Introductory Topics in Quantum Paradigm

Subhamoy Maitra

Indian Statistical Institute
[subho@isical.ac.in]

21 May, 2016

Outline of the talk

- Preliminaries of Quantum Paradigm
  - What is a Qubit?
  - Entanglement
  - Quantum Gates
  - No Cloning
  - Indistinguishability of quantum states
- Details of BB84 Quantum Key Distribution Algorithm
  - Description
  - Eavesdropping
  - State of the art: News and Industries
- Walsh Transform in Deutsch-Jozsa (DJ) Algorithm
  - Deutsch-Jozsa Algorithm
  - Walsh Transform
  - Relating the above two
  - Some implications

Qubit and Measurement

- A qubit:

$$\alpha|0\rangle + \beta|1\rangle,$$

$\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$.

- Measurement in $\{|0\rangle, |1\rangle\}$ basis: we will get $|0\rangle$ with probability $|\alpha|^2$, $|1\rangle$ with probability $|\beta|^2$. The original state gets destroyed.
- Example:

$$\frac{1+i}{2}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle.$$

After measurement: we will get
$|0\rangle$ with probability $\frac{1}{2}$,
$|1\rangle$ with probability $\frac{1}{2}$.

Basic Algebra

- Basic algebra:
  $(\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle)$
  $= \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle,$
  can be seen as tensor product.
- Any 2-qubit state may not be decomposed as above. Consider the state

$$\gamma_1|00\rangle + \gamma_2|11\rangle$$

  with $\gamma_1 \neq 0, \gamma_2 \neq 0$. This cannot be written as
  $(\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle)$.
- This is called entanglement. Known as Bell states or EPR pairs. An example of maximally entangled state is

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

Quantum Gates

n inputs, n outputs. Can be seen as $2^n \times 2^n$ unitary matrices where the elements are complex numbers.

Single input single output quantum gates.

Quantum input	Quantum gate	Quantum Output
$\alpha\|0\rangle + \beta\|1\rangle$	X	$\beta\|0\rangle + \alpha\|1\rangle$
$\alpha\|0\rangle + \beta\|1\rangle$	Z	$\alpha\|0\rangle - \beta\|1\rangle$
$\alpha\|0\rangle + \beta\|1\rangle$	H	$\alpha\frac{\|0\rangle+\|1\rangle}{\sqrt{2}} + \beta\frac{\|0\rangle-\|1\rangle}{\sqrt{2}}$

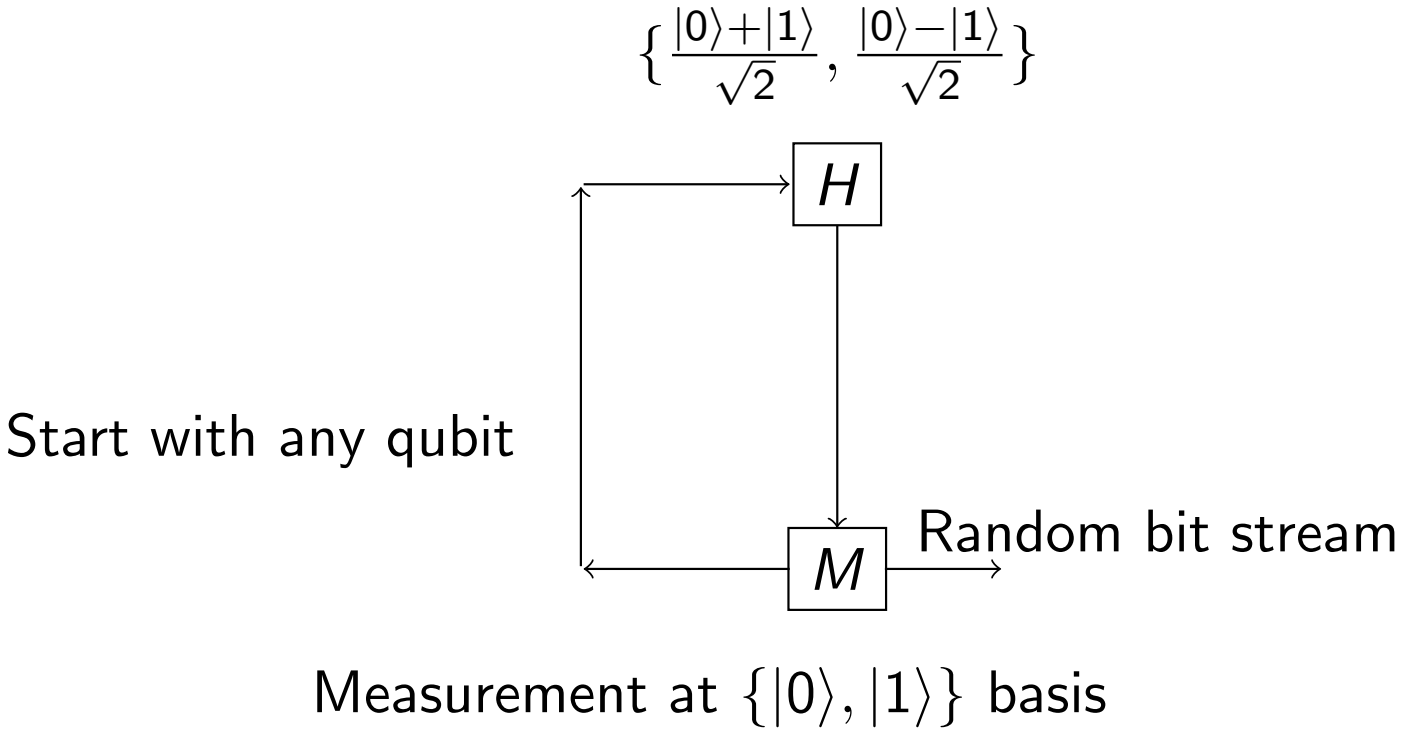
Quantum Gates (contd.)

1 input, 1 output. Can be seen as $2^1 \times 2^1$ unitary matrices where the elements are complex numbers.

