Notice that the second summation is essentially a geometric progression with difference r . Therefore, this can be simplified to

$$\sum_{k=0}^{N-1} x^k = \frac{1 - x^N}{1 - x}$$

Since these need not be a **real** number, we can use this with our complex numbers in (22) to obtain:

$$\begin{aligned} \left(\sum_{r=0}^{q-1} \eta^{Pr} \right) &= \sum_{r=0}^{q-1} \exp(2\pi i (l/N)p)r \\ &= \frac{1 - \exp(2\pi i lpq/N)}{1 - \exp(2\pi i lp/N)} \end{aligned}$$

Notice a problem, if $l, N \in \mathbb{Z}$ it implies that $\exp(2\pi i) = 1$. Therefore, if we substitute into the previous equation, we get a form $\frac{0}{0}$.

This section is to be edited and corrected

F. Algorithms

1. Deutsch-Jozsa Algorithm

Consider a function $f(x)$ defined as:

$$\begin{aligned} f(x) &= x \in \{0, 1, \dots, 2^n - 1\} \text{ n-bit argument} \\ f(x) &= x \in \{0, 1\} \end{aligned}$$

The objective of the Deutsch-Jozsa Algorithm [6] is to determine whether $f(x)$ is either **constant** or **balanced**. That is to say, $f(x) = 0 \forall x$ **or** $f(x) = 1 \forall x$ (*constant function*) or **equal number of 0 and 1** (*balanced*).

Classically distinguishing between constant and balanced functions requires $2^{n-1} + 1$ calls on the oracle.

The algorithm can be represented using the circuit in figure 8

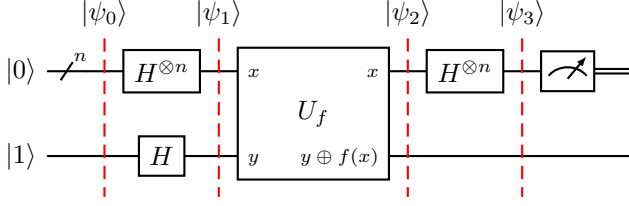


FIG. 8: Quantum Circuit diagram for representing the Deutsch-Jozsa Algorithm for evaluating if a given binary function $f(x)$ is balanced

$$\begin{aligned}
 |\psi_2\rangle &= U_f |\psi_1\rangle \\
 &= \sum_{x=0}^{2^n-1} \frac{|x\rangle}{\sqrt{2^n}} \left(\frac{|f(x)\rangle - |\overline{f(x)}\rangle}{\sqrt{2}} \right) \\
 \Rightarrow U_f |x\rangle |y\rangle &= |x\rangle |y \oplus f(x)\rangle
 \end{aligned}$$

For a 1 qubit argument, $|\psi_1\rangle$ is easy to evaluate:

$$\begin{aligned}
 H|x\rangle &= \begin{cases} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) & \text{if } x = 0 \\ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) & \text{if } x = 1 \end{cases} \\
 &= \frac{(|0\rangle + (-1)^x |1\rangle)}{\sqrt{2}}
 \end{aligned}$$

Similarly, for a 2 qubit argument, one can evaluate $|\psi_2\rangle$. Notice that this is essentially multiplication modulo two.

$$\begin{aligned}
 (H \otimes H) |x_1 x_0\rangle &= \frac{(|0\rangle + (-1)^{x_1} |1\rangle)}{\sqrt{2}} \frac{(|0\rangle + (-1)^{x_0} |1\rangle)}{\sqrt{2}} \\
 &= \sum_{z=0}^3 (-1)^{z_1 x_1 + z_0 x_0} |z\rangle \\
 \text{in general } \Rightarrow H^{\otimes n} |x\rangle &= \sum_{z=0}^{2^n-1} \frac{(-1)^{x \cdot z}}{\sqrt{2^n}} |z\rangle \\
 \Rightarrow x \cdot z &= (x_0 z_0) \oplus (x_1 z_1) \oplus \cdots \oplus (x_{n-1} z_{n-1}) \\
 &= \bigoplus_{i=0}^{n-1} x_i z_i
 \end{aligned}$$

Finally one can extrapolate to the n -qubit case shown in figure 8. Say we have $|\psi_3\rangle = (H^{\otimes n} \otimes I)$ (note that I is the unitary acting on the function register and H is the unitary acting on the argument register).

$$\begin{aligned}
 |\psi_3\rangle &= (H^{\otimes n} \otimes I) \\
 &= \left(\sum_{x,z=0}^{2^n-1} (-1)^{x \cdot z + f(x)} |z\rangle \right) \left\{ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right\} \\
 &= \sum_{z=0}^{2^n-1} c_z |z\rangle \\
 \Rightarrow c_z &= \sum_{x=0}^{2^n-1} \frac{(-1)^{z \cdot x + f(x)}}{2^n}
 \end{aligned}$$

As a test, Suppose that $f(x)$ is constant.

$$\begin{aligned}
 c_0 &\propto \left(\sum_{x=0}^{2^n-1} \frac{1}{2^n} \right) (-1)^{f(0)} \\
 &\propto 1 (-1)^{f(0)} \quad \because \text{summation evaluates to 1}
 \end{aligned}$$

If all n argument register qubits are in state $|0\rangle$ it implies that $f(x)$ is **constant**. If any qubit in the state $|1\rangle$ $f(x)$ must be **balanced**. This requires only 1 call on the oracle when classically it would require $2^n - 1$.

2. Bernstein-Vazariani Algorithm

3. Grover's Algorithm

4. Shor's Algorithm

G. Quantum Error Correction

Let there be some arbitrary quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Inevitably the following will happen[7]:

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

This ruins our algorithms, hence this begs the question, how can you cope with an error like a bit flip in your Q-Computer.

