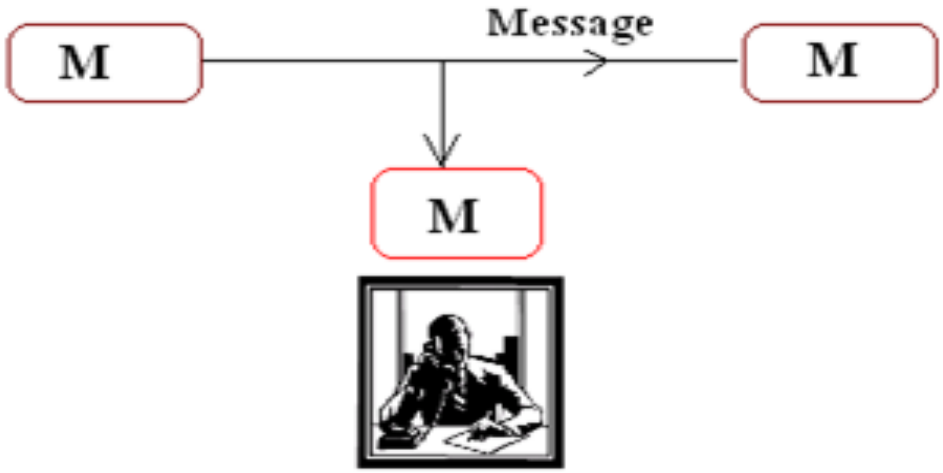
Quantum Information Processing and Quantum Computation

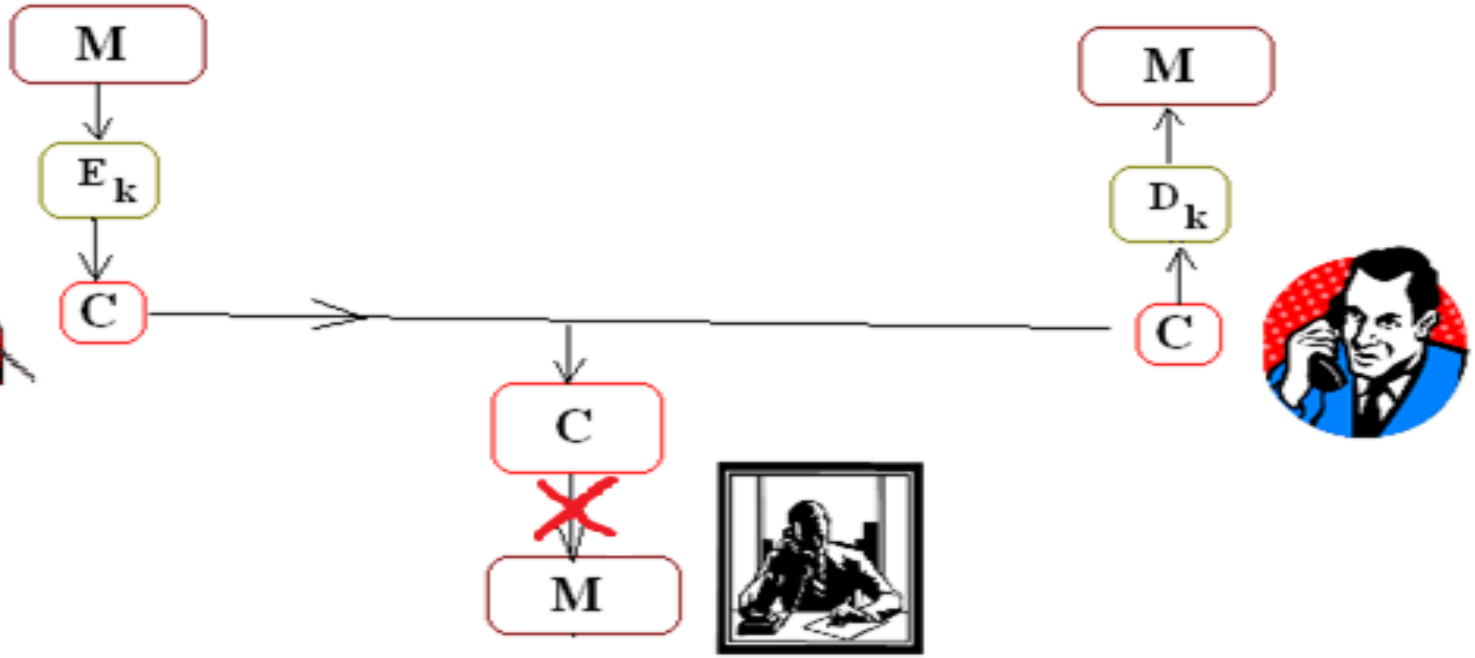
Guruprasad Kar

Quantum key generation

Problem of secrecy



Art of cryptography



M = 1 0 1 0 1 1 0

⊕

K = 1 1 0 0 1 0 1

C = 0 1 1 0 0 1 1

Bob

0 1 1 0 0 1 1 = C

⊕

1 1 0 0 1 0 1 K

1 0 1 0 1 1 0 = M

Alice

C

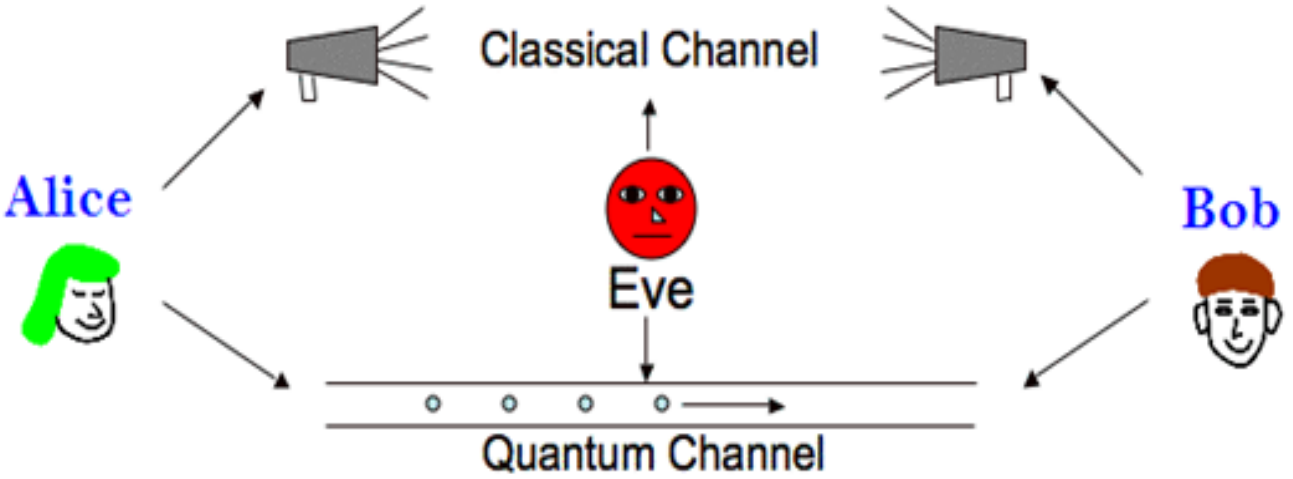
C

Eve

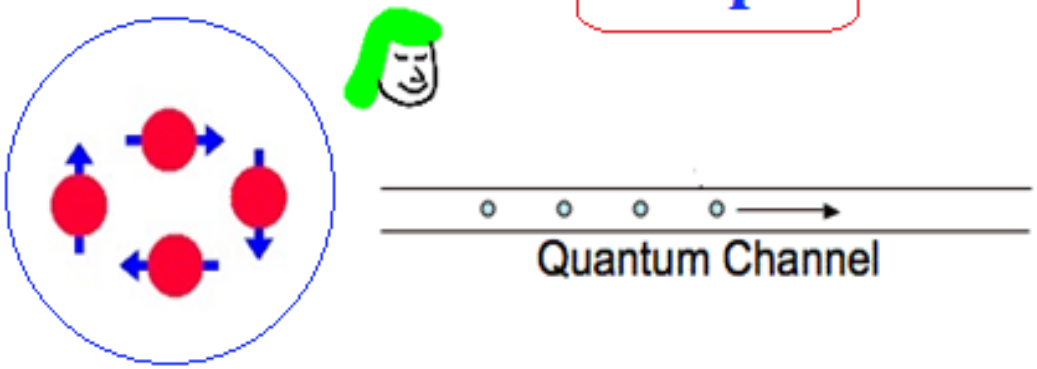
M

- **How to generate the key when Alice and Bob are far apart.**
- **Classical laws provide no solution.**
- **Quantum laws provide a secure protocol.**

BB-84 key generation protocol



Step-1



Alice selects qubits randomly and sends them to Bob one by one.

