LECTURES:

1-2. **MP472 QUANTUM INFORMATION PROCESSING**

3-4. **QUANTUM MECHANICS FOUNDATIONS OF QUANTUM INFORMATION PROCESSING.** STATES

5-6. **QUANTUM MECHANICS FOUNDATIONS OF QUANTUM INFORMATION PROCESSING.** OPERATORS

7-8. **QUANTUM MECHANICS FOUNDATIONS OF QUANTUM INFORMATION PROCESSING.** DYNAMICS

9-10. **QUANTUM MECHANICS FOUNDATIONS OF QUANTUM INFORMATION PROCESSING.** MEASUREMENT

11-12. **CLASSICAL AND QUANTUM COMPUTATION.**
COMPUTATIONAL COMPLEXITY CLASSES

13-14. **CLASSICAL AND QUANTUM COMPUTATION.**
QUANTUM ALGORITHMS

MP472 QUANTUM INFORMATION PROCESSING

Classical information
- classical bit
- Boolean function
- Boolean circuit

Quantum information
- quantum bit(s)
- quantum operations
- quantum state measurement
- quantum circuit
- example: quantum entangler

Example of quantum information processing:
Teleportation

Classical information and its processing

An elementary unit of classical information is **bit**

$$\mathbb{B} = \{0, 1\}$$

Information is physical (Rolf Landauer, IBM):

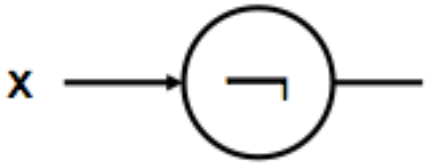
The values 0 and 1 of the bit correspond to two distinct values (states) of some physical quantity, for example electric voltage.

A **Boolean function** on n variables

$$F(x_1, x_2, ..., x_n) : \mathbb{B}^n \rightarrow \mathbb{B}^k$$

Examples: simple Boolean functions

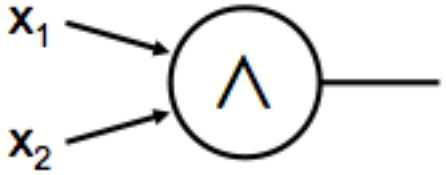
negation $\neg x$
(bit flip)



x	¬x
0	1
1	0

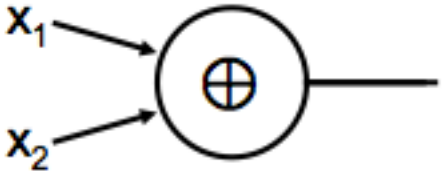
(bit flip)

conjunction $x_1 \wedge x_2$



x_1	x_2	$x_1 \wedge x_2$
0	0	0
0	1	0
1	0	0
1	1	1

addition mod(2) $x_1 \oplus x_2$



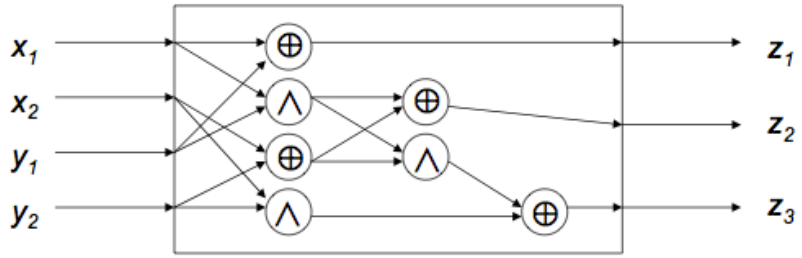
x_1	x_2	$x_1 \oplus x_2$
0	0	0
0	1	1
1	0	1
1	1	0

A **Boolean circuit** is a representation of a Boolean function as a composition of other Boolean functions from a set $\mathcal{B}$, for example:

$$\mathcal{B}\{\wedge, \oplus\}$$

A circuit over $\mathcal{B}$ is a sequence of assignments involving n input variables $\{x_1, x_2, ..., x_n\}$ and several auxiliary variables $\{y_1, y_2, ..., y_k\}$ where $y_k = f_k(u_1, ..., u_r)$ and each of the variables $u_1, ..., u_r$ are either input variables or auxiliary variables preceeding y_k.

Example: Addition of two 2-digit numbers (Kitaev et al.)



A basis $\mathcal{B}$ is called complete , if for any Boolean function f, there is a circuit over $\mathcal{B}$ that computes f. For example $\mathcal{B}\{\wedge, \oplus\}$.

Quantum information

Quantum bit or **qubit** is a two dimensional Hilbert space $\mathcal{H}^2 \simeq \mathbb{C}^2$.

Qubit values are vectors, states, from this Hilbert space:

$$|\phi\rangle = c_0|0\rangle + c_1|1\rangle$$

where $|0\rangle$ and $|1\rangle$ are an orthonormal set called the **standard computational basis** and $c_0, c_1 \in \mathbb{C}$ and $|c_0|^2 + |c_1|^2 = 1$.

Physical realization of a qubit can for example be a spin-1/2 particle:

$$|0\rangle = |\uparrow\rangle \qquad |1\rangle = |\downarrow\rangle \qquad\qquad |\phi\rangle = c_{\uparrow}|\uparrow\rangle + c_{\downarrow}|\downarrow\rangle$$

or two energy levels of an atom or ion,
or opposite superconducting fluxes in a superconducting flux qubit,
or ...

Quantum logic operations are rotations of a quantum state vector in a Hilbert space:

they are **unitary**, and thus **reversible**, operations.

(Classical computation can be made reversible.)

Qubits

A quantum state of n qubits is a vector in 2^n-dimensional Hilbert space:

$$\bigotimes_{k=1}^{n} \mathcal{H}^2 = \mathcal{H}^2 \otimes \mathcal{H}^2 \otimes ... \mathcal{H}^2 \quad \text{(n-times)} = \mathcal{H}^{2^n}$$

Examples: Composite product states

$$|\phi\rangle = |0\rangle \otimes |0\rangle = |0\rangle|0\rangle = |00\rangle$$

or

$$|\psi\rangle = (c_0|0\rangle + c_1|1\rangle) \otimes |0\rangle = c_{00}|00\rangle + c_{10}|10\rangle$$

where in the latter we identified $c_{00} = c_0$ and $c_{10} = c_1$.

Examples: Entangled states: the Bell states

$$
\begin{aligned}
|\beta_{00}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
|\beta_{01}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\
|\beta_{10}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\
|\beta_{11}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)
\end{aligned}
$$

No-cloning theorem: Quantum information can not be cloned (copied):

Assume there is a cloning operator $\hat{C}$ such that

$$\hat{C}|0\rangle = |0\rangle \otimes |0\rangle = |00\rangle \quad \text{and} \quad \hat{C}|1\rangle = |1\rangle \otimes |1\rangle = |11\rangle$$

then applying it onto a superposition $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$ proofs the theorem

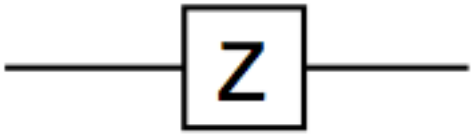
$$\hat{C}|\psi\rangle \neq |\psi\rangle \otimes |\psi\rangle$$

$$\begin{aligned}
\hat{C}\left(c_0|0\rangle + c_1|1\rangle\right) &= c_0\hat{C}|0\rangle + c_1\hat{C}|1\rangle \\
&= c_0|00\rangle + c_1|11\rangle \\
&\neq \left(c_0|0\rangle + c_1|1\rangle\right) \otimes \left(c_0|0\rangle + c_1|1\rangle\right) \\
&= c_0^2|00\rangle + c_0c_1|01\rangle + c_0c_1|10\rangle + c_1^2|11\rangle
\end{aligned}$$

Quantum computing operations

Single qubit gates

Phase flip $\hat{Z}$



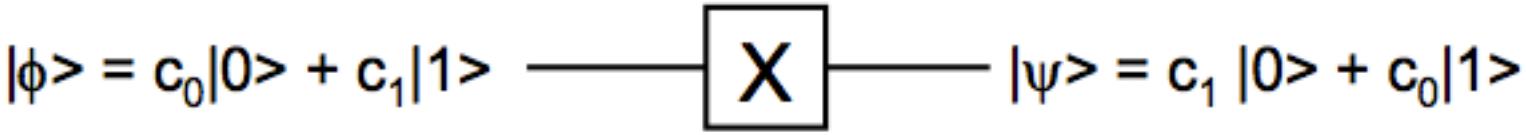
$$\begin{aligned} \hat{Z}|0\rangle &= |0\rangle \\ \hat{Z}|1\rangle &= -|1\rangle \\ \hat{Z}\left(c_0|0\rangle + c_1|1\rangle\right) &= c_0\,\hat{Z}\,|0\rangle + c_1\,\hat{Z}\,|1\rangle = c_0|0\rangle - c_1|1\rangle \end{aligned}$$

This operation or gate has no analog in classical world.

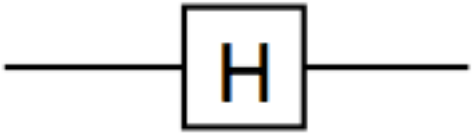
Homework:
Show that the states $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$ and $|\hat{Z}\psi\rangle = \hat{Z}|\psi\rangle$ are orthogonal.

Bit flip $\hat{X}$

$$\begin{aligned} \hat{X}|0\rangle &= |1\rangle \\ \hat{X}|1\rangle &= |0\rangle \\ \hat{X}\left(c_0|0\rangle + c_1|1\rangle\right) &= c_0\,\hat{X}\,|0\rangle + c_1\,\hat{X}\,|1\rangle = c_1|0\rangle + c_0|1\rangle \end{aligned}$$



Hadamard gate $\hat{H}$



$$
\begin{aligned}
\hat{H}|0\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \\
\hat{H}|1\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \\
\hat{H}\left(c_0|0\rangle + c_1|1\rangle\right) &= c_0\,\hat{H}\,|0\rangle + c_1\,\hat{H}\,|1\rangle \\
&= \frac{c_0}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) + \frac{c_1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \\
&= \frac{c_0 + c_1}{\sqrt{2}}|0\rangle + \frac{c_0 - c_1}{\sqrt{2}}|1\rangle
\end{aligned}
$$

Homework:

Show what operations correspond to the following products $\hat{H}\hat{H}$, $\hat{H}\hat{Z}\hat{H}$, $\hat{H}\hat{X}\hat{H}$.

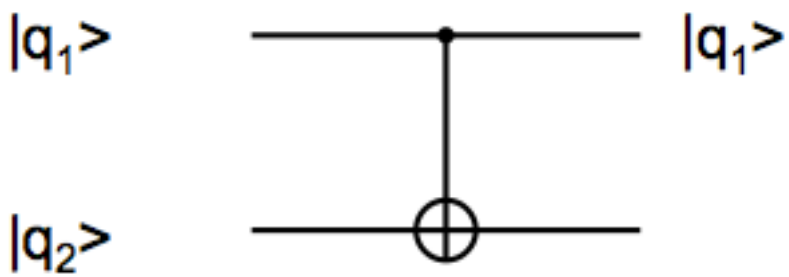
Two-qubit gates

Two-qubit states have the standard computational basis $\mathcal{B} = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

Controlled-NOT

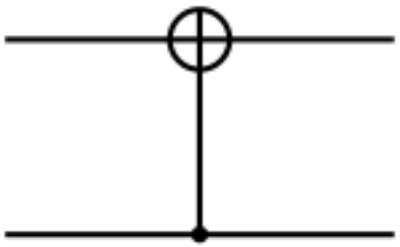
$CNOT_{12}$ (the first qubit is the control qubit, the second is the target qubit):

$$
\begin{aligned}
CNOT_{12}|00\rangle &= |00\rangle \\
CNOT_{12}|01\rangle &= |01\rangle \\
CNOT_{12}|10\rangle &= |11\rangle \\
CNOT_{12}|11\rangle &= |10\rangle \\
CNOT_{12}\left(c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle\right) &= c_{00}|00\rangle + c_{01}|01\rangle + c_{11}|10\rangle + c_{10}|11\rangle
\end{aligned}
$$



$CNOT_{21}$:

$$
\begin{aligned}
CNOT_{21}|00\rangle &= |00\rangle \\
CNOT_{21}|01\rangle &= |11\rangle \\
CNOT_{21}|10\rangle &= |10\rangle \\
CNOT_{21}|11\rangle &= |01\rangle \\
CNOT_{21}\left(c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle\right) &= c_{00}|00\rangle + c_{11}|01\rangle + c_{10}|10\rangle + c_{01}|11\rangle
\end{aligned}
$$



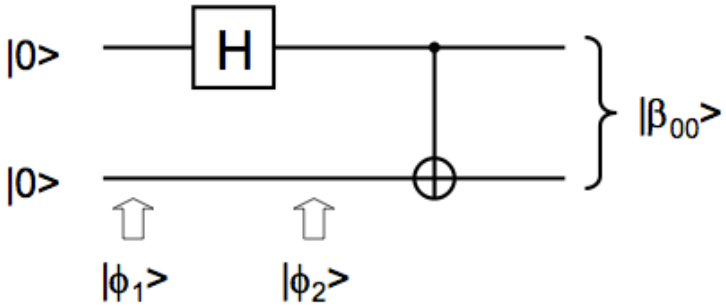
Application: **the Bell state generator**

$$|\phi_1\rangle = |0\rangle \otimes |0\rangle = |00\rangle$$

$$|\phi_2\rangle = \left(\hat{H} \otimes \hat{1}\right)|\phi_1\rangle = \hat{H}|0\rangle \otimes \hat{1}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$$

$$|\beta_{00}\rangle = CNOT|\phi_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

(Here $CNOT$ stays for $CNOT_{12}$.)



Homework: Design circuits to generate the other Bell states

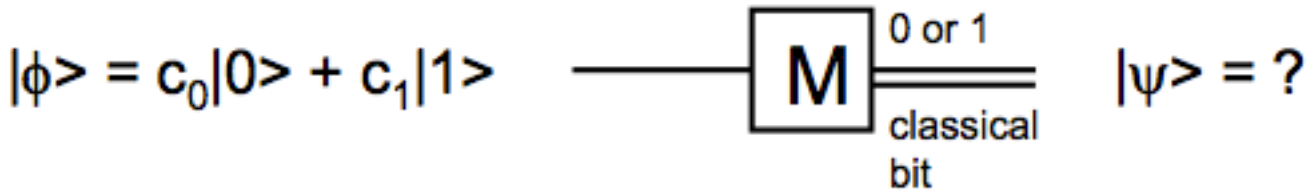
$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \qquad |\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \qquad |\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Single qubit measurement

Measurement of one qubit $|\phi\rangle = c_0|0\rangle + c_1|1\rangle$ in the standard computational basis gives classical bit of information:

- with the probability $\left|c_0\right|^2$ the measurement gives the result $M = 0$ and the quantum state immediately after the measurement has collapsed to $|\psi\rangle = |0\rangle$;

- with the probability $|c_1|^2$ the measurement gives the result $M = 1$ and the quantum state immediately after the measurement has collapsed to $|\psi\rangle = |1\rangle$.