Clue: **Classical Error Correction**, let's send 3 bits instead of one.

$$0 \mapsto 000$$

$$1 \mapsto 111$$

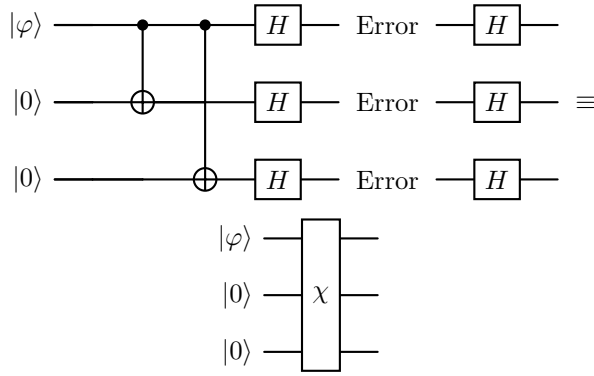


FIG. 9: Error Correction Circuit Intro

Say there some bit flip error (could be one of the following)

$$000 \longrightarrow 100, 010, 001$$

$$111 \longrightarrow 011, 101, 110$$

Now here's a problem, what if two flip (screws everything up)? Well the has t do with the probability of an error occurring (square of error [dc with prof]).

But now we have issues with error correction (in a quantum state), in order to do error correction you must measure a state thereby destroying it. Shor (and one other) showed this is not true and that **you can do error correction on a quantum state.**

H. Error Correcting Codes

Lets take the above with the state $|\varphi\rangle = \alpha|000\rangle + \beta|111\rangle$. The following are the possible errors.

$$e(|\varphi\rangle) = \begin{cases} \alpha|000\rangle + \beta|111\rangle & \text{Correct State} \\ \alpha|001\rangle + \beta|110\rangle & \text{Bitflip on } \mathbb{Q}_1 \\ \alpha|010\rangle + \beta|101\rangle & \text{Bitflip on } \mathbb{Q}_2 \\ \alpha|100\rangle + \beta|011\rangle & \text{Bitflip on } \mathbb{Q}_3 \end{cases}$$

Lets use a few auxiliary qubits to correct.

Bit flip errors aren't actually all that common. Rather, time evolution is more of an issue. In fact this is a more likely scenario:

$$\begin{aligned} |\phi\rangle &= \alpha|0\rangle + \beta|1\rangle \rightarrow \alpha e^{i\epsilon}|0\rangle + \beta e^{-i\epsilon}|1\rangle \\ &= \exp\{i\epsilon\hat{Z}\}|\phi\rangle \\ &\approx |\phi\rangle + i\epsilon\hat{Z}|\psi\rangle \end{aligned}$$

I. Decoherence Free Spaces

J. Quantum Key Distribution

K. Device Physics

The device physics limits what you can implement experimentally. What do you actually need to make a quantum computer?

1. DiVincenzo's Requirements for a Physical Quantum Computer

1. A lot of qubits
2. must be able to initialize them (i.e. they have to be in the ground state $|0\rangle$, \therefore they have to be very very cold)
3. Must be reliable (you can have your probability amplitudes becoming *decoherent*, i.e. α and β become randomized). The time it takes for a state to experience *decoherence* is **long**.
4. Must be able to perform unitary operations/ quantum gates
5. Must be able to measure them.

This "shopping list" was made by David DiVincenzo in 2000.

2. Methods of Physical Implementation

1. Photons (1988)
2. Ions (1994)
3. Nuclear Spins (in molecules)
4. Super conducting QuBits (currently lots of potential)

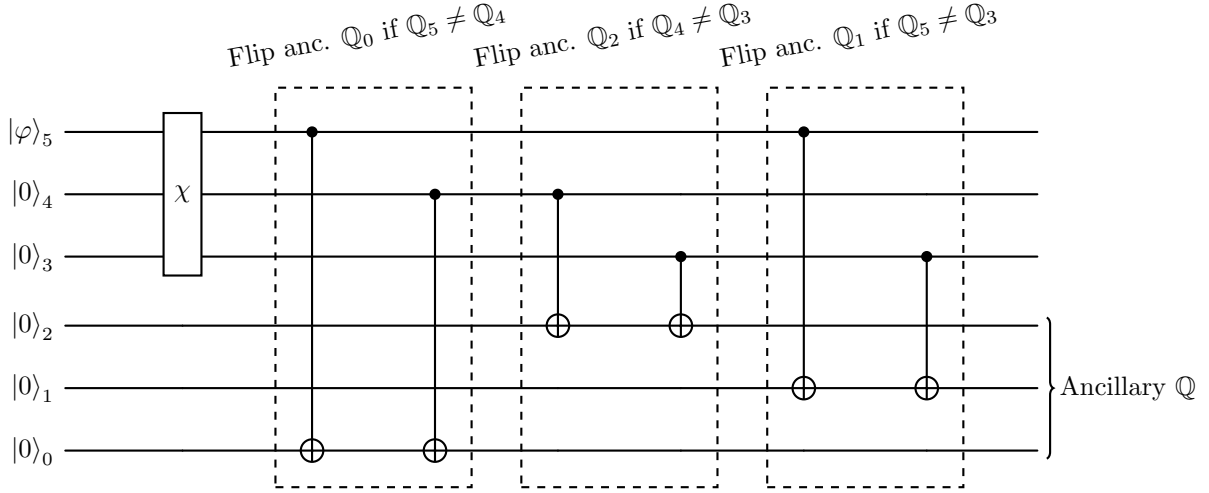


FIG. 10: Full 3-bit error correction circuit using auxiliary qubit measurements to correct state. The **Ancillary Q (qubits) are the qubits used for error correction**. Qubit indices are explicitly denoted on the left of the diagram for clarity.

From 4 we have a problem. We must engineer every single quantum system in a super conducting Qubit, it becomes a lot harder to fabricate. By definition every **Ca** atom is the same as every other **Ca** atom.

There is a *bias* that more things should be solid state.