Bob randomly selects one of the measurements

σ_z and σ_x

and records the basis and results.

Step - 2

Classical Channel

Alice announces the basis but not the resuts (up or down)

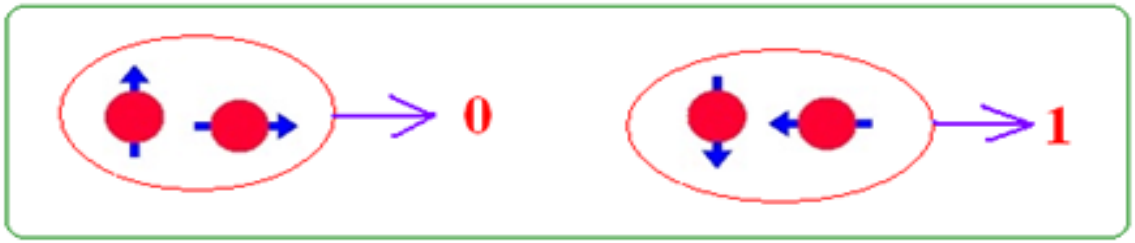
Step - 3

Classical Channel

Bob discards the cases when the basis do not match and informs Alice

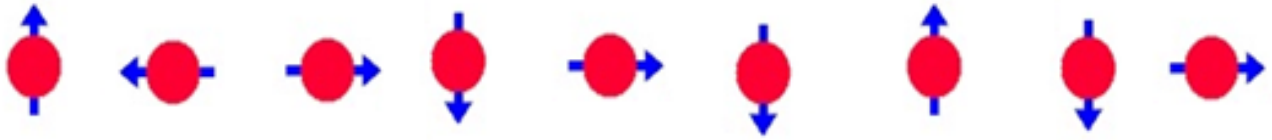
Step - 4

For the rest they assign bit according to



And generate the key

An example

Alice sends : 

Bob measures: σ_z σ_x σ_z σ_x σ_x σ_z σ_z σ_x σ_x

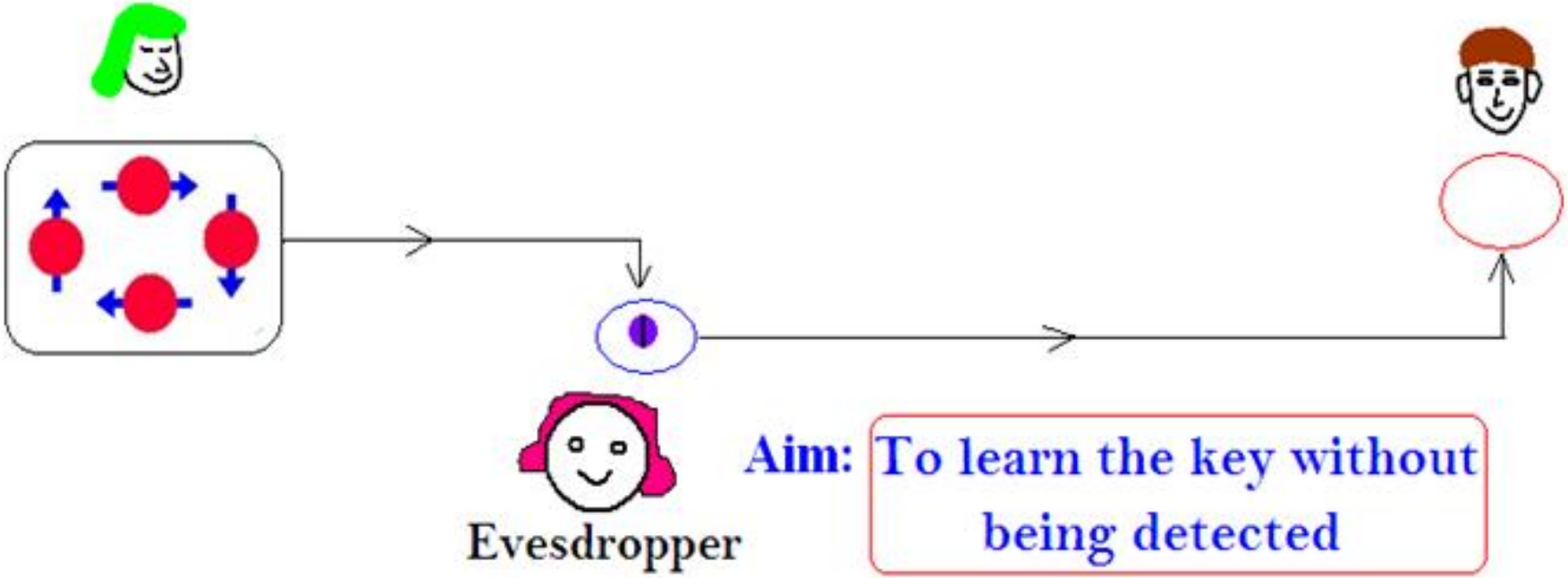
Accepted/Discarded : ✓ ✓ X X ✓ ✓ ✓ X ✓

Results : u d u d u u

Bit assignment : 0 1 0 1 0 0

Generated Key: 010100

Constraint on Eavesdrpper's options



Aim: To learn the key without being detected

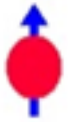
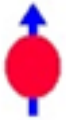
In classical world, in principle,
every different states can be learnt or copied.

In quantum world, information about the states can be gained only through measurement.

Measurement Collapse (Law of QM) helps detect Eve

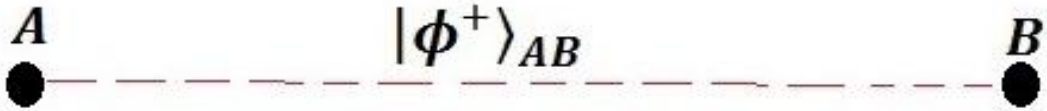
Alice and Bob disclose some of their results

Analysis of a case:

Alice	Eve	Results	Final state	Bob	Results	Eve's status
	σ_z	+1		σ_z	+1	Eve gains
	σ_x	+1 (50%)		σ_z	+1 (50%)	No gain No detection
		-1 (50%)			-1(50%)	Eve detected

Law of QM enables detecting the eavesdropper.

BBM key generation protocol:



$$|\phi^+\rangle = \frac{1}{\sqrt{2}}[|00\rangle + |11\rangle]$$

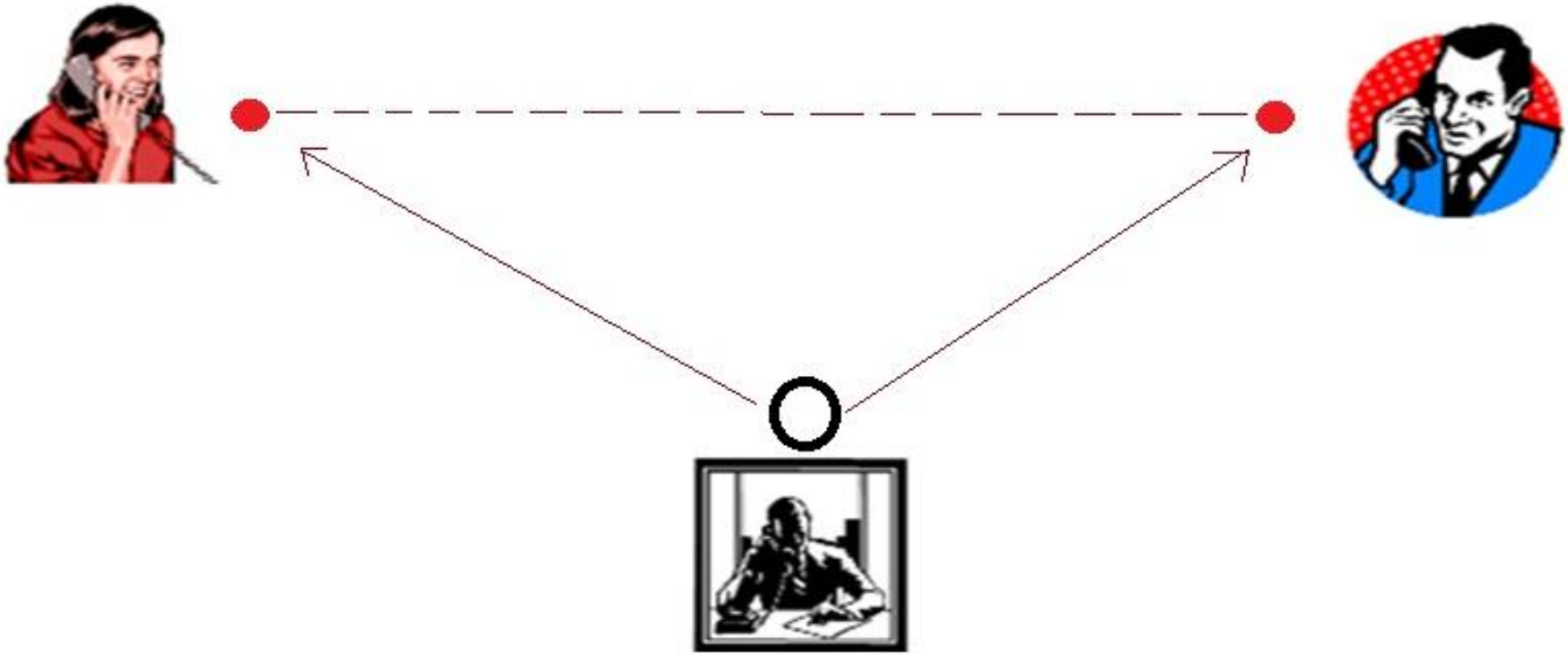
$$|\phi^+\rangle = \frac{1}{\sqrt{2}}[|++\rangle + |--\rangle]$$