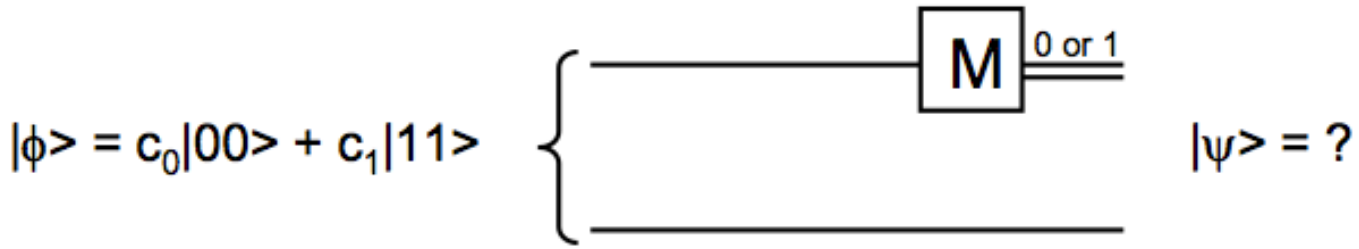
Measurement of an entangled state - Einstein-Podolsky-Rosen paradox

Measurement of the first qubit of a two-qubit entangled state $|\phi\rangle = c_{00}|00\rangle + c_{11}|11\rangle$ yields the following outcome:

- with the probability $|c_{00}|^2$ the measurement gives the result $M_1 = 0$ and the quantum state immediately after the measurement has collapsed to $|\psi\rangle = |00\rangle$;

- with the probability $|c_{11}|^2$ the measurement gives the result $M_1 = 1$ and the quantum state immediately after the measurement has collapsed to $|\psi\rangle = |11\rangle$.

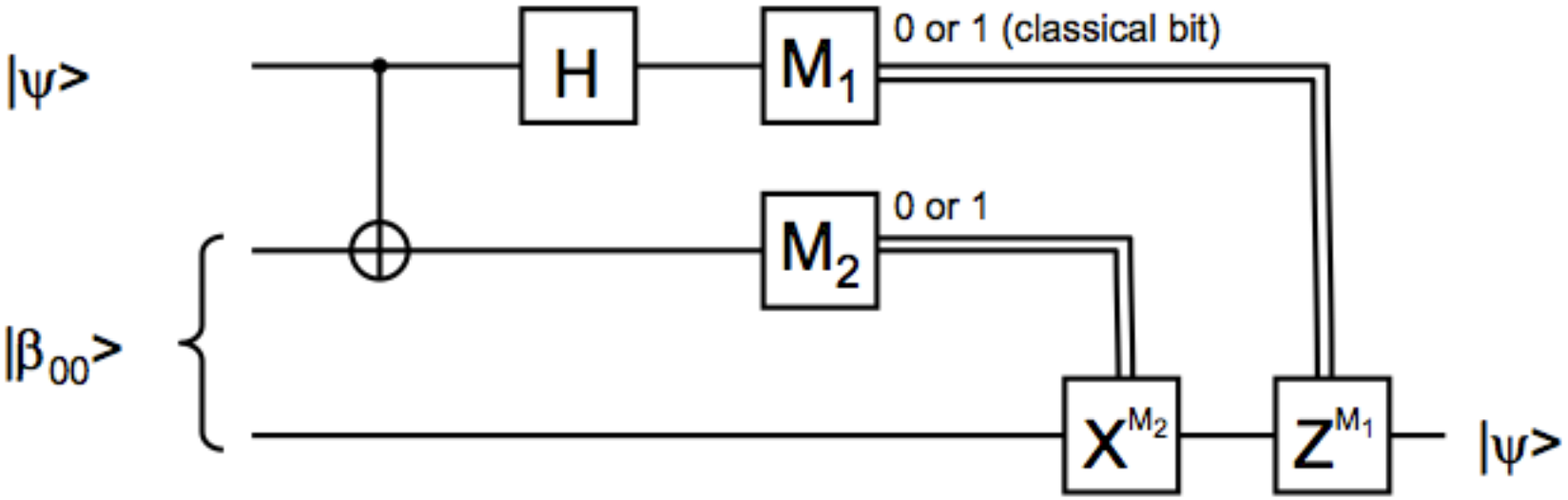
The measurement of one qubit of an entangled two-qubit state completely determines the state of the other qubit after the measurement even if both qubits are spatially separated and can not communicate or interact.



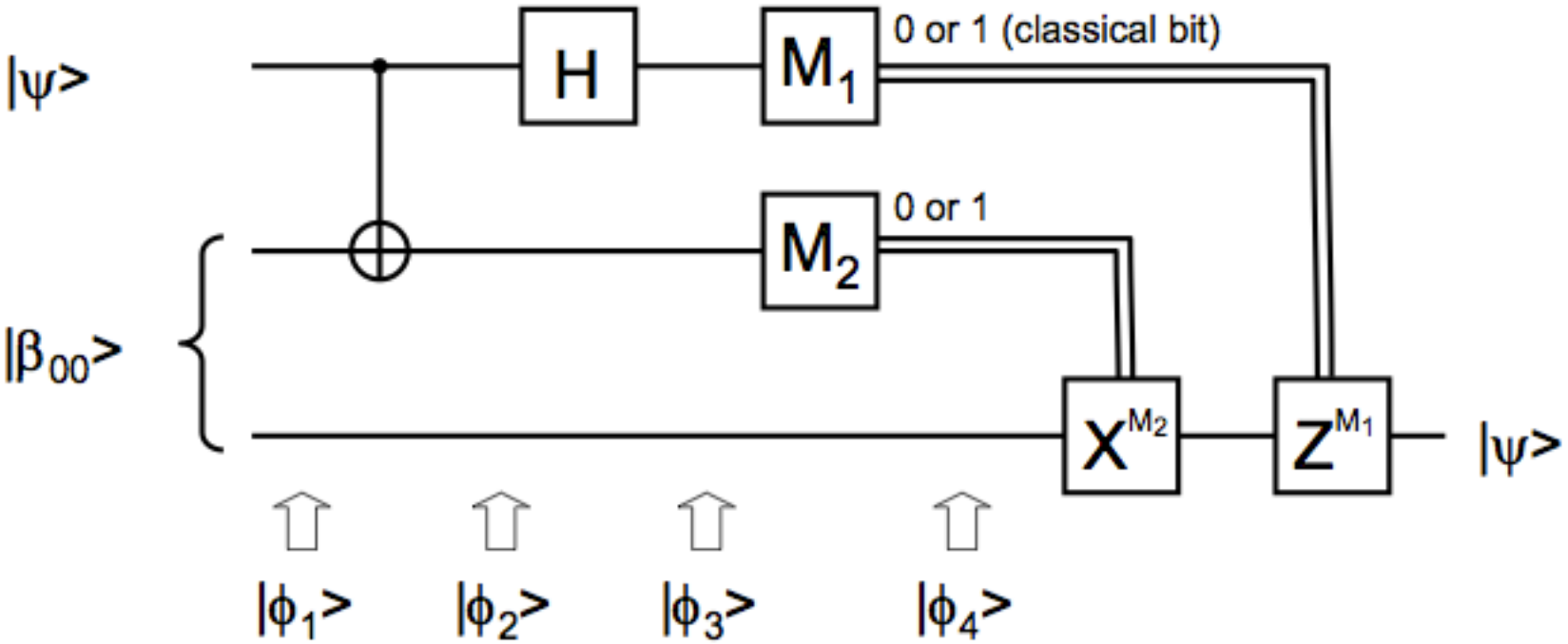

No classical analog !!!
Teleportation

Teleportation

Teleport an unknown qubit state $|\psi\rangle$ using the Bell state $|\beta_{00}\rangle$ and single-qubit and two-qubit operations, two measurements and communication of two classical bits.

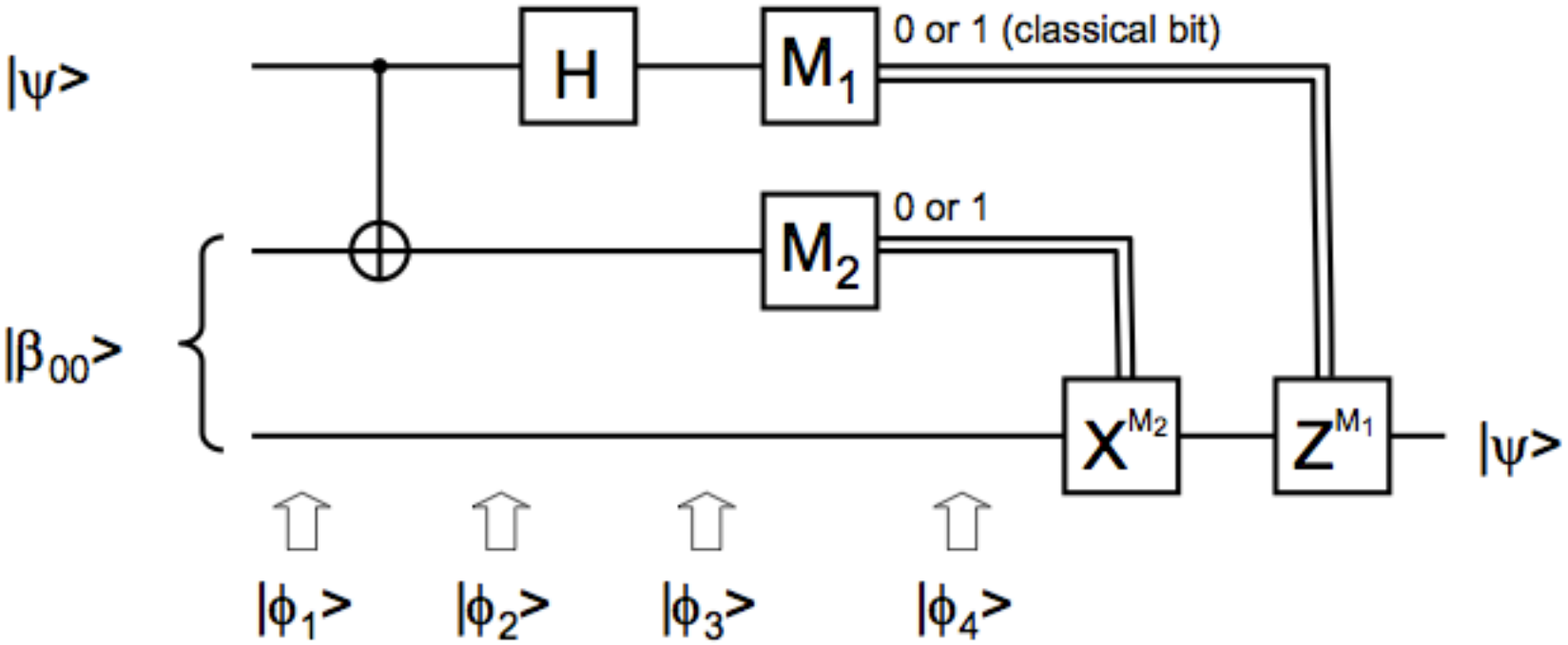


$$
\begin{aligned}
|\psi\rangle &= c_0|0\rangle + c_1|1\rangle \qquad |\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
|\phi_1\rangle &= |\psi\rangle \otimes |\beta_{00}\rangle = |\psi\rangle|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(c_0|000\rangle + c_0|011\rangle + c_1|100\rangle + c_1|111\rangle) \\
|\phi_2\rangle &= \frac{1}{\sqrt{2}}(c_0|000\rangle + c_0|011\rangle + c_1|110\rangle + c_1|101\rangle)
\end{aligned}
$$



$$|\phi_2\rangle = \frac{1}{\sqrt{2}}(c_0|000\rangle + c_0|011\rangle + c_1|110\rangle + c_1|101\rangle)$$

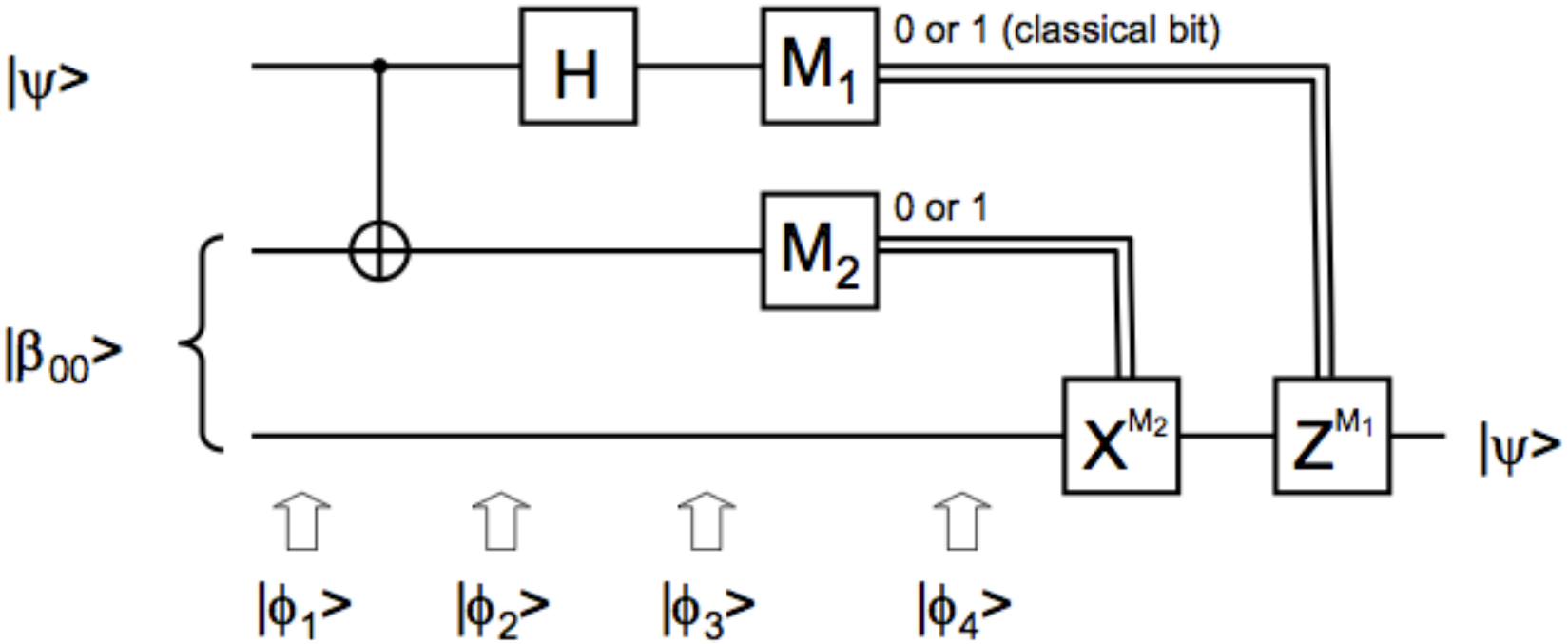
$$|\phi_3\rangle = \frac{1}{\sqrt{2}}(c_0|000\rangle + c_0|100\rangle + c_0|011\rangle + c_0|111\rangle + c_1|010\rangle - c_1|110\rangle + c_1|001\rangle - c_1|101\rangle)$$



$$|\phi_3\rangle \;=\; \frac{1}{\sqrt{2}}\left(c_0|000\rangle + c_0|100\rangle + c_0|011\rangle + c_0|111\rangle + c_1|010\rangle - c_1|110\rangle + c_1|001\rangle - c_1|101\rangle\right)$$