The X gate: $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$

The H gate: $\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \frac{\alpha+\beta}{\sqrt{2}} \\ \frac{\alpha-\beta}{\sqrt{2}} \end{bmatrix}$

A True Random Number Generator



Quantum Gates (contd.)

2-input 2-output quantum gates. Can be seen as $2^2 \times 2^2$ unitary matrices where the elements are complex numbers.

These are basically 4×4 unitary matrices. An example is the CNOT gate.

$$
\begin{aligned}
|00\rangle &\rightarrow |00\rangle, \\
|01\rangle &\rightarrow |01\rangle, \\
|10\rangle &\rightarrow |11\rangle, \\
|11\rangle &\rightarrow |10\rangle.
\end{aligned}
$$

The matrix is as follows:

$$
\begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0
\end{bmatrix}
$$

Preliminaries (circuit for entangled state)

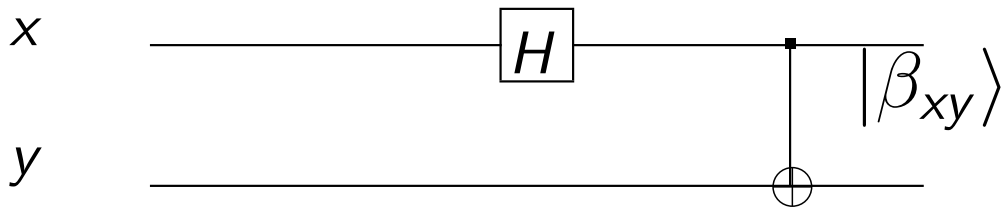


Figure: Quantum circuit for creating entangled state

Bell State	Description
$\|\beta_{00}\rangle$	$\frac{\|00\rangle+\|11\rangle}{\sqrt{2}}$
$\|\beta_{01}\rangle$	$\frac{\|01\rangle+\|10\rangle}{\sqrt{2}}$
$\|\beta_{10}\rangle$	$\frac{\|00\rangle-\|11\rangle}{\sqrt{2}}$
$\|\beta_{11}\rangle$	$\frac{\|01\rangle-\|10\rangle}{\sqrt{2}}$

Teleportation

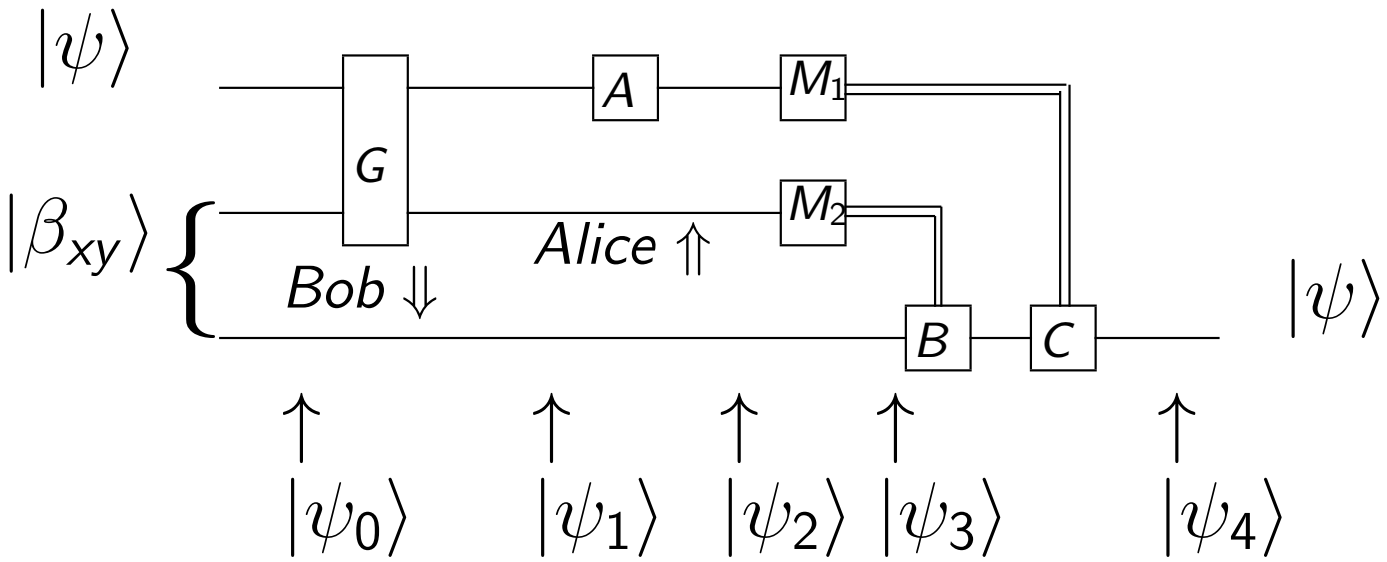


Figure: Quantum circuit for teleporting a qubit

Teleportation (Example)

1. $|\beta_{xy}\rangle = |\beta_{00}\rangle$,
2. G is CNOT, i.e., $|00\rangle \to |00\rangle$, $|01\rangle \to |01\rangle$, $|10\rangle \to |11\rangle$, $|11\rangle \to |10\rangle$.
3. $A = H, B = X^{M_2}, C = Z^{M_1}$

An extension:

1. Use any $|\beta_{xy}\rangle$,
2. G is CNOT,
3. $A = H, B = X^{M_2 \oplus x}, C = Z^{M_1 \oplus y}$

We are studying the effect of other gates apart from CNOT.

Teleportation (step by step)

- $|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle = (\alpha|0\rangle + \beta|1\rangle)\frac{(|00\rangle+|11\rangle)}{\sqrt{2}}$
- $|\psi_1\rangle = \alpha|0\rangle\frac{(|00\rangle+|11\rangle)}{\sqrt{2}} + \beta|1\rangle\frac{(|10\rangle+|01\rangle)}{\sqrt{2}}$
- $|\psi_2\rangle = \alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{(|00\rangle+|11\rangle)}{\sqrt{2}} + \beta\frac{|0\rangle-|1\rangle}{\sqrt{2}}\frac{(|10\rangle+|01\rangle)}{\sqrt{2}} =$
  $\frac{1}{2}(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\beta|0\rangle + \alpha|1\rangle) +$
  $|10\rangle(\alpha|0\rangle - \beta|1\rangle) - |11\rangle(\beta|0\rangle - \alpha|1\rangle))$
- Observe 00, nothing to do.
- Observe 01, apply X.
- Observe 10, apply Z.
- Observe 11, apply both X, Z.