Say we have a qubit in the following states

$$\begin{aligned}
 |\varphi\rangle & \begin{cases} |0\rangle & E_0 \\ |1\rangle & E_1 \end{cases} \\
 E_1 - E_0 &= \hbar\omega \\
 |\phi\rangle &= A|0\rangle + B|1\rangle \\
 \mathcal{H} &= \begin{bmatrix} E_0 & 0 \\ 0 & E_1 \end{bmatrix} \\
 &= I \left(\frac{E_0 + E_1}{2} \right) + \frac{\hbar\omega}{2} Z
 \end{aligned}$$

3. Temperature Bound

Notice the Maxwell-Boltzman Distribution

$$p_n \propto \exp\{-E_n/k_B\theta_T\}$$

Therefore it follows that the probability of being in a

state p_1/p_0 is

$$\begin{aligned}
 p_1/p_0 &= \exp\{-(E_1 - E_0)/k_B\theta_T\} \\
 &= \exp\{-\hbar\omega/k_B\theta_T\} \\
 &\ll 1 \implies \frac{\hbar\omega}{k_B\theta_T} \gg 1 \\
 \therefore \theta_T &\ll \frac{\hbar\omega}{k_B}
 \end{aligned}$$

4. Time Evolution

Notice the Schrödinger equation

$$i\hbar \frac{\partial}{\partial t} |\phi\rangle = \mathcal{H} |\phi\rangle \quad (23)$$

Therefore it follows that

$$\begin{aligned}
 i\hbar \frac{\partial}{\partial t} A &= E_0 A \\
 \implies A(t) &= A(0) \exp\{-iE_0 t/\hbar\} \\
 i\hbar \frac{\partial}{\partial t} B &= E_1 B \\
 \implies B(t) &= B(0) \exp\{-iE_1 t/\hbar\}
 \end{aligned}$$

We see then that our coefficients A and B will be **constantly changing in time** as follows



$$\begin{aligned}
|\phi(t)\rangle &= A(0)e^{\frac{-iE_0t}{\hbar}}|0\rangle + B(0)e^{\frac{-iE_1t}{\hbar}}|1\rangle \\
&= \exp\left(-i\frac{(E_0 + E_1)t}{\hbar}\right) \left\{ A(0)e^{\frac{i\omega t}{\hbar}}|0\rangle + B(0)e^{\frac{-i\omega t}{\hbar}}|1\rangle \right\} \\
&\quad (\star)
\end{aligned}$$

The first term is the *global phase* and can be ignored for our purposes.

(\star) can be rewritten using Euler's formula

$$A(0)\{\cos(\omega t/2) + i\sin(\omega t/2)\}|0\rangle + B(0)\{\cos(\omega t/2) - i\sin(\omega t/2)\}|1\rangle$$

It then follows as a unitary

$$\begin{aligned}
U_0(t) &= \cos(\omega t/2)I + i\sin(\omega t/2)Z \\
\implies |\phi(t)\rangle &= U_0(t)|\phi(0)\rangle
\end{aligned}$$

That means the operators must also change in time as well!!!

Therefore it follows that

$$\langle\zeta|X|\varphi\rangle = (\langle\zeta|U_0^\dagger)U_0XU_0^\dagger(U_0|\varphi\rangle)$$

1. Energy gap between $|0\rangle$ and $|1\rangle$ (E_0 and E_1 , $\hbar\omega = E_1 - E_0$).

- (a) Temperature must be $T \ll \frac{\hbar\omega}{k_B}$
- (b) Driver Synchronization $\omega_d = \omega$

2. Single Qubit Gates can be implemented using a *time-harmonic force* $\vec{f}(t) = \vec{f}_0 \cos(\omega t + \phi)$.

$$\hat{U}(t) = \cos\left(\frac{\Omega t}{2}\right)\hat{I} - i\sin\left(\frac{\Omega t}{2}\right)\{\cos\phi\hat{X} + \sin\phi\hat{Y}\}$$

- (a) Rabi Oscillations $\Omega \propto f_0$
- (b) $\Omega t = \pi$ “pi-pulse” which means (substitute into equation)

$$\hat{U}\left(\frac{\pi}{\Omega}\right) = -i\{\cos\phi\hat{X} + \sin\phi\hat{Y}\}$$

- (c) \therefore Pauli Gates $\implies \pi$ - pulse
- (d) $\Omega t = \pi/2, \phi = \frac{3\pi}{2}$ “pi-upon-two-pulse” which

means (substitute into equation)

$$\hat{U} = \frac{1}{\sqrt{2}}(\hat{I} + i\hat{Y}) = i\hat{H}$$

- (e) $\Omega t = 2\pi$ Allows you to make $\hat{U} = -\hat{I}$

3. Two qubit gates (two methods)

- (a) Method (1)

- i. Remember they are two physical entities
Therefore it follows that they *will* interact as defined in the Schrödinger equation.

$$i\hbar\frac{\partial}{\partial t}|\Phi_{AB}\rangle = \{ \}$$

III. PROBLEM SET QUESTIONS

A. Problem Set One

1. *Question One: Eigenvalues and Properties of Pauli Matrices*

- a. *Question:* The three *Pauli matrices* are given by:

$$\hat{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \hat{Y} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \hat{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Find the eigenvectors, eigenvalues, and diagonal representations of \hat{X} , \hat{Y} , and \hat{Z} .

2. *Question Two: Playing with Pauli Matrices*

- a. *Question:* Show that:

$$\hat{X}\hat{Y} = i\hat{Z}, \hat{Y}\hat{Z} = i\hat{X}, \hat{Z}\hat{X} = i\hat{Y}$$

And hence $\hat{X}\hat{Z}\hat{X} = -\hat{Z}$

3. Question Three: Verifying a Matrix is Unitary

a. Question: A unitary matrix is a matrix whose inverse is equal to its Hermitian adjoint (i.e take the transpose and the complex-conjugate). Show that

$$\hat{U} = \begin{bmatrix} a & b \\ -b^* & a^* \end{bmatrix}$$

(where $|a|^2 + |b|^2 = 1$) is unitary.

$c|0\rangle + d|1\rangle$ in a two-dimensional Hilbert space is a 2x2 matrix defined by

$$|\psi\rangle\langle\phi| = \begin{bmatrix} a \\ b \end{bmatrix} \begin{bmatrix} c^* & d^* \end{bmatrix} = \begin{bmatrix} ac^* & ad^* \\ bc^* & bd^* \end{bmatrix}$$

(i) Find the eigenvalues of $|\psi\rangle\langle\psi|$

(ii) Show that $|\psi\rangle\langle\psi| = \frac{1}{2}(\hat{I} + \mathbf{S} \cdot \hat{\sigma})$ (where $\mathbf{S} \cdot \hat{\sigma} = \sum_{i=1}^3 S_i \hat{\sigma}_i$)

B. Problem Set 2

1. Question One: Looking at the Bloch Sphere

a. Question: The Bloch vector is alternative way to represent the state of a qubit in a real three-dimensional space \mathbb{R}^3 (rather than a complex two-dimensional space \mathbb{C}^2). It is defined by

$$S_i = \langle\varphi|\hat{\sigma}_i|\varphi\rangle$$

where $\hat{\sigma}_i$ ($i = 1, 2, 3$) are the Pauli matrices.