Four possible results of the measurements on the first and second qubit are

$$(i)\quad M_1 = 0,\quad M_2 = 0 \qquad (ii)\quad M_1 = 0,\quad M_2 = 1$$
$$(iii)\quad M_1 = 1,\quad M_2 = 0 \qquad (iv)\quad M_1 = 1,\quad M_2 = 1$$

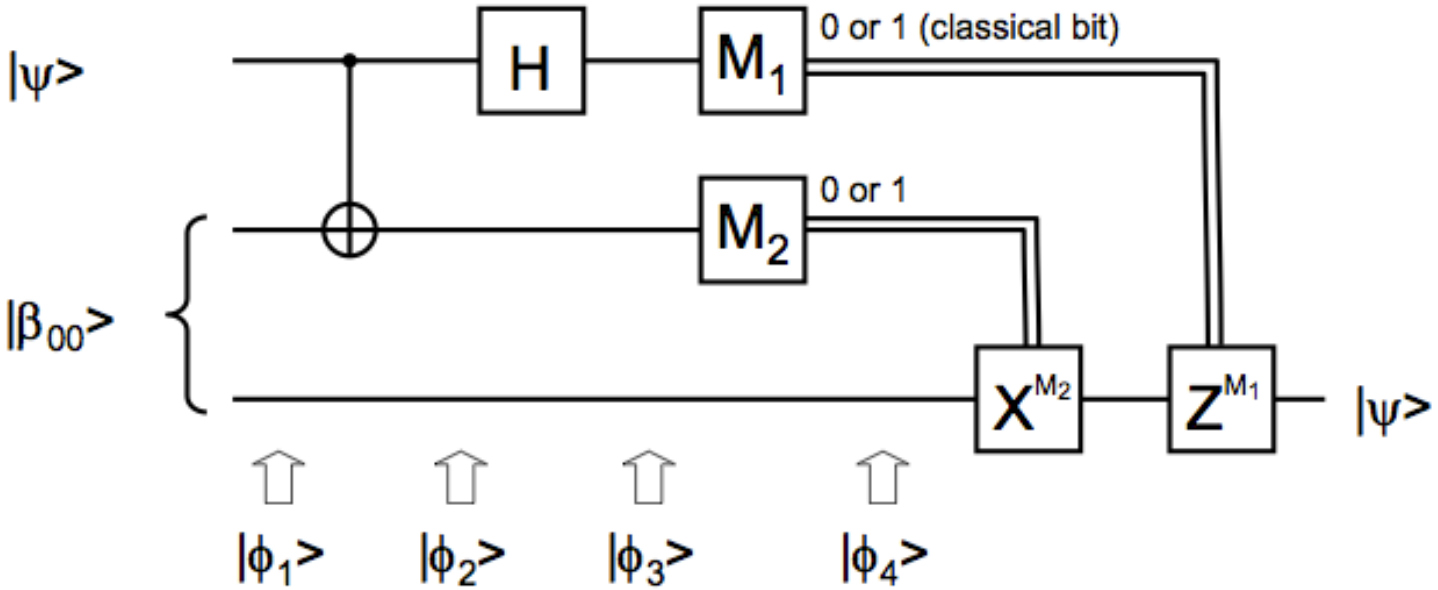


$$|\phi_3\rangle = \frac{1}{\sqrt{2}}(c_0|000\rangle + c_0|100\rangle + c_0|011\rangle + c_0|111\rangle + c_1|010\rangle - c_1|110\rangle + c_1|001\rangle - c_1|101\rangle)$$

Measurement results: $M_1 = 0, \quad M_2 = 0$

$$|\phi_4\rangle = c_0|000\rangle + c_1|001\rangle = |00\rangle \otimes (c_0|0\rangle + c_1|1\rangle) = |00\rangle \otimes |\psi'\rangle$$
$$|\psi\rangle = \hat{Z}^0 \hat{X}^0 |\psi'\rangle = |\psi'\rangle = c_0|0\rangle + c_1|1\rangle$$

The final state of the third qubit is now the same as the initial state of the first qubit.

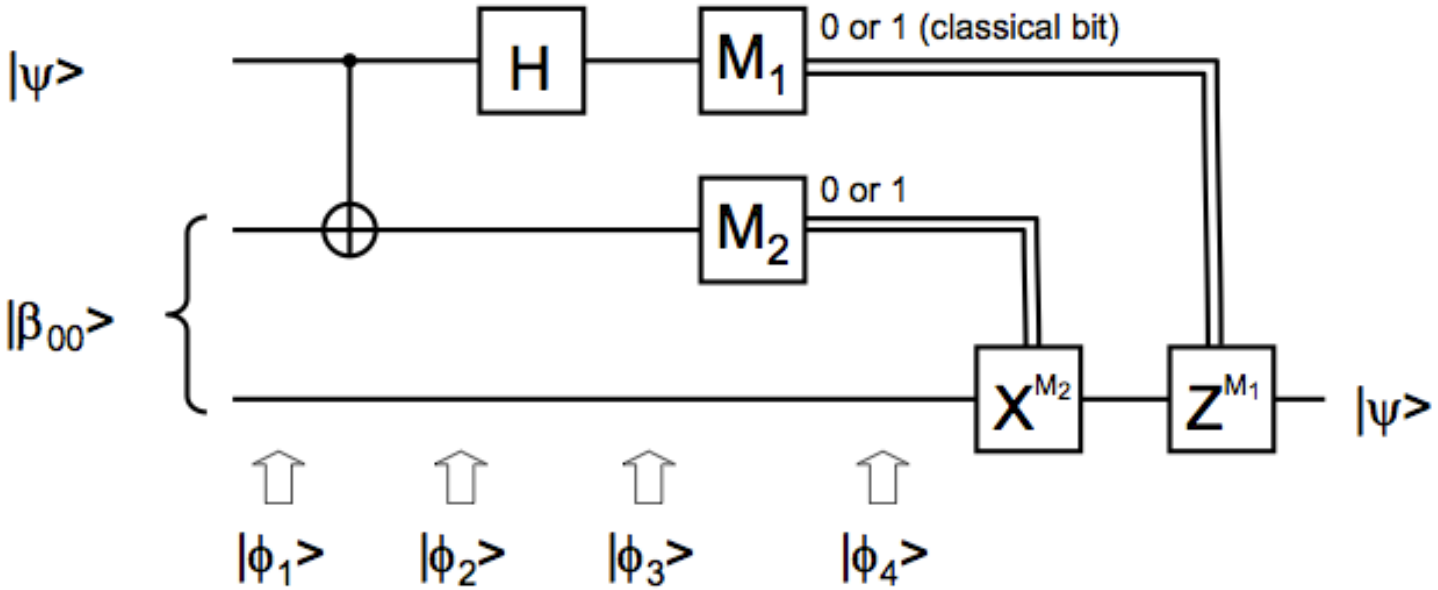


$$|\phi_3\rangle = \frac{1}{\sqrt{2}}(c_0|000\rangle + c_0|100\rangle + c_0|011\rangle + c_0|111\rangle + c_1|010\rangle - c_1|110\rangle + c_1|001\rangle - c_1|101\rangle)$$

Measurement results: $M_1 = 1, \quad M_2 = 0$

$$|\phi_4\rangle = c_0|100\rangle - c_1|101\rangle = |10\rangle \otimes (c_0|0\rangle - c_1|1\rangle) = |10\rangle \otimes |\psi'\rangle$$
$$|\psi\rangle = \hat{Z}^1 \hat{X}^0 |\psi'\rangle = \hat{Z}(c_0|0\rangle - c_1|1\rangle) = c_0|0\rangle + c_1|1\rangle$$

The final state of the third qubit is now the same as the initial state of the first qubit.

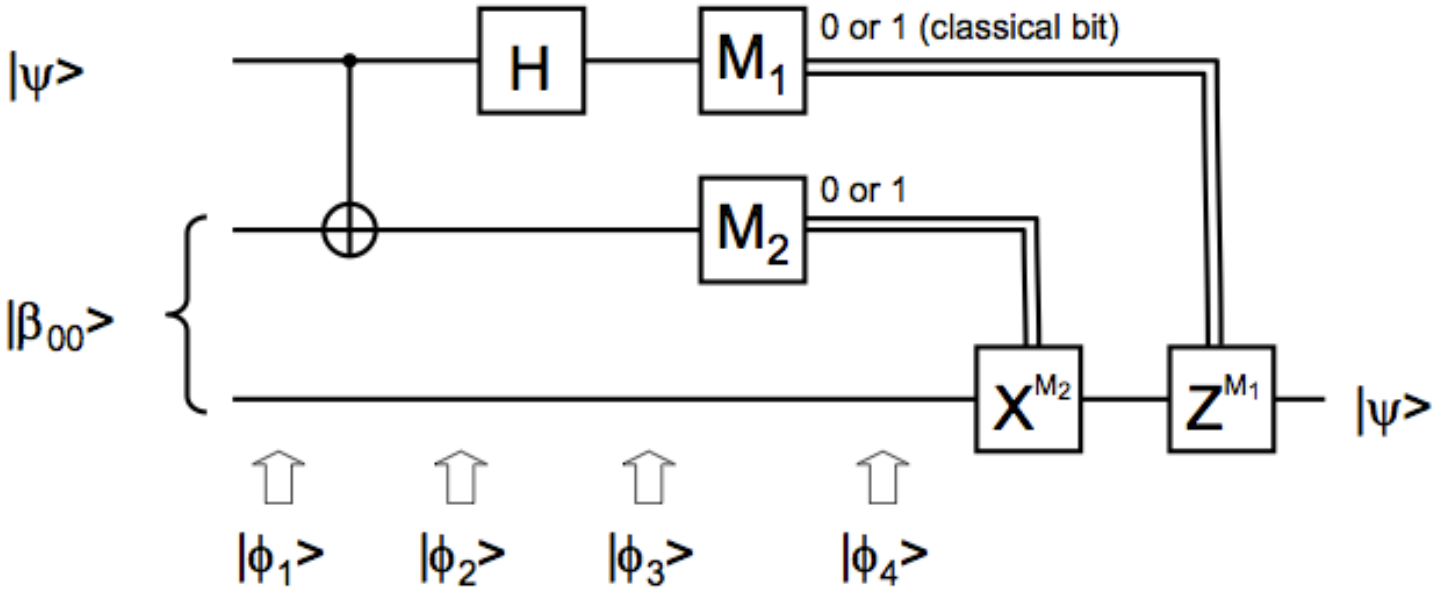


$$|\phi_3\rangle = \frac{1}{\sqrt{2}}(c_0|000\rangle + c_0|100\rangle + c_0|011\rangle + c_0|111\rangle + c_1|010\rangle - c_1|110\rangle + c_1|001\rangle - c_1|101\rangle)$$

Measurement results: $M_1 = 0, \quad M_2 = 1$

$$|\phi_4\rangle = c_0|011\rangle + c_1|010\rangle = |01\rangle \otimes (c_1|0\rangle + c_0|1\rangle) = |01\rangle \otimes |\psi'\rangle$$
$$|\psi\rangle = \hat{Z}^0 \hat{X}^1 |\psi'\rangle = \hat{X}(c_1|0\rangle + c_0|1\rangle) = c_0|0\rangle + c_1|1\rangle$$

The final state of the third qubit is now the same as the initial state of the first qubit.

