PH558/964 Advanced Quantum Mechanics: Assignment 3

Dr Daniel K. L. Oi[1] and Dr Jasminder Sidhu[1]
[1] *Department of Physics, University of Strathclyde, Glasgow G4 0NG, UK*

Provide clear and concise explanations of your solutions. The due date is **TBA**, this will be announced via MyPlace once a date can be found to avoid too much of a clash with exams and assignments of other classes. It is anticipated that the due date will be in May 2021 to allow sufficient time to complete the assignment. As usual, solutions should be uploaded as a single PDF document to MyPlace. Typed or handwritten solutions acceptable, however they must be easily readable. There are numerous online tools for converting images into a PDF.

I. BERNSTEIN-VAZIRANI ALGORITHM

Consider a classical Boolean function $\{0,1\}^n \to \{0,1\}$ that is defined as,

$$f_a(x) = x.a \mod 2, \tag{1}$$

where $x = x_0 x_1 \dots x_{n-1}$ and $a = a_0 a_1 \dots a_{n-1}$ are n-bit strings, and $x.a = \sum_{j=0}^{n-1} x_j a_j$. The function is given to us as a black box and we are not told the value of a. Our task is to determine a with as few uses as possible.

A. 2 Marks

Classically, how can you determine the n-bits of a with n uses of the black box function? I.e. what values of x do you input into f_a, and how do you use the outputs to determine a?

B. 3 Marks

We are also given a unitary black box that encodes f_a whose action is defined as:

$$\hat{U}_a |x\rangle_S |y\rangle_A = |x\rangle_S |y \oplus f_a(x)\rangle_A \tag{2}$$

where x is an n-bit number and $\{|x\rangle_A\}$ is the computational basis for the System, and y is a single bit, and $\{|y\rangle_A\}$ is the computational basis for the Ancilla.

We start off with an initial quantum state $|\Psi_0\rangle = |0\rangle_S \otimes |1\rangle_A$ and apply the Hadamard gate to all of the first n (system) qubits and the ancilla qubit to get the state,

$$\begin{aligned} |\Psi_1\rangle_{SA} &= H_S^{\otimes n} \otimes H_A |\Psi_0\rangle = (H|0\rangle)_S^{\otimes n} \otimes H_A |1\rangle \\ &= \frac{1}{(\sqrt{2})^n} \left(\sum_{x=0}^{2^n-1} |x\rangle_S \right) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)_A. \end{aligned} \tag{3}$$

Show that if we now apply $\hat{U}_a$ to $|\Psi_1\rangle$, we get the resultant state,

$$\begin{aligned} |\Psi_2\rangle_{SA} &= \hat{U}_a |\Psi_1\rangle_{SA} = |\psi_2\rangle_S \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)_A \\ &= \frac{1}{(\sqrt{2})^n} \left(\sum_{x=0}^{2^n-1} (-1)^{f_a(x)} |x\rangle_S \right) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)_A. \end{aligned} \tag{4}$$

C. 5 Marks

We will now ignore the Ancilla and only consider the state on the System,

$$|\psi_2\rangle_S = \frac{1}{(\sqrt{2})^n} \sum_{x=0}^{2^n-1} (-1)^{f_a(x)} |x\rangle_S. \tag{5}$$

We now apply the Hadamard gate to all the n (system) qubits. Show that the state of the system is now,

$$\begin{aligned} |\psi_3\rangle_S &= H^{\otimes n} |\psi_2\rangle_S \\ &= \frac{1}{2^n} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} (-1)^{x.a} (-1)^{x.y} |y\rangle_S, \end{aligned} \tag{6}$$

where y is an n-bit number and $\{|y\rangle_S\}$ is the computational basis for the System.

D. 5 Marks

Hence show that if the System is now measured in the computational basis, the result will be $|a\rangle$. Hint: Consider the cases where $y \neq a$ and $y = a$ separately and determine how many terms are $+1$ or -1 for the sum over x (for a given y).

E. 5 Marks

Draw the quantum circuit diagram representing the algorithm acting on an initial state $|\Psi_0\rangle_{SA}$.

F. 10 Marks

For $n = 2, a = 10$, demonstrate the quantum algorithm in action, i.e. show the steps B-D explicitly, expanding out terms and showing the interference.

II. GROVER'S ALGORITHM

We are told that out of a basis set of N orthonormal states $\{|x\rangle\}_{x=1}^{N}$, some states are solutions that we would like to find. We denote this set of **multiple** solutions $\mathcal{A}$ and we also know that there are M solutions, $1 \leq M \ll N$. We will use Grover's algorithm to find one of the solutions $x \in \mathcal{A}$ in order $\mathcal{O}\left(\sqrt{\frac{N}{M}}\right)$ steps.

We define the *superposition of solutions* as

$$|w\rangle = \frac{1}{\sqrt{M}} \sum_{x \in \mathcal{A}} |x\rangle, \tag{7}$$

and are given a quantum oracle (black box),

$$\hat{U}_w = \mathbb{I} - 2|w\rangle\langle w|, \tag{8}$$

that encodes the solutions. The superposition of all states is denoted,

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=1}^{N} |x\rangle, \tag{9}$$

and we define another operator,

$$\hat{U}_s = 2|s\rangle\langle s| - \mathbb{I}. \tag{10}$$

A. 3 Marks

Show that both $\hat{U}_w$ and $\hat{U}_s$ are unitary.

B. 2 Marks

Calculate the overlap $\langle s|w\rangle$ between $|s\rangle$ and $|w\rangle$.

C. 3 Marks

The states $|s\rangle$ and $|w\rangle$ are non-orthogonal but independent hence span a 2-dimensional subspace we will call $\mathcal{G}$. We define two normalised states within $\mathcal{G}$ as,

$$\left|s^{\perp}\right\rangle = \frac{1}{\sqrt{N-M}} \left(\sqrt{N}|w\rangle - \sqrt{M}|s\rangle\right) \tag{11}$$

$$\left|w^{\perp}\right\rangle = \frac{1}{\sqrt{N-M}} \left(\sqrt{N}|s\rangle - \sqrt{M}|w\rangle\right), \tag{12}$$

where $|s\rangle$ and $|w\rangle$ act as a **non-orthogonal** (but normalised) basis for $\mathcal{G}$.

Show that $\left|s^{\perp}\right\rangle, \left|w^{\perp}\right\rangle$ are in fact orthogonal to $|s\rangle, |w\rangle$ respectively

D. 2 Marks

Show how to express $|s\rangle$ as a superposition of the $|w\rangle$ and $\left|w^{\perp}\right\rangle$ states. Note: $\{|w\rangle, \left|w^{\perp}\right\rangle\}$ form an orthonormal basis of $\mathcal{G}$ in which we can use to write further calculations.

E. 8 Marks

Show that in the $\{|w\rangle, \left|w^{\perp}\right\rangle\}$ basis,

$$U_G = (U_s U_w) = \begin{pmatrix} \frac{N-2M}{N} & 2\frac{\sqrt{M(N-M)}}{N} \\ -2\frac{\sqrt{M(N-M)}}{N} & \frac{N-2M}{N} \end{pmatrix}. \tag{13}$$

F. 4 Marks

Show that $\frac{1}{\sqrt{2}}\left(|w\rangle \pm i\left|w^{\perp}\right\rangle\right)$ are eigenstates of $\hat{U}_G$ with eigenvalues $\frac{N-2M}{N} \pm 2i\frac{\sqrt{M(N-M)}}{N}$. **Hint:** This may be done directly! No need to solve eigenvalue equation!

G. 6 Marks

Determine the rotation axis and angle of $\hat{U}_G$ in the qubit subspace $\mathcal{G}$. Illustrate the action of $\hat{U}_G$ on $|s\rangle$ on the Bloch sphere. Include $|w\rangle$ in your diagram and label suitable axes and angles between relevant vectors.