Remote state preparation

- In teleportation the state $|\psi\rangle$ is unknown. In this case the state is known: $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\phi}|1\rangle$.
- Entangled state $\frac{|01\rangle - |10\rangle}{\sqrt{2}}$ is shared between two parties.
- Transformed to different basis $|\psi\rangle$, $|\psi_\perp\rangle$. The entangled state on the new basis can be seen as $\frac{|\psi\psi_\perp\rangle - |\psi_\perp\psi\rangle}{\sqrt{2}}$.
- Alice measures on $|\psi\rangle, |\psi_\perp\rangle$ basis.
- If Alice gets $|\psi_\perp\rangle$, then Bob obtains $|\psi\rangle$, so no change is required. Alice sends cbit 0 in this case.
- If Alice gets $|\psi\rangle$, then Bob obtains $|\psi_\perp\rangle$, so he needs to apply a transformation. Alice sends cbit 1 in this case.
- Note that only one cbit communication is required for remote state preparation.

Multi Party Pseudo Telepathy

- For any $n \geq 3$, the game G_n consists of n players. The bit string $x_1 \ldots x_n$ contains even number of 1's.
- Each player A_i receives a single input bit x_i and is requested to produce an output bit y_i.
- $x_1 \ldots x_n$ is the question and $y_1 \ldots y_n$ is the answer.
- The game G_n will be won by this team of n players if

$$\sum_{i=1}^{n} y_i \equiv \frac{1}{2} \sum_{i=1}^{n} x_i (\mathrm{mod} 2).$$

Multi Party Pseudo Telepathy (Contd.)

- No communication is allowed among the n participants after receiving the inputs and before producing the outputs.
- It has been proved that no classical strategy for the game G_n can be successful with a probability better than $\frac{1}{2} + 2^{-\lceil n/2 \rceil}$.
- Quantum entanglement serves to eliminate the classical need to communicate and it is shown that there exists a perfect quantum protocol where the n parties will always win the game.

Pseudo Telepathy (the set up)

- Define

$$|\Phi_n^+\rangle = \frac{1}{\sqrt{2}}|0^n\rangle + \frac{1}{\sqrt{2}}|1^n\rangle$$

and

$$|\Phi_n^-\rangle = \frac{1}{\sqrt{2}}|0^n\rangle - \frac{1}{\sqrt{2}}|1^n\rangle.$$

- H denotes Hadamard transform. S denotes the unitary transformation $S|0\rangle \mapsto |0\rangle,\ S|1\rangle \mapsto i|1\rangle$.
- If S is applied to any two qubits of $|\Phi_n^+\rangle$ leaving the other qubits undisturbes then the resulting state is $|\Phi_n^-\rangle$ and vice versa.

Pseudo Telepathy (the set up, contd.)

- If $|\Phi_n^+\rangle$ is distributed among n players and if exactly m of them apply S to their qubit, then the resulting global state will be $|\Phi_n^+\rangle$ if $m \equiv 0 \bmod 4$ and $|\Phi_n^-\rangle$ if $m \equiv 2 \bmod 4$.
- Note that

$$(H^{\otimes n})|\Phi_n^+\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{wt(y)\equiv 0 \bmod 2} |y\rangle$$

and

$$(H^{\otimes n})|\Phi_n^-\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{wt(y)\equiv 1 \bmod 2} |y\rangle.$$

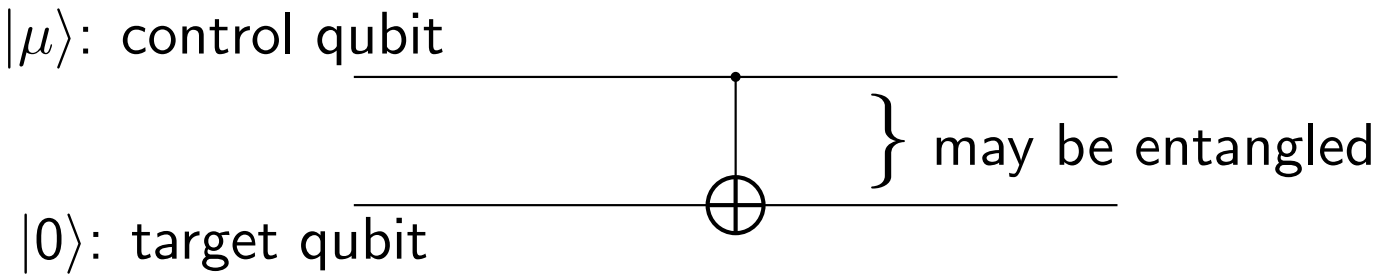
Pseudo Telepathy (the quantum algorithm)

The players are allowed to share a prior entanglement, the state $|\Phi_n^+\rangle$.

1. If $x_i = 1$, A_i applies transformation S to his qubit; otherwise he does nothing.
2. He applies H to his qubit.
3. He measures his qubit in order to obtain y.
4. He produces y_i as his output.

The game G_n is always won by the n distributed parties without any communication among themselves.
Open question: In this algorithm $n \geq 3$. It is open to find a two party pseudo telepathy problem that admits a perfect quantum solution, yet any classical protocol would have probability of success close to half.

More on CNOT



- $|\mu\rangle$ is either $|0\rangle$ or $|1\rangle$. Then it will be copied perfectly without creating any disturbance to $|\mu\rangle$.
- Say $|\mu\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$. Then at the output we will get entangled state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$. Thus copying is not successful here.