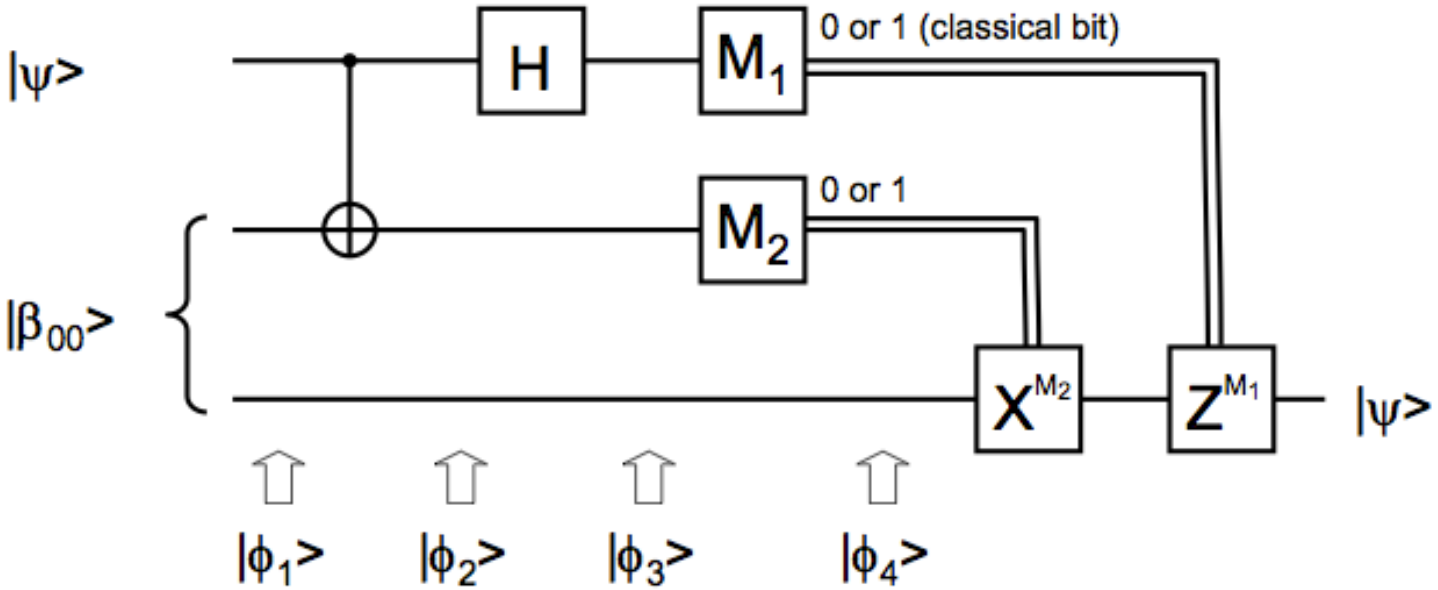


$$|\phi_3\rangle = \frac{1}{\sqrt{2}}(c_0|000\rangle + c_0|100\rangle + c_0|011\rangle + c_0|111\rangle + c_1|010\rangle - c_1|110\rangle + c_1|001\rangle - c_1|101\rangle)$$

Measurement results: $M_1 = 1, \quad M_2 = 1$

$$|\phi_4\rangle = c_0|111\rangle - c_1|110\rangle = |11\rangle \otimes (-c_1|0\rangle + c_0|1\rangle) = |11\rangle \otimes |\psi'\rangle$$
$$|\psi\rangle = \hat{Z}^1 \hat{X}^1 |\psi'\rangle = \hat{Z}\hat{X}(-c_1|0\rangle + c_0|1\rangle) = \hat{Z}(c_0|0\rangle - c_1|1\rangle) = c_0|0\rangle + c_1|1\rangle$$

The final state of the third qubit is now the same as the initial state of the first qubit.



QUANTUM MECHANICS FOUNDATIONS OF QUANTUM INFORMATION PROCESSING

STATES

FIRST POSTULATE

At a fixed time t, the state of a physical system is defined by specifying a ket $|\psi(t)\rangle$ belonging to the state space $\mathcal{H}$.

The state space is a space of all possible states of a given physical system, and it is a Hilbert space, i.e.

(1) a vector space over the field of complex numbers $\mathbb{C}$
(2) with inner product, and
(3) with a norm and a metric induced by the inner product, and
(4) it is also a complete space (relevant to infinite dimensions).

Definition of a vector space.

A vector space over the field of complex numbers $\mathbb{C}$ is a set of elements, called vectors, with an operation of *addition*, which for each pair of vectors $|\psi\rangle$ and $|\phi\rangle$ specifies a vector $|\psi\rangle + |\phi\rangle$, and an operation of *scalar multiplication*, which for each vector $|\psi\rangle$ and a number $c \in \mathbb{C}$ specifies a vector $c|\psi\rangle$ such that (s.t.)

1) $|\psi\rangle + |\phi\rangle = |\phi\rangle + |\psi\rangle$

2) $|\psi\rangle + (|\phi\rangle + |\chi\rangle) = (|\psi\rangle + |\phi\rangle) + |\chi\rangle$

3) there is a unique zero vector s.t. $|\psi\rangle + 0 = |\psi\rangle$

4) $c(|\psi\rangle + |\phi\rangle) = c|\psi\rangle + c|\phi\rangle$

5) $(c + d)|\psi\rangle = c|\psi\rangle + d|\psi\rangle$

6) $c(d|\psi\rangle) = (cd)|\psi\rangle$

7) $1.|\psi\rangle = |\psi\rangle$

8) $0.|\psi\rangle = 0$

Example:

A set of N-tuples of complex numbers.

An inner product.

Dirac bra-ket notation:

$$\begin{aligned} |\psi\rangle, |\phi\rangle &\in \mathcal{H} \\ \langle\phi|\psi\rangle &\in \mathbb{C} \end{aligned}$$

A bra $\langle\phi|$ is the adjoint of a ket $|\phi\rangle$, e.g.

$$\begin{aligned} \text{if} \quad & |\psi\rangle = c_1|\phi_1\rangle + c_2|\phi_2\rangle, \\ \text{then} \quad & \langle\psi| = c_1^*\langle\phi_1| + c_2^*\langle\phi_2| \end{aligned}$$

We call $|\phi_1\rangle$ and $|\phi_2\rangle$ a **basis** (or basis elements) of $\mathcal{H}$ if and only if

$$\begin{aligned} \text{span}\{|\phi_1\rangle, |\phi_2\rangle\} &= \mathcal{H} \\ \text{and } \langle\phi_i|\phi_j\rangle &= \delta_{ij} \end{aligned}$$

where δ_{ij} is the Kronecker delta-symbol. And with a norm and metric induced by the inner product.

Norm:

$$\begin{aligned} \text{e.g. } \langle \phi_i | \phi_j \rangle &= \delta_{ij} \text{ i.e.} \\ \langle \phi_1 | \phi_1 \rangle^{1/2} &= \| \phi_1 \| = 1 \\ &\equiv \text{the norm of } |\phi_1\rangle \end{aligned}$$

If the norm is 1, the state is said to be normalized, i.e. its length equals 1.

Two vectors are orthogonal if their inner product is zero. A set of mutually orthogonal vectors of unit norm is said to be orthonormal.

Metric: a metric is a map which assigns to each pair of vectors $|\psi\rangle$, $|\phi\rangle$ a scalar $\rho \geq 0$ such that

1. $\rho(|\psi\rangle, |\phi\rangle) = 0$ iff $|\psi\rangle = |\phi\rangle$;

2. $\rho(|\psi\rangle, |\phi\rangle) = \rho(|\phi\rangle, |\psi\rangle)$

3. $\rho(|\psi\rangle, |\chi\rangle) \leq \rho(|\psi\rangle, |\phi\rangle) + \rho(|\phi\rangle, |\chi\rangle)$ (triangle identity)

We say that the metric is induced by the norm if

$$\rho(|\psi\rangle, |\phi\rangle) \quad = \quad ||| \psi\rangle - |\phi\rangle||$$

So the Hilbert space is normed and a metric space. What else?

It is also a complete space so every Cauchy sequence of vectors, i.e.

$$\| |\psi_n\rangle - |\psi_m\rangle \| \to 0 \quad \text{as} \quad m, n \to \infty$$

converges to a limit vector in the space.
(We need this condition to be able to handle systems with infinite-dimensional Hilbert spaces, i.e. with infinite degrees of freedom.)

Can we be more concrete about quantum states? What really is a ket $|\psi\rangle$?

Now, we need the concept of representation.
Let us say we have the Hilbert space $\mathcal{H}$ and the basis

$$\mathcal{B} \quad = \quad \{|\phi_1\rangle, |\phi_2\rangle\}$$

and we have a ket

$$|\psi\rangle \quad \in \quad \mathcal{H}$$

which we wish to express in the representation given by the basis $\mathcal{B}$.
We use the completeness relation

$$\sum_i |\phi_i\rangle\langle\phi_i| \quad = \quad \hat{1}$$

as follows

$$\begin{aligned} |\psi\rangle \quad &= \quad \sum_i |\phi_i\rangle \quad \underbrace{\langle\phi_i|\psi\rangle}_{\text{a number}\in\mathbb{C}} \\ &= \quad \sum_i c_i|\phi_i\rangle \end{aligned}$$

Our state becomes a specific superposition of the basis set elements, i.e. we have expanded $|\psi\rangle$ in terms of $\{|\phi_i\rangle\}$.

Quantum bit

Quantum bit or **qubit** is a two dimensional Hilbert space $\mathcal{H}^2 \simeq \mathbb{C}^2$. Its values are vectors, states, or kets, from this Hilbert space:

$$|\phi\rangle = c_0|0\rangle + c_1|1\rangle = \begin{pmatrix} c_0 \\ c_1 \end{pmatrix}$$

The vectors $|0\rangle$ and $|1\rangle$ are the basis vectors from the **standard computational basis**:

$$\mathcal{B} = \{|0\rangle, |1\rangle\} = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$$

so that $\mathcal{H}^2 = \text{span}\,(\mathcal{B})$. The conjugate bra $\langle\phi| = c_0^*\langle 0| + c_1^*\langle 1| = \begin{pmatrix} c_0^* & c_1^* \end{pmatrix}$
The coefficients c_0 and c_1 are complex numbers, $c_0, c_1 \in \mathbb{C}$, satisfying $|c_0|^2 + |c_1|^2 = 1$.

Recall that multiplying a quantum states by global phase, a complex number of unit modulus $e^{i\theta}$, has no observable consequences:

$$|\phi\rangle = c_0|0\rangle + c_1|1\rangle \qquad \rightarrow \qquad |\phi'\rangle = e^{i\theta}|\phi\rangle = c_0 e^{i\theta}|0\rangle + c_1 e^{i\theta}|1\rangle = c'_0|0\rangle + c'_1|1\rangle$$

The probability of obtaining the measurement result 0 or 1 when measuring the qubit in the standard basis remains the same:

$$\begin{aligned} \left|c'_0\right|^2 &= c'^*_0\, c'_0 = c^*_0 e^{-i\theta}\, c_0 e^{i\theta} = c^*_0 c_0 = \left|c_0\right|^2 \\ \left|c'_1\right|^2 &= c'^*_1\, c'_1 = c^*_1 e^{-i\theta}\, c_1 e^{i\theta} = c^*_1 c_1 = |c_1|^2 \end{aligned}$$

The expectation value or average value of an observable $\hat{O}$, obtained from its repeated measurement on the qubits in an equally prepared state, is also invariant with the global phase:

$$< \hat{O} >_{\phi'} = \langle \phi'|\hat{O}|\phi'\rangle = e^{-i\theta} e^{i\theta} \langle \phi|\hat{O}|\phi\rangle = < \hat{O} >_{\phi}$$

This suggests that we need three real numbers to specify a state of one qubit.

Density operator/matrix

We can represent a qubit state $|\phi\rangle$, and any quantum state, by the projector onto the one-dimensional subspace it spans:

$$\begin{aligned}\hat{\rho} &= |\phi\rangle\langle\phi| = (c_0|0\rangle + c_1|1\rangle)\left(c_0^*\langle 0| + c_1^*\langle 1|\right) \\ &= \left|c_0\right|^2 |0\rangle\langle 0| + c_0 c_1^* |0\rangle\langle 1| + c_0^* c_1 |1\rangle\langle 0| + |c_1|^2 |1\rangle\langle 1|\end{aligned}$$

In matrix representation given by the standard computational basis, we have

$$\hat{\rho} = \begin{pmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{pmatrix} = \begin{pmatrix} c_0 \\ c_1 \end{pmatrix} \begin{pmatrix} c_0^* & c_1^* \end{pmatrix} = \begin{pmatrix} \left|c_0\right|^2 & c_0 c_1^* \\ c_0^* c_1 & |c_1|^2 \end{pmatrix}$$

We observe that the **norm** of a state is $\mathrm{Tr}(\hat{\rho}) = |c_0|^2 + |c_1|^2 = 1$ and also that $\rho_{10} = \rho_{01}^*$.

Bloch representation

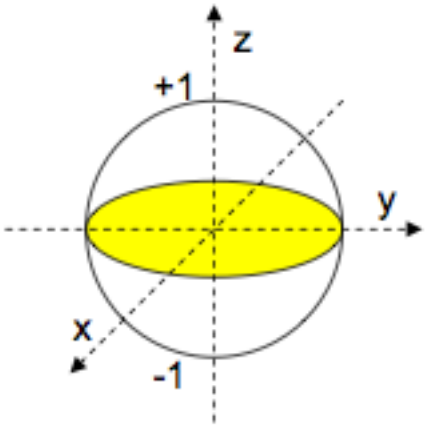
The single-qubit density matrix can be decomposed as follows

$$\begin{aligned}\hat{\rho} &= \frac{1}{2}\left(\hat{I} + \vec{r}\,.\,\vec{\sigma}\right) = \frac{1}{2}\left(\hat{I} + r_x\,\sigma_x + r_y\,\sigma_y + r_z\,\sigma_z\right) \\ &= \frac{1}{2}\left[\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + r_x \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + r_y \begin{pmatrix} 0 & -i \\ i & 1 \end{pmatrix} + r_z \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right]\end{aligned}$$

where σ_x, σ_y, and σ_z are the Pauli matrices.

The vector $\vec{r} = \left(r_x, r_y, r_z\right)$ is called the **Bloch vector** and its components, real numbers between 0 between 1, are related to the density matrix elements as follows:

$$\begin{aligned} r_x &= 2\ \mathrm{Re}\left(\rho_{10}\right) \\ r_y &= 2\ \mathrm{Im}\left(\rho_{10}\right) \\ r_z &= \rho_{00} - \rho_{11} \end{aligned}$$



Examples

To construct their Bloch representation of pure states of one qubit (mixed states will come later) we use

$$r_x = 2\,\mathrm{Re}\,(\rho_{10}) = 2\,\mathrm{Re}\left(c_0^* c_1\right)$$

$$r_y = 2\,\mathrm{Im}\,(\rho_{10}) = 2\,\mathrm{Im}\left(c_0^* c_1\right)$$

$$r_z = \rho_{00} - \rho_{11} = \left|c_0\right|^2 - |c_1|^2$$

1. $|\phi\rangle = |0\rangle$

$$\hat{\rho} = |0\rangle\langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 1^* & 0^* \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \Rightarrow \quad \vec{r} = (0, 0, 1)$$

2. $|\phi\rangle = |1\rangle$

$$\hat{\rho} = |1\rangle\langle 1| = \begin{pmatrix} 0 \\ 1 \end{pmatrix}\begin{pmatrix} 0^* & 1^* \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \quad \Rightarrow \quad \vec{r} = (0, 0, -1)$$

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

$$\hat{\rho} = |\phi\rangle\langle\phi| = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \\ \frac{1}{\sqrt{2}} \end{pmatrix}\begin{pmatrix} \frac{1}{\sqrt{2}}^* & \frac{1}{\sqrt{2}}^* \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ \\ 1 & 1 \end{pmatrix} \quad \Rightarrow \quad \vec{r} = (1, 0, 0)$$

4. $|\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$$\hat{\rho} = |\phi\rangle\langle\phi| = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \\ -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}}^* & -\frac{1}{\sqrt{2}}^* \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & -1 \\ \\ -1 & 1 \end{pmatrix} \quad \Rightarrow \quad \vec{r} = (-1, 0, 0)$$

5. $|\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$

$$\hat{\rho} = |\phi\rangle\langle\phi| = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \\ i\,\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}}^* & \left(i\,\frac{1}{\sqrt{2}}\right)^* \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & -i \\ \\ i & 1 \end{pmatrix} \quad \Rightarrow \quad \vec{r} = (0, 1, 0)$$

Bloch sphere

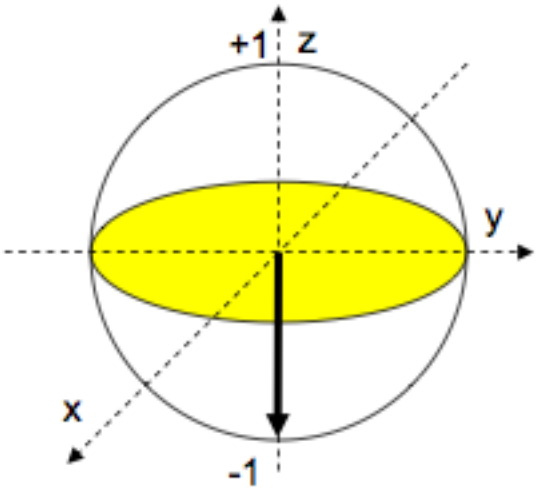
The set of all Bloch vectors for single qubit pure states form a surface of a sphere of unit radius.

