# Quantum Sheet #2

by Ahmed Khaled to $|Dr\rangle$ Nathan. 13 Dec 2025
Night 12 AM

بسم الله الرحمن الرحيم

Q1

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

Apply $X \otimes I$ operator to each Basis state Seprately

$(X \otimes I)|00\rangle = X|0\rangle \otimes I|0\rangle = |1\rangle \otimes |0\rangle = |10\rangle$
$(X \otimes I)|01\rangle = X|0\rangle \otimes I|1\rangle = |1\rangle \otimes |1\rangle = |11\rangle$
$(X \otimes I)|10\rangle = |00\rangle$
$(X \otimes I)|11\rangle = |01\rangle$

Restore the original Coefficients $\alpha\ \beta\ \gamma\ \delta$

$(X \otimes I)|\psi\rangle = \alpha|10\rangle + \beta|11\rangle + \gamma|00\rangle + \delta|01\rangle$

$Q_2$ If A, B Matrices 2x2

$|\psi\rangle$, $|\phi\rangle$ Single-Qubit States

Show Tensor-Product Property

$$(A \oplus B)(|\psi\rangle \oplus |\phi\rangle) = (A|\psi\rangle) \oplus (B|\phi\rangle)$$

Two Qubit Operator: A on 1st Qubit, B on 2nd Qubit

Two Qubit State 4x1

means it acts independently on each subsystem

let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$, $|\psi\rangle = \begin{pmatrix} x \\ y \end{pmatrix}$, $|\phi\rangle = \begin{pmatrix} u \\ v \end{pmatrix}$

$$|\psi\rangle \oplus |\phi\rangle = \begin{pmatrix} xu \\ xv \\ yu \\ yv \end{pmatrix} = \begin{pmatrix} \boxed{x\,|\phi\rangle} \\ \boxed{y\,|\phi\rangle} \end{pmatrix}_{2x1}$$

$$A \oplus B = \begin{pmatrix} \boxed{a \cdot B} & \boxed{b \cdot B} \\ \boxed{c \cdot B} & \boxed{e \cdot B} \end{pmatrix}_{2x2}$$

keep in Block Form (Concise)

$$(A \oplus B)(|\psi\rangle \oplus |\phi\rangle) = \begin{pmatrix} \boxed{(ax+by)}\,B|\phi\rangle \\ \boxed{(cx+dy)}\,B|\phi\rangle \end{pmatrix}_{2x1}$$

$\begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}$ is $A|\psi\rangle$

So, $(A \oplus B)(|\psi\rangle \oplus |\phi\rangle) = A|\psi\rangle \oplus B|\phi\rangle$

$Q_3$ - SWAP = 3 CNOT Gates . show

SWAP Gate ? exchonges Two Qubits $|ab\rangle \rightarrow |ba\rangle$

CNOT Gate ? has Control & Target

$$\underset{C \to t}{CNOT}\ |C,t\rangle = |C, C \oplus t\rangle$$

By Tracing Arbittraty Basis States

let some State $|a,b\rangle$

APPly CNOT $1 \to 2$

Qubit 2 is Target

Qubit 1 is Control

$$|a,b\rangle \longmapsto |a, b \oplus a\rangle$$

APPly CNOT $2 \to 1$

$$|a, b\oplus a\rangle \longmapsto |a \oplus (b \oplus a), b \oplus a\rangle$$

$$a \oplus b \oplus a = a \oplus a \oplus b = 0 \oplus b = b$$

APPly CNOT $1 \to 2$

$$|b, b\oplus a\rangle \longmapsto |b, b \oplus b \oplus a\rangle$$

$$b \oplus b \oplus a = 0 \oplus a = a$$

Final Result $|b,a\rangle$ From $|a,b\rangle$

SWAP

Q4 - Controlled Hadamad Gate
Control First bit, Target Second Bit

Any 2-Qubit Gate is Represented by 4x4 Matrix In the ordered
Basis $|00\rangle$ $|01\rangle$ $|10\rangle$ $|11\rangle$