(a) Show that for states given by a properly normalized vector in \mathbb{C}^2 , the Bloch vector is a real unit vector (i.e. $\sum_{i=1}^3 S_i^2 = 1$)

(b) Work out the components of the Bloch vector for the following states

(i) $|0\rangle$

(ii) $|1\rangle$

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

(iv) $\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$

(c) The Kronecker Product (also called the outer product) of two vectors $|\psi\rangle = a|0\rangle + b|1\rangle$ and $|\phi\rangle =$

2. Question Two: Unitary Operations on the Bloch Sphere

a. Question: Now let's consider the effect of unitary operations on the Bloch vector.

(a) Show that the operator given by the following expression is unitary

$$\hat{U} = \cos \frac{\theta}{2} \hat{I} + i \sin \frac{\theta}{2} \mathbf{n} \cdot \hat{\sigma}$$

where \mathbf{n} is a real unit vector.

(b) If $|\varphi'\rangle = \hat{U}|\varphi\rangle$, show that the transformed Bloch vector $\mathbf{S}' = \langle\varphi'|\hat{\sigma}|\varphi'\rangle$ is the original Bloch vector rotated by an angle θ about an axis along the unit vector \mathbf{n} , i.e.:

$$\mathbf{S}' = \cos \theta \mathbf{S} + (1 - \cos \theta)(\mathbf{n} \cdot \mathbf{S})\mathbf{n} - \sin \theta (\mathbf{n} \times \mathbf{S})$$

C. Problem Set 3

1. Question One: Evaluating Concurrence

a. *Question:* Consider the following 2-qubit state

$$|\phi\rangle = \frac{1}{10}\{i\sqrt{27}|00\rangle + 3|01\rangle - 4|10\rangle - i\sqrt{48}|11\rangle\}$$

(a) Is the state entangled? If so, calculate its concurrence.

(b) Calculate the Schmidt numbers of the state

b. *Answer:*

Part (a) Using (25),

$$\begin{aligned} C &= 2|\alpha\delta - \beta\gamma| \\ &= 2\left|\frac{(i\sqrt{27}) \cdot (-i\sqrt{48}) - (3) \cdot (-4)}{100}\right| \\ &= \frac{1}{50}\left|3\sqrt{3} \cdot 4\sqrt{3} + 12\right| \\ &= \frac{48}{50} \\ &= 0.96 \end{aligned}$$

Therefore the state is **entangled with a concurrence of $C = 96\%$**

Part (b) From Theorem ?? we have (21)

$$\begin{aligned} \lambda^2 &= \frac{1 \pm \sqrt{1 - C^2}}{2} \\ &= \frac{1 \pm 0.28}{2} \\ \Rightarrow \lambda_0 &= \sqrt{0.64} = 0.8; \lambda_1 = \sqrt{0.36} = 0.6 \end{aligned}$$

(c) Can **SWAP** be used to create entanglement? If so, write out the quantum circuit.

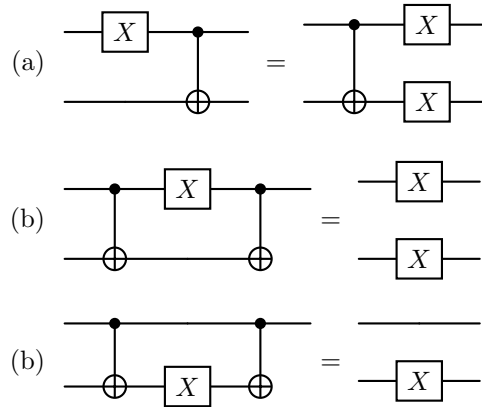
(d) Derive an expression $\sqrt{\text{SWAP}}$, defined by $\sqrt{\text{SWAP}}\sqrt{\text{SWAP}} = \text{SWAP}$

(e) Can $\sqrt{\text{SWAP}}$ be used to create entanglement? Find a separable state that will become maximally entangled when $\sqrt{\text{SWAP}}$ is applied to it.

D. Problem Set 4

1. Question One: Proving Circuit Identities

a. *Question:* Prove the following quantum circuit identities



2. Question Two: The SWAP gate

a. *Question:* The **SWAP** gate swaps the states of the two qubits, so that:

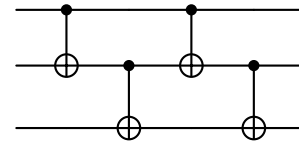
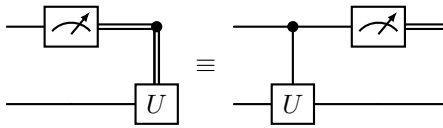
$$\text{SWAP}(\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle) = \alpha|00\rangle + \gamma|01\rangle + \beta|10\rangle + \delta|11\rangle$$

(a) Write down the 4x4 matrix for **SWAP**

(b) Can you write the **SWAP** gate as local operations on the two qubits? *Hint: try writing out the block-matrix for $\hat{U}_1 \otimes \hat{U}_2$ and comparing it to the matrix form for **SWAP***

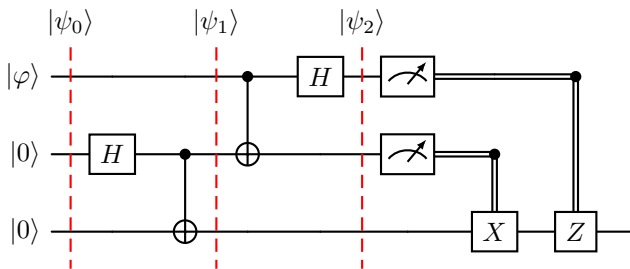
2. Question Two: The Griffiths-Niu Theorem

a. *Question:* **Griffiths-Niu Theorem** Given two qubits A and B , show that, if a measurement is performed on A followed by a conditional application of a unitary, \hat{U} , on B then the resultant state is equivalent to a controlled- \hat{U} gate on B followed by a measurement on A (see figure).