H. 2 Marks

We apply $\hat{U}_G$ a total of $T \in \mathbb{Z}^+$ times to the initial state $|s\rangle$ to generate a final state $|f\rangle = (\hat{U}_G)^T|s\rangle$. We then projectively measure $|f\rangle$ in the $\{|x\rangle\}_{x=1}^{N}$ basis. In order to maximise the probability of obtaining a solution $x \in \mathcal{A}$, what value of T should you choose?

III. ANCILLA-DRIVEN QUANTUM COMPUTATION

Consider the 2-qubit unitary $\hat{U}_{SA}$ shown in Fig. 1.

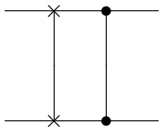


FIG. 1. Control-$\sigma_Z \circ$ SWAP gate

We prepare an input state $|\Psi_0\rangle_{SA} = |\psi_0\rangle_S \otimes |+\rangle_A$, where $|\psi\rangle_S = (\alpha|0\rangle + \beta|1\rangle)_S$ is a general pure qubit state of the system, and $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. We then apply $\hat{U}_{SA}$ to get $|\Psi_1\rangle_{SA} = \hat{U}_{SA}|\Psi_0\rangle_{SA}$. Note that gate $c{-}\sigma_Z = |0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes \sigma_Z$ is symmetric between the two qubits, and that $C{-}Z$ and SWAP commute.

A. 5 Marks

Show that $|\Psi_1\rangle_{SA} = \alpha|+\rangle_S|0\rangle_A + \beta|-\rangle_S|1\rangle_A$, where $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

B. 5 Marks

We now measure the *Ancilla* of $|\Psi_1\rangle_{SA}$ in the basis, $\{|+\phi\rangle, |-\phi\rangle\}$, where $|\pm\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm e^{i\phi}|1\rangle)$. If the outcome $|+\phi\rangle_A$ is obtained, then show that the conditional state of the System is,

$$\left|\psi_2^+\right\rangle_S = \frac{1}{\sqrt{2}}\left[\left(\alpha + e^{-i\phi}\beta\right)|0\rangle + \left(\alpha - e^{-i\phi}\beta\right)|1\rangle\right]_S \quad (14)$$

Hint: $\hat{\mathbb{I}}_A = |+\phi\rangle\langle+\phi|_A + |-\phi\rangle\langle-\phi|_A$ and that $\langle\pm\phi| = \frac{1}{\sqrt{2}}(\langle 0| \pm e^{-i\phi}\langle 1|)$.

C. 5 Marks

In the case of the measurement outcome $|+\phi\rangle_A$, what is the conditional single qubit unitary operation that has been applied to the system? I.e. $\left|\psi_2^+\right\rangle_S = \hat{U}^{+\phi}|\psi_0\rangle_S$ for what unitary operator $\hat{U}^{+\phi}$? Express $\hat{U}^{+\phi}$ in terms of the Hadamard and a diagonal operator.

D. 5 Marks

If instead, the measurement outcome $|-\phi\rangle_A$ is obtained and the state of the system is denoted $\left|\psi_2^-\right\rangle$, what Pauli correction operator relates $\left|\psi_2^-\right\rangle$ to $\left|\psi_2^+\right\rangle$.

IV. 2-STATE QUANTUM KEY DISTRIBUTION

Alice sends to Bob a sequence of qubits either in the state $|+x\rangle$ or $|+z\rangle$ representing the bits "0" or "1" respectively, each state randomly and independently chosen with equal probability. For each qubit Bob receives, he randomly and independently chooses to measure it either in the Z or X basis with equal probability. Alice does not tell Bob what she sent. Depending on his measurement settings and results, Bob broadcasts (publicly) to Alice "Success" or "Failure" according to Table I without announcing his result.

General Hint: Draw probability trees.

Bob's Basis	Bob's Result	Bob's Announcement
Z basis	$\|+z\rangle$	Fail
Z basis	$\|-z\rangle$	Success (record "0")
X basis	$\|+x\rangle$	Fail
X basis	$\|-x\rangle$	Success (record "1")

TABLE I. 2-State QKD Procedure. In the cases of Bob publicly announcing "Success", Alice and Bob both keep a record of their respective data, and then use the associated binary string that is created as an encryption key. In the "Fail" cases, they discard the data.

A. 5 Marks

What is the rate at which Alice and Bob generate an encryption key? The rate r is defined as,

$$r = \frac{\text{Number of "Success" results}}{\text{Total number of signals sent by Alice}}. \quad (15)$$

Assume here that there are no losses and that the quantum channel is perfect (no errors).

B. 5 Marks

When Bob announces "Success", show that he can determine whether Alice sent a 0 or a 1. Assume that the channel is perfect (no errors) and that there are no losses.

C. 5 Marks

From now on, we consider the case of an eavesdropper who intercepts all the states that Alice tries to send to Bob. Eve also randomly and independently chooses to measure each qubit in the Z or X basis with equal probability. She then performs the actions according to Table II.

Eve's Basis	Eve's Result	Eve's Action
Z basis	$\|+z\rangle$	Sends nothing to Bob
Z basis	$\|-z\rangle$	Sends $\|+x\rangle$ to Bob
X basis	$\|+x\rangle$	Sends nothing to Bob
X basis	$\|-x\rangle$	Sends $\|+z\rangle$ to Bob

TABLE II. Eve's eavedropping attack

Alice and Bob publicly discuss the rate at which Bob receives the qubits that Alice sends, i.e. Bob knows when to expect a particular qubit from Alice and can let her know which of the qubits that she sent was actually received. What is the transmission rate η that they will find? The transmission rate η is defined as,

$$\eta = \frac{\text{Number of qubits Bob Received}}{\text{Total number of qubits sent by Alice}}. \quad (16)$$

D. 5 Marks

With Eve tampering with the channel, assume that Alice and Bob still perform the same procedure as in Table I. Assuming the eavesdropping strategy described in Table II, is the binary string that Alice and Bob generate with their procedure secure? I.e. Does Eve have negligible knowledge of the qubits and associated bits that Alice and Bob record in the cases of "Success"?

V. BONUS MARKS

Note: Bonus marks will only count if the marks obtained in the main assignment (the above sections, marked out of 100) is below 60. In that case, any marks obtained in this bonus section will be capped at the amount required to take the total score to 60, i.e. 60%. If the main assignment marks are 60 or above, the bonus marks will not count.

A. 10 Marks

Consider a 3 qubit stabilizer state $|\psi\rangle_{ABC}$ defined by its eigenvalues for the stabilizer operators $\{Z_A X_B I_C, X_A Z_B X_C, I_A X_B Z_C\}$,

$$Z_A X_B I_C |\psi\rangle = (+1)|\psi\rangle_{ABC} \tag{17}$$
$$X_A Z_B X_C |\psi\rangle = (-1)|\psi\rangle_{ABC} \tag{18}$$
$$I_A X_B Z_C |\psi\rangle = (+1)|\psi\rangle_{ABC} \tag{19}$$

Show that the state $|\psi'\rangle_{ABC} = I_A X_B I_C |\psi\rangle_{ABC}$ is also stabilized by the above operators and determine the eigenvalues of $|\psi'\rangle_{ABC}$ for each of the stabilizers. **Hint:** There is no need to explicitly work out $|\psi\rangle_{ABC}$.

B. 10 Marks

Draw the quantum circuit corresponding to,

$$(H_A \otimes H_B)\text{C-NOT}_{\text{A-B}}(H_A \otimes H_B), \tag{20}$$

where we have added Hadamard gates both before and after to the C-NOT's control (A) and target (B) qubits.

Now show that placing the Hadamard gates in this way swaps the roles of control and target qubits of the C-NOT gate. I.e. prove the quantum circuit identity,

$$\text{C-NOT}_{B-A} = (H_A \otimes H_B)\text{C-NOT}_{\text{A-B}}(H_A \otimes H_B). \tag{21}$$

Hint: This can be shown by using the properties of the Pauli operators and Hadamard gate.