Controlled - Hadamard
IF the First Qubit is $|0\rangle$ then Target Unchanged
$|0\rangle|\psi\rangle \mapsto |0\rangle|\psi\rangle$
IF the Second Qubit is $|1\rangle$ then Target APPlied by H
$|1\rangle|\psi\rangle \mapsto |1\rangle H|\psi\rangle$

APPly to each Basis

$|00\rangle \mapsto |00\rangle$
$|01\rangle \mapsto |01\rangle$
$|10\rangle \mapsto |1\rangle H|0\rangle = |1\rangle \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ As Firs Qubit is Zero
$|11\rangle \mapsto |1\rangle H|1\rangle = |1\rangle \frac{|0\rangle-|1\rangle}{\sqrt{2}}$

Build the 4x4 Matrix
Images of Basis Vectors In Order

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & H \end{pmatrix}$$

Block Form

Meaning
If $|0\rangle$ Control Block APPlies I on Target
If $|1\rangle$ Control Block APPlies H on Target

It's analogeous to CNot $\begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix}$

Q5 - Build CNOT using Hadamard and Controlled Z
then Varify by Mattix multiplication

Single-qubit

X Is a bit fliP

Z Is a Phase fliP

H should change the Basis so that, Phase fliPs becomes Bit fliP

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Controlled Z (control = first, target = second) $= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$

CNOT (control = first, target = second) $= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

So

APPly H to Target before and After CZ to get CNOT

$$CNOT = (I \otimes H)\, CZ\, (H \otimes I) \qquad (1)$$

## Verification

$CZ = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z$ Block Form

Substitute In (1)

$$(I \otimes H)\,(|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z)\,(H \otimes I)$$

$$= |0\rangle\langle 0| \otimes (HIH) + |1\rangle\langle 1| \otimes HZH$$

From Property $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$

$$= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$

Since $HIH = I$ and $HZH = X$

It's exactly Controlled X Gated !

## $Q_6$ - Bell States are Orthonormal Basis for $C^4$

A Set of Vectors $\{|e_1\rangle, \ldots, |e_4\rangle\}$ is an Orthonormal Basis if

① orthonormality

$$\langle e_i | e_j \rangle = \delta_{ij}$$

each Vector has norm $\langle e_i | e_i \rangle = 1$

Diff. Vectors are orthogonal $\langle e_i | e_j \rangle = 0 \quad i \neq j$

② Basis (Spans the Space)

In 4-dim Space, any Set of 4 orthogonal Vectors Automatically forms a Basis

Bell States

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

$$\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

each Norm is 1, Try $\langle \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \,|\, \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \rangle$

$$= \frac{1}{2}(\langle 00|00\rangle + \langle 00|11\rangle + \langle 11|00\rangle + \langle 11|11\rangle$$

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

$$= 1$$

Same Patterns Repeat For other three

each different Pair Is orthogonal

Try $\langle \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \,|\, \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \rangle$

$$= \frac{1}{2}(\langle 00| + \langle 11|)(|00\rangle + |11\rangle)$$

$$= \frac{1}{2}(\langle 00|00\rangle - \langle 00|11\rangle + \langle 11|00\rangle + \langle 11|11\rangle)$$

$$= \frac{1}{2}(0) = 0 \quad \text{orthogonal}$$

the Same Pattern Repeat For other three

So, Bell States are Basis For $C^4$

# $Q_7$ - Superdence Coding, Reduced State, Protocol

In Superdence coding, Information is Stored In Correlations of
the Two-Qubit entangled State
Joint

Alice has Qubit
Wants to Send 2 Classical Bits
encodes them by one of:
1- I
2- X
3- Z
4- XZ

Bob has the other entangled Qubit
Perform Bell-Basis measurements
to decode the Two Bits

Eve
Is Attacker

Eve Intercepts only the Single Qubit, (a Subsystem of Two entangled Pair)
What Eve can See? Eve have Reduced State
If you only have one Qubit of the Pair, there Is No Measurement
Can Reveal Which Bell State the Pair is in.