Protocol:

- Alice and Bob both measures one of the spin observable chosen randomly from $\{\sigma_x, \sigma_z\}$ for each pair of Bell state and record their choices as well as the results.
- Alice and Bob publicly discuss their measurement choice (not results) and reject the cases where the choices do not match.
- With ther rest they generate the key by using the following encoding:

$$(|0\rangle, |+\rangle) \rightarrow 0 \; and \; (|1\rangle, |-\rangle) \rightarrow 1$$

Eavesdropper in the scenario



We shall consider the scenario where Eavesdropper himself is the supplier of Bell state.

Possibly this is the most favourable situation for Eve to get the secret key.

To be sure that supplier has really sent Bell state Alice and Bob checks the following:

(1) When they select the same measurement basis, their results are correlated.

(2) For both the measurements, results are completely random.

To get the secret key Eve as supplier, will try to correlate his system with the qubits of Alice and Bob.

Now whatever state Eve prepares can be written in the following form:

$$|\psi\rangle_{ABE} = c_{00}|00\rangle_{AB}|\phi_{00}\rangle_E + c_{01}|01\rangle_{AB}|\phi_{01}\rangle_E + c_{10}|10\rangle_{AB}|\phi_{10}\rangle_E + c_{11}|11\rangle_{AB}|\phi_{11}\rangle_E$$

Conditions to be obeyed by Eve as supplier:

But the results of spin measurement along z-axis has to be correlated, This restricts the choice and the state has to be of the following form:

$$|\psi\rangle_{ABE} = c_{00}|00\rangle_{AB}|\phi_{00}\rangle_E + c_{11}|11\rangle_{AB}|\phi_{11}\rangle_E$$

Both results are completely random which restricts the state further:

$$|\psi\rangle_{ABE} = \frac{1}{\sqrt{2}}|00\rangle_{AB}|\phi_{00}\rangle_E + \frac{1}{\sqrt{2}}|11\rangle_{AB}|\phi_{11}\rangle_E$$

But the results of spin measurement along x-axis has also to be correlated:

$$|\psi\rangle_{ABE} = \frac{1}{\sqrt{2}}|00\rangle_{AB}|\phi_{00}\rangle_E + \frac{1}{\sqrt{2}}|11\rangle_{AB}|\phi_{11}\rangle_E$$

Write the state of A and B in $\{|+\rangle, |-\rangle\}$ ***basis.***

$$|\psi\rangle_{ABE} = \frac{1}{2\sqrt{2}}|++\rangle_{AB}(|\phi_{00}\rangle_E + |\phi_{11}\rangle_E)$$

$$+\frac{1}{2\sqrt{2}}|+-\rangle_{AB}(|\phi_{00}\rangle_E - |\phi_{11}\rangle_E)$$

$$+\frac{1}{2\sqrt{2}}|-+\rangle_{AB}(|\phi_{00}\rangle_E - |\phi_{11}\rangle_E)$$

$$+\frac{1}{2\sqrt{2}}|--\rangle_{AB}(|\phi_{00}\rangle_E + |\phi_{11}\rangle_E)$$

The result along X axis has also to be correlated. Hence the following condition has to be satisfied.

$$|\phi_{00}\rangle_E = |\phi_{11}\rangle_E$$

Then

$$|\psi\rangle_{ABE} = \frac{1}{2\sqrt{2}}|++\rangle_{AB}(2|\phi_{00}\rangle_E) + \frac{1}{2\sqrt{2}}|--\rangle_{AB}(2|\phi_{00}\rangle_E)$$

$$|\psi\rangle_{ABE} = \frac{1}{\sqrt{2}}(|++\rangle_{AB} + |--\rangle_{AB})|\phi_{00}\rangle_E$$

Hence Eavesdropper to be a faithful supplier has to remain completely uncorrelated with Alice and Bob.

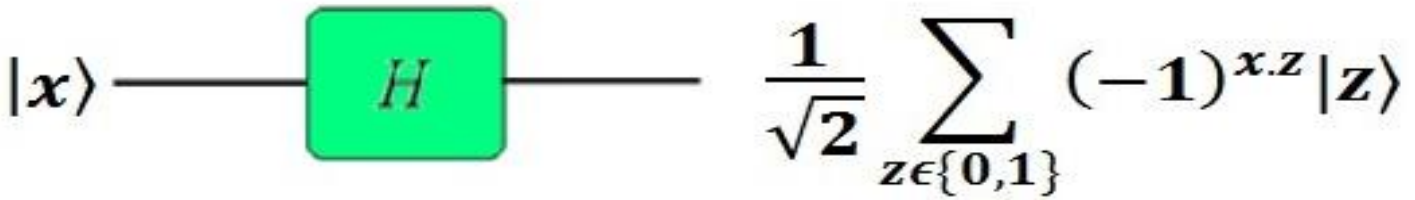
Quantum Computation

Hadamard Gate:

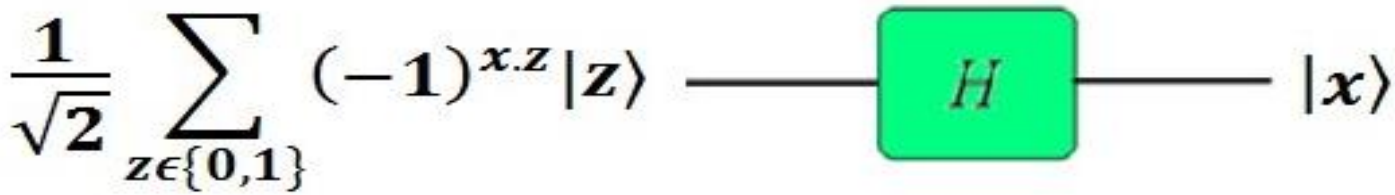
$$H|0\rangle = \frac{1}{\sqrt{2}}\,(|0\rangle + |1\rangle), \quad H|1\rangle = \frac{1}{\sqrt{2}}\,(|0\rangle - |1\rangle)$$

$$H|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle) = \frac{1}{\sqrt{2}}\sum_{z\epsilon\{0,1\}}(-1)^{x.z}|z\rangle$$

Bit information is encoded in the relative phase:



Bit information encoded in phase is decoded:



Multi Qubit Hadamard Gate

$$|x\rangle \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{z\epsilon\{0,1\}^n} (-1)^{x.z}|z\rangle \xrightarrow{H^{\otimes n}} |x\rangle$$

$$H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \ldots\ldots = \frac{1}{\sqrt{2^n}} \sum_{x\epsilon\{0,1\}^n} |x\rangle$$

$$|x\rangle = |x_1\rangle|x_2\rangle|x_3\rangle \ldots\ldots |x_n\rangle, \quad x_i\epsilon\{0,1\}^n$$