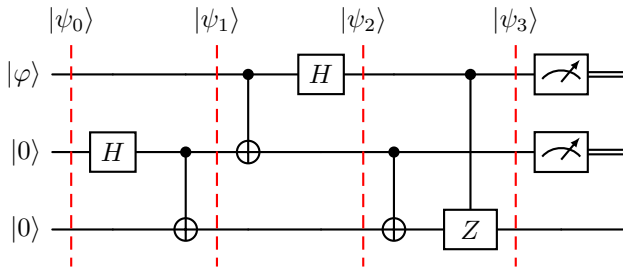


3. Question Three: Simplifying The Quantum Teleportation Circuit

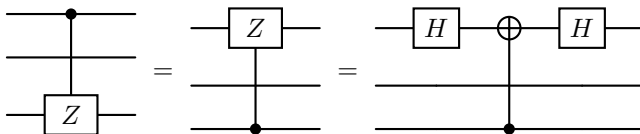
a. **Question: Circuit-Based Proof for Teleportation** Here is the full teleportation circuit discussed in class:



- (a) Use the Griffiths-Niu Theorem to show that the teleportation circuit has the same effect as the circuit below.

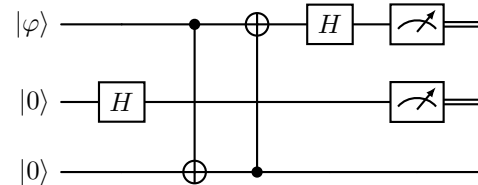


- (b) Use the identity $\hat{H}\hat{X}\hat{H} = \hat{Z}$ to rewrite the appropriate part of the circuit

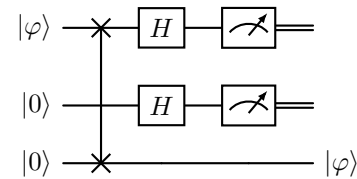


- (c) Use $\hat{H}\hat{H} = \hat{I}$ and the fact that $\hat{H}|0\rangle$ is an eigenstate of \hat{X} to add another CNOT (whose significance will soon be apparent).
- (d) Work out what appropriate single CNOT gate replaces the CNOT gate combination below:

- (e) Apply what you found in (d) on the teleportation circuit to simplify it further; this is what it should be looking like by now:



- (f) You will find that qubit #2 will no longer be involved in any multi-qubit gates. In other words, it has become a *spectator* qubit. Move the Hadamard gate acting on this qubit all the way to the right just before measurement.
- (g) Make a SWAP gate by creating a combination of CNOT gate (remember question 2 of the Term Test), acting on qubits #3 and #1, by inserting a CNOT gate with qubit #1 being the control qubit. Since qubit C is in a state $|0\rangle$, that will have no effect. You should end up with the circuit shown below:



E. Problem Set 5

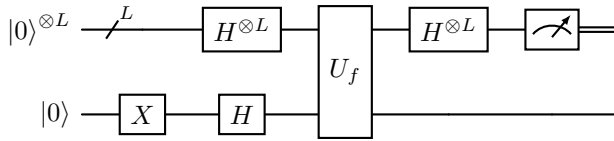
1. Question One: Introduction to Oracles

a. *Question:* The *bit-by-bit modulo-2 product* of two L -bit integers a and b is defined as

$$a \cdot b = (a_{L-1}b_{L-1}) \oplus (a_{L-2}b_{L-2}) \oplus \cdots \oplus (a_1b_1) \oplus (a_0b_0)$$

where a_k is the value of the k -th binary digit when a is written in base 2 (and likewise for b); \oplus is addition modulo 2 (i.e. add the two numbers, then calculate the remainder when dividing by 2).

- If $a = 5$ and $b = 6$ (both in base 10), find $a \cdot b$
- Prove that, in general, $a \cdot b \neq ab \pmod{2}$
- Prove that, for two qubits, $\text{CNOT} |x, y\rangle = |x, y \oplus x\rangle$ (where the first qubit is the control and the second the target of the CNOT , and x and y can both take the values of 0 or 1).
- Let $f(x) = a \cdot x$, where a is some unknown constant. Defining the oracle operator in the usual way (i.e. $\hat{U}_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$), show that the output of the following quantum circuit yields the value of a .



Hint: you may use the identity $H^{\otimes L} |y\rangle = \frac{1}{\sqrt{2^L}} \sum_{n=0}^{2^L-1} (-1)^{x \cdot y} |y\rangle$ without proof.

2. Question Two: Using Qubit to Store Binary

a. *Question:* **Qubit registers as classical data storage devices** Let x be a 3-bit number with binary digits $\{x_0, x_1, x_2\}$, i.e. $x = \sum_{n=0}^2 x_n 2^n$. This number can be represented as a quantum state of two qubits as follows:

$$|\psi(x)\rangle = \frac{1}{2}(|11\rangle + \zeta_2 |10\rangle + \zeta_1 |01\rangle + \zeta_0 |00\rangle)$$

where $\zeta_n = 2x_n - 1$ (i.e. the bits of x stored in the phases of the probability amplitudes of the computational basis states, with phase $\phi_n = 0$ corresponding to $x_n = 1$ and $\phi_n = \pi$ corresponding to $x_n = 0$)

- Why cannot we use the probability amplitude of the state $|11\rangle$ to store a fourth bit?
- Devise simple quantum circuits to store the following numbers:
 - $x = 7$
 - $x = 3$
 - $x = 4$
- It has been estimated that all the information stored in all of the electronic data storage technology world-wide amounts to about $1.4 \cdot 10^{24}$ bits. If we decided to encode this information in a multi-qubit state, now many qubits would be needed?
- À propos the previous question, why would such an approach to data storage be of dubious utility?

F. Problem Set 6

1. Question One: Using the Discrete Fourier Transform

a. *Question:* Find, simplify and plot the *Discrete Fourier Transform* of the following sequences analytically:

- $\{0, 1, 0, 1\}$
- $\{0, 1, 2, 0, 1, 2, 0, 1, 2\}$
- $\{0, 4, 2, 0, 4, 2, 0, 4\}$

2. *Question Two: Finding and Plotting Frequencies using the Discrete Fourier Transform*

a. *Question:*

- (a) Consider the array of $N = 12$ values of a function of period $p = 4$:

$$f_k = \{-3, 1, -1, 3, -3, 1, -1, 3, -3, 1, -1, 3\}$$

Numerically calculate the Discrete Fourier Transform and plot $|\tilde{f}_l|$ for $l = 0, 1, \dots, 11$.