Eve can Infer no Information

Two bits Alice encoded In the joint State

$$\grave{P}_{AB} = (U \otimes I) P_{AB} (U^{\dagger} \otimes I)$$

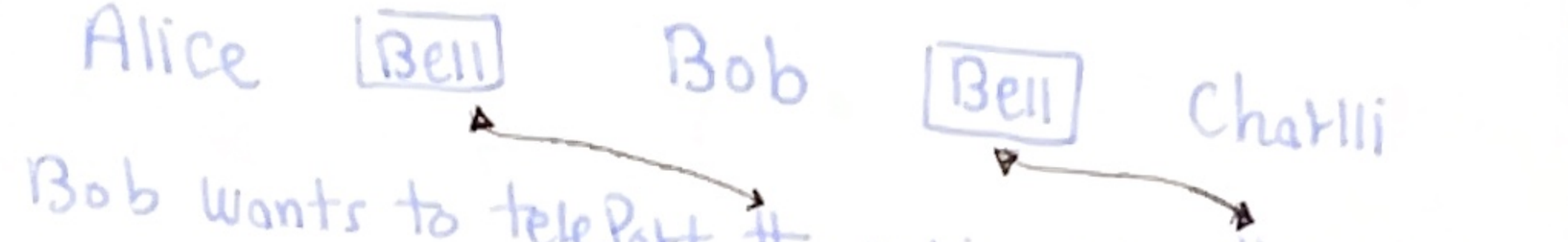
Eve's Reduced State $\grave{P}_A = Tr_B(\grave{P}_{AB})$

Same local State Independent of What Alice's Sent
, At Best She Sees a Fair Coin Flip. (Completely Random)

# Q8 - TelePortation

TelePort — moving Quantum State without moving the Qubit
Destroy the State here, recreate it there
using entanglement + Classical Bits

Monogamy In Entanglement
IF A and B are maximally entangled
,then A can not be entangled with Anyone else




When Bob do Bell measurement In his Two Qubits
Bob's Qubit are Consumed
Entanglement Is Swapped
Alice & Charli become entangled !

Bob's disapeared,
Alice and Charli share the Bell State

TelePortation Can Transfer entanglement, not just States.

→ Qubits are "Fragile" Secret, You Can not Copy, You can not look without disturbing !

# Q9 - BB84 Protocol

Alice and Bob Compare a Bit String of length n
Eve Want to Intercept - measure - Resend Attack
What's th Probability that Eve's Attack remains undetected?

## BB84

Alice has Two (Basis) to encode a Bit
- Z-Basis (Computational)
- X-Basis (Hadamard)

For each bit Position
- Choose a Random Bit 0, 1
- Choose a Random Bases X, Z

Only Four Combinations Alice can Sends $|0\rangle$ $|1\rangle$ $|+\rangle$ $|-\rangle$

Measuring In the Wrong Basis gives Random Result

How Detection may be Revealed
After many Qubits
Alex, Bob reveals the Basis they used, keep only matched Position and it should all match, otherwise → evaesdropping detected.

Eve (Attacke)
Recieve a bit at atime, Guess a Basis (Z or X), measure, Send to Bob a new Qubit In the State She measured.

$$P(\text{undetected on one Bit}) = \underbrace{\frac{1}{2}}_{\text{Bob ettor}} \cdot \underbrace{1}_{P(\text{correct guess})} + \underbrace{\frac{1}{2}}_{P(\text{Bobs})} \cdot \underbrace{\frac{1}{2}}_{P(\text{correct guess})} = \frac{3}{4}$$

$$P(\text{detected}) = \frac{1}{4}$$

For n checked Bits

$$P(\text{Eve remains undetected}) = \left(\frac{3}{4}\right)^n$$

Q10 - Attack with Entanglment

Eve Prepare Qubit In $|0\rangle$
Intercepts Alice's Qubit,
Applies CNoT, Alice's Qubit as Control, her Qubit as Target
Then Forward Alice's Qubit to Bob

Can She learn the Information without being detected?