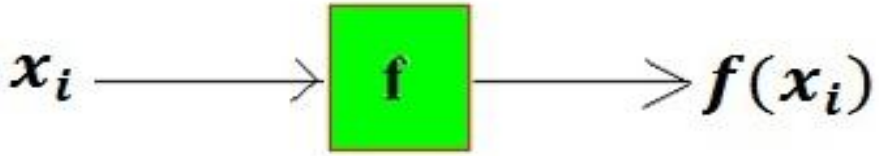
$$H^{\otimes n}|x\rangle = H|x_1\rangle H|x_2\rangle H|x_3\rangle \ldots\ldots H|x_n\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_{x\epsilon\{0,1\}^n} (-1)^{x_1.z_1}|z_1\rangle \sum_{x\epsilon\{0,1\}^n} (-1)^{x_2.z_2}|z_2\rangle \ldots. \sum_{x\epsilon\{0,1\}^n} (-1)^{x_n.z_n}|z_n\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_{z_1 z_2 \ldots z_n\epsilon\{0,1\}^n} (-1)^{x_1.z_1 + x_2.z_2 + \cdots x_n.z_n}|z_1\rangle|z_2\rangle \ldots\ldots |z_n\rangle$$

$$\boxed{H|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{z\epsilon\{0,1\}^n} (-1)^{x.z}|z\rangle}$$

Modelling quantum computation:



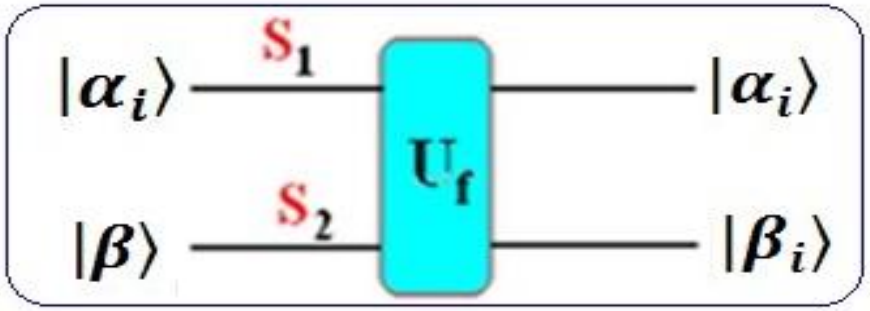
$System\ S_1 \mapsto \{|\alpha_i\rangle\}$ $System\ S_2 \mapsto \{|\beta_j\rangle\}$

Encoding input and output:

$$x_i \rightarrow |\alpha_i\rangle, i = 1, 2, 3 \ldots..$$

$$f(x_i) \rightarrow |\beta_i\rangle, \quad i = 1, 2, 3 \ldots..$$

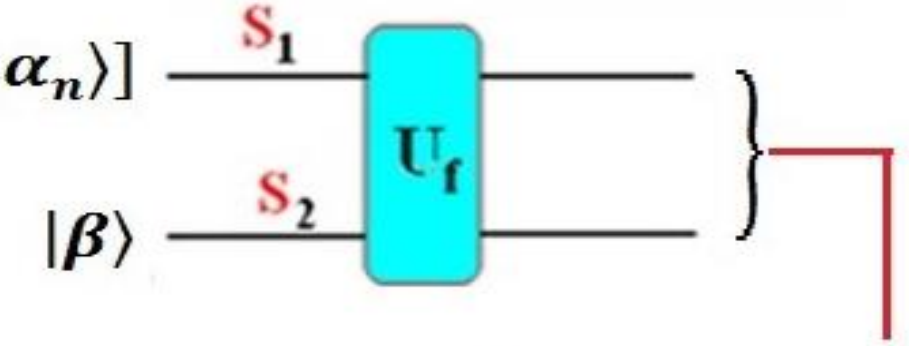
Quantum version of computation:



$$U_f|\alpha_i\rangle|\beta\rangle = |\alpha_i\rangle|\beta_i\rangle$$

Quantum Parallelism

$$\frac{1}{\sqrt{n}}[|\alpha_1\rangle + |\alpha_2\rangle + .. |\alpha_n\rangle]$$



$$\frac{1}{\sqrt{n}}[|\alpha_1\rangle|\beta_1\rangle + |\alpha_2\rangle|\beta_2\rangle + .. |\alpha_n\rangle|\beta_n\rangle]$$

$$U_f\left(\frac{1}{\sqrt{n}}[|\alpha_1\rangle + |\alpha_2\rangle + .. |\alpha_n\rangle]|\beta\rangle\right)$$

$$= \frac{1}{\sqrt{n}}[|\alpha_1\rangle|\beta_1\rangle + |\alpha_2\rangle|\beta_2\rangle + .. |\alpha_n\rangle|\beta_n\rangle]$$

$$= \frac{1}{\sqrt{n}}[|x_1\rangle|f(x_1)\rangle + |x_2\rangle|f(x_2)\rangle + \cdots \quad |x_n\rangle|f(x_n)\rangle]$$

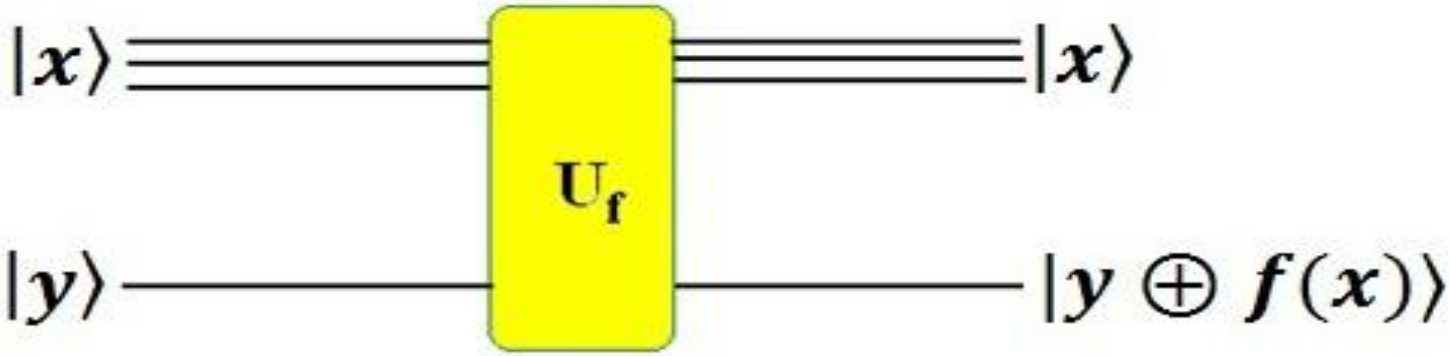
The function has been calculated at all points at one go!

But due to measurement collapse there will be no gain.

Phase kick back mechanism

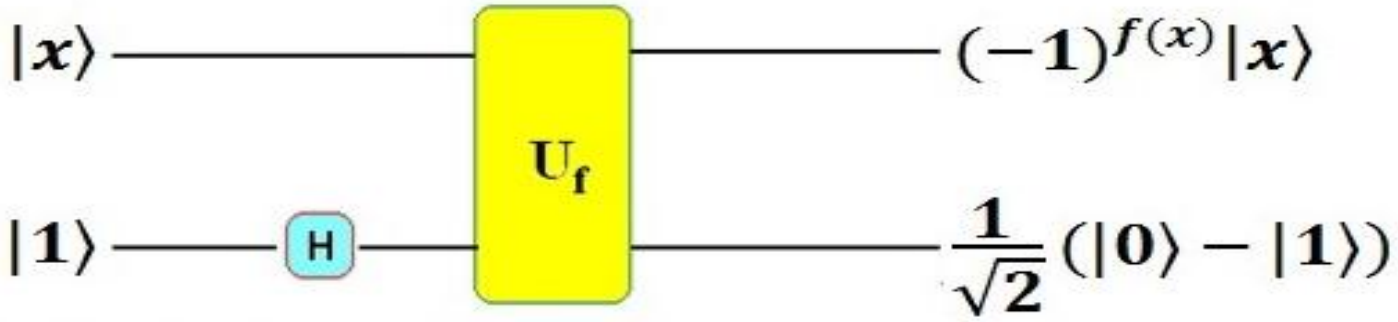
Consider the following function:

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



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

$$x \in \{0,1\}^n \; and \; y \in \{0,1\}$$



For $f(x) = 0$,

$$U_f|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}[U_f|x\rangle|0\rangle - U_f|x\rangle|1\rangle]$$

$$= \frac{1}{\sqrt{2}}[|x\rangle|0 \oplus f(x)\rangle - |x\rangle|1 \oplus f(x)\rangle$$

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

For $f(x) = 1$,

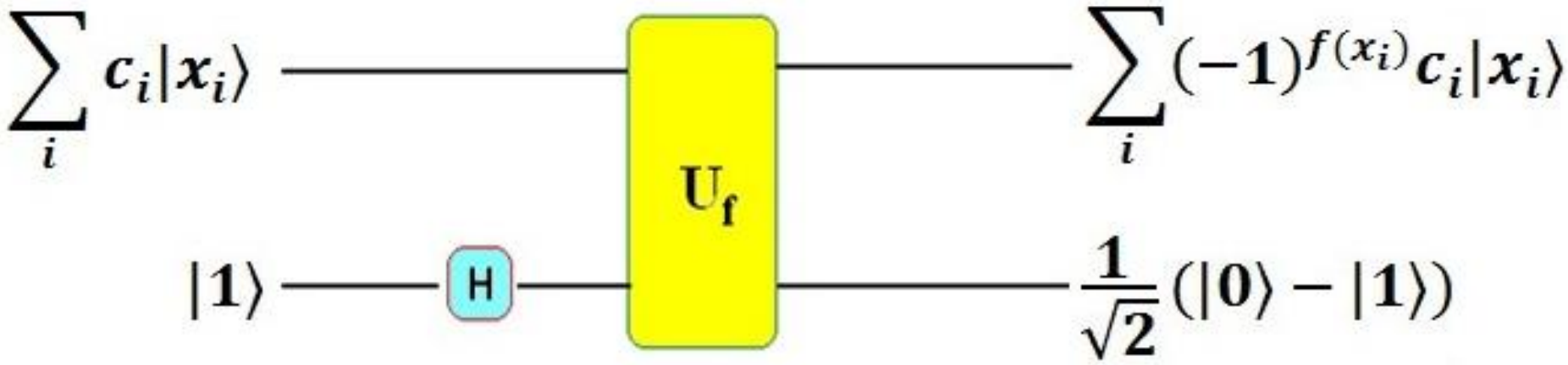
$$U_f|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}[U_f|x\rangle|0\rangle - U_f|x\rangle|1\rangle]$$

$$= \frac{1}{\sqrt{2}}[|x\rangle|0 \oplus f(x)\rangle - |x\rangle|1 \oplus f(x)\rangle$$

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

Simple quantum algorithm by exploiting

1) The phase kick back mechanism applied to superposition of states.



2) Properties of transferring phase information to bit value and vice-versa by Hadamard gate.

—Deutsch algorithm—

Consider the function $f : \{0, 1\} \longrightarrow \{0, 1\}$

(a) Function may be constant [$f(1) = f(0)$] :

$f(0) = 0$	or	$f(0) = 1$
$f(1) = 0$		$f(1) = 1$

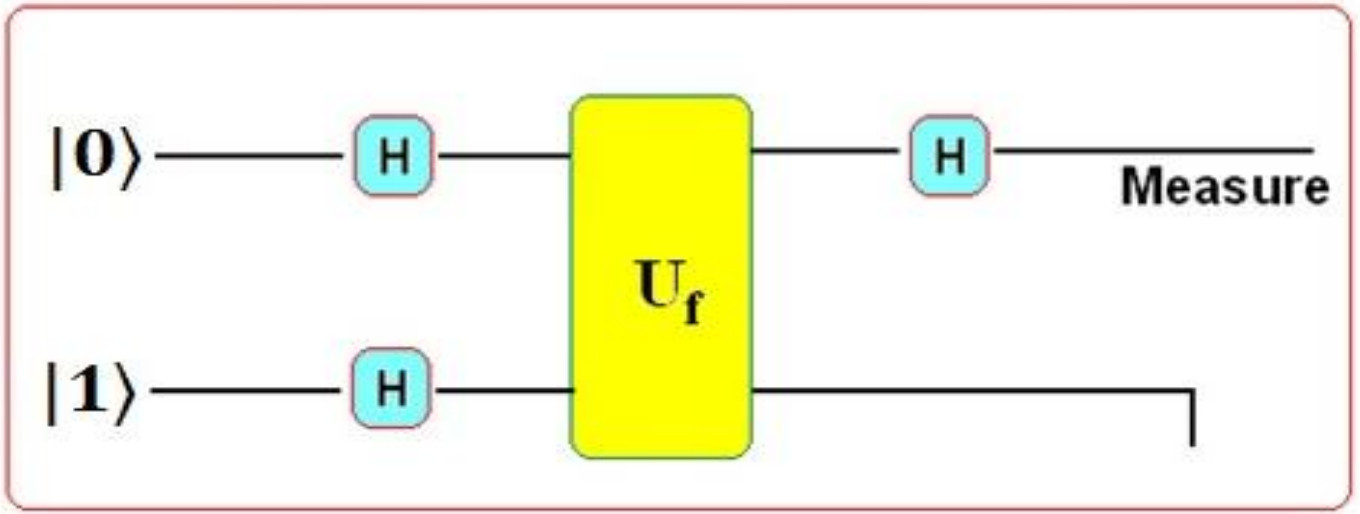
(b) Function may be balanced [$f(1) \neq f(0)$] :

$f(0) = 0$	or	$f(0) = 1$
$f(1) = 1$		$f(1) = 0$

To learn whether the function is constant or balanced one has to compute it at both the points.

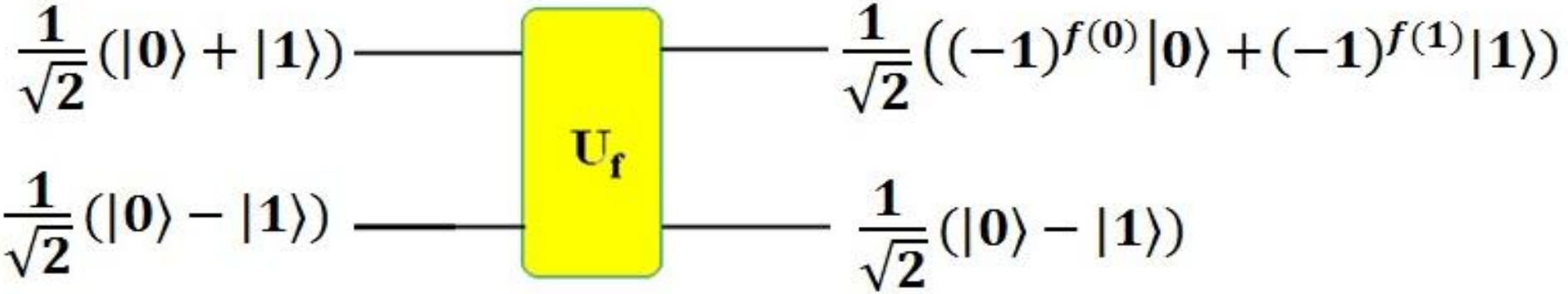
— Quantum protocol —

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



Result	Conclusion
Up	f is constant
Down	f is balanced

How it works:



State of the 1st qubit

Constant function $f(0) = f(1)$

Balanced function $f(0) \neq f(1)$

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

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

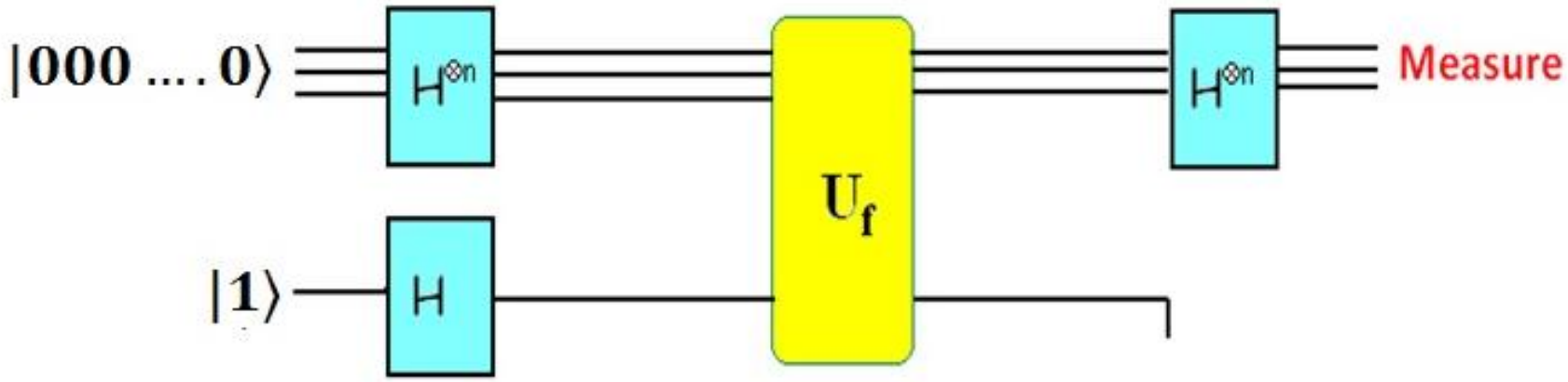
} **orthogonal**

	Result	Conclusion
Apply H and measure σ_z	Up	function is constant
	Down	function is balanced