- (b) Now consider the array of $N = 14$ values of the same function

$$f_k = \{-3, 1, -1, 3, -3, 1, -1, 3, -3, 1, -1, 3, -3, 1\}$$

Numerically calculate the Discrete Fourier Transform and plot $|\tilde{f}_l|$ for $l = 0, 1, \dots, 13$.

3. *Question Three: The Quantum Fourier Transform*

a. *Question:* The Quantum Fourier Transform on n qubits is defined by

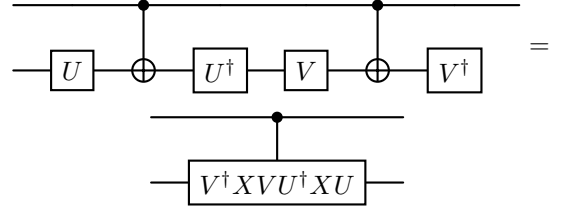
$$\hat{U}_{QFT} |l\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \exp\left\{2\pi i \frac{kl}{2^n}\right\} |k\rangle$$

Prove \hat{U}_{QFT} is unitary.

G. Problem Set 7

1. *Question One: Generalizing Controlled Unitaries*

a. *Question:* Prove the following quantum circuit identity:



where U and V are unitary operators. Prove that any unitary operator can be expressed in the form $V^\dagger X V U^\dagger X U$ (thus this circuit allows *any* controlled unitary to be performed using local unitaries and CNOTs).

2. *Question Two: Generalizing Unitaries Analytically*

a. *Question:* Let $\hat{U}(\theta) = \cos \frac{\theta}{2} \hat{I} + i \sin \frac{\theta}{2} \hat{Z}_0$, where \hat{I} and \hat{Z}_0 is the standard (θ -independent) Pauli operator (similarly for \hat{X}_0 and \hat{Y}_0 below). Find:

- (a) $\hat{X}(\theta) = \hat{U}(\theta) \hat{X}_0 \hat{U}^\dagger(\theta)$ *Hint: slogging through the matrix multiplication will get you there, but it might be quicker to use $\hat{Z}_0 \hat{X}_0 = -\hat{X}_0 \hat{Z}_0$, (which implies $\hat{Z}_0 \hat{X}_0 \hat{Z}_0 = -\hat{X}_0$), and $[\hat{Z}_0, \hat{X}_0] = i2\hat{Y}_0$*

(b) $\hat{Y}(\theta) = \hat{U}(\theta) \hat{Y}_0 \hat{U}^\dagger(\theta)$

(c) $\hat{Z}(\theta) = \hat{U}(\theta) \hat{Z}_0 \hat{U}^\dagger(\theta)$

- (d) Suppose one could implement $\hat{X}(\theta)$ for an arbitrary value of θ . How would use use it to implement the following (If you can't find a solution, try proving it's impossible instead):

(i) \hat{Y}_0

(ii) \hat{Z}_0

(iii) The Hadamard gate \hat{H}

H. Problem Set 8

1. Question One: Time Dependence in Quantum Information

We saw in class that realistic physical qubits are continuously evolving in time, so that the state of a single qubit is $|\phi(t)\rangle = A(t)|0\rangle + B(t)|1\rangle$. Here we are going to consider the case of single qubit operations in which the drive frequency is slightly detuned from the qubit resonance frequency. Let $\omega = \frac{E_1 - E_0}{\hbar}$ be the natural frequency of the qubit; when an external force, oscillating at frequency ω_d , is applied, the amplitudes $A(t)$ and $B(t)$ obey the following differential equations:

$$\begin{aligned} i\dot{A} &= -\frac{\omega}{2}A - \Omega_0 \cos(\omega_d t)B \\ i\dot{B} &= -\frac{\omega}{2}B - \Omega_0 \cos(\omega_d t)A \end{aligned}$$

where \dot{A} is the time derivative of $A(t)$, and Ω_0 is a constant with units of frequency, and proportional to the strength of the applied force.

- (a) Introducing the new variables $\alpha(t) = \exp(-i\omega_d t/2)A(t)$ and $\beta(t) = \exp(i\omega_d t/2)B(t)$, and using the rotating wave approximation, show that $\alpha(t)$ and $\beta(t)$ obey the following time-independent equations:

$$i\dot{\alpha} = \frac{\Delta\alpha + \Omega_0\beta}{2} \quad (\text{A})$$

$$i\dot{\beta} = \frac{-\Delta\beta + \Omega_0\alpha}{2} \quad (\text{B})$$

where $\Delta = \omega_d - \omega$

- (b) By differentiating (A) and substituting from (A) and (B), one can obtain a simple second-order ordinary differential equation for α . By solving this equation (and the similar equation for β), show that

$$\begin{bmatrix} \alpha(t) \\ \beta(t) \end{bmatrix} = \hat{U}(t) \begin{bmatrix} \alpha(0) \\ \beta(0) \end{bmatrix}$$

where $\hat{U}(t) = \cos(\omega t/2)\hat{I} - i\sin(\Omega t/2)\{\Delta\hat{Z} - \Omega_0\hat{X}\}/\Omega$, and $\Omega = \sqrt{\Omega_0^2 + \Delta^2}$

2. Question Two: Solving the Equations of Motion for Quantum States

- a. Question: The evolution of the state $|\varphi_{AB}(t)\rangle = \alpha(t)|00\rangle + \beta(t)|01\rangle + \gamma(t)|10\rangle + \delta(t)|11\rangle$ of two interacting qubits has the following form:

$$i\hbar \frac{\partial}{\partial t} \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix} = \hbar\Omega_0 \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & w & 0 \\ 0 & w & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix}$$

where Ω_0 and w are real constants.

- (a) Solve the equation of motion to find the state after a time t .
- (b) At what time t does the state correspond to a $\sqrt{\text{SWAP}}|\varphi_{AB}(0)\rangle$?
- (c) Does this evolution constitute a “universal gate” for quantum computing? Give a quantum circuit diagram to illustrate how it might be used to create a CNOT.

I. Extra Problems

1. Question One: Quantum Fourier Transform

- a. Question: The Quantum Fourier Transform on n qubits is defined by

$$\hat{U}_{QFT}|l\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \exp\left\{2\pi i \frac{kl}{2^n}\right\} |k\rangle$$

Prove \hat{U}_{QFT} is unitary.