Case #1

Alice used Z Basis

If Alice Send $|0\rangle$

$|0\rangle|0\rangle \longmapsto |0\rangle|0\rangle$

IF Sends $|1\rangle$

$|1\rangle|0\rangle \longmapsto |1\rangle|1\rangle$

Eve Can measute Perfectly
Bob won't notice

Case #2

Alice Used X Basis

If Alice Sends $|+\rangle$

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

Random

IF Alice Sends $|-\rangle$

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

Random

Eve Can not learn Somthing
Bob Will notice

• Eve Can Not Successfully learn BB84 key without Creating Ettors that Reveals her,

# Q11 - Information Encoded In Phases rather Amplitudes

Quantum Computers can extract Global Information about a function using Interference

In Deutsch-Jozsa, the oracle is a Unitry

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

x : Input Register
y : output Qubit
$f(x) \in \{0,1\}$

Oracle does no Reveal $f(x)$ directly, it hides it in the second qubit

(a) Phase kickback

Initial State $|\psi_1\rangle = \sum_{x \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |x\rangle \; (|0\rangle - |1\rangle)$

↳ special second Qubit $|-\rangle$

Apply the Oracle

$$U_f \left( |x\rangle (|0\rangle - |1\rangle) \right) = |x\rangle \left( |f(x)\rangle - |1 \oplus f(x)\rangle \right)$$

Since $U_f |x\rangle |0\rangle = |x\rangle |f(x)\rangle$

, $U_f |x\rangle |1\rangle = |x\rangle |1 \oplus f(x)\rangle$

Check For both Cases :-

$f(x) = 0$ $\quad |0\rangle - |1\rangle$

$f(x) = 1$ $\quad |1\rangle - |0\rangle = -(|0\rangle - |1\rangle)$

So In All Cases

$$= (-1)^{f(x)} |x\rangle \; (|0\rangle - |1\rangle)$$

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

the Function is kicked Back as a Phase on $|x\rangle$

, Second Qubit Return Unchanged.

Q11 - B  Uniform SuperPosition via Hadamard

Tensor Product for Single Qubit $H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$

Tensor Product For n Qubits $H^{\otimes n}|0\rangle^{\otimes n}$

$= \langle H|0\rangle^{\otimes n}$

each Qubit splits into $|0\rangle + |1\rangle$

So All Combinations appear

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

Hadamard on [All Zero State] Produces equal SuperPositions of All Inputs

Q11 - C

For bit Strings $X, Z \in [0,1]^n$:

$X \cdot Z = X_1 Z_1 \oplus X_2 Z_2 \oplus \dots \oplus X_n Z_n$

dot Product Definition

Since each Hadamard Contributes (+1) or (-1)
the sign of X.y depends weather both bits are 1
X.Z gives us the Parity of the overlap (Total Phase)

therefore $H^{\oplus n}|X\rangle = \frac{1}{\sqrt{2^n}} \sum_{X [0,1]^n} (-1)^{X \cdot Z} |Z\rangle$

Q12 - Duetsch-Jozo with 2 Qubits

Having:

Two Qubits = 4 Possible outcomes 00 01 10 11

One Prepared Qubit In $|1\rangle$

Apply Hadamard, $H^{\otimes 2}$ on Input, H on $|1\rangle$

$$|00\rangle|1\rangle \xrightarrow{H^{\otimes 2}\otimes H} \left(\frac{1}{2}\sum_{x\{0,1\}^n}|x\rangle\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

So, $$|\psi_1\rangle = \frac{1}{2}\sum_x |x\rangle\,|-\rangle$$

Oracle Step (Phase kickback)

$$U_f\,(|x\rangle|-\rangle) = (-1)^{f(x)}\,|x\rangle\,|-\rangle$$

After the Oracle

$$|\psi_2\rangle = \frac{1}{2}\sum (-1)^{f(x)}\,|x\rangle\,|-\rangle$$

Final Hadamards on the Two Input Qubits

$$|\psi_3\rangle = (H^{\otimes 2}\otimes I)\,|\psi_2\rangle$$

Case: $f(x)=0$ for All X (Constant)

$$Amp(z) = \frac{1}{4}\sum_x (-1)^{x\cdot z}$$

For n=2 Qubits

measure $z=00$, as $f(x)$ Const.