Cloning: Possible in classical domain, not in quantum

Possible to copy a classical bit

Not possible for an unknown quantum bit

No cloning

- A result of quantum mechanics
- Not possible to create identical copies of an arbitrary unknown quantum state
- It was stated by Wootters, Zurek, and Dieks in 1982
- W. K. Wootters and W. H. Zurek. A Single Quantum Cannot be Cloned, Nature 299 (1982), pp. 802803.
- D. Dieks. Communication by EPR devices, Physics Letters A, vol. 92(6) (1982), pp. 271272.
- Huge implications in quantum computing, quantum information, quantum cryptography and related fields.

No cloning (contd.)

- It is not possible to copy an unknown Quantum state.
- Consider a quantum slot machine with two slots labeled A and B.
- A is the data slot set in a pure unknown quantum state $|\psi\rangle$ whereas B is target slot set in a pure state $|s\rangle$ where A will be copied.

No cloning (contd.)

- Let there exist a unitary operator which does the copying procedure. Mathematically it is written as $U(|\psi\rangle|s\rangle) = |\psi\rangle|\psi\rangle$.
- U: unitary operator, $UU^\dagger = I$.
  $(U^\dagger)_{ij} = \overline{U}_{ji}$, transpose and scalar complex conjugate.
- Let this copying procedure works for two particular pure states, $|\psi\rangle$ and $|\phi\rangle$. Then we have

$$U(|\psi\rangle|s\rangle) = |\psi\rangle|\psi\rangle, U(|\phi\rangle|s\rangle) = |\phi\rangle|\phi\rangle$$

- Take the inner product: $\langle s|\langle\psi|U^\dagger U|\phi\rangle|s\rangle = \langle\psi|\langle\psi||\phi\rangle|\phi\rangle$.
  This implies $\langle\psi|\phi\rangle = (\langle\psi|\phi\rangle)^2$.

No Cloning (contd.)

- $x = x^2$ has only two solutions: $x = 0$ and $x = 1$.
- Thus we get either $|\psi\rangle = |\phi\rangle$ or inner product of them equals to zero, i.e., $|\psi\rangle$ and $|\phi\rangle$ are orthogonal to each other.
- Thus a cloning device can only clone orthogonal states. Therefore a general quantum cloning device is impossible.
- Example: it is given that the unknown state is one of $|0\rangle$, $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, two nonorthogonal states. Then it is not possible to clone the state without knowing which one it is.

Orthogonal quantum states: distinguishable

Possible to distinguish two orthogonal states only

- Given two orthogonal states $\{|\psi\rangle, |\psi_\perp\rangle\}$, it is possible to distinguish them with certainty.
- For example,

$$\{|0\rangle, |1\rangle\};$$

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

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

Distinguishability of Nonorthogonal quantum states

Not possible to distinguish two nonorthogonal quantum states with certainty

- Given two nonorthogonal states $\{|\psi_0\rangle, |\psi_1\rangle\}$, it is not possible to distinguish them with probability 1.
- Example: it is given that the two states are $|0\rangle$, $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, two nonorthogonal states. Then it is not possible to exactly identify each one.

Key Exchange and Public Key Protocols: Scenario given the Quantum Paradigm

- Factorization and Discrete Logarithm Problems are believed to be hard in Classical domain.
- However, they can be solved efficiently using quantum algorithms.
- There are certain Lattice based and Code based public key cryptosystems that are resistant to attacks using quantum algorithms.
- However, they are quite complicated.
- Quantum key distribution is very easy to understand and it has already been implemented in practice.

BB84 History: As told by Brassard

The story begins in the early 1960s, when Stephen Wiesner and Charles Bennett were undergraduate students together at Brandeis University. Having many common friends, they enjoyed talking with each other. Later, after Wiesner had gone to graduate school at Columbia and Bennett at Harvard, they kept in touch. In particular, the former payed frequent visits to the latters communal house in Boston. During one of those visits in the late 60s or early 70s, Wiesner told Bennett of his ideas for using quantum mechanics to make bank-notes that would be impossible to counterfeit according to the laws of nature, as well as of a "quantum multiplexing" channel, which would allow one party to send two messages to another in a way that the receiving party could decide which message to read but only at the cost of destroying the other message irreversibly.

Wiesner submitted his paper "Conjugate Coding" to the IEEE Transactions on Information Theory. Unfortunately, it was rejected, ...

BB84 History: As told by Brassard (contd.)

One fine afternoon in late October 1979, I was swimming at the beach of a posh hotel in San Juan, Puerto Rico. Imagine my surprise when this complete stranger swims up to me and starts telling me, without apparent provocation on my part, about Wiesners quantum banknotes! This was probably the most bizarre, and certainly the most magical, moment in my professional life. Within hours, we had found ways to mesh Wiesners coding scheme with some of the then-new concepts of public-key cryptography. Thus was born a wonderful collaboration that was to spin out quantum teleportation, entanglement distillation, the first lower bound on the power of quantum computers, privacy amplification, and, of course, quantum cryptography. ...

BB84 History: As told by Brassard (contd.)

... Shortly thereafter, my good friend Vijay Bhargava was in charge of a special session on coding and information theory for yet another IEEE conference, which took place in Bangalore, India, in December 1984. He invited me to give a talk on any subject of my choice, and naturally I chose Quantum Cryptography considering how difficult it was to get these ideas published at the time. The resulting paper gave its name to the "BB84 protocol" even though it had been described in detail as early as 1983 at the IEEE ISIT talk but not in the paper (how much can you say in a one-page abstract?). Retrospectively, it is amusing to note that the only reason the BB84 protocol was finally published is that it had not been submitted to the conference that printed it in its proceedings! Thanks Vijay!