Deutsch-Jozsa algorithm

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

The function **f** is either constant or balanced (f(x) =0 for half of the possible input)



Result	Conclusion
All spins are up	f is constant
All spins are not up	f is balanced

How it works:

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

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

Discard

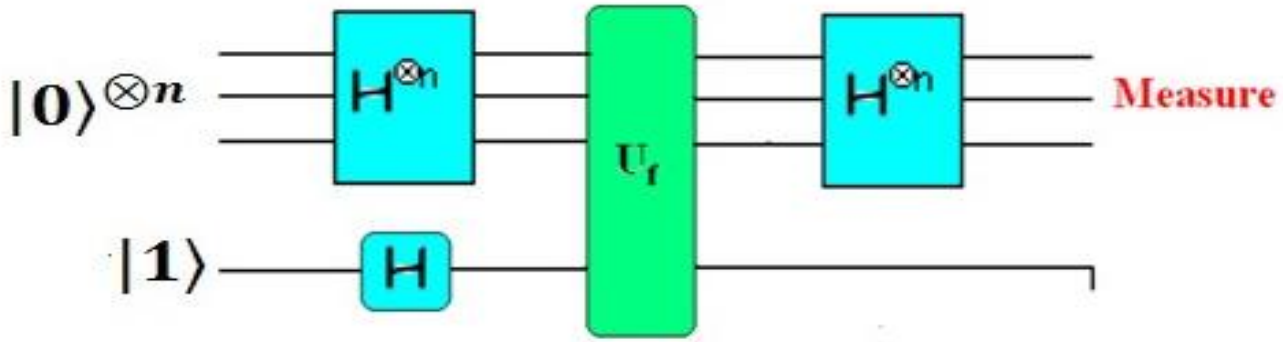
$$\xrightarrow{H^{\otimes n}} \frac{1}{2^n} \sum_{x=0}^{2^n-1} \sum_{z=0}^{2^n-1} (-1)^{f(x)} (-1)^{x.z} |z\rangle$$

	f is constant	f is balanced
Coefficient of $\|000 \ldots . 0\rangle$	+1 or –1	0
Probability for all spin up	1	0

Bernstein-Vazirani Problem

$$f_a(x) = x.a, \quad x,a \in \{0,1\}^n$$

Determine a



How it works:

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

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

Discard

$$= \sum_{x=0}^{2^n-1} (-1)^{x.a} |x\rangle \xrightarrow{H^{\otimes n}} |a\rangle$$

Simon's Algorithm

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

which is two to one.

The function has a period given by the n-bit string a.

$$f(x) = f(y), \qquad iff \quad y = x \oplus a$$

$$x = x_1 x_2 x_3 \ldots\ldots x_n, \; x_i \in \{0,1\}$$

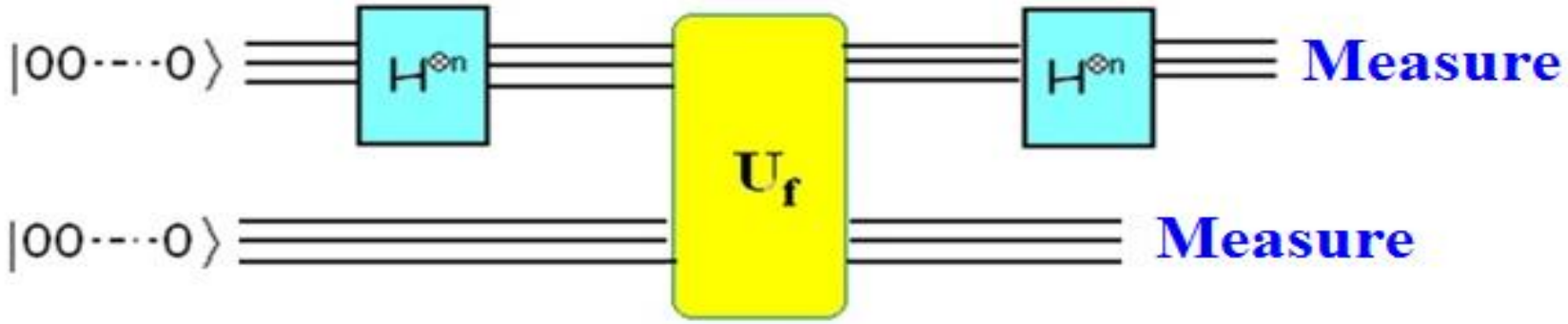
$$x \oplus a = (x_1 \oplus a_1)(x_2 \oplus a_2) \ldots\ldots (x_n \oplus a_n)$$

$$x.a = (x_1.a_1) \oplus (x_2.a_2) \oplus \ldots\ldots \oplus (x_n.a_n)$$

The problem is to find a.

In classical computation, this is exponentially hard problem.

Quantum algorithm



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

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

$$= \frac{1}{\sqrt{2^n}} [(|x_0\rangle + |x_0 \oplus a\rangle)|f(x_0\rangle + (|x_1\rangle + |x_1 \oplus a\rangle)|f(x_1\rangle$$

$$+ \cdots\cdots\cdots\cdots\cdots\cdots (|x_i\rangle + |x_i \oplus a\rangle)|f(x_i\rangle \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots]$$

Measure the second registrar:

Let the result is $|f(x_i)\rangle$

The final state of the first registrar:

$$\frac{1}{\sqrt{2}}\left(|x_i\rangle + |x_i \oplus a\rangle\right)$$

$$\frac{1}{\sqrt{2}}\left(|x_i\rangle + |x_i \oplus a\rangle\right) \xrightarrow{H^{\otimes n}}$$

$$= \frac{1}{\sqrt{2^{n+1}}} \sum_{y=0}^{2^n-1} [(-1)^{x_i \cdot y} + (-1)^{(x_i \oplus a)\cdot y}]|y\rangle$$

(a) For $a.y = 1$

$$[(-1)^{x_0.y} + (-1)^{(x_0 \oplus a).y}] = [(-1)^{x_0.y} + (-1)^{(x_0.y \oplus 1)}] = 0$$

(b) For $a.y = 0$

$$[(-1)^{x_0.y} + (-1)^{(x_0 \oplus a).y}] = 2(-1)^{x_0.y}$$

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{y=0}^{2^n-1} [(-1)^{x_0.y} + (-1)^{(x_0 \oplus a).y}] |y\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{a.y=0} (-1)^{x_0.y} |y\rangle$$

Measurement on the first registrar and repeating the process we get

$y_1, y_2, \ldots \ldots . y_n$ that satifies;

$$a.y_1 = 0$$
$$a.y_2 = 0$$
$$a.y_3 = 0$$
$$\ldots\ldots\ldots\ldots$$
$$a.y_n = 0$$

Hence we can determine a by $o(n)$ repetitions of the process.

Grover's search algorithm

Consider a function:

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

$$f(x) = 1 \; for \; x = x_k$$

$$f(x) = 0 \; for \; x \neq x_k$$

The task is to find x_k.