C. 10 Marks

Consider a system qubit in a pure state $|\psi\rangle_S = (\alpha|0\rangle + \beta|1\rangle)_S$ and a ancilla qubit in the state $|+\rangle_A = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_A$. We apply a $c{-}\sigma_Z$ gate between system and ancilla to get $|\Psi\rangle_{SA} = c{-}\sigma_Z(|\psi\rangle_S \otimes |+\rangle_A)$. Note that gate $c{-}\sigma_Z = |0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes \sigma_Z$ is symmetric between the two qubits.

We now measure the ancilla qubit of $|\Psi\rangle_{SA}$ in the Z (computational basis) basis and obtain the result a, where $a = 0, 1$ for the $\{|0\rangle, |1\rangle\}$ outcomes respectively.

Show that we can express the conditional state of the system as $Z^a|\psi\rangle_S$, where Z represents the single qubit unitary gate σ_Z.

D. 10 Marks

Show that the SWAP gate between two qubits can be implemented as three CNOT gates as shown in Fig. 2. The SWAP gate may be defined by its action, $|\psi\rangle|\phi\rangle \to |\phi\rangle|\psi\rangle$ for all pure qubit states $|\psi\rangle, |\phi\rangle$. **Hint:** SWAP can also be defined in terms of its action on a suitable orthonormal basis for two qubits, e.g. the computational basis.

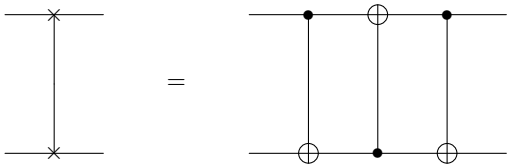


FIG. 2. SWAP Gate Decomposition. The SWAP gate (left) can be decomposed into 3 C-NOT gates (right).

E. 10 Marks

In the ideal BB84 protocol, Alice sends to Bob a sequence of single qubits encoded in $\{|+z\rangle, |-z\rangle, |+x\rangle, |-x\rangle\}$ states, each state chosen randomly and independently (with 25% probability). Bob independently and randomly chooses to measure each qubit received either in the Z or X bases (with 50% probability for each basis). We assume that the quantum channel is lossless and otherwise perfect, except for the presence of an eavesdropper (Eve).

Eve intercepts all the qubits sent by Alice to Bob. For each qubit, she decides with probability p_x to measure it in the X basis, with probability p_z she decides to measure it in the Z basis, and with probability $1 - p_x - p_z$ (and $p_x + p_z \leq 1$) she decides not to measure it but pass it to Bob unchanged. In the cases she does measure the qubit, she records the result and passes onto Bob the resulting eigenstate of the outcome.

Alice and Bob, as usual, announce the bases that they used to send and measure the qubits, respectively. They keep the cases where they used the same basis (sifted/reconciled qubits), discarding the cases of mismatched bases. The quantum bit error rate is defined as,

$$QBER = \frac{N_{wrong}^{sifted}}{N_{total}^{sifted}}, \tag{22}$$

where N_{wrong}^{sifted} is the total number of sifted qubits where Bob's result do not match Alices, and $N_{total}^{sifted} = N_{wrong}^{sifted} + N_{right}^{sifted}$ is the total number of sifted qubits.

As a function of p_x and p_z, what is the quantum bit error rate of these sifted qubits that Alice and Bob have kept? **Hint:** Draw a probability tree.

Orion
PAGE:
DATE: / /

ASSIGNMENT 3

I. BERNSTEIN - VAZIRANI ALGORITHM

$$f:\{0,1\}^n \to \{0,1\}$$

$$f_a(x) = x.a \mod 2$$

where $x = x_0 x_1 \ldots\ldots x_{n-1}$

$a = a_0 a_1 \ldots\ldots a_{n-1}$

$$x.a = \sum_{j=0}^{n-1} x_j a_j$$

A. to determine ⇒ n-bits of a with n uses of function.

[Classically]

$$f_a(x) = x_0 a_0 + x_1 a_1 + x_2 a_2 + \ldots\ldots\ldots + x_{n-1} a_{n-1}$$

put $x_0 = 1$, rest 0, find $f_a(x)$ ..... we get a_0

$x_1 = 1$, rest 0, find $f_a(x)$ ..... we get a_1

$\vdots$

$x_{n-1} = 1$, rest 0, find $f_a(x)$ ..... we get a_{n-1}

With n uses of black box function,

we get a.

B. unitary black box

$$\hat{U}_a |x\rangle_S |y\rangle_A = |x\rangle_S |y \oplus f_a(x)\rangle_A$$

$\{|x\rangle_A\}$ → computational basis for the system

$\{|y\rangle_A\}$ → computational basis for ancilla

Orion
PAGE:
DATE: / /

$$|\psi_0\rangle = |0\rangle_S \otimes |1\rangle_A$$

Applying Hadamard gate to all n qubits and ancilla qubit,

$$|\psi_1\rangle_{SA} = H_S^{\otimes n} \otimes H_A |\psi_0\rangle$$

$$= (H|0\rangle_S^{\otimes n} \otimes H_A|1\rangle)$$

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

Now we apply $\hat{U}_f$ to $|\psi_1\rangle$,

$$\text{So } |\psi_2\rangle_{SA} = \hat{U}_f |\psi_1\rangle_{SA} = \hat{U}_f \left(\sum_{x=0}^{2^n-1} \frac{|x,0\rangle_n - |x,1\rangle}{\sqrt{2}} \right)$$

$$= |\psi_2\rangle_S \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)_A$$

$$|\psi_2\rangle_S = U_f |\psi_1\rangle_S$$

Since $\hat{U}_f |x\rangle_S |y\rangle_A = |x\rangle_S |y \oplus f_a(x)\rangle_A$

$$\text{So } |\psi_2\rangle_{SA} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \frac{1}{\sqrt{2}} \left(\hat{U}_f (|x\rangle_n \otimes |0\rangle) - \hat{U}_f (|x\rangle_n \otimes |1\rangle) \right)$$

$$= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \frac{1}{\sqrt{2}} \left((|x\rangle_n \otimes |0 \oplus f_a(x)\rangle) - (|x\rangle_n \otimes |1 + f_a(x)\rangle) \right)$$

$$= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle_n \otimes \left(\frac{|f_a(x)\rangle - |\overline{f_a(x)}\rangle}{\sqrt{2}} \right)$$

We know that $\frac{f_a|x\rangle - \overline{f_a(x)}}{\sqrt{2}} = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ or $\frac{|1\rangle - |0\rangle}{\sqrt{2}}$

$$\text{So } |\psi_2\rangle_{SA} = \left[\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f_a(x)} |x\rangle_n \right]_S \otimes \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]_A$$

Orion
PAGE:
DATE: / /

Therefore $$|\psi_2\rangle_{SA} = \frac{1}{\sqrt{2^n}} \left(\sum_{x=0}^{2^n-1} (-1)^{f_a(x)} |x\rangle_S \right) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)_A$$

c) Now ignoring the ancilla, we get:

$$|\psi_2\rangle_S = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f_a(x)} |x\rangle_S$$

Applying Hadamard gate to all n qubits.

$$|\psi_3\rangle_S = H^{\otimes n} |\psi_2\rangle_S$$

$$= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f_a(x)} H^{\otimes n} |x\rangle_n$$

∴ Expanding $$H^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{\langle x,y \rangle} |y\rangle$$

Putting in, we get.

$$|\psi_3\rangle_S = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f_a(x)} \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{\langle x,y \rangle} |y\rangle$$

$$= \frac{1}{2^n} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} (-1)^{f_a(x)} \cdot (-1)^{\langle x,y \rangle} |y\rangle$$