BB84 History (summary)

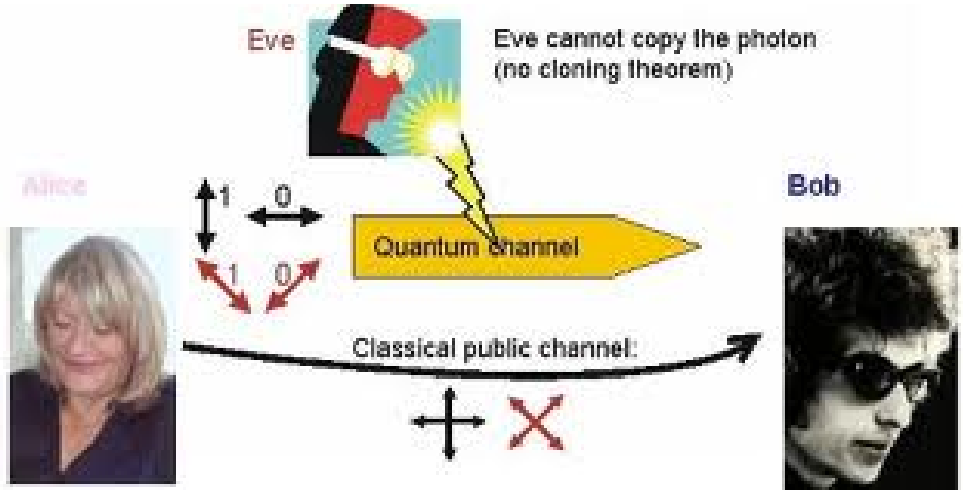
- Initiated by Charles Bennett and Gilles Brassard in 1979

  G. Brassard. Brief History of Quantum Cryptography: A Personal Perspective. [quant-ph/0604072]
- The paper was not getting accepted initially
- Finally published as Quantum Cryptography: Public key distribution and coin tossing, in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, p. 175 (1984)
- Citation: 2886 in June 2012 to 2954 in August, 2012, Google Scholar
- A scheme for quantum key distribution scheme
- The first protocol in the area of quantum cryptography
- The basics of this protocol comes from the seminal concept by Wiesner.

  S. Wiesner. Conjugate Coding. Manuscript 1970, subsequently published in SIGACT News 15:1, 78–88, 1983.

BB84 (contd.)

- The protocol is provably secure
- Based on no cloning theorem



- The proof comes from the quantum property that information gain is only possible at the expense of disturbing the signal
- If the two states we are trying to distinguish are not orthogonal, it is not possible to distinguish them with certainty
- The protocol is a method of securely communicating a private key from Alice to Bob

BB84: Basic Idea

- To transmit 0 or 1 securely.
- Choose some basis:

$$\{|0\rangle, |1\rangle\};$$

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

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

- Take any basis. Encode 0 to one qubit and 1 to another qubit.
- If we use only a single basis, then anybody can measure in that basis, get the information and reproduce.
- Thus Alice needs to encode randomly with more than one bases.
- Bob will also measure in random basis.
- Basis will match in a proportion of cases and from that key will be prepared.

BB84 Algorithm

- Alice chooses $(4+\delta)n$ many random data bits referred as binary string a
- Alice further chooses a random binary string b of $(4+\delta)n$ bits
- For $i = 0$ to $(4+\delta)n - 1$
  - if $a_i = 0$ and $b_i = 0$ Alice selects the qubit $|0\rangle$
  - if $a_i = 1$ and $b_i = 0$ Alice selects the qubit $|1\rangle$
  - if $a_i = 0$ and $b_i = 1$ Alice selects the qubit $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
  - if $a_i = 1$ and $b_i = 1$ Alice selects the qubit $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- Alice sends the resulting state (qubits) to Bob
- After receiving $(4+\delta)n$ many qubits Bob announces the fact and measures each qubit either in $|0\rangle, |1\rangle$ basis or in $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ basis at random
- Alice then announces b

BB84 Algorithm (contd.)

- Bob then discards the bits where he measured the qubit in a different basis than Alice prepared and Alice also does the same thing; with high probability there are at least $2n$ bits left (not discarded) and if this does not happen then the protocol is aborted; they work with $2n$ bits
- A subset of n bits are selected by Alice that will serve as checks on the interference of Eve; Alice also tells Bob which bits she actually selected
- Both Alice and Bob announce and compare the values of the n many check bits; if the number of disagreement is more than an acceptable limit then the protocol will be aborted
- Information reconciliation and privacy amplification are performed by Alice and Bob on the remaining n bits to obtain m shared key bits

BB84 Algorithm (example)

$+$: $\{\uparrow = |0\rangle, \rightarrow = |1\rangle\}$, i.e., Z basis

$\times$: $\{\nearrow = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \nwarrow = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$, i.e., X basis

a	0	1	1	0	1	0	0	1
b	0	0	1	0	1	1	1	0
Basis	$+$	$+$	$\times$	$+$	$\times$	$\times$	$\times$	$+$
Polarization	$\uparrow$	$\rightarrow$	$\nwarrow$	$\uparrow$	$\nwarrow$	$\nearrow$	$\nearrow$	$\rightarrow$
Bob's Basis	$+$	$\times$	$\times$	$\times$	$+$	$\times$	$+$	$+$
Bob's measurement	$\uparrow$	$\nearrow$	$\nwarrow$	$\nearrow$	$\rightarrow$	$\nearrow$	$\rightarrow$	$\rightarrow$
Public Discussion	M		M			M		M
Shared Key	0		1			0		1

Attack Models (partial)

Alice and Bob are communicating and Eve is sitting in between.

- Intercept (measure) and resend: Choice of wrong basis in 50% cases and then out of them, measurement may be wrong in 50% cases. Thus the error rate will be 25%.
- Man in the middle attack: This attack is possible when the communication is being without any authentication. Weakness is same as any other classical protocol.
- Photon number splitting attack: Algorithm using single photon. In practice more than one photon may travel with a single laser pulse. Eve may get hold of the extra photon.
- Denial of service attack: Cutting or blocking the line. We need Quantum Key Distribution Networks.