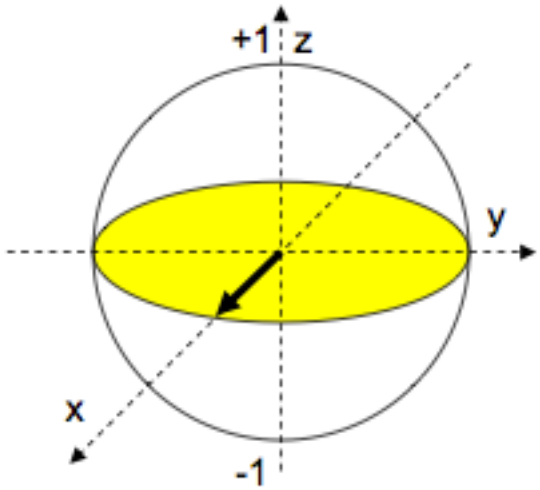
Examples

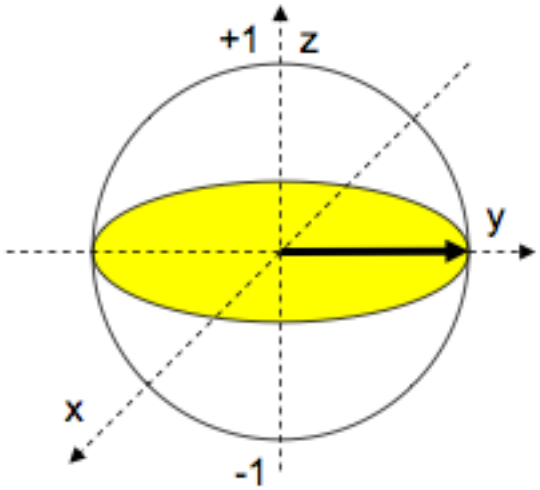
$$|\phi\rangle = |1\rangle \qquad \vec{r} = (0, 0, -1)$$

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad \vec{r} = (1, 0, 0)$$

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \qquad \vec{r} = (0, 1, 0)$$







Composition of Hilbert spaces

A tensor product of vector space $\mathcal{V}$ and $\mathcal{U}$ is a vector space $\mathcal{W}$ whose dimension is $(\dim\mathcal{V}).(\dim\mathcal{U})$.

Let $\mathcal{B}_\mathcal{U} = \{|u_1\rangle, |u_2\rangle, \ldots, |u_n\rangle\}$ be a basis of $\mathcal{U}$ and $\mathcal{B}_\mathcal{V} = \{|v_1\rangle, |v_2\rangle, \ldots, |v_n\rangle\}$ be a basis of $\mathcal{V}$, then a basis of $\mathcal{W} = \mathcal{U} \otimes \mathcal{V}$ is $\mathcal{B}_\mathcal{W} = \{|u_1v_1\rangle, |u_1v_2\rangle, \ldots, |u_nv_n\rangle\}$ where $|u_kv_l\rangle = |u_k\rangle \otimes |v_l\rangle$.

Example

Let $\mathcal{B}_\mathcal{U} = \{|0\rangle, |1\rangle\}$, $\mathcal{B}_\mathcal{V} = \{|0\rangle, |1\rangle\}$, then $\mathcal{B}_\mathcal{W} = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

Qubits

A quantum state of n qubits is a vector in 2^n-dimensional Hilbert space:

$$\bigotimes_{k=1}^{n} \mathcal{H}^2 = \mathcal{H}^2 \otimes \mathcal{H}^2 \otimes ...\mathcal{H}^2 \quad \text{(n-times)} = \mathcal{H}^{2^n}$$

The **standard computational basis** of n-qubit Hilbert space:

$$\mathcal{B}_{\mathcal{H}^{2^n}} = \{|0\ldots000\rangle, |00\ldots001\rangle, |00\ldots010\rangle, |00\ldots011\rangle, \ldots |1\ldots111\rangle\}$$

Example: The standard basis of a two-qubit Hilbert space

$$\mathcal{B}_{\mathcal{H}^4} = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$$

Examples of two-qubit states:

(i) Composite product states

$$
\begin{aligned}
|\phi\rangle &= |0\rangle \otimes |0\rangle = |0\rangle|0\rangle = |00\rangle \\
|\psi\rangle &= (c_0|0\rangle + c_1|1\rangle) \otimes |0\rangle = c_{00}|00\rangle + c_{10}|10\rangle
\end{aligned}
$$

(ii) Entangled states: the Bell states

$$
\begin{aligned}
|\beta_{00}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
|\beta_{01}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\
|\beta_{10}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\
|\beta_{11}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)
\end{aligned}
$$

Superdense coding

Task:
Alice wants to send two classical bits of information, that is one of the bit strings $\{00, 01, 10, 11\}$, to Bob.

Resources:
i) Alice and Bob share two qubits in the Bell state $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
ii) Alice can send her one quantum bit to Bob.

$|\beta_{00}> = 2^{-1/2}(|00> + |11>)$

Alice

Bob

Superdense coding protocol

1. Alice and Bob share two qubits in the Bell state $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
2. Depending on what bit string, $00, 01, 10, 11$, Alice wants to send to Bob, she applies one of the following transformations to her qubit:

$$
\begin{array}{lll}
00: & \hat{I}: & |\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \rightarrow |\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
01: & \hat{Z}: & |\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \rightarrow |\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\
10: & \hat{X}: & |\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \rightarrow |\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\
11: & \hat{Z}\hat{X} = i\hat{Y}: & |\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \rightarrow |\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)
\end{array}
$$

3. The resulting Bell states are orthogonal and hence Bob can distinguish them by a measurement in the Bell basis.

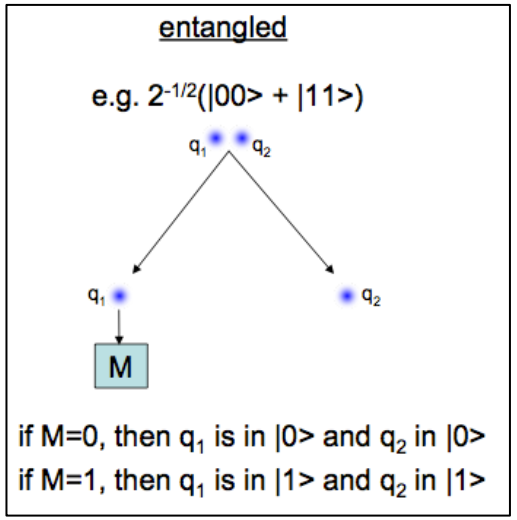
One qubit is sufficient to transmit two bits of classical information.

Einstein-Podolsky-Rosen paradox

The measurement of one qubit of an entangled two-qubit state completely determines the state of the other qubit after the measurement even if both qubits are spatially separated. This implies that the first qubit communicates with the other instantaneously, that is, faster than light, across the space ⇒ **spooky action at a distance** - A. Einstein.

Resolving the paradox:
Hidden variables theory: Quantum mechanics can not be complete. There must be some unknown mechanism acting on quantum mechanical variables to give rise to observable effects of noncommutative quantum observables like Heisenberg uncertainty principle.

Bell inequalities: No hidden variable theory.

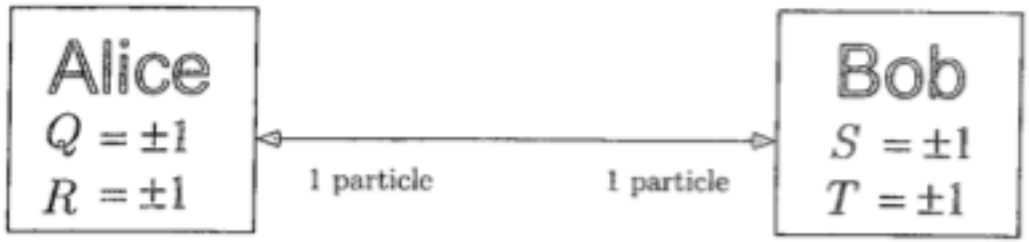


Bell inequalities John S. Bell 1962

Alice and Bob share a two-particle system.

Each can perform one of two different measurements and they can decide which measurement to perform by flipping a coin once they receive a particle. The measurement outcome can be $+1$ or -1.

Alice can measure physical properties of her particle P_Q or P_R, and Bob can measure properties P_S or P_T of his particle; both measurements take place at the same time.



We calculate the quantity

$$QS + RS + RT - QT = (Q + R)S + (R - Q)T$$

Because $R, Q = \pm 1$ it follows that either

$$(Q + R)S = 0 \quad \text{or} \quad (R - Q)T = 0$$

In either case

$$QS + RS + RT - QT = \pm 2$$

Suppose that $p(q, r, s, t)$ is the probability that before the measurements, the system is in the state where $Q = q$, $R = r$, $S = s$, and $T = t$.
The mean value

$$E(QS + RS + RT - QT) = \sum_{q,r,s,t} p(q, r, s, t)(qs + rs + rt - qt) \leq \sum_{q,r,s,t} p(q, r, s, t) \times 2 = 2$$

Also

$$\begin{aligned} E(QS + RS + RT - QT) &= \sum_{q,r,s,t} p(q, r, s, t)qs + \sum_{q,r,s,t} p(q, r, s, t)rs \\ &\quad + \sum_{q,r,s,t} p(q, r, s, t)rt - \sum_{q,r,s,t} p(q, r, s, t)qt \\ &= E(QS) + E(RS) + E(RT) - E(QT) \end{aligned}$$

Comparing both gives the **Bell inequality**

$$E(QS) + E(RS) + E(RT) - E(QT) \leq 2$$

Now let Alice and Bob share a quantum system of two qubits in the state

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \qquad (\; = \; |\beta_{11}\rangle \;)$$

They perform measurements of the following observables:

Alice: $\quad Q = \hat{Z}_1 \quad R = \hat{X}_1 \quad$ Bob: $\quad S = \frac{-\hat{Z}_2 - \hat{X}_2}{\sqrt{2}} \quad T = \frac{\hat{Z}_2 - \hat{X}_2}{\sqrt{2}}$

The expectation values of these observables are

$$< QS >= \frac{1}{\sqrt{2}}; \quad < RS >= \frac{1}{\sqrt{2}}; \quad < RT >= \frac{1}{\sqrt{2}}; \quad < QT >= -\frac{1}{\sqrt{2}}$$

Thus **quantum mechanical systems violate the Bell inequality**:

$$< QS > + < RS > + RT > - < QT >= 2\sqrt{2}$$

Experiment: Alain Aspect 1982.

Evaluation of the expectation values:

$$
\begin{aligned}
< QS > &= \langle\psi|\frac{-\hat{Z}_1 \otimes \hat{Z}_2 - \hat{Z}_1 \otimes \hat{X}_2}{\sqrt{2}}|\psi\rangle = \frac{1}{2\sqrt{2}}((\langle 01| - \langle 10|)(-\hat{Z}_1 \otimes \hat{Z}_2 - \hat{Z}_1 \otimes \hat{X}_2)((|01\rangle - |10\rangle) \\
&= \frac{1}{2\sqrt{2}}(\langle 01|(-\hat{Z}_1 \otimes \hat{Z}_2)|01\rangle + \langle 10|(-\hat{Z}_1 \otimes \hat{Z}_2)|10\rangle) = \frac{1}{2\sqrt{2}}(1+1) = \frac{1}{\sqrt{2}} \\
< RS > &= \langle\psi|\frac{-\hat{X}_1 \otimes \hat{Z}_2 - \hat{X}_1 \otimes \hat{X}_2}{\sqrt{2}}|\psi\rangle = \frac{1}{\sqrt{2}} \\
< RT > &= \langle\psi|\frac{\hat{X}_1 \otimes \hat{Z}_2 - \hat{X}_1 \otimes \hat{X}_2}{\sqrt{2}}|\psi\rangle = \frac{1}{\sqrt{2}} \\
< QT > &= \langle\psi|\frac{\hat{Z}_1 \otimes \hat{Z}_2 - \hat{Z}_1 \otimes \hat{X}_2}{\sqrt{2}}|\psi\rangle = -\frac{1}{\sqrt{2}}
\end{aligned}
$$

Entanglement on bipartite systems

Theorem: Schmidt's decomposition

Suppose $|\psi\rangle$ is a pure state of a bipartite system, AB. Then there exist orthonormal states $|i_A\rangle$ for system A, and $|i_B\rangle$ for system B such that

$$|\psi\rangle = \sum_i \lambda_i \, |i_A\rangle |i_B\rangle$$

where λ_i are non-negative real numbers satisfying $\sum_i \lambda_i^2 = 1$ known as the **Schmidt coefficients**.

The number of non-zero values λ_i is called the **Schmidt number**.

Proof

Let us assume for the sake of simplicity that the Hilbert spaces for the system A and the system B have the same dimension. Let $\{|j\rangle\}$ and $\{|k\rangle\}$ be any fixed basis for systems A and B, respectively. Then $|\psi\rangle$ can be written as

$$|\psi\rangle = \sum_{jk} a_{jk} |j\rangle|k\rangle$$

for some matrix a of complex numbers a_{jk}.