Since $f_a(x) = x.a$

$$|\psi_3\rangle_S = \frac{1}{2^n} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} (-1)^{x.a} (-1)^{x.y} |y\rangle_S$$

where y is an n-bit number

$\{|y\rangle_S\}$ is the computational basis of the system

D. After U_f, the state of the system is

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle_n \otimes \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$$

After the effect of applying $H^{\otimes n}$ on an n-qubit computational basis state, we have

$$H^{\otimes}|x\rangle_n = \sum_{y_{n-1}=0}^{1} \cdots \sum_{y_1=0}^{1} \sum_{y_0=0}^{1} (-1)^{\sum_{i=0}^{n-1} x_i y_i} |y_{n-1}\rangle \cdots |y_1\rangle|y_0\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle_n$$

We combine the eq^{n}s to find amplitude in the upper register in state $|y\rangle = |y_{n-1}\rangle |y_{n-2}\rangle \cdots |y_1\rangle |y_0\rangle$

$$c_y = \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)+x \cdot y}$$

$$= \frac{1}{2^n} \prod_{j=0}^{n-1} \left[\sum_{x_j=0}^{1} (-1)^{(a_j + y_j) x_j} \right]$$

For $y_j = a_j \ \forall j \Rightarrow (a_j + y_j) x_j = 2$ or 0 and since this quantity is power of -1, all factors of $(-1)^{(a_j+y_j)x_j}$ are $+1$.

Amplitude for $y = a$ is $+1$.

For $y_j \neq a_j$, $a_j + y_j = 1$, so the sum over x_j for these qubits gives zero.

Amplitude for $y \neq a$ is 0.

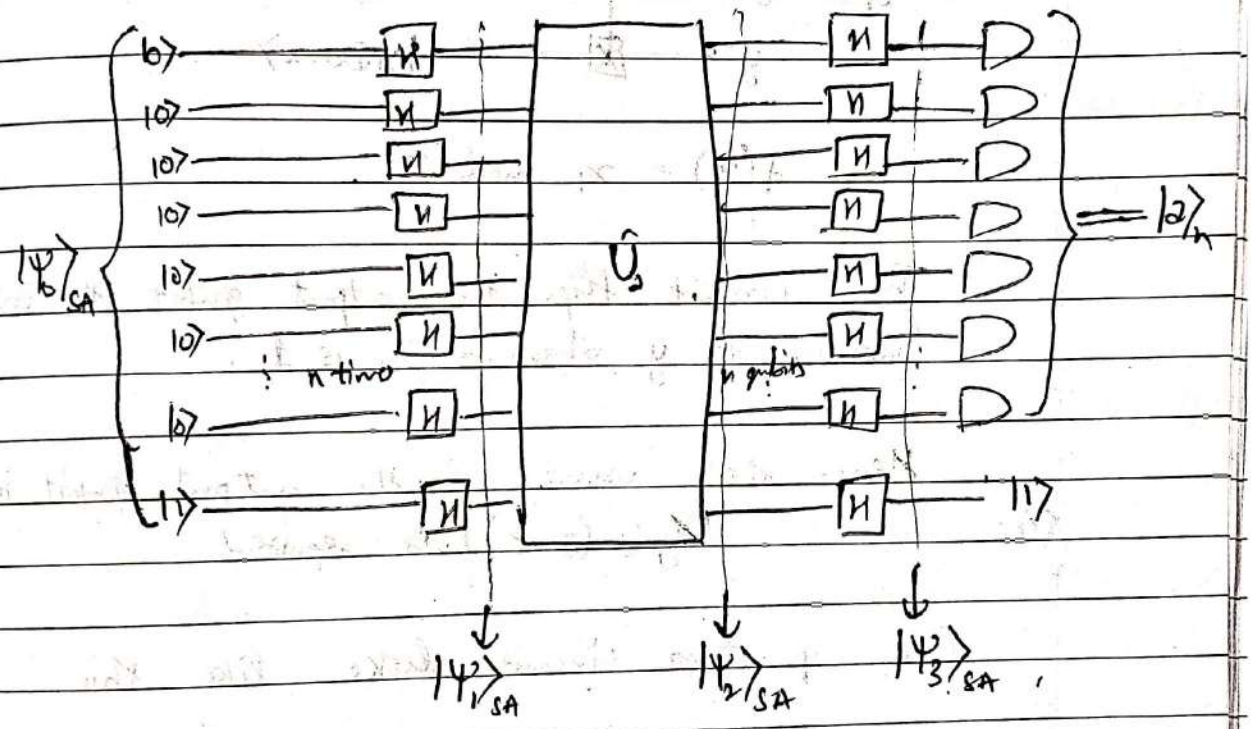
The final result is a product over terms for each qubit and so we get zero, as required.

Including the output qubit, the final state is

$$|a\rangle_n \otimes |1\rangle$$

We just 1 call to the function and a is the measurement of the upper register.

E:



Here $|\psi_0\rangle_{SA}$ is the system with ancilla input. which is $|0\rangle_S \otimes |1\rangle_A$ (initial quantum state)

$|\psi_1\rangle_{SA}$ is the state after Hadamard gate

$|\psi_2\rangle_{SA}$ is the state after applying unitary operator.

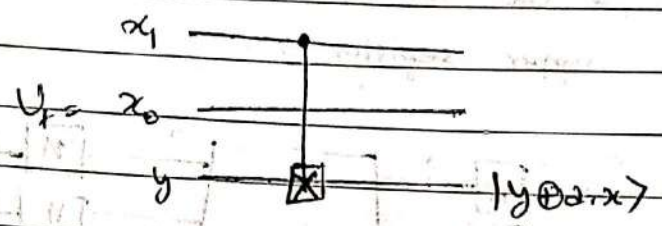
$|\psi_3\rangle_{SA}$ is the state after apply Hadamard gate.

Orion
PAGE:
DATE: / /

F. for $n = 2$, $a = 10$

So $x_0 = 0$, $x_1 = 1$.

The function $a \cdot x$ can be implemented by the gates

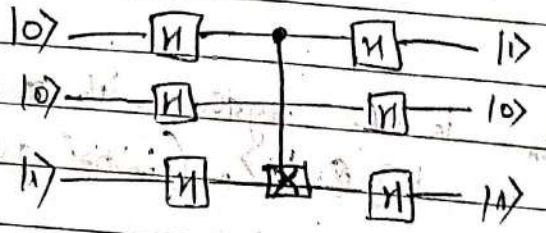


So $f(a) = x_1 \bmod 2$.

The circuit flips the output qubit, the lowest one, initialized to y, whenever x_1 is 1.

Hence the value of the output qubit is $y \oplus (a \cdot x)$ as required.

Our quantum circuit looks like this



Here, the quantum superposition of all possible inputs and then applies operations leads to perfect destructive interference of all states in the superposition except for the one in which the input register is in the state $|2\rangle$

Orion

PAGE:
DATE: / /

~~After applying the 1st Hadamard gate,~~

The initial state of the system is

$$|\psi_0\rangle_{SA} = |0\rangle|0\rangle_S \otimes |1\rangle_A$$

After applying the 1st Hadamard gate.

$$|\psi_1\rangle_{SA} = \frac{1}{\sqrt{2^2}}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right)_S \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$= \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right)_S \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

After applying the operator U_f.

$$|\psi_2\rangle_{SA} = \frac{1}{2}\left((-1)^{0\cdot 1}|00\rangle + (-1)^{1\cdot 0}|10\rangle + (-1)^{1\cdot 0}|11\rangle\right)_S \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

~~$|10\rangle$~~

After applying the Hadamard gate again.

The ancilla $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \xrightarrow[\text{back}]{\text{converts}} |1\rangle$.

and $|\psi_3\rangle_{SA} = |10\rangle_S \otimes |1\rangle_A$

All other terms cancel out. and only term with $y=2$ survives.

II. GROVER'S ALGORITHM

N orthonormal states $\{|x\rangle\}_{x=1}^{N}$

M solutions, $1 \leq M \ll N$.