2. Question Two: Quantum Fourier Transform

a. Question:

3. Question Three: Quantum Fourier Transform

a. Question:

4. Question Four: Quantum Fourier Transform

a. Question:

5. Question Five: Quantum Fourier Transform

a. Question: The bit-by-bit modulo-2 product of two L-bit integers a and b is defined as

$$pipgijq$$

IV. MIDTERM QUESTIONS

A. Midterm One

1. Question One: Unitaries in \mathbb{C}^2

a. Question: We saw in class that a generic 2x2 unitary matrix of determinant-1 has the form

$$\hat{U} = \begin{bmatrix} a & b \\ -b^* & a^* \end{bmatrix} = \begin{bmatrix} |a| \exp\{i\alpha\} & |b| \exp\{i\beta\} \\ -|b| \exp\{-i\beta\} & |a| \exp\{-i\alpha\} \end{bmatrix}$$

where $|a|^2 + |b|^2 = 1$. Defining the phase-shift gate:

$$\hat{R}_z(\phi) = \begin{bmatrix} \exp\{i\phi\} & 0 \\ 0 & \exp\{-i\phi\} \end{bmatrix}$$

show that \hat{U} may be written as $\hat{R}_z(\phi)\hat{H}\hat{R}_z(\theta)\hat{H}\hat{R}_z(\chi)$ and find expressions for $|a|$, $|b|$, α and β in terms of ϕ , θ and χ .

b. Answer: First notice:

$$\hat{R}_z(\phi)\hat{H}\hat{R}_z(\theta)\hat{H}\hat{R}_z(\chi) = \hat{R}_z(\phi)\hat{R}_x(\theta)\hat{R}_z(\chi)$$

Therefore it follows that:

$$\begin{aligned} \hat{R}_z(\phi)\hat{R}_x(\theta)\hat{R}_z(\chi) &= \begin{bmatrix} \exp\{i\phi\} & 0 \\ 0 & \exp\{-i\phi\} \end{bmatrix} \\ &\cdot \begin{bmatrix} 0 & \exp\{i\theta\} \\ \exp\{i\theta\} & 0 \end{bmatrix} \cdot \begin{bmatrix} \exp\{i\chi\} & 0 \\ 0 & \exp\{-i\chi\} \end{bmatrix} \\ &= \begin{bmatrix} \exp\{i\phi\} & 0 \\ 0 & \exp\{-i\phi\} \end{bmatrix} \\ &\cdot \begin{bmatrix} 0 & \exp\{i(\theta - \chi)\} \\ \exp\{i(\theta + \chi)\} & 0 \end{bmatrix} \\ &= \begin{bmatrix} 0 & \exp\{i(\theta + \phi - \chi)\} \\ \exp\{i(\theta + \chi - \phi)\} & 0 \end{bmatrix} \\ &= \begin{bmatrix} |a| \exp\{i\alpha\} & |b| \exp\{i\beta\} \\ -|b| \exp\{-i\beta\} & |a| \exp\{-i\alpha\} \end{bmatrix} \end{aligned}$$

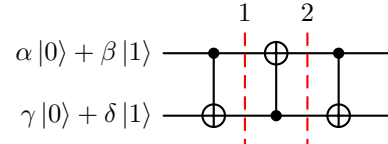
Therefore, it follows that

$$a = 0; b = \exp\{i(\phi - \chi)\}$$

$$\alpha = 0; \beta = \theta$$

2. Question Two: Tracing Circuits

a. Question: Consider the following quantum circuit:



(a) Write down the quantum state at point 1

(b) Write down the quantum state at point 2

(c) What is the final state?

(d) Is the final state entangled? If so, calculate its concurrence.

b. Answer: Let $|\psi_n\rangle$ denote the state at step n , further, let $|\psi_0\rangle$ be the initial state and $|\psi_3\rangle$ be the final state.

$$\begin{aligned}
|\psi_0\rangle &= (\alpha|0\rangle_1 + \beta|1\rangle_1) \otimes (\gamma|0\rangle_0 + \delta|1\rangle_0) \\
&= \alpha\gamma|0\rangle_1|0\rangle_0 + \alpha\delta|0\rangle_1|1\rangle_0 \\
&\quad + \beta\gamma|1\rangle_1|0\rangle_0 + \beta\delta|1\rangle_1|1\rangle_0 \\
&= \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle \\
\therefore |\psi_1\rangle &= \text{CNOT}|\psi_0\rangle \\
&= \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|11\rangle + \beta\delta|10\rangle \\
\therefore |\psi_2\rangle &= \text{CNOT}^{-1}|\psi_1\rangle \\
&= \alpha\gamma|00\rangle + \alpha\delta|11\rangle + \beta\gamma|01\rangle + \beta\delta|10\rangle \\
\therefore |\psi_3\rangle &= \text{CNOT}|\psi_2\rangle \\
&= \alpha\gamma|00\rangle + \alpha\delta|10\rangle + \beta\gamma|01\rangle + \beta\delta|11\rangle \\
&= (\gamma|0\rangle + \delta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle)
\end{aligned}$$

Since the state is separable, it is not entangled. Effectively, the set of gates shown above is a **SWAP** gate this can be verified by calculating the concurrence as

$$\begin{aligned}
C &= 2|\alpha\gamma\beta\delta - \alpha\delta\beta\gamma| \\
&= 0
\end{aligned}$$

Therefore, the state is not entangled.

2. Question Two: Base 10 in Quantum States

a. *Question:* Let x be a 3-bit number with binary digits $\{x_2, x_1, x_0\}$, i.e. $x = \sum_{n=0}^2 x_n 2^n$. This number can be represented as a quantum state of two qubits as follows:

$$|\psi(x)\rangle = \frac{1}{2}(|11\rangle + \zeta_2|10\rangle + \zeta_1|01\rangle + \zeta_0|00\rangle)$$

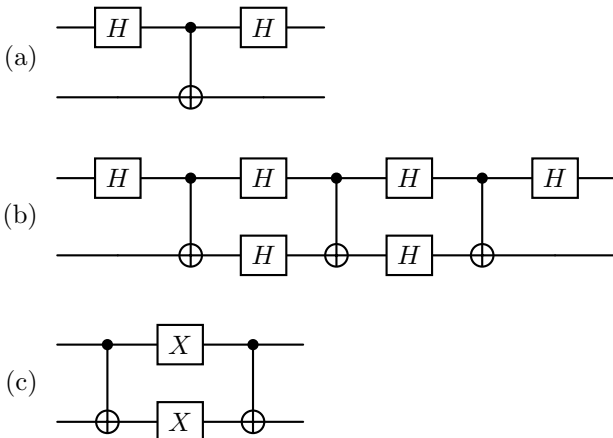
where $\zeta_n = 2x_n - 1$ (i.e. the bits of x stored in the phases of the probability amplitudes of the computational basis states, with phase $\phi_n = 0$ corresponding to $x_n = 1$ and phase $\phi_n = \pi$ corresponding to $x_n = 0$.)