By singular value decomposition, $a = udv$, where d is a diagonal matrix with non-negative real elements, and u and v are unitary matrices. Thus

$$|\psi\rangle = \sum_{ijk} u_{ji} d_{ii} v_{ik} |j\rangle|k\rangle$$

Defining $|i_A\rangle = \sum_j u_{ji} |j\rangle$ and $|i_B\rangle = \sum_k v_{ik} |k\rangle$, and $\lambda_i = d_{ii}$ we get

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle$$

Both $|i_A\rangle$ and $|i_B\rangle$ form orthonormal sets. This follows from the unitarity of u and v and orthonormality of $|j\rangle$ and $|k\rangle$. Q.E.D.

If the Schmidt number is 1, then the quantum state of the bipartite system is a product state, otherwise it is an entangled states.

Examples

(i) Schmidt number = 1

a) Let us have the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle$. The matrix a is then

$$a = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 \end{pmatrix}$$

Now we construct the matrix $aa^\dagger$

$$aa^\dagger = udvv^\dagger d^\dagger u^\dagger = ud^2u^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

where $d = d^\dagger$ because d is diagonal matrix with real entries.The matrix $aa^\dagger$ is already diagonal and has one nonzero eigenvalue.Thus the state $|\psi\rangle$ is a **product state**.

b) Let us have the state $|\psi\rangle = \frac{1}{2}(|00\rangle + |01\rangle - |10\rangle - |11\rangle)$. The matrix a is then

$$a = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & -\frac{1}{2} \end{pmatrix}$$

Now we construct the matrix $aa^\dagger$

$$aa^\dagger = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

The matrix $aa^\dagger$ is not diagonal so we have to diagonalize it. The eigenvalues are given as the roots of the characteristic equation

$$\det\left(aa^\dagger - \lambda\hat{I}\right) = \left(\frac{1}{2} - \lambda\right)^2 - \frac{1}{4} = 0$$

we get $\lambda_1 = 1$ and $\lambda_2 = 0$, so the state is again a **product state**.

(ii) Schmidt number = 2

a) Let us have the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle$. The matrix a is then

$$a = \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 \\ \\ 0 & \frac{1}{\sqrt{2}} \end{pmatrix}$$

Now we construct the matrix $aa^\dagger$

$$aa^\dagger = udvv^\dagger d^\dagger u^\dagger = ud^2u^\dagger = \begin{pmatrix} \frac{1}{2} & 0 \\ \\ 0 & \frac{1}{2} \end{pmatrix}$$

The matrix $aa^\dagger$ is diagonal and has **two** nonzero eigenvalues.Thus the state $|\psi\rangle$ is **entangled**.

b) Let us have the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - i|10\rangle$. The matrix a and $a^\dagger$ are then

$$a = \begin{pmatrix} 0 & \frac{1}{\sqrt{2}} \\ -i\frac{1}{\sqrt{2}} & 0 \end{pmatrix} \qquad a^\dagger = \begin{pmatrix} 0 & i\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 \end{pmatrix}$$

Now we construct the matrix $aa^\dagger$

$$aa^\dagger = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$$

The Schmidt number thus equals to 2, and therefore the state $|\psi\rangle$ is **entangled**.

QUANTUM MECHANICS FOUNDATIONS OF QUANTUM INFORMATION PROCESSING

OPERATORS

SECOND POSTULATE

Every measurable physical quantity $\mathcal{A}$ is described by an operator $\hat{A}$ acting on $\mathcal{H}$; this operator is an observable.

An operator $\hat{A} : \mathcal{H} \to \mathcal{F}$ such that $|\psi'\rangle = \hat{A}|\psi\rangle$ for

$$|\psi\rangle \in \underbrace{\mathcal{H}}_{\text{domain } D(\hat{A})}$$

and $$|\psi'\rangle \in \underbrace{\mathcal{F}}_{\text{range } R(\hat{A})}$$

Properties:

1. Linearity $\hat{A} \sum_i c_i |\phi_i\rangle = \sum_i c_i \hat{A} |\phi_i\rangle$

2. Equality $\hat{A} = \hat{B}$ iff $\hat{A}|\psi\rangle = \hat{B}|\psi\rangle$ and $D(\hat{A}) = D(\hat{B})$

3. Sum $\hat{C} = \hat{A} + \hat{B}$ iff $\hat{C}|\psi\rangle = \hat{A}|\psi\rangle + \hat{B}|\psi\rangle$

4. Product $\hat{C} = \hat{A}\hat{B}$ iff

$$\begin{aligned} \hat{C}|\psi\rangle &= \hat{A}\hat{B}|\psi\rangle \\ &= \hat{A}\left(\hat{B}|\psi\rangle\right) = \hat{A}|\hat{B}\psi\rangle \end{aligned}$$

5. Functions $\hat{A}^2 = \hat{A}\hat{A}$, then $\hat{A}^n = \hat{A}\hat{A}^{n-1}$ and if a function $f(\xi) = \sum_n a_n \xi^n$, then by the function of an operator $f(\hat{A})$ we mean

$$f\left(\hat{A}\right) = \sum_n a_n \hat{A}^n$$

e.g.

$$e^{\hat{A}} = \sum_{n=0}^{\infty} \frac{1}{n!} \hat{A}^n$$

We will see later how to calculate a function of an operator using its spectral decomposition.

Iff the operator is diagonal, the function of the operator is obtained by taking the function of each of its diagonal elements, its eigenvalues.

Example:

Let

$$\hat{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

then

$$\hat{S} = \sqrt{\hat{Z}} = \begin{pmatrix} \sqrt{1} & 0 \\ 0 & \sqrt{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{pmatrix}$$

Commutator and anticommutator

In contrast to numbers, a product of operators is generally not commutative, i.e.

$$\hat{A}\hat{B} \neq \hat{B}\hat{A}$$

For example: three vectors $|x\rangle$, $|y\rangle$ and $|z\rangle$ and two operators $\hat{R}_x$ and $\hat{R}_y$ such that:

$$\begin{aligned} \hat{R}_x|x\rangle &= |x\rangle, & \hat{R}_y|x\rangle &= -|z\rangle, \\ \hat{R}_x|y\rangle &= |z\rangle, & \hat{R}_y|y\rangle &= |y\rangle, \\ \hat{R}_x|z\rangle &= -|y\rangle, & \hat{R}_y|z\rangle &= |x\rangle \end{aligned}$$

then

$$\begin{aligned} \hat{R}_x\hat{R}_y|z\rangle = \hat{R}_x|x\rangle = |x\rangle \quad \neq \\ \hat{R}_y\hat{R}_x|z\rangle = -\hat{R}_y|y\rangle = -|y\rangle \end{aligned}$$

An operator $\left[\hat{A},\hat{B}\right]=\hat{A}\hat{B}-\hat{B}\hat{A}$ is called commutator.
We say that $\hat{A}$ and $\hat{B}$ commute iff $\left[\hat{A},\hat{B}\right]=0$ in which case also $\left[f(\hat{A}),f(\hat{B})\right]=0$.
An operator $\left\{\hat{A},\hat{B}\right\}=\hat{A}\hat{B}+\hat{B}\hat{A}$ is called anticommutator.

Basic properties:

$$\begin{aligned}\left[\hat{A},\hat{B}\right] &= -\left[\hat{B},\hat{A}\right]\\ \left\{\hat{A},\hat{B}\right\} &= \left\{\hat{B},\hat{A}\right\}\\ \left[\hat{A},\hat{B}+\hat{C}\right] &= \left[\hat{A},\hat{B}\right]+\left[\hat{A},\hat{C}\right]\\ \left[\hat{A},\hat{B}\hat{C}\right] &= \left[\hat{A},\hat{B}\right]\hat{C}+\hat{B}\left[\hat{A},\hat{C}\right]\end{aligned}$$

the Jacobi identity:

$$\left[\hat{A},\left[\hat{B},\hat{C}\right]\right]+\left[\hat{B},\left[\hat{C},\hat{A}\right]\right]+\left[\hat{C},\left[\hat{A},\hat{B}\right]\right] = 0$$

Types of operators (examples)

1. $\hat{A}$ is bounded iff $\exists \beta > 0$ such that $\left\| \hat{A}|\psi\rangle \right\| \leq \beta \, \| |\psi\rangle \|$ for all $|\psi\rangle \in D(\hat{A})$. Infimum of β is called the norm of $\hat{A}$

2. $\hat{A}$ is symmetric if $\langle \psi_1 | \hat{A} \psi_2 \rangle = \langle \hat{A} \psi_1 | \psi_2 \rangle$ for all $|\psi_1\rangle, |\psi_2\rangle \in D(\hat{A})$.

3. $\hat{A}$ is hermitian if it is bounded and symmetric.

4. Let $\hat{A}$ be a bounded operator (with $D(\hat{A})$ dense in $\mathcal{H}$); then there is an adjoint operator $\hat{A}^\dagger$ such that

$$\langle \psi_1 | \hat{A}^\dagger \psi_2 \rangle \quad = \quad \langle \hat{A} \psi_1 | \psi_2 \rangle$$

i.e.

$$\langle \psi_1 | \hat{A}^\dagger \psi_2 \rangle \;=\; \langle \psi_2 | \hat{A} \psi_1 \rangle^*$$

for all $|\psi_1\rangle, |\psi_2\rangle \in D(\hat{A})$.

Properties:

$$\begin{aligned}
\left\| \hat{A}^\dagger \right\| &= \left\| \hat{A} \right\| \\
\left(\hat{A}^\dagger \right)^\dagger &= \hat{A} \\
\left(\hat{A} + \hat{B} \right)^\dagger &= \hat{A}^\dagger + \hat{B}^\dagger \\
\left(\hat{A}\hat{B} \right)^\dagger &= \hat{B}^\dagger \hat{A}^\dagger \text{ (the order changes)} \\
\left(\lambda \hat{A} \right)^\dagger &= \lambda^* \hat{A}^\dagger
\end{aligned}$$

How can we construct an adjoint?
E.g. Let us have an operator in a matrix representation (so it is also a matrix) then

$$\hat{A}^\dagger = \left(A^{\mathrm{T}}\right)^* \quad = \quad \text{transpose \& complex conjugation}$$

5. $\hat{A}$ is selfadjoint if $\hat{A}^\dagger = \hat{A}$.
   This is the property of observables!
   Their eigenvalues are real numbers, e.g. $\hat{X}|x\rangle = x|x\rangle$

6. $\hat{A}$ is positive if $\langle\psi|\hat{A}|\psi\rangle \geq 0$ for all $|\psi\rangle \in \mathcal{H}$

7. $\hat{A}$ is normal if $\hat{A}\hat{A}^\dagger = \hat{A}^\dagger\hat{A}$ i.e. $\underbrace{\left[\hat{A}, \hat{A}^\dagger\right] = 0}_{\text{commutator}}$

8. Let $\hat{A}$ be an operator. If there exists an operator $\hat{A}^{-1}$ such that $\hat{A}\hat{A}^{-1} = \hat{A}^{-1}\hat{A} = \hat{1}$ (identity operator) then $\hat{A}^{-1}$ is called an inverse operator to $\hat{A}$
   Properties:

$$\begin{aligned} \left(\hat{A}\hat{B}\right)^{-1} &= \hat{B}^{-1}\hat{A}^{-1} \\ \left(\hat{A}^{\dagger}\right)^{-1} &= \left(\hat{A}^{-1}\right)^{\dagger} \end{aligned}$$

9. an operator $\hat{U}$ is called unitary if $\hat{U}^{\dagger} = \hat{U}^{-1}$, i.e. $\hat{U}\hat{U}^{\dagger} = \hat{U}^{\dagger}\hat{U} = \hat{1}$.

   Formal solution of the Schrödinger equation leads to a unitary operator: if $\hat{H}$ is the Hamiltonian (total energy operator),

$$\begin{aligned} i\hbar\frac{\mathrm{d}}{\mathrm{d}t}|\psi(t)\rangle &= \hat{H}|\psi(t)\rangle \\ \Rightarrow \int_0^t \frac{\mathrm{d}|\psi(t')\rangle}{|\psi(t')\rangle} &= -\frac{i}{\hbar}\int_0^t \hat{H}\mathrm{d}t' \end{aligned}$$

If the Hamiltonian is time independent then

$$|\psi(t)\rangle \quad = \quad e^{-\frac{i}{\hbar}\hat{H}t}|\psi(0)\rangle = \hat{U}|\psi(0)\rangle$$

10. An operator $\hat{P}$ satisfying $\hat{P} = \hat{P}^\dagger = \hat{P}^2$ is a projection operator or projector
e.g. if $|\psi_k\rangle$ is a normalized vector then

$$\hat{P}_k \quad = \quad |\psi_k\rangle\langle\psi_k|$$

is the projector onto one-dimensional space spanned by all vectors linearly dependent on $|\psi_k\rangle$.

Matrix representation of quantum computing operations

Matrix representation in general

Operator is uniquely defined by its action on the basis vectors of the Hilbert space.
Let $\mathcal{B} = \left\{|\psi_j\rangle\right\}$ be a basis of $\mathcal{H}$ $(= D(\hat{A}))$

$$\begin{aligned} \hat{A}|\psi_j\rangle &= \sum_k |\psi_k\rangle\langle\psi_k|\hat{A}|\psi_j\rangle \\ &= \sum_k A_{kj}|\psi_k\rangle \end{aligned}$$

where $A_{kj} = \langle\psi_k|\hat{A}|\psi_j\rangle$ are the matrix elements of the operator $\hat{A}$ in the matrix representation given by the basis $\mathcal{B}$.