Using Grover's Algorithm for solution $x \in A$ in order $O\left(\sqrt{\frac{N}{M}}\right)$ steps

The superposition of solutions is

$$|w\rangle = \frac{1}{\sqrt{M}} \sum_{x \in A} |x\rangle$$

quantum oracle (black box) $\hat{U}_w = \mathbb{I} - 2|w\rangle\langle w|$

The superposition of all states is

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=1}^{N} |x\rangle$$

and operator $\hat{U}_s = 2|s\rangle\langle s| - \mathbb{I}$

A. To prove $\Rightarrow$ $\hat{U}_w$ and $\hat{U}_s$ are unitary

for unitary we know $\hat{U}\hat{U}^\dagger = \mathbb{I}$

so $\hat{U}_w \hat{U}_w^\dagger = (\mathbb{I} - 2|w\rangle\langle w|)(\mathbb{I} - 2|w\rangle\langle w|)^\dagger$

$= (\mathbb{I} - 2|w\rangle\langle w|)(\mathbb{I} - 2|w\rangle\langle w|)$

$= \mathbb{I} - 2|w\rangle\langle w| - 2|w\rangle\langle w| + 4|w\rangle\langle w|$

$= \mathbb{I}$.

Orion
PAGE:
DATE: / /

$$\hat{U}_s \hat{U}_s = (2|s\rangle\langle s| - \mathbb{I})(2|s\rangle\langle s| - \mathbb{I})^\dagger$$

$$= (2|s\rangle\langle s| - \mathbb{I})(2|s\rangle\langle s| - \mathbb{I})$$

$$= 4|s\rangle\langle s| - 2|s\rangle\langle s| - 2|s\rangle\langle s| + \mathbb{I}$$

$$= \mathbb{I}$$

Hence, $\hat{U}_s$ and $\hat{U}_w$ are unitary

B. overlap $\langle s|w\rangle$ between $|s\rangle$ and $|w\rangle$

The superposition of non-solutions is

$$|w'\rangle = \frac{1}{\sqrt{N-M}} \sum_{x \notin A} |x\rangle$$

$\langle s|w\rangle$ can be found by the angle between the two vectors.

$$\sin\theta = \sqrt{\frac{M}{N}}$$

which indicates $\langle s|w\rangle = \sqrt{\frac{M}{N}}$

PAGE:
DATE: / /

C. $|s^\perp\rangle = \frac{1}{\sqrt{N-M}}\left(\sqrt{N}|\omega\rangle - \sqrt{M}|s\rangle\right)$

$|\omega^\perp\rangle = \frac{1}{\sqrt{N-M}}\left(\sqrt{N}|s\rangle - \sqrt{M}|\omega\rangle\right)$

for orthogonality,

we find $\langle s|s^\perp\rangle = \frac{1}{\sqrt{N-M}}\left(\sqrt{N}\langle s|\omega\rangle - \sqrt{M}\langle s|s\rangle\right)$

$= \frac{1}{\sqrt{N-M}}\left(\sqrt{N}\times\sqrt{\frac{M}{N}} - \sqrt{M}\right)$

$= 0$

~~$\langle\omega|\omega^\perp\rangle = \frac{1}{\sqrt{N-M}}\left(\sqrt{N}|s\rangle - \sqrt{M}|\omega\rangle\right)$~~

$\langle\omega|\omega^\perp\rangle = \frac{1}{\sqrt{N-M}}\left(\sqrt{N}\langle\omega|s\rangle - \sqrt{M}\langle\omega|\omega\rangle\right)$

$= 0$

Thus, we have $\langle s|s^\perp\rangle$ and $\langle\omega|\omega^\perp\rangle = 0$ which are orthogonal to each other.

D. Now express $|s\rangle$ in terms of $|\omega\rangle$ and $|\omega^\perp\rangle$

Since we know $|\omega\rangle = \frac{1}{\sqrt{M}}\sum|x\rangle$

so $|s\rangle = \sqrt{\frac{N-M}{N}}\left(\frac{1}{\sqrt{N-M}}\sum|x\rangle\right) + \sqrt{\frac{M}{N}}\left(\frac{1}{\sqrt{M}}\sum|x\rangle\right)$

$$\boxed{|s\rangle = \sqrt{\frac{N-M}{N}}\,|\omega^\perp\rangle + \sqrt{\frac{M}{N}}\,|\omega\rangle}$$

Orion

PAGE:
DATE: / /

E. in $\{|w\rangle, |w^+\rangle\}$ basis

$$U_G = (U_s U_w)$$

U_w performs a reflection about the vector $|w^+\rangle$ and orthogonal to $|w\rangle$.
U_s performs a flipping action about $|s\rangle$.

$$U_G = (2|s\rangle\langle s| - \mathbb{I})(\mathbb{I} - 2|w\rangle\langle w|)$$
$$= 2|s\rangle\langle s| - 4|s\rangle\langle s|w\rangle\langle w| - \mathbb{I} + 2|w\rangle\langle w|$$

$$|s\rangle\langle s| = \left(\sqrt{\frac{N-M}{N}}|w^+\rangle + \sqrt{\frac{M}{N}}|w\rangle\right)\left(\sqrt{\frac{N-M}{N}}|w^+\rangle + \sqrt{\frac{M}{N}}|w\rangle\right)$$

$$= \begin{pmatrix} \frac{M}{N} & \sqrt{\frac{M}{N}} \times \sqrt{\frac{N-M}{N}} \\ \sqrt{\frac{N-M}{N}} \times \sqrt{\frac{M}{N}} & \frac{N-M}{N} \end{pmatrix}$$

$$\langle s|w\rangle|s\rangle\langle w| = \sqrt{\frac{M}{N}} \begin{pmatrix} \sqrt{\frac{M}{N}} \\ \sqrt{\frac{N-M}{N}} \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} \frac{M}{N} & 0 \\ \sqrt{\frac{N-M}{N}}\sqrt{\frac{M}{N}} & 0 \end{pmatrix}$$

$$|w\rangle\langle w| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$U_G = 2\begin{pmatrix} \frac{M}{N} & \sqrt{\frac{M}{N}} \times \sqrt{\frac{N-M}{N}} \\ \left(\sqrt{\frac{M}{N}}\right)\left(\sqrt{\frac{N-M}{N}}\right) & \frac{N-M}{N} \end{pmatrix} - 4\begin{pmatrix} \frac{M}{N} & 0 \\ \sqrt{\frac{N-M}{N}}\sqrt{\frac{M}{N}} & 0 \end{pmatrix}$$

$$- \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + 2\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\boxed{U_G = \begin{pmatrix} \frac{N-2M}{N} & \frac{2\sqrt{M(N-M)}}{N} \\ -\frac{2\sqrt{M(N-M)}}{N} & \frac{N-2M}{N} \end{pmatrix}}$$

Orion
PAGE:
DATE: / /

F. For eigenstates $\frac{1}{\sqrt{2}}(|\omega\rangle \pm i|\omega^\perp\rangle)$, applying U_G

$$U_G\left(\frac{1}{\sqrt{2}}|\omega\rangle \pm i|\omega^\perp\rangle\right) = \begin{pmatrix} \frac{N-2M}{N} & \frac{2\sqrt{M(N-M)}}{N} \\ \frac{-2\sqrt{M(N-M)}}{N} & \frac{N-2M}{N} \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} |\omega\rangle & i|\omega^\perp\rangle \\ -i|\omega^\perp\rangle & |\omega\rangle \end{pmatrix}$$

$$= \left(\frac{N-2M}{N} \pm \frac{2i\sqrt{M(N-M)}}{N}\right) \cdot \left(\frac{1}{\sqrt{2}}|\omega\rangle \pm i|\omega^\perp\rangle\right)$$

So the eigenvalues are $\frac{N-2M}{N} \mp \frac{2i\sqrt{M(N-M)}}{N}$

H. We apply $\hat{U}_G$ a total of $T \in \mathbb{Z}^+$ times to initial state $|s\rangle$ to generate $|f\rangle = (\hat{U}_G)^T |s\rangle$.