Eavesdropping in Quantum Channel

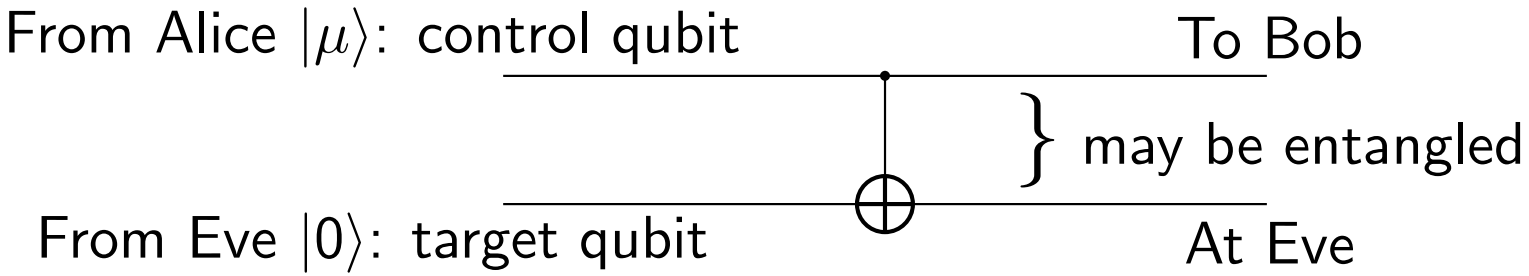
- The security in the protocol is based on the fact that if one wants to distinguish two non-orthogonal quantum states, then obtaining any information is only possible at the expense of introducing disturbance in the state(s).

  - There are several works in the literature, that studied the relationship between "the amount of information obtained by Eve" and "the amount of disturbance created on the qubits that Bob receives from Alice".

Eavesdropping: Different Models

- Eve can work on each individual qubit as opposed to a set of qubits studied together
  - the first one is called the *incoherent attack*,
  - the second one is known as *coherent attack*.
- Another interesting issue in specifying the eavesdropping scenario is whether there will be equal error probability at Bob's end corresponding to different bases.
  - If this is indeed equal, then we call it *symmetric*.
  - There is also another model where this is not equal and then we call the eavesdropping model as *asymmetric*. Different error rates for different bases would be a clear indication to Alice and Bob that an eavesdropper (Eve) is interfering in the communication line.

Eavesdropping: CNOT attack



- Alice communicates in Z basis, i.e., $|\mu\rangle$ is either $|0\rangle$ or $|1\rangle$.
- Then Eve can copy that perfectly without creating any disturbance to $|\mu\rangle$.
- Thus the bit error rate in this case will be 0 between Alice and Bob and Eve's success probability in guessing the correct bit will be 1.

CNOT attack (contd.)

- Alice communicates in X basis, i.e., $|\mu\rangle$ is either $|+\rangle$ or $|-\rangle$.
- Then the output of the CNOT gate is an entangled state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ or $\frac{|00\rangle-|11\rangle}{\sqrt{2}}$ (respectively).
- Consider the $|+\rangle$ case.
- $\frac{|00\rangle+|11\rangle}{\sqrt{2}} = \frac{|++\rangle+|--\rangle}{\sqrt{2}}$
- If Bob measures in X basis, then he will observe $|+\rangle$ with probability $\frac{1}{2}$ and $|-\rangle$ with probability $\frac{1}{2}$.
- Thus the bit error rate in this case will be $\frac{1}{2}$ between Alice and Bob and Eve's success probability in guessing the correct bit will also be $\frac{1}{2}$.
- The eavesdropping is asymmetric.

Eavesdropping: How to interact

- Alice sends a qubit $|\mu\rangle$ to Bob and Eve lets a probe $|W\rangle$ of that interacts unitarily with $|\mu\rangle$.
- Eve's measurement is delayed till Alice announces the basis that has been used (i.e., by that time Bob has already measured the state).

- One can model it as $U(|\mu\rangle, |W\rangle) = |\tau\rangle$, where U is the unitary operator and after its application, $|\tau\rangle$ is the entangled state of the qubit that Alice sent to Bob and the probe applied by Eve.
- The probe $|W\rangle$ could be of one or two or more qubits. The most efficient model considers a two-qubit probe.

Eavesdropping: Exact analysis

Let D be the disturbance in the channel due to the interaction by Eve and $F = 1 - D$ be the fidelity. For the $|0\rangle, |1\rangle$ basis, i.e., the Z basis, one can write the eavesdropping interaction as

$$\begin{aligned} U(|0\rangle, |W\rangle) &= \sqrt{F}|E_{00}\rangle|0\rangle + \sqrt{D}|E_{01}\rangle|1\rangle, \\ U(|1\rangle, |W\rangle) &= \sqrt{D}|E_{10}\rangle|0\rangle + \sqrt{F}|E_{11}\rangle|1\rangle. \end{aligned} \quad (1)$$

Similar equations can be written for the X basis. These are in the line of the following works.

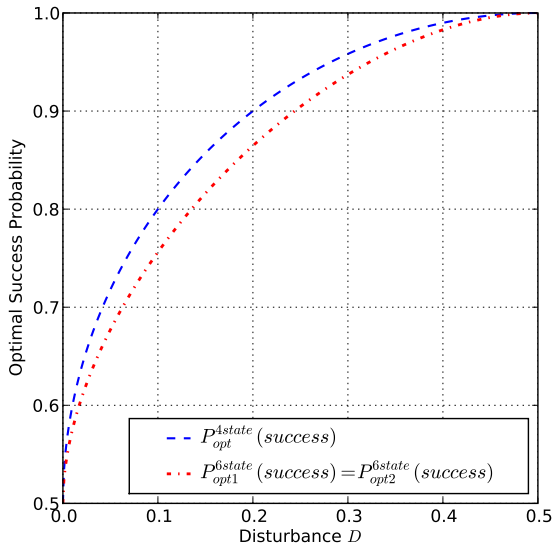
- C. A. Fuchs, N. Gisin, R. B. Griffiths, C. S. Niu, and A. Peres. Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy. Physical Review A, 56(2), 1163–1172 (1997)
- D. Bruß. Optimal eavesdropping in quantum cryptography with six states. Physical Review Letters, 81, 3018–3021 (1998) [quant-ph/9805019].