Understanding Grover's operation

An $n-$ qubit unitary operation U_0 is defined in the following way:

$$U_0|0\rangle = |0\rangle$$
$$U_0|x\rangle = -|x\rangle, \quad x \neq 0$$

Let $|\psi\rangle = H|0\rangle$

Then unitary HU_0H *acts in the following way:*

$$HU_0H|\psi\rangle = |\psi\rangle$$

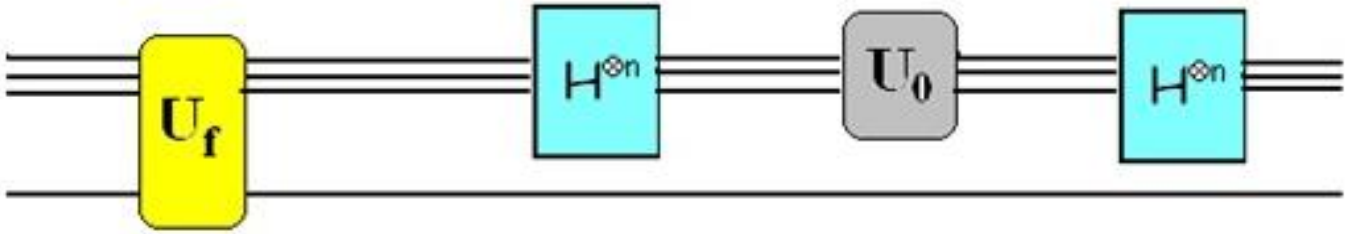
Subspace orthogonal to $H|0\rangle$ *is apanned by the collection of the orthogonal vectors* $\{H|x\rangle, x \neq 0\}$

$$HU_0H(H|x\rangle) = -H|x\rangle, \; x \neq 0$$

Grover's operation G consists of

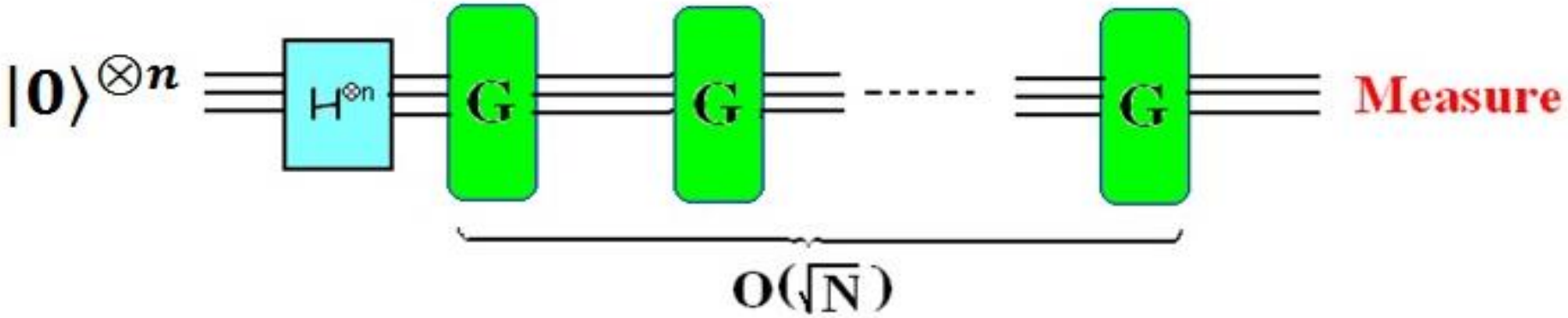
1) Phase kickback mechanism $U_f|x\rangle \rightarrow (-1)^{f(x)}|x\rangle$

2) HU_0H



$$G = HU_0HU_f$$

Grover's algorithm



Geometric understanding of the operations

$$H|0\rangle = \frac{1}{\sqrt{N}}\sum_{x}|x\rangle = \frac{1}{\sqrt{N}}|x_k\rangle + \frac{1}{\sqrt{N}}\sum_{x\neq x_k}|x\rangle$$

$$= \frac{1}{\sqrt{N}}|x_k\rangle + \frac{\sqrt{N-1}}{\sqrt{N}}|\bar{x}_k\rangle$$

$$H|0\rangle = Sin\theta|x_k\rangle + Cos\theta|\bar{x}_k\rangle$$

$$\overline{H|0\rangle} = Cos\theta|x_k\rangle - Sin\theta|\bar{x}_k\rangle$$

$$|x_k\rangle = Sin\theta H|0\rangle + Cos\theta\overline{H|0\rangle}$$

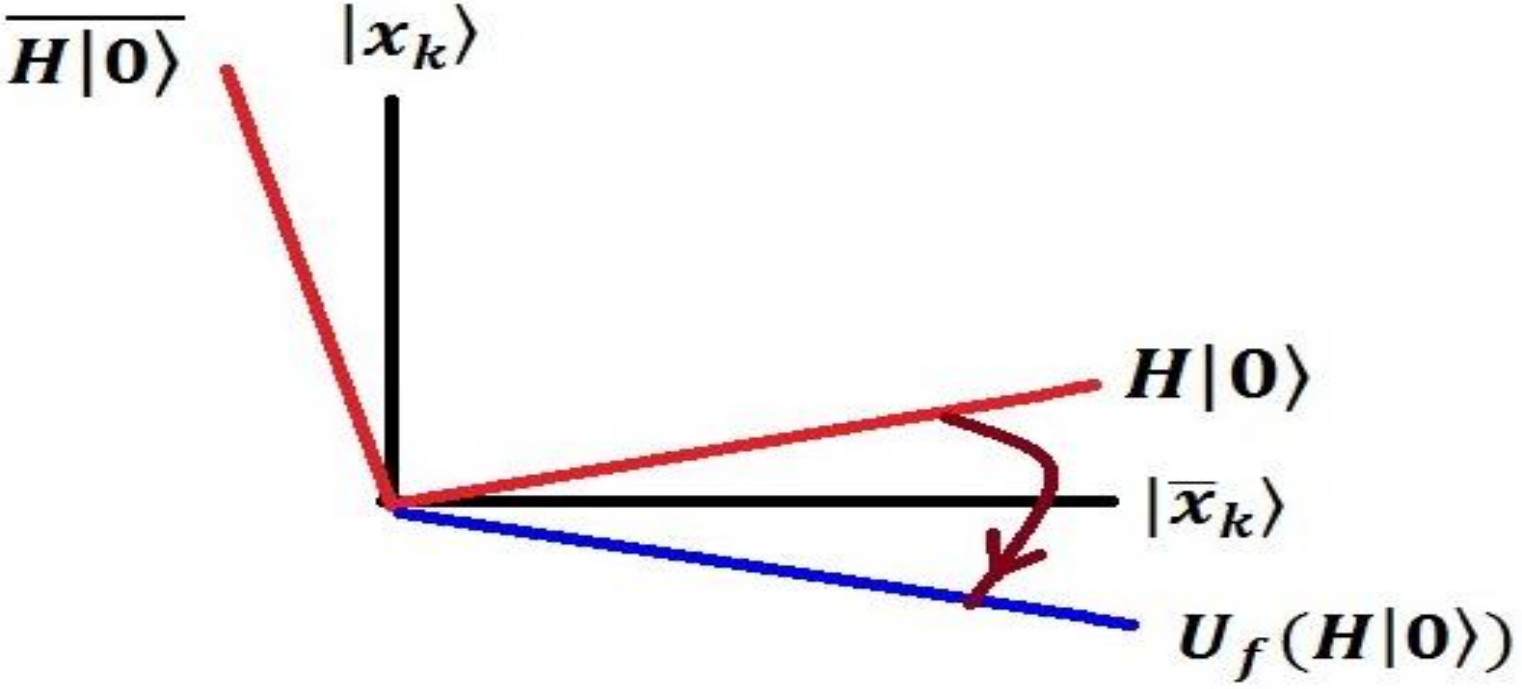
$$|\bar{x}_k\rangle = Cos\theta H|0\rangle - Sin\theta\overline{H|0\rangle}$$

U_f is a reflection against the vector $|\overline{x}_k\rangle$

$$U_f : H|0\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_x (-1)^{f(x)} |x\rangle$$

$$= -\frac{1}{\sqrt{N}} |x_k\rangle + \frac{1}{\sqrt{N}} \sum_{x \neq x_k} |x\rangle$$