We projectively measure $|f\rangle$ in the $\{|x\rangle\}_{x=0}^{N}$ basis.

In our case, the angle between them is

$$\sin\gamma = \sqrt{\frac{M}{N}}$$

and initial angle is $\gamma_0 = \frac{\pi}{2} - \gamma$

$$= \frac{\pi}{2} - \sin^{-1}\sqrt{\frac{M}{N}}.$$

After T iterations.

$$\gamma T = \frac{\pi}{2} - (2T+1)\sin^{-1}\sqrt{\frac{M}{N}}.$$

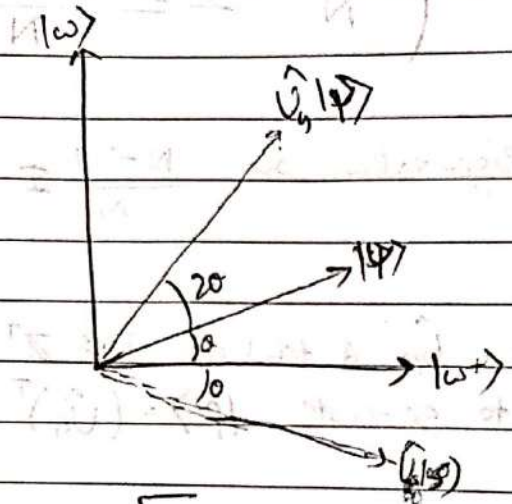
We get probability of obtaining the state $|s\rangle$ as

$$\sin^2\left((2T+1)\sin^{-1}\sqrt{\frac{M}{N}}\right)$$

$$\Rightarrow \boxed{T = \frac{\pi}{4}\sqrt{\frac{N}{M}}}$$

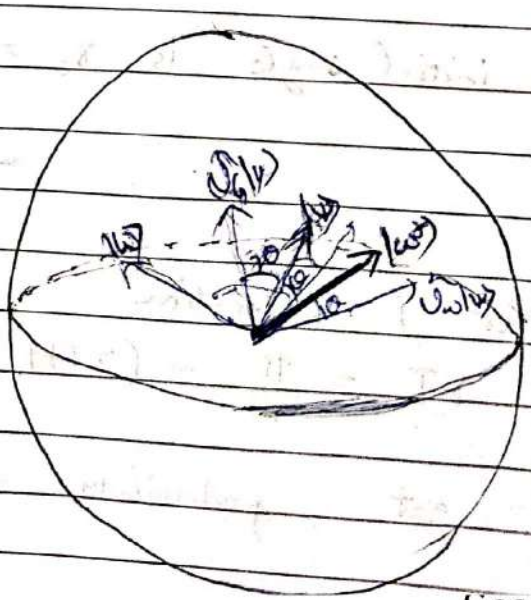
Q. determine ⇒ rotation axis and angle of $\hat{U}_f$ in the qubit subspace of

$\hat{U}_f$ action on $|s\rangle$ on the Bloch sphere.



$$\sin\theta = \sqrt{\frac{M}{N}}$$

$\hat{U}_G = \hat{U}_s\hat{U}_\omega$ where first the reflection is take and then the function is flipped along $|\psi\rangle$.



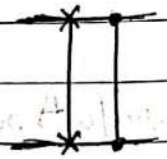
Orion

PAGE:
DATE: / /

$\hat{U}_G$ acts on $|\psi\rangle$ again and again to obtain the solution.

Orion
PAGE:
DATE: / /

III. ANCILLA - DRIVEN QUANTUM COMPUTATION



control-σ_z o SWAP gate

$$|\psi_0\rangle_{SA} = |\psi_0\rangle_S \otimes |+\rangle_A$$

where $|\psi_0\rangle_S = (\alpha|0\rangle + \beta|1\rangle)_S$ is a general pure qubit state

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

Then apply $\hat{U}_{SA}$

$$|\psi_1\rangle_{SA} = \hat{U}_{SA}|\psi_0\rangle_{SA}$$

gate $c\text{-}\sigma_z = |0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes \sigma_z$ is symmetric both the two qubits, and that C-Z and SWAP commute

A.

$$|\psi_0\rangle_S = \alpha|0\rangle + \beta|1\rangle$$

$$|\psi_0\rangle_{SA} = (\alpha|0\rangle + \beta|1\rangle)_S \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_A$$

$$= \frac{1}{\sqrt{2}}(\alpha|0\rangle_S|0\rangle_A + \beta|1\rangle_S|0\rangle_A + \alpha|0\rangle_S|1\rangle_A + \beta|1\rangle_S$$

Now we know that

$$|\psi_1\rangle_{SA} = \hat{U}_{SA}|\psi_0\rangle_{SA}$$

where $\hat{U}_{SA} \rightarrow$ C-Z gate.

Since $C_Z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$

$$\longrightarrow \frac{1}{\sqrt{2}}\left(\alpha|0\rangle_A|0\rangle_B + \alpha|0\rangle_A|1\rangle_B + \beta|1\rangle_A|0\rangle_B - \beta|1\rangle_A|1\rangle_B\right)$$

$$= \alpha\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)_S|0\rangle_A + \beta\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)_S|1\rangle_A$$

$$= \boxed{\alpha|+\rangle_S|0\rangle_A + \beta|-\rangle_S|1\rangle_A .}$$

B. Now measure ancilla in the basis $\{|+\phi\rangle, |-\phi\rangle\}$

$$|\pm\phi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle \pm e^{i\phi}|1\rangle\right)$$

$\downarrow$

$|+\phi\rangle_A$ is obtained.

To find $\Rightarrow |\psi_2^+\rangle$

$$\langle\pm\phi| = \frac{1}{\sqrt{2}}\left(\langle 0| \pm e^{-i\phi}\langle 1|\right)$$

and $\hat{\Pi}_A = |+\phi\rangle\langle+\phi|_A + |-\phi\rangle\langle-\phi|_A .$

When we measure in the $\{|\pm\phi\rangle\}$ basis, we have the measurement as

$$|+\phi\rangle\langle+\phi|\psi^+\rangle + \phi|-\phi\rangle\langle-\phi|\psi^+\rangle$$

↑ we don't calculate this since we know the result of ancilla is $|+\phi\rangle$

So our system is -

$$|\psi\rangle_{SA} = |\phi^+\rangle\langle \frac{1}{\sqrt{2}}\langle 0| + e^{-i\phi}\langle 1| \Big| \alpha|+\rangle_S|0\rangle_A + \beta|-\rangle_S|1\rangle_A \Big)$$

$$= |\phi^+\rangle\left(\frac{1}{\sqrt{2}}\alpha\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) + e^{-i\phi}\beta\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\right)$$

$$= \frac{|\phi^+\rangle_A}{\sqrt{2}}\left[\frac{1}{\sqrt{2}}\left[(\alpha + e^{-i\phi}\beta)|0\rangle + (\alpha - e^{-i\phi}\beta)|1\rangle\right]\right]_S$$

So the system is given by

$$|\psi_2^+\rangle_S = \frac{1}{\sqrt{2}}\left[(\alpha + e^{-i\phi}\beta)|0\rangle + (\alpha - e^{-i\phi}\beta)|1\rangle\right]$$

c.