For practical calculations

$$\hat{A} = \sum_{kj} |\psi_k\rangle\langle\psi_k|\hat{A}|\psi_j\rangle\langle\psi_j| = \sum_{kj} A_{kj}|\psi_k\rangle\langle\psi_j|$$

Single-qubt operations in the standard computational basis

(i) Phase flip

$$
\begin{aligned}
\hat{Z} &= \left(\sum_{k=0,1} |k\rangle\langle k|\right)\hat{Z}\left(\sum_{l=0,1} |l\rangle\langle l|\right) = \sum_{k,l}\langle k|\hat{Z}|l\rangle\ |k\rangle\langle l| \\
&= \langle 0|\hat{Z}|0\rangle|0\rangle\langle 0| + \langle 0|\hat{Z}|1\rangle|0\rangle\langle 1| + \langle 1|\hat{Z}|0\rangle|1\rangle\langle 0| + \langle 1|\hat{Z}|1\rangle|1\rangle\langle 1| \\
&= \langle 0|\hat{Z}|0\rangle\begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \end{pmatrix} + \langle 0|\hat{Z}|1\rangle\begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \end{pmatrix} \\
&+ \langle 1|\hat{Z}|0\rangle\begin{pmatrix} 0 \\ 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \end{pmatrix} + \langle 1|\hat{Z}|1\rangle\begin{pmatrix} 0 \\ 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} \langle 0|\hat{Z}|0\rangle & \langle 0|\hat{Z}|1\rangle \\ \langle 1|\hat{Z}|0\rangle & \langle 1|\hat{Z}|1\rangle \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \sigma_z
\end{aligned}
$$

(ii) Bit flip

$$\hat{X} = \begin{pmatrix} \langle 0|\hat{X}|0\rangle & \langle 0|\hat{X}|1\rangle \\ \langle 1|\hat{X}|0\rangle & \langle 1|\hat{X}|1\rangle \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma_x$$

(iii) $\hat{Y} = i\hat{Z}\hat{X}$

$$\hat{Y} = \begin{pmatrix} \langle 0|\hat{Y}|0\rangle & \langle 0|\hat{Y}|1\rangle \\ \langle 1|\hat{Y}|0\rangle & \langle 1|\hat{Y}|1\rangle \end{pmatrix} = \begin{pmatrix} \langle 0|i\hat{Z}\hat{X}|0\rangle & \langle 0|i\hat{Z}\hat{X}|1\rangle \\ \langle 1|i\hat{Z}\hat{X}|0\rangle & \langle 1|i\hat{Z}\hat{X}|1\rangle \end{pmatrix} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \sigma_y$$

(iv) $\hat{S} = \sqrt{\hat{Z}}$

$$\hat{S} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

(v) $\hat{T} = \sqrt{\hat{S}}$

$$\hat{T} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

(vi) Hadamard gate

$$\hat{H} = \begin{pmatrix} \langle 0|\hat{H}|0\rangle & \langle 0|\hat{H}|1\rangle \\ \langle 1|\hat{H}|0\rangle & \langle 1|\hat{H}|1\rangle \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z)$$

Two-qubt operations in the standard computational basis

(i) $CNOT_{12}$ (the first qubit is the control qubit, the second is the target):

$$CNOT_{12} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = |0\rangle\langle 0| \otimes \hat{I} + |1\rangle\langle 1| \otimes \hat{X} = \hat{P}_0 \otimes \hat{I} + \hat{P}_1 \otimes \hat{X}$$

(ii) $CNOT_{21}$:

$$CNOT_{21} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} = \hat{I} \otimes |0\rangle\langle 0| + \hat{X} \otimes |1\rangle\langle 1| = \hat{I} \otimes \hat{P}_0 + \hat{X} \otimes \hat{P}_1$$

(iii) $SWAP = CNOT_{12}CNOT_{21}CNOT_{12}$

$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Composition of operators (by example)

1. Direct sum $\hat{A} = \hat{B} \oplus \hat{C}$

   $\hat{B}$ acts on $\mathcal{H}_B$ (2 dimensional) and $\hat{C}$ acts on $\mathcal{H}_C$ (3 dimensional)

   Let

$$\hat{B} = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \quad \text{and} \quad \hat{C} = \begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{pmatrix}$$

$$\hat{A} = \begin{pmatrix} b_{11} & b_{12} & 0 & 0 & 0 \\ b_{21} & b_{22} & 0 & 0 & 0 \\ 0 & 0 & c_{11} & c_{12} & c_{13} \\ 0 & 0 & c_{21} & c_{22} & c_{23} \\ 0 & 0 & c_{31} & c_{32} & c_{33} \end{pmatrix}$$

   Acts on $\mathcal{H}_B \oplus \mathcal{H}_C$

Properties:

$$\begin{aligned} \mathrm{Tr}\left(\hat{B} \oplus \hat{C}\right) &= \mathrm{Tr}\left(\hat{B}\right) + \mathrm{Tr}\left(\hat{C}\right) \\ \det\left(\hat{B} \oplus \hat{C}\right) &= \det\left(\hat{B}\right) \det\left(\hat{C}\right) \end{aligned}$$

2. Direct product $\hat{A} = \hat{B} \otimes \hat{C}$:

$$|\psi\rangle \in \mathcal{H}_B,\ |\phi\rangle \in \mathcal{H}_C, \qquad |\chi\rangle \in \mathcal{H}_B \otimes \mathcal{H}_C$$

$$\begin{aligned} \hat{A}|\chi\rangle &= \left(\hat{B} \otimes \hat{C}\right) \underbrace{(|\psi\rangle \otimes |\phi\rangle)}_{|\psi\rangle|\phi\rangle \text{ to simplify the notation}} \\ &= \hat{B}|\psi\rangle\hat{C}|\phi\rangle \end{aligned}$$

$$\hat{A} = \begin{pmatrix} b_{11}c_{11} & b_{11}c_{12} & b_{11}c_{13} & b_{12}c_{11} & b_{12}c_{12} & b_{12}c_{13} \\ b_{11}c_{21} & b_{11}c_{22} & b_{11}c_{23} & b_{12}c_{21} & b_{12}c_{22} & b_{12}c_{23} \\ b_{11}c_{31} & b_{11}c_{32} & b_{11}c_{33} & b_{12}c_{31} & b_{12}c_{32} & b_{12}c_{33} \\ b_{21}c_{11} & b_{21}c_{12} & b_{21}c_{13} & b_{22}c_{11} & b_{22}c_{12} & b_{22}c_{13} \\ b_{21}c_{21} & b_{21}c_{22} & b_{21}c_{23} & b_{22}c_{21} & b_{22}c_{22} & b_{22}c_{23} \\ b_{21}c_{31} & b_{21}c_{32} & b_{21}c_{33} & b_{22}c_{31} & b_{22}c_{32} & b_{22}c_{33} \end{pmatrix}$$

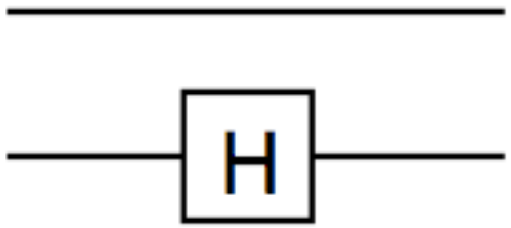
Examples Hadamard gates

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

on two qubit states:

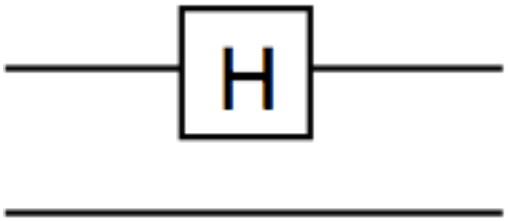
(i) Hadamard gate on the second qubit:

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



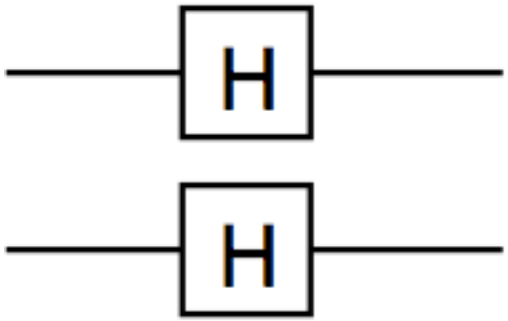
(ii) Hadamard gate on the first qubit:

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



(iii) Hadamard gates on both qubits:

$$\hat{H} \otimes \hat{H} = \begin{pmatrix} \frac{1}{\sqrt{2}}.\hat{H} & \frac{1}{\sqrt{2}}.\hat{H} \\ \frac{1}{\sqrt{2}}.\hat{H} & -\frac{1}{\sqrt{2}}.\hat{H} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$$



Eigenvalues and eigenvectors

Solving a quantum mechanical system means to find the eigenvalues and eigenvectors of the complete set of commuting observables (C.S.C.O.)

1. The eigenvalue equation

$$\hat{A}|\psi_\alpha\rangle = \underbrace{\alpha}_{\text{eigenvalue}} \underbrace{|\psi_\alpha\rangle}_{\text{eigenvector}}$$

   If $n > 1$ vectors satisfy the eigenvalue equation for the same eigenvalue α, we say the eigenvalue is n-fold degenerate.

2. The eigenvalues of a self-adjoint operator $\hat{A}$, which are observables and represent physical quantities, are real numbers

$$\begin{aligned} \alpha\langle\psi_\alpha|\psi_\alpha\rangle &= \langle\psi_\alpha|\hat{A}\psi_\alpha\rangle \\ &= \langle\hat{A}\psi_\alpha|\psi_\alpha\rangle^* = \alpha^*\langle\psi_\alpha|\psi_\alpha\rangle \\ \Rightarrow \alpha = \alpha^* &\Rightarrow \alpha \in \mathbb{R} \end{aligned}$$

3. Eigenvectors of self-adjoint operators corresponding to distinct eigenvalues are orthogonal.
   Proof: if $\beta \neq \alpha$ is also an eigenvalue of $\hat{A}$ then

$$\langle \psi_\alpha | \hat{A} \psi_\beta \rangle = \beta \langle \psi_\alpha | \psi_\beta \rangle$$

   and also

$$\begin{aligned} \langle \psi_\alpha | \hat{A} \psi_\beta \rangle &= \langle \psi_\beta | \hat{A} \psi_\alpha \rangle^* \\ &= \alpha^* \langle \psi_\beta | \psi_\alpha \rangle^* = \alpha \langle \psi_\alpha | \psi_\beta \rangle \end{aligned}$$

   which implies

$$\langle \psi_\alpha | \psi_\beta \rangle = 0$$

Spectral decomposition of an operator

Assume that the eigenvectors of $\hat{A}$ define a basis $\mathcal{B} = \left\{|\psi_j\rangle\right\}$,
then $A_{kj} = \langle\psi_k|\hat{A}|\psi_j\rangle = \alpha_j \delta_{kj}$.
Operator in this basis is a diagonal matrix with eigenvalues on the diagonal

$$\begin{aligned}\hat{A} &= \sum_{kj} A_{kj}|\psi_k\rangle\langle\psi_j| \\ &= \sum_{j} \alpha_j|\psi_j\rangle\langle\psi_j| \\ &= \sum_{j} \alpha_j \hat{E}_j\end{aligned}$$

$\hat{E}_j$ is a projector onto 1-dim. space spanned by $|\psi_j\rangle \Rightarrow$ Spectral decomposition!

Function of an operator using its spectral decomposition

$$f(\hat{A}) \;=\; \sum_j f(\alpha_j)|\psi_j\rangle\langle\psi_j| = \sum_j f(\alpha_j)\hat{E}_j$$

If and only if the operator is diagonal, the function of the operator is obtained by taking the function of each of its diagonal elements, its eigenvalues.

Example:

$$\hat{S} \;=\; \sqrt{\hat{Z}} = \begin{pmatrix} \sqrt{1} & 0 \\ 0 & \sqrt{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{pmatrix}$$

QUANTUM MECHANICS FOUNDATIONS OF QUANTUM INFORMATION PROCESSING

DYNAMICS

THIRD POSTULATE
(Time Evolution)

The time evolution of the state vector $|\psi(t)\rangle$ is governed by the Schrödinger equation

$$i\hbar\frac{\mathrm{d}}{\mathrm{d}t}|\psi(t)\rangle \quad = \quad \hat{H}(t)|\psi(t)\rangle$$

where $\hat{H}(t)$ is the observable associated with the total energy of the system.

Formal solution of the Schrödinger equation:

(i) Time-dependent Hamiltonian

$$|\psi(t)\rangle \quad = \quad e^{-\frac{i}{\hbar}\int_0^t \hat{H}(t')\,dt'}\,|\psi(0)\rangle = \hat{U}_t\,|\psi(0)\rangle$$

(ii) Time-independent Hamiltonian

$$|\psi(t)\rangle \quad = \quad e^{-\frac{i}{\hbar}\hat{H}t}\,|\psi(0)\rangle = \hat{U}_t\,|\psi(0)\rangle$$

The operator $\hat{U}_t$ is called **evolution operator** or **propagator**. It evolves or propagates state of a quantum mechanical system from the initial time $t' = 0$ to a final time $t' = t$.