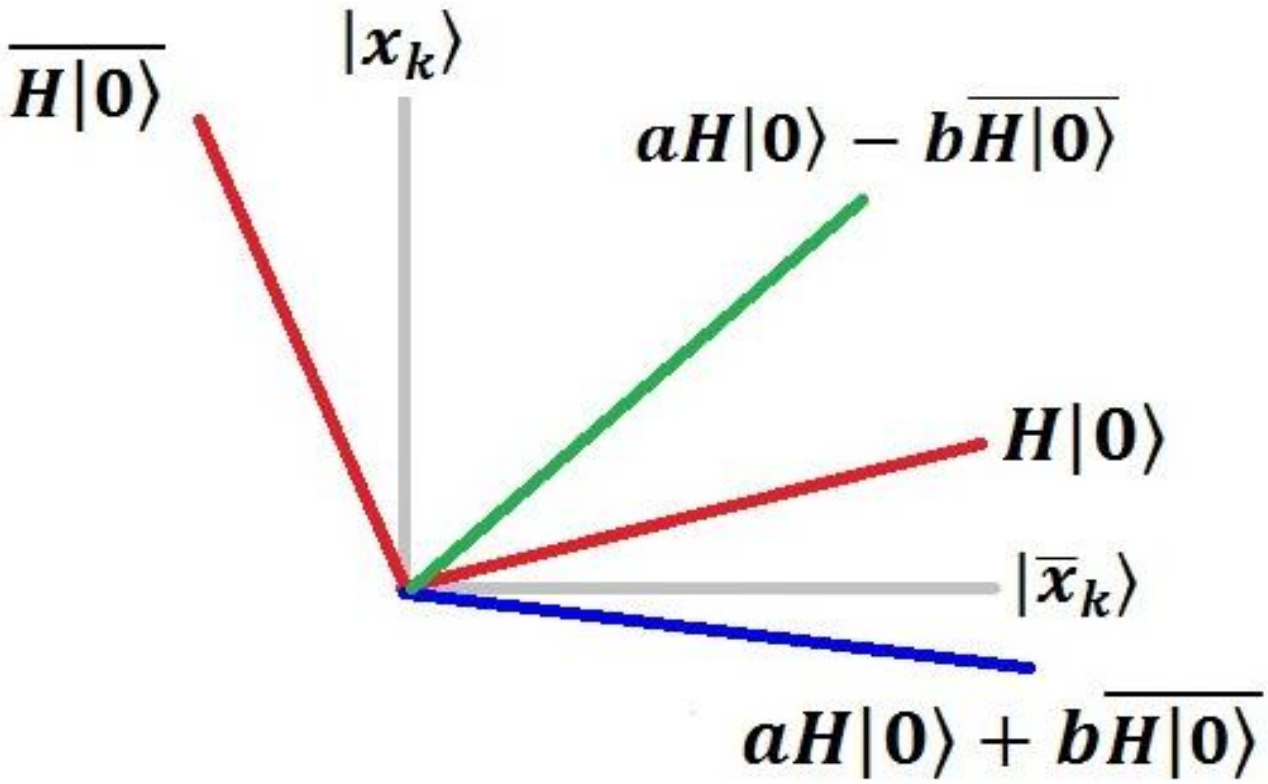
$$= -Sin\theta |x_k\rangle + Cos\theta |\overline{x}_k\rangle$$



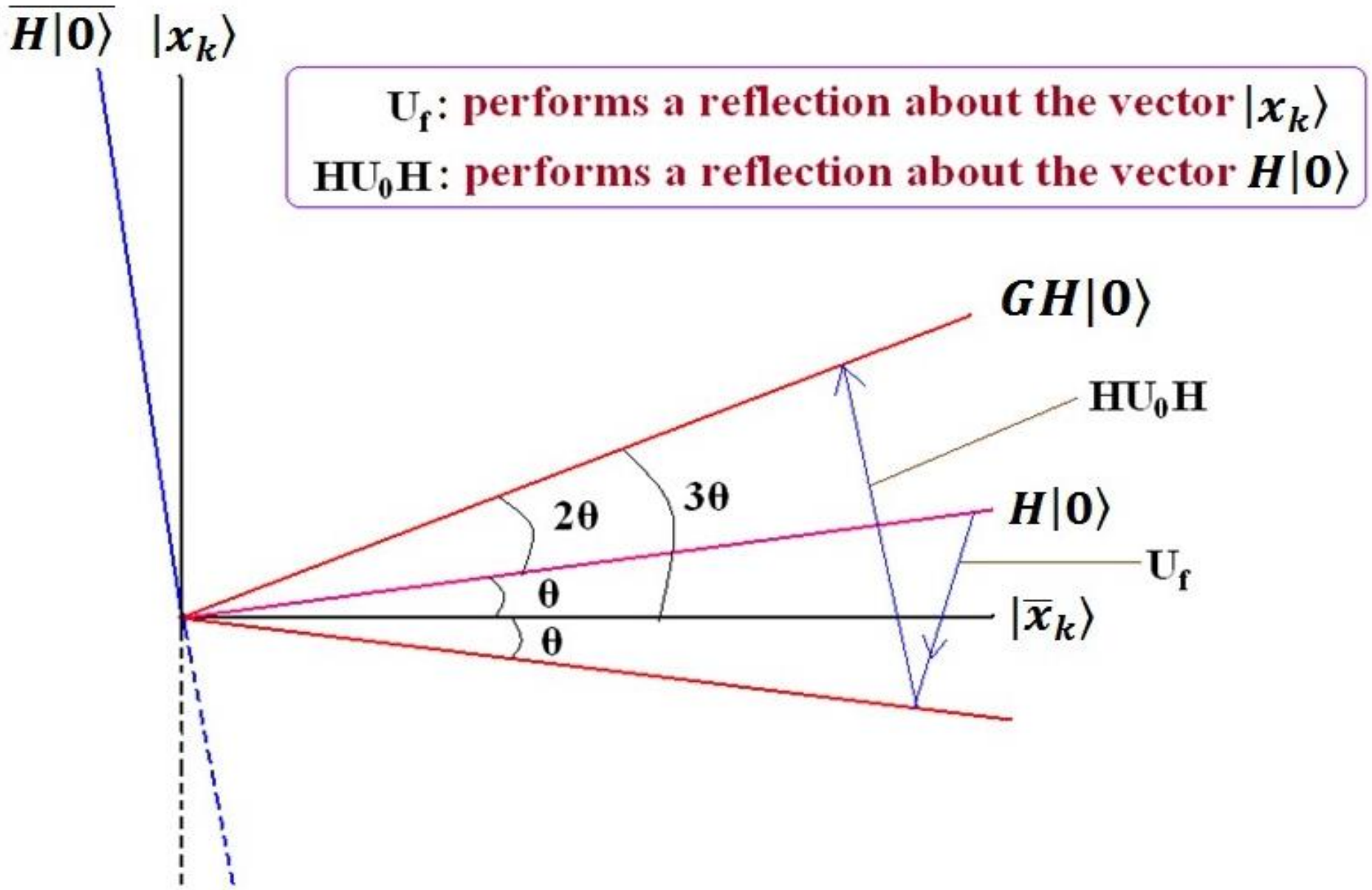
HU_0H *is a reflection against the vector* $H|0\rangle$

$$HU_0H\,(aH|0\rangle + b\overline{H|0\rangle})$$

$$= aH|0\rangle - b\overline{H|0\rangle}$$



Geometric picture of Action of Grover's operation



The Initial state:

$$H|0\rangle = Sin\theta|x_k\rangle + Cos\theta|\overline{x}_k\rangle$$

$$\xrightarrow{U_f} \quad -Sin\theta|x_k\rangle + Cos\theta|\overline{x}_k\rangle$$

When expressed in $\{H|0\rangle, \overline{H|0\rangle}\}$ ***basis:***

$$U_f H|0\rangle = Cos2\theta H|0\rangle - Sin2\theta\overline{H|0\rangle}$$

$$\xrightarrow{HU_0H} \quad Cos2\theta H|0\rangle + Sin2\theta\overline{H|0\rangle}$$

When expressed in $\{|x_k\rangle, |\overline{x}_k\rangle\}$ ***basis:***

$$HU_0HU_fH|0\rangle = GH|0\rangle = Sin3\theta|x_k\rangle + Cos3\theta|\overline{x}_k\rangle$$

After applying G *k times*:

$$G^K H|0\rangle = Sin(2k+1)\theta|x_k\rangle + Cos(2k+1)\theta|\overline{x}_k\rangle$$

To obtain the desired result in measurement i.e to collapse on $|x_k\rangle$

$$Sin(2k+1)\theta \approx 1$$

$$(2k+1)\theta \approx \frac{\pi}{2}$$

$$k \approx \frac{\pi}{4\theta} - \frac{1}{2}$$

For large N:

$$Sin\theta = \theta = \frac{1}{\sqrt{N}}$$

$$k \approx \frac{\pi}{4}\sqrt{N} \approx O(\sqrt{N})$$

Hence there is a quadratic speed up.