then $x\cdot z = 0$

So, $Amp(00) = \frac{1}{4}(1+1+1+1)$

$= 1$

if $z\neq 00$

the +1, -1 Cancels each other

$Amp(z) = 0$

So,

$P(00) = 1$

$P(01) = 0$

$P(10) = 0$

$P(11) = 0$

Balanced

Case#2: $f(x)=0$ if X is even

$f(x)=1$ otherwise

$Amp(00) = \frac{1}{4}\sum_x (-1)^{f(x)} = 1-1+1-1 = 0$

$Amp(01) = \frac{1}{4}\sum_x (-1)^{f(x)} = \frac{1}{4}+\frac{1}{4}+\frac{1}{4}+\frac{1}{4} = 1$

$Amp(10) = \frac{1}{4}\sum_x (-1)^{f(x)} = \frac{1}{4}(-1+1-1+1) = 0$

$Amp(11) = \frac{1}{4}\sum_x (-1)^{f(x)} = \frac{1}{4}(1+1-1-1) = 0$

So, Probabilities

$P(00) = 0$

$P(01) = 1$

$P(10) = 0$

$P(11) = 0$

Outputs 01 with certainty, not 00

Q13 - $C_{n-1}X$ Quali-X Gate Controlled by n-1 Anded Qubits.

Could be Implemented by Toffoli Gate & Some other Workspace Qubits ?

Toffoli Gate ? Controlled-controlled Not

$CCX(a,b \to X): X \mapsto X \oplus (a \wedge b)$ a,b unchanged

Workspace Qubits ? to Store Partial ANDs

$W_1 = C_1 \wedge C_2$, $W_2 = \ \wedge C_3$, ..

Use n-3 Toffoli to Compute Partial ANDs

1. $CCX(C_1, C_2 \to W_1)$
2. For $k = 2,3,\dots,n-3$ $CCX(W_{k-1}, C_{k+1} \to W_k)$

So Any Workspace Qubit at time k

$W_k = C_1 C_2 .. C_{k+1}$

In Particular

$W_{n-3} = C_1 C_2 .. C_{n-2}$

then 1 Toffoli - Target Flip ( actual multi control effect )

$CCX(W_{n-3}, C_{n-1} \to t)$

Which Implements

$C_{n-1}X$ Functionality

Q14 - Grover's Algorithm In 3 Qubit Register
In Which only the State $|1010\rangle$ is marked
what's the Prob. of measuring it after APPlying Grover's
iterate 0,1,2,3 times.

3 Qubit Register, 8 Possible States
one Marked State M=1 $|1010\rangle$

Grover ? a Rotation in a 2D Plane

let's define Two orthonormal Directions
$|w\rangle$ the marked State $|1010\rangle$
$|w^{\perp}\rangle$ normalized SuperPosition of 7 unmarked State

the Uniform Starting State $|s\rangle$

$$|s\rangle = \frac{1}{\sqrt{8}} \sum_{x=0}^{7} |x\rangle = \sin\theta\,|w\rangle + \cos\theta\,|w^{\perp}\rangle$$

where $\sin\theta = \sqrt{\frac{M}{N}} = \sqrt{\frac{1}{8}} = \frac{1}{\sqrt{8}}$

Grover Iterate = Oracle Phase Flip + defusion
It Perform a rotation by angle $2\theta$ In the Span of $|w\rangle, |w^{\perp}\rangle$

After k iterations

$$|\chi_k\rangle = \sin((2k+1)\theta)\,|w\rangle + \cos((2k+1)\theta)\,|w^{\perp}\rangle$$

Therefore the Success Probability at each iteration k

$$P_k = \sin^2[(2k+1)\theta]$$

Since $\sin\theta = \frac{1}{\sqrt{8}}$, So

$$P_0 = \sin^2(\theta) = \frac{1}{8}, \quad P_1 = \sin^2(3\theta) = \frac{25}{35}, \quad P_2 = \sin^2(5\theta) = \frac{121}{128}$$

$$P_4 = \sin^2(7\theta) = \frac{169}{512}$$

the Highest Prob. of measuring the marked State at $P_2$ (k=2)