Signifying it as a unitary operator, we have

$$|\psi_2^+\rangle_S = \hat{U}^{+\phi}|\psi_0\rangle_S$$

Since we know $|\psi_2^+\rangle_S = \frac{1}{\sqrt{2}}\left[(\alpha + e^{-i\phi}\beta)|0\rangle + (\alpha - e^{-i\phi}\beta)|1\rangle\right]$

and $|\psi_0\rangle_S = \alpha|0\rangle + \beta|1\rangle$

we have $\hat{U}^{+\phi} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & e^{i\phi} \\ 1 & -e^{i\phi} \end{pmatrix}$

Also taking diagonal operator as phase gate

$$\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$$

we have

$$H\phi = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & e^{i\phi} \\ 1 & -e^{-i\phi} \end{pmatrix}$$

so $\boxed{\hat{U}^{+\phi} = H\phi}$

or $\boxed{\hat{U}^{+\phi}|\psi_0\rangle_s = H\phi|\psi_0\rangle_s}$

D. If $|-\phi\rangle_A$ is obtained and state of system denoted by $|\psi_2^-\rangle$,

we have the system as $|-\phi\rangle\langle-\phi|\psi^+\rangle$. # Here we ignored the - positive term.

so $|\psi\rangle_{SA} = |\phi^-\rangle\left\langle \frac{1}{\sqrt{2}}\langle 0| - e^{-i\phi}\langle -1| \;\middle|\; \alpha|+\rangle_s|0\rangle_A + \beta|-\rangle_s|1\rangle_A \right\rangle$

$$= \frac{|\phi^-\rangle}{\sqrt{2}}\left(\alpha\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) - e^{-i\phi}\beta\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\right)$$

$$= \frac{|\phi^-\rangle}{\sqrt{2}}_A\left[\frac{1}{\sqrt{2}}\left[(\alpha - e^{-i\phi}\beta)|0\rangle + (\alpha + e^{-i\phi}\beta)|1\rangle\right]\right]$$

so $|\psi_2^-\rangle = \frac{1}{\sqrt{2}}\left[(\alpha - e^{-i\phi}\beta)|0\rangle + (\alpha + e^{-i\phi}\beta)|1\rangle\right]$

Here we have $\hat{U}^{-\phi} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -e^{i\phi} \\ 1 & e^{-i\phi} \end{pmatrix}$

To convert $\hat{U}^{-\phi} \rightarrow \hat{U}^{+\phi}$, we apply

Orion
PAGE:
DATE: / /

σ_x pauli correction : which is given by $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

therefore $\boxed{\hat{U}^{+\beta} = \sigma_x \hat{U}^{-\beta}}$

IV. 2-STATE QUANTUM KEY DISTRIBUTION

A $\longrightarrow$ B in $|+x\rangle$ or $|+z\rangle$ representing "0" or "1"

B randomly chooses basis.

Depending on measurement B broadcasts "Success" or "Failure".

Bob's basis	Bob's Result	Bob's Announcement
Z basis	$\|+z\rangle$	Fail
Z basis	$\|-z\rangle$	Success (record "0")
X basis	$\|+x\rangle$	Fail
X basis	$\|-x\rangle$	Success (record "1")

A. To find $\Rightarrow$ rate at which Alice and Bob generate an encryption key.

rate r = $\frac{\text{Number of "success" results}}{\text{Total number of signals sent by Alice}}$

No losses

Since Bob discards when he uses Z basis and gets $|+z\rangle$ and X basis gets $|+x\rangle$, and the bases when Alice and Bob chose different are discarded.

Orion
PAGE:
DATE: / /

Let H/V basis be basis for $|x\rangle$ and D/A basis be basis for $|z\rangle$

We know that Alice sends either $|+x\rangle$ or $|+z\rangle$ represent "0" or "1",

if Alice sends $|+x\rangle$, when Bob measures in H/V basis, $p = 1$ for H and $V = 0$,
but for D/A basis, $p = 1/2$ for either $|+z\rangle$ or $|-z\rangle$

and if Alice sends $|+z\rangle$, when Bob measures in D/A basis, $p = 1$ for D and $A = 0$.
but for H/V basis, $p = 1/2$ for either $|+x\rangle$ or $|-x\rangle$

So, we can say with certainty only in $|+z\rangle$ or $|+x\rangle$ basis.

For success we have

Alice's bit	Bob's basis	Bob's measurement
$\|+x\rangle$ $(p=1/2)$	Z basis $(p=1/2)$	$\|-z\rangle$ $(p=1/2)$
$\|+z\rangle$ $(p=1/2)$	X basis $(p=1/2)$	$\|-x\rangle$ $(p=1/2)$

So $$p = \frac{1}{2}\times\frac{1}{2}\times\frac{1}{2} + \frac{1}{2}\times\frac{1}{2}\times\frac{1}{2}$$

$$= \frac{1}{8} + \frac{1}{8} = \frac{1}{4}.$$

which is also the rate r.

So $$\boxed{\text{rate } r = \frac{1}{4}}$$

Orion
PAGE:
DATE: / /

B. When Bob announces "Success", he can determine whether Alice sent a 0 or a 1

No losses, no errors.

When Bob announces "Success"

if Bob's measurement

is $|-z\rangle$ → then only possibility is it is sent by $|+x\rangle$ so bit is "0"

is $|-x\rangle$ → then only possibility is it is sent by $|+z\rangle$ so bit is "1"

Therefore Bob can say with 100% probability the bit by "Success" rate.

C. Eve intercepts the signal.

Eve's Basis	Eve's Result	Eve's Action
Z basis	$\|+z\rangle$	Sends nothing to Bob
Z basis	$\|-z\rangle$	sends $\|+x\rangle$ to Bob
X basis	$\|+x\rangle$	Sends nothing to Bob
X basis	$\|-x\rangle$	Sends $\|+z\rangle$ to Bob

Alice and Bob publicly discuss the rate at which Bob receives the qubits that Alice sends.

Transmission rate η → ??

Orion
PAGE:
DATE: / /

η = Number of qubits Bob received / Total Number of qubits sent by Alice.

Now when Eve is present.

Alice sends qubit if Eve intercepts and sends message, then no. of qubits received by Bob will decrease.

1. Alice sends qubit.
2. Eve checks in the basis and discards if not $|-z\rangle$ or $|-x\rangle$.

So Alice's bit	Eve's basis	Eve's measurement
$\|+x\rangle$ $p=1/2$	Z basis $(p=1/2)$	$\|-z\rangle$ $(p=1/2)$
$\|+z\rangle$ $p=1/2$	X basis $(p=1/2)$	$\|+x\rangle$ $(p=1/2)$

p of qubit being forwarded is $\frac{1}{2}\times\frac{1}{2}\times\frac{1}{2} + \frac{1}{2}\times\frac{1}{2}\times\frac{1}{2}$

$= \frac{1}{4}$

$\eta = \frac{1}{4}$ or 25%.

So the transmission rate η will be only $\frac{1}{4}$.

Orion

PAGE:
DATE: / /

D. Now, when Eve is tampering with the channel.

Eve's Basis	Eve's Result	Eve's Action
Z basis	$\|+z\rangle$	sends nothing to Bob
Z basis	$\|-z\rangle$	send $\|+x\rangle$ to Bob
X basis	$\|+x\rangle$	sends nothing to Bob
X basis	$\|-x\rangle$	send $\|+z\rangle$ to Bob

Since Bob discards any message that is not in $|+x\rangle$ or $|+z\rangle$ direction, which is the exact mode Eve sends the signal in,

It is a totally insecure channel.

Next, Eve knows exactly what Alice sent in the cases where Bob receives a signal, hence all subsequent reconciled bits.

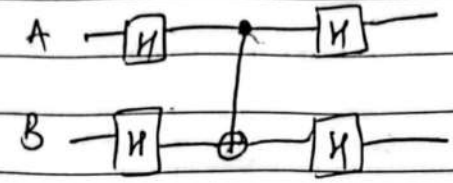
Alice and Bob do not detect any error due to Eve!