Since the Hamiltonian is self-adjoined, the evolution operator is **unitary**:

$$\begin{aligned}
\hat{U}_t &= e^{-\frac{i}{\hbar}\hat{H}t} \\
\hat{U}_t^\dagger &= e^{\frac{i}{\hbar}\hat{H}t} = \hat{U}_{-t} = \hat{U}_t^{-1} \\
\hat{U}_t\hat{U}_t^\dagger &= e^{-\frac{i}{\hbar}\hat{H}t}\, e^{\frac{i}{\hbar}\hat{H}t} = \hat{U}_t^\dagger\hat{U}_t = e^{\frac{i}{\hbar}\hat{H}t}\, e^{-\frac{i}{\hbar}\hat{H}t} = \hat{I}
\end{aligned}$$

The evolution operator can also evolve the state given by a density operator. Since $|\psi(t)\rangle = \hat{U}_t|\psi(0)\rangle$ and the adjoint is $\langle\psi(t)| = \langle\psi(0)|\hat{U}_t^\dagger$, the density matrix at time t is given as

$$\rho(t) = |\psi(t)\rangle\langle\psi(t)| = \hat{U}_t\,|\psi(0)\rangle\langle\psi(0)|\,\hat{U}_t^\dagger = \hat{U}_t\,\rho(0)\,\hat{U}_t^\dagger$$

Example: A two-level atom

Let us have an atoms with two energy levels separated by the energy $\hbar\omega$:

$$\begin{aligned} E_- &= -\hbar\omega/2 \\ E_+ &= +\hbar\omega/2 \end{aligned}$$

In the representation given by the corresponding eigenvectors, $|E_-\rangle$ and $|E_+\rangle$ respectively, the Hamiltonian is

$$\hat{H} = \frac{\hbar\omega}{2}\,\sigma_z$$

and the evolution operator then reads as

$$\hat{U}_t = e^{-\frac{i}{\hbar}\hat{H}t} = e^{-i\ \omega\ t\ \sigma_z/2} = \begin{pmatrix} e^{-i\omega t/2} & 0 \\ 0 & e^{i\omega t/2} \end{pmatrix}$$

Connecting with Bloch representation

We can rewrite the evolution operator above as

$$\begin{aligned}
\hat{U}_t &= \begin{pmatrix} e^{-i\omega t/2} & 0 \\ 0 & e^{i\omega t/2} \end{pmatrix} = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix} \\
&= \begin{pmatrix} \cos\theta/2 & 0 \\ 0 & \cos\theta/2 \end{pmatrix} - i \begin{pmatrix} \sin\theta/2 & 0 \\ 0 & -\sin\theta/2 \end{pmatrix} \\
&= \cos\frac{\theta}{2}\,\hat{I} - i\sin\frac{\theta}{2}\,\sigma_z = \hat{R}_z(\theta)
\end{aligned}$$

and examine its action on a qubit $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$, where $|0\rangle = |E_-\rangle$ and $|1\rangle = |E_+\rangle$, whose initial state is given by the density matrix in the Bloch representation

$$\rho(0) = \frac{1}{2}\left(\hat{I} + \vec{r}(0)\,.\,\vec{\sigma}\right)$$

We evaluate the action of the evolution operator as follows

$$\begin{aligned}
\rho(t) &= \hat{U}_t\,\rho(0)\,\hat{U}_t^\dagger = \hat{R}_z(\theta)\,\rho(0)\,\hat{R}_z^\dagger(\theta) = \hat{R}_z(\theta)\left[\frac{1}{2}\left(\hat{I} + \vec{r}(0)\,.\,\vec{\sigma}\right)\right]\hat{R}_z^\dagger(\theta) \\
&= \frac{1}{2}\left(\hat{I} + \hat{R}_z(\theta)\vec{r}(0)\,.\,\vec{\sigma}\hat{R}_z^\dagger(\theta)\right) \\
&= \frac{1}{2}\left[\hat{I} + \left(\cos\frac{\theta}{2}\,\hat{I} - i\sin\frac{\theta}{2}\,\sigma_z\right)\left(r_x\sigma_x + r_y\sigma_y + r_z\sigma_z\right)\left(\cos\frac{\theta}{2}\,\hat{I} + i\sin\frac{\theta}{2}\,\sigma_z\right)\right] \\
&= \frac{1}{2}\left[\hat{I} + (r_x\cos\theta - r_y\sin\theta)\,\sigma_x + (r_x\sin\theta + r_y\cos\theta)\,\sigma_y + r_z\,\sigma_z\right]
\end{aligned}$$

We observe that it causes the rotation of the Bloch vector around the axis z by the angle θ:

$$\vec{r}(0) = (r_x, r_y, r_z) \qquad \rightarrow \qquad \vec{r}(t) = (r_x\cos\theta - r_y\sin\theta, r_x\sin\theta + r_y\cos\theta, r_z)$$

Similarly, we can define the rotation operators about any axis in the Bloch representation

$$\hat{R}_x(\theta) = e^{-i\theta\sigma_x/2} = \cos\frac{\theta}{2}\,\hat{I} - i\sin\frac{\theta}{2}\,\sigma_x = \begin{pmatrix} \cos\theta/2 & -i\sin\theta/2 \\ -i\sin\theta/2 & \cos\theta/2 \end{pmatrix}$$

$$\hat{R}_y(\theta) = e^{-i\theta\sigma_y/2} = \cos\frac{\theta}{2}\,\hat{I} - i\sin\frac{\theta}{2}\,\sigma_y = \begin{pmatrix} \cos\theta/2 & -\sin\theta/2 \\ \sin\theta/2 & \cos\theta/2 \end{pmatrix}$$

$$\hat{R}_z(\theta) = e^{-i\theta\sigma_z/2} = \cos\frac{\theta}{2}\,\hat{I} - i\sin\frac{\theta}{2}\,\sigma_z = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}$$

Using the Taylor expansion of exponential function and properties of the Pauli operators, we can show that the operator for rotation by an angle θ about an axis defined by a real unit vector $\vec{n}$ is

$$\begin{aligned}
\hat{R}_{\vec{n}}(\theta) &= e^{-i\theta\ \vec{n}\ .\ \vec{\sigma}\ /2} \\
&= \cos\frac{\theta}{2}\,\hat{I} - i\sin\frac{\theta}{2}\,\vec{n}\ .\ \vec{\sigma} \\
&= \begin{pmatrix} \cos\frac{\theta}{2} - in_z\sin\frac{\theta}{2} & -in_x\sin\frac{\theta}{2} - n_y\sin\frac{\theta}{2} \\ -in_x\sin\frac{\theta}{2} + n_y\sin\frac{\theta}{2} & \cos\frac{\theta}{2} + in_z\sin\frac{\theta}{2} \end{pmatrix}
\end{aligned}$$

Properties of the set of all unitary operators $\hat{R}_{\vec{n}}(\theta)$:

1. product of two operators from this set is again a unitary operator

$$\begin{aligned}
\hat{R}_{\vec{n}}(\theta)\hat{R}_{\vec{n'}}(\theta')\left(\hat{R}_{\vec{n}}(\theta)\hat{R}_{\vec{n'}}(\theta')\right)^{\dagger} &= \hat{R}_{\vec{n}}(\theta)\hat{R}_{\vec{n'}}(\theta')\hat{R}^{\dagger}_{\vec{n'}}(\theta')\hat{R}^{\dagger}_{\vec{n}}(\theta) = \hat{I} \\
\left(\hat{R}_{\vec{n}}(\theta)\hat{R}_{\vec{n'}}(\theta')\right)^{\dagger}\hat{R}_{\vec{n}}(\theta)\hat{R}_{\vec{n'}}(\theta') &= \hat{R}^{\dagger}_{\vec{n'}}(\theta')\hat{R}^{\dagger}_{\vec{n}}(\theta)\hat{R}_{\vec{n}}(\theta)\hat{R}_{\vec{n'}}(\theta') = \hat{I};
\end{aligned}$$

   ad since it is a product of two rotations in the Bloch representation we can trust that the product itself also corresponds to a rotation and is therefore an element of the same set.

Baker-Campbell-Hausdorff formula

It is to be said that we can **not** in general rewrite the product $\hat{R}_{\vec{n}}(\theta)\hat{R}_{\vec{n'}}(\theta')$ above as a single exponential function. In the non-commutative world, the product of two exponential functions of non-commuting operators is **not** an exponential function of the sum of the two operators. Instead the product is given by the **Baker-Campbell-Hausdorff formula** which for two non-commuting operators $\hat{A}$ and $\hat{B}$ reads as

$$e^{\hat{A}}\ e^{\hat{B}} = e^{\hat{A}+\hat{B}+\frac{1}{2}[\hat{A},\hat{B}]+\frac{1}{12}([\hat{A},[\hat{A},\hat{B}]]+[[\hat{A},\hat{B}],\hat{B}])+...}$$

2. The set contains an identity operator $\hat{R}_{\vec{n}}(\theta = 0) = \hat{I}$.

3. every element of the set $\hat{R}_{\vec{n}}(\theta)$ has an inverse $\hat{R}^{\dagger}_{\vec{n}}(\theta) = \hat{R}^{-1}_{\vec{n}}(\theta)$;

4. every element of the set has the unit determinant: $\det \hat{R}_{\vec{n}}(\theta) = 1$.

The properties above contain the group axioms. The set of unitary operators $\hat{R}_{\vec{n}}(\theta)$ hence forms a group, specifically, of 2-by-2 unitary matrices of unit determinant, called

the special unitary group $SU(2)$.

$SU(2)$ is a Lie group

A **Lie group** is a group which is also a smooth manifold G. The neighborhood of any point of a Lie group, considered as a manifold, looks exactly like that of any other. Thus the group dimension and much of its structure can be understood by examining the immediate vicinity of any chosen point, for instance, the identity element.

Example: a near identity element of the general linear group $GL(n,\mathbb{R})$, which consists of invertible n-by-n real matrices, can be written as $g = I + \epsilon A$ where A is an arbitrary n-by-n matrix. This matrix consists of n^2 entries and therefore the group manifold itself is n^2 dimensional. $GL(n,\mathbb{C})$ has $2n^2$ real dimensions.

The special linear group $SL(n,\mathbb{R})$ consists of elements of $GL(n,\mathbb{R})$ characterized by the unit determinant $\det g = 1$. For the element near identity $g = I + \epsilon A$ this implies

that $\mathrm{tr}\, A = 0$ as $\det(I + \epsilon A) = 1 + \epsilon\, \mathrm{tr}\, A + O(\epsilon^2)$. Consequently $SL(n, \mathbb{R})$ is $n^2 - 1$ dimensional. The dimension of $SU(n)$ is also $n^2 - 1$, so $SU(2)$ is three dimensional as a manifold.

The vectors lying in the tangent space at the identity element make up the **Lie algebra** of the group. We say that the Lie group is generated by its Lie algebra.

Example: $SU(2)$
The Taylor expansion of $\hat{R}_{\vec{n}}(\theta) \in SU(2)$ to the first order in small $\theta = \epsilon$ is

$$\hat{R}_{\vec{n}}(\epsilon) = e^{-i\epsilon\, \vec{n}\, .\, \vec{\sigma}\, /2} = \hat{I} - i\epsilon \left(n_x\, \frac{\sigma_x}{2} + n_y\, \frac{\sigma_y}{2} + n_z\, \frac{\sigma_z}{2} \right) + O(\epsilon^2)$$

where the expression in the bracket on r.h.s. is an element of the $su(2)$ algebra and $T_a = \frac{\sigma_a}{2}$ where $a = x, y, z$ are its generators.

More generally, the Lie algebra generators can be obtained from the group elements $g \in G$ directly. In our case, we introduce $\vec{\theta} = \theta\ \vec{n} = (\theta n_x, \theta n_y, \theta n_z) = (\theta_x, \theta_y, \theta_z)$ and identify $g\left(\vec{\theta}\right) = \hat{R}_{\vec{n}}(\theta)$. The generators are then obtained by through the following expression

$$T_a = i\ g^{-1}\left(\vec{\theta}\right)\ \frac{\partial g\left(\vec{\theta}\right)}{\partial \theta_a}$$

Explicitely:

$$\begin{aligned}
T_x &= i\ e^{i\left(\theta_x\sigma_x + \theta_y\sigma_y + \theta_z\sigma_z\right)\ /\ 2}\ \frac{\partial}{\partial\theta_x} e^{-i\left(\theta_x\sigma_x + \theta_y\sigma_y + \theta_z\sigma_z\right)\ /\ 2} = \frac{\sigma_x}{2} \\
T_y &= i\ e^{i\left(\theta_x\sigma_x + \theta_y\sigma_y + \theta_z\sigma_z\right)\ /\ 2}\ \frac{\partial}{\partial\theta_y} e^{-i\left(\theta_x\sigma_x + \theta_y\sigma_y + \theta_z\sigma_z\right)\ /\ 2} = \frac{\sigma_y}{2} \\
T_z &= i\ e^{i\left(\theta_x\sigma_x + \theta_y\sigma_y + \theta_z\sigma_z\right)\ /\ 2}\ \frac{\partial}{\partial\theta_z} e^{-i\left(\theta_x\sigma_x + \theta_y\sigma_y + \theta_z\sigma_z\right)\ /\ 2} = \frac{\sigma_z}{2}
\end{aligned}$$

The generators of $su(2)$ algebra are indeed similar to the operators for components of the spin angular momentum of a spin-1/2 particle, up to the scaling by $\hbar$.

They also satisfy the same commutation, known as the **Lie bracket**,

$$[T_a, T_b] \;=\; i\epsilon_{abc}\, T_c$$

where ϵ_{abc} is the Levi-Civita tensor.

The Lie bracket is antisymmetric, $[X, Y] = -[Y, X]$, linear, $[\lambda X + \mu Y, Z] = \lambda [X, Z] + \mu [Y, Z]$, and obeys the Jacobi identity $[[X, Y], Z] + [[Y, Z], X] + [[Z, X], Y] = 0$.

The generators T_a satisfy the following anticommutation relations:

$$\{T_a, T_b\} \;=\; \delta_{ab}\, \hat{I}$$

Single-qubit operations are in $U(2)$

$U(2)$ is the group of 2-by-2 unitary matrices or operators. In contrast to the elements $SU(2)$, the determinant of the elements of the group $u \in U(2)$ is not fixed to unity. Each element $u \in U(2)$ can be expressed in terms of an element of $SU(2)$ as

$$u = e^{i\alpha} g$$

where $g \in SU(2)$. The exponential function involving $\alpha \in \mathbb{R}$ will shift a global phase of the qubit state. To see this we rewrite the exponential term as $e^{i\alpha} = \left(e^{i\alpha}\hat{I}\right)$. Considering the determinant of the product of two n-by-n matrices A and B, $\det(AB) = \det A \det B$, and the determinant $\det\left(e^{i\alpha}\hat{I}\right) = e^{i2\alpha}$ we obtain the map from the elements of $U(2)$ and $SU(2)$

$$g = \frac{u}{\sqrt[2]{\det u}}$$

In general, for $u \in U(n)$ we get $g = u/\sqrt[n]{\det u}$ with $g \in SU(n)$.

Examples:

(i) Phase flip

$$\hat{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = i \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = e^{i\pi/2} \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = e^{i\pi/2} e^{-i\pi\sigma_z/2}$$

The nontrivial term $e^{-i\pi\sigma_z/2}$ on r.h.s. can be implemented via quantum evolution under the Hamiltonian $\hat{H} = \hbar\omega\sigma_z/2$ for time of the duration given by $t = \pi/\omega$:

$$\hat{U}_{t=\pi/\omega} = e^{-\frac{i}{\hbar}\hat{H}t} = e^{-i\,\omega\,\frac{\pi}{\omega}\,\sigma_z/2} = e^{-i\pi\sigma_z/2}$$

(ii) Bit flip

$$\hat{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = e^{i\pi/2} \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} = e^{i\pi/2} e^{-i\pi\sigma_x/2} = e^{i\pi/2} \begin{pmatrix} \cos\pi/2 & -i\sin\pi/2 \\ -i\sin\pi/2 & \cos\pi/2 \end{pmatrix}$$

(iii) Phase-bit fip $\hat{Y}$

$$\hat{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = e^{i\pi/2} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = e^{i\pi/2} e^{-i\pi\sigma_y/2} = e^{i\pi/2} \begin{pmatrix} \cos\pi/2 & -\sin\pi/2 \\ \sin\pi/2 & \cos\pi/2 \end{pmatrix}$$

The operations above can be implemented via evolution under the appropriate Hamiltonian