BB84: 4 state vs 6 state

- Traditional BB84 uses four states $\{|0\rangle, |1\rangle\}$ and $\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$. Eavesdropping on this model was studied by Fuchs et al.
- To obtain better security, Bruß (PRL 1998) proposed use of $\{\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)\}$ too.
- For the traditional 4-state protocol, half of the states will be discarded as Bob will measure those in wrong basis.
- For the 6-state protocol, two third of the states will be discarded as Bob will measure them in wrong basis.
- Thus, the security comes at the cost of wasting more qubits.

Eavesdropping: Analytic results

- For 4-state (traditional) BB84, providing a disturbance D the eavesdropper can guess the bit correctly at a probability $\frac{1}{2} + \sqrt{D(1-D)}$ (more)
- For 6-state BB84, providing a disturbance D the eavesdropper can guess the bit correctly at a probability $\frac{1}{2} + \frac{D+\sqrt{D(2-3D)}}{2}$ (less)



Press Release: Max Planck Institute of Quantum Optics, Garching, Germany, 14 June 2012

Although physicists have already developed methods to write quantum states into different types of memory and read them out again, the problem is either that these methods work only just above absolute zero temperature which excludes routine use – or that the quantum information stored is lost after only a few milliseconds.
Researchers at Harvard University in Cambridge near Boston, the Max Planck Institute of Quantum Optics in Garching, and Caltech in Pasadena have now successfully stored a quantum state in a diamond crystal for more than a second at room temperature. The researchers even believe that a storage time of one-and-a-half days is possible if they improve their method.
Peter Maurer, Georg Kucsko, Christian Latta, Lian Jiang, Norman Jao, Steven Bennett, Fernando Pastawski, David Hunger, Nicholas Chisholm, Matthew Markham, Daniel Twitchen, Ignacio Cirac and Mikhail Lukin.
Room-Temperature Quantum Bit Memory Exceeding One Second.

Science, June 2012

Companies that implement the products

- Quantum Key Distribution Equipment.
  ID Quantique (IDQ).
  `http://www.idquantique.com/`
- Quantum Key Distribution System (Q-Box).
  MagiQ Technologies Inc.
  `http://www.magiqtech.com`

National Perspective

- "Miles to go" before commercial availability of quantum computers (if at all possible)
- However, quantum key distribution has advanced a lot (many proposals and commercial products available)
- More focus towards research in Quantum Cryptography
- Installing existing products
- Plan for indigenous implementation

Concluding QKD

We have presented basics of cryptographic key distributions.

We have pointed out the issues related to the (in)security of some classical domain protocols against quantum attacks.

- Schemes based on factorization/DLP: Insecure
- Schemes based on lattices/coding: Secure (so far)

We introduced quantum paradigm and explained the BB84 quantum key distribution protocol.

Background towards DJ algorithm

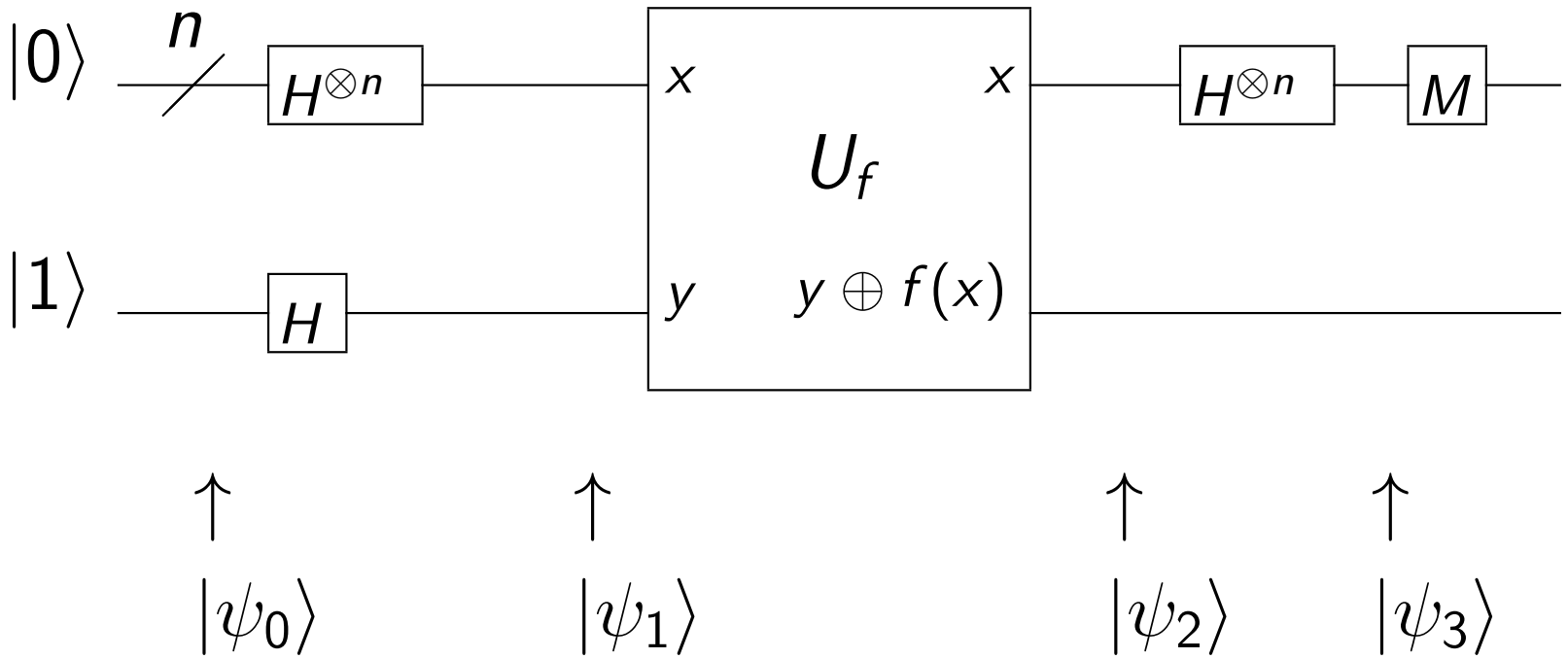
- Given a classical circuit f, there is a quantum circuit of comparable efficiency which computes the transformation U_f that takes input $|x, y\rangle$ and produces output $|x, y \oplus f(x)\rangle$.
- Let f be either constant or balanced. Consider f as an oracle. How fast one can decide which one it is.
- Deterministic classical algorithm may require $2^{n-1} + 1$ queries in worst case. Probabilistic classical algorithm requires a few steps to give an answer with very good probability.