V. A. $|\psi'\rangle = I \otimes I |\psi\rangle$

$$(Z \otimes I)|\psi'\rangle = (Z \otimes I)(I \otimes I)|\psi\rangle$$
$$= (I \otimes I)(+1)|\psi\rangle$$
$$= (+1)|\psi'\rangle$$
$$(X \otimes Z)|\psi'\rangle = (X \otimes Z)(I \otimes I)|\psi\rangle$$
$$= (-1)(I \otimes I)(X \otimes Z)|\psi\rangle \quad \because ZX = -XZ$$
$$= (+1)|\psi'\rangle$$
$$(I \otimes Z)|\psi'\rangle = (+1)|\psi'\rangle \quad \text{(similarly)}$$

Orion
PAGE:
DATE: / /

B.



$$(H_A \otimes H_B)\,(C\text{-}NOT_{A-B})\,(H_A \otimes H_B) = (H\otimes H)(|0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \sigma_z)(H\otimes H)$$

$$= |+x\rangle\langle +x| \otimes \mathbb{1} + |-x\rangle\langle -x| \otimes \sigma_z$$

$$= |+x\rangle\langle +x| \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|) + |-x\rangle\langle -x| \otimes (|0\rangle\langle 0| - |1\rangle\langle 1|)$$

$$= \mathbb{1} \otimes |0\rangle\langle 0| + (|+x\rangle\langle +x| - |-x\rangle\langle -x|) \otimes |1\rangle\langle 1|$$

$$= \mathbb{1}_A \otimes |0\rangle\langle 0|_B + \sigma_x^A \otimes |1\rangle\langle 1|_B$$

$$= C\text{-}NOT_{B-A}$$

C. Initial state $|\Psi\rangle_S = (\alpha|0\rangle + \beta|1\rangle)_A |+x\rangle_B$

$$= (\alpha|0\rangle + \beta|1\rangle)_S \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)_A$$

C-Z $\alpha|0\rangle|+x\rangle + \beta|1\rangle|-x\rangle$

$$= \frac{(\alpha|0\rangle + \beta|1\rangle)}{\sqrt{2}}|0\rangle + \frac{(\alpha|0\rangle - \beta|1\rangle)}{\sqrt{2}}|1\rangle$$

$d=0$ $\quad$ $d=1$

Prob $= \left(\frac{1}{\sqrt{2}}\right)^2$ if result $\quad$ Measurement

If $d=0$, system in $\alpha|0\rangle + \beta|1\rangle$ (normalized)

If $d=1$, system in $\alpha|0\rangle - \beta|1\rangle$

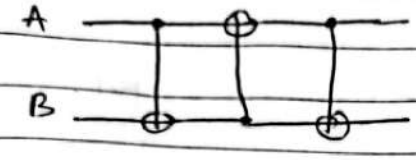
$$= \sigma_z (\alpha|0\rangle + \beta|1\rangle)$$

$\Rightarrow$ Conditional state $Z^d|\Psi\rangle$

Orion

PAGE:
DATE: / /

D.



Consider computational basis state.

$x, y = 0, 1$

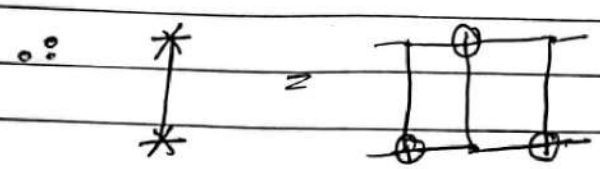
$\Rightarrow CNOT\ |x\rangle|y\rangle = |x\rangle|x \oplus y\rangle$

So $|x\rangle|y\rangle \xrightarrow{CNOT_{AB}} |x\rangle|y \oplus x\rangle$

$\xrightarrow{CNOT_{BA}} |y \oplus x \oplus x\rangle|y \oplus x\rangle$

$\xrightarrow{CNOT_{AB}} |y \oplus x \oplus x\rangle|y \oplus x \oplus y \oplus x \oplus x\rangle$

$= |y\rangle|x\rangle$, $\left(\because \begin{matrix} x \oplus x = 0 \\ y \oplus y = 0 \end{matrix}\right)$

$\therefore$ 

E. Ideal BB84 protocol used.

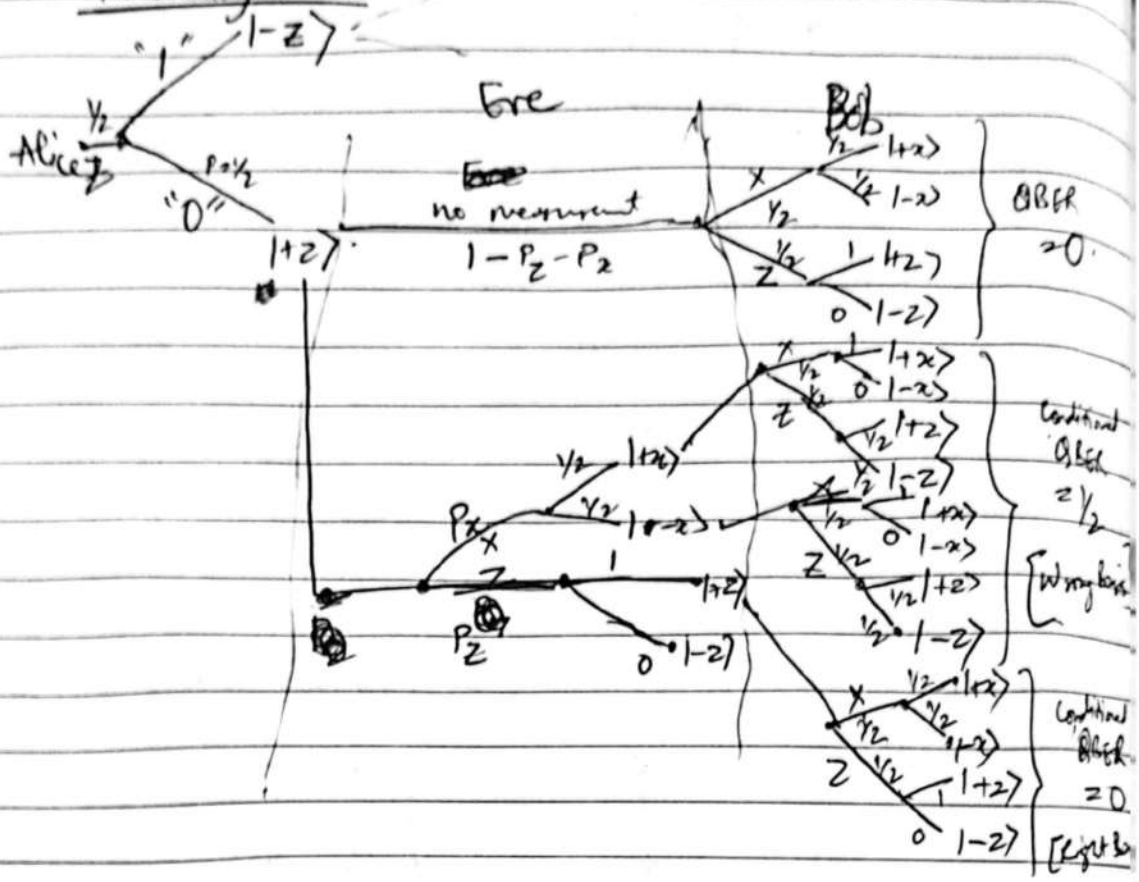
lossless and perfect channel except Eve (eavesdropper) present.

Eve $\Rightarrow$ p_x (probability to measure in X basis) } $\rightarrow$ possible types of outcome
p_z (probability to measure in Z basis) }

$1 - p_x - p_z$ (probability she decides not measure and pass to Bob unchanged)

To find $\Rightarrow$ QBER $= \frac{N_{\text{sifted wrong}}}{N_{\text{sifted total}}}$.

Probability tree



so $QBER = (1 - P_z - P_x)\, QBER_{\text{No measurement}} + P_x\, QBER_{X\text{measurement}} + P_z\, QBER_{Z\text{measurement}}$

$= \dfrac{(P_x + P_z)}{4}$ · (on average)