- What is the state $|\psi(5)\rangle$?
- What is the concurrence of the state $|\psi(5)\rangle$?
- Give a simple quantum circuit to create the state $|\psi(5)\rangle$.

B. Midterm Two

1. Question One

a. *Question: Circuit Simplification* Simplify the following quantum circuits



V. EQUATIONS & FORMULAS

A. Concurrence and Schmidt Decomposition

$$|\varphi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \quad (24)$$

$$|\varphi\rangle = \lambda_0|u_0\rangle|v_0\rangle + \lambda_1|u_1\rangle|v_1\rangle$$

$$C = 2|\alpha\delta - \beta\gamma| = 2\lambda_0\lambda_1 \quad (25)$$

$$C = \begin{cases} 0 & \text{Not at all entangled} \\ 1 & \text{Completely entangled} \end{cases} \quad (26)$$

$$\hat{Z}\hat{X} = i\hat{Y} = -\hat{X}\hat{Z} \quad (36)$$

$$\hat{Y}\hat{Z} = i\hat{X} = -\hat{Z}\hat{Y} \quad (37)$$

$$\lambda_0^2 + \lambda_1^2 = 1 \quad (27)$$

$$\hat{X}\hat{X} = \hat{Y}\hat{Y} = \hat{Z}\hat{Z} = \hat{I} \quad (38)$$

$$\lambda^2 = \frac{1 \pm \sqrt{1-C}}{2} \quad (28)$$

$$\hat{\sigma}_i \hat{\sigma}_j = \hat{I} \delta_{ij} + i \sum_{k=1}^3 \epsilon_{ijk} \hat{\sigma}_k \quad (39)$$

1. Pauli Matrices

Where δ is the *Kronecker delta*, i.e. 1 if $i = j$ or 0 if $i \neq j$ and ϵ is the Levi-Civita symbol, i.e. if an even permutation then $\epsilon_{ijk} = 1$, $\epsilon_{ijk} = -1$, and $\epsilon_{iik} = 0$ (any two or more subscripts are the same).

$$\hat{I} = \hat{\sigma}_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad (29)$$

$$\exp\{i\theta \mathbf{n} \cdot \hat{\sigma}\} = \cos \theta \hat{I} + i \sin \theta \mathbf{n} \cdot \hat{\sigma} \quad (40)$$

$$\hat{X} = \hat{\sigma}_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad (30)$$

B. Fourier Transform

$$\hat{Y} = \hat{\sigma}_2 = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad (31)$$

$$\hat{U}_{QFT} |l\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \exp\left\{2\pi i \frac{kl}{2^n}\right\} |k\rangle \quad (41)$$

$$\hat{Z} = \hat{\sigma}_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad (32)$$

$$H^{\otimes L} |y\rangle = \frac{1}{\sqrt{2^L}} \sum_{n=0}^{2^L-1} (-1)^{x \cdot y} |y\rangle \quad (42)$$

$$\hat{H} = \frac{1}{\sqrt{2}}(\hat{X} + \hat{Z}) = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (33)$$

$$x \oplus y = \begin{cases} 0 & x = y \\ 1 & x \neq y \end{cases} \quad (43)$$

$$\hat{X}\hat{Y} = i\hat{Z} = -\hat{Y}\hat{X} \quad (34)$$

Defined for $\forall x, y \in \{0, 1\}$

$$\hat{X}\hat{Z} = i\hat{Y} = -\hat{Z}\hat{X} \quad (35)$$

VI. THEOREMS

-
- [1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2010).
 - [2] Also known as an EPR Pair or an entangled state.
 - [3] A. Einstein, B. Podolsky, and N. Rosen, Can quantum-mechanical description of physical reality be considered complete?, *Phys. Rev.* **47**, 777 (1935).
 - [4] Vague, but it involves either the same and negative or applying a few Pauli operators and other unitaries.
 - [5] That is a state which has concurrence $C = 1$.
 - [6] D. Deutsch and R. Jozsa, Rapid solution of problems by quantum computation, *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences* **439**, 553–558 (1992).
 - [7] Something like this bitflip error.
 - [8] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels, *Phys. Rev. Lett.* **70**, 1895 (1993).
 - [9] A. K. Rao, Investigating locality in quantum systems (2023), preprint on https://drive.google.com/file/d/11Jxuwosy_RHILA6zE0KnV90gzT-gSnZz/view?usp=drive_link.
 - [10] D. Deutsch and P. Hayden, Information flow in entangled quantum systems, *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences* **456**, 1759–1774 (2000).
 - [11] F. Hirsch, M. T. Quintino, J. Bowles, and N. Brunner, Genuine hidden quantum nonlocality, *Physical Review Letters* **111**, 10.1103/physrevlett.111.160402 (2013).
 - [12] M. Nagasawa, On the locality of hidden-variable theories in quantum physics, *Chaos, Solitons & Fractals* **8**, 1773–1792 (1997).
 - [13] H. L. Zhao, On the implication of bell’s probability distribution and proposed experiments of quantum measurement, *Journal of Experimental and Theoretical Physics* **117**, 999–1010 (2013).
 - [14] D. H. McIntyre, *Quantum Mechanics* (Cambridge University Press, 2022).
 - [15] B. Li, Y. Cao, Y.-H. Li, W.-Q. Cai, W.-Y. Liu, J.-G. Ren, S.-K. Liao, H.-N. Wu, S.-L. Li, L. Li, N.-L. Liu, C.-Y. Lu, J. Yin, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, Quantum state transfer over 1200 km assisted by prior distributed entanglement, *Phys. Rev. Lett.* **128**, 170501 (2022).