Given such an U_f is available, Deutsch-Jozsa (1992) provided a quantum algorithm that can solve this problem in constant time deterministically.

D. Deutsch and R. Jozsa. Rapid solution of problems by quantum computation. Proceedings of Royal Society of London, A439:553–558 (1992).

Deutsch-Jozsa Algorithm

Quantum circuit to implement Deutsch-Jozsa Algorithm



DJ Algorithm

- A Boolean function f on n variables is available in the form of the transformation U_f
- Take an $(n+1)$ qubit state $|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle$
- Apply Hadamard Transform on $|\psi_0\rangle$ to get a superposition $|\psi_1\rangle = \sum_{x\in\{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$
- Apply U_f on $|\psi_1\rangle$ to get $|\psi_2\rangle = \sum_{x\in\{0,1\}^n} \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$
- Apply Hadamard Transform on the first n qubits of $|\psi_2\rangle$
- $|\psi_3\rangle = \sum_{z\in\{0,1\}^n} \sum_{x\in\{0,1\}^n} \frac{(-1)^{x\cdot z \oplus f(x)}|z\rangle}{2^n} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$.
- Measurement at M: measure the first n qubits of $|\psi_3\rangle$; all zero state implies that the function is constant, otherwise it is balanced.

Walsh transform

Suppose that $X, \omega \in \{0,1\}^n$ are two vectors in $\mathbb{F}_2^n$
Represent $X = (X_1, X_2, \ldots, X_n)$ and $\omega = (\omega_1, \omega_2, \ldots, \omega_n)$

Inner Product:

$$X \cdot \omega = X_1\omega_1 \oplus X_2\omega_2 \oplus \cdots \oplus X_n\omega_n$$

Walsh Transform of $f \in \Omega_n$ is defined as

$$W_f(\omega) = \sum_{X \in \{0,1\}^n} (-1)^{f(X) \oplus X \cdot \omega}$$

Walsh Transform & Deutsch-Jozsa Algorithm (contd.)

We have

$$\sum_{z\in\{0,1\}^n}\sum_{x\in\{0,1\}^n}\frac{(-1)^{x\cdot z\oplus f(x)}|z\rangle}{2^n}=\sum_{z\in\{0,1\}^n}\frac{W_f(z)}{2^n}|z\rangle,$$

i.e., the associated probability with a state $|z\rangle$ is $\frac{W_f^2(z)}{2^{2n}}$.

Given an n-variable Boolean function f, the Deutsch-Jozsa algorithm produces a superposition of all the states $z\in\{0,1\}^n$ at the measurement point M with amplitude $\frac{W_f(z)}{2^n}$ corresponding to each state z.

Walsh Transform & Deutsch-Jozsa Algorithm

Theorem

Given an n-variable Boolean function f, the Deutsch-Jozsa algorithm produces a superposition of all the states $z \in \{0,1\}^n$ at the measurement point M with amplitude $\frac{W_f(z)}{2^n}$ corresponding to each state $|z\rangle$.

Though the result is almost immediate, it was first pointed out in

S. Maitra and P. Mukhopadhyay. Deutsch-Jozsa Algorithm Revisited in the Domain of Cryptographically Significant Boolean Functions. In International Journal on Quantum Information 3(2), 359-370 (2005).

Parity Problem

E. Bernstein and U. Vazirani. Quantum complexity theory. In Proceedings of 25th Annual ACM Symposium on Theory of Computing, 1993, pages 11–20.

Problem

Let f be an linear n-variable Boolean function, i.e., $f(x) = \omega \cdot x$, available in the form of an oracle, Find out the ω.

- For a linear function $f(x) = \omega \cdot x$, $W_f(\omega) = 2^n$ and $W_f(z) = 0$, for $z \neq \omega$.
- Thus the observed state of n bits after DJ algorithm will output ω itself (with probability $\frac{W_f^2(\omega)}{2^{2n}} = 1$).
- Thus the Deutsch-Jozsa algorithm solves this problem in constant time.
- In classical model this problem clearly needs $O(n)$ time.

Finding Nonzero Walsh Spectrum Point

Problem

A Boolean function f is given in the form of an oracle. Find out an ω, such that $W_f(\omega) \neq 0$.

- Let $S = \{\omega | W_f(\omega) \neq 0\}$. For any $\omega \in \{0,1\}^n \setminus S$, $W_f(\omega) = 0$.
- After DJ algo, the associated probability with $|z\rangle$ is $\frac{W_f^2(z)}{2^{2n}}$.
- The probability associated with $|z\rangle$ is nonzero when $z \in S$ and the probability associated with $|z\rangle$ is 0 when $z \in \{0,1\}^n \setminus S$.
- Thus, the state, say ω, observed after application of DJ algorithm, belongs to S and for the observed ω, $W_f(\omega) \neq 0$.
- Hence the problem can be solved in constant time using the Deutsch-Jozsa algorithm.

Major Question

- It is known that factorization is in NP. It can be solved in polynomial time in Quantum paradigm.

  P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring, In Proceedings of 35th Annual Symposium on Foundations of Computer Science, IEEE Press, Los Alamitos, CA (1994).
- Factorization has no known deterministic polynomial time algorithm on classical computational framework. Only sub-exponential algorithms are known.
- Consider a problem $\mathcal{P}$ related to Walsh spectrum that can be solved efficiently using DJ algorithm.
- Try to prove that $\mathcal{P}$ is NP-complete or NP-Hard. Can we relate it to satisfiability problem?


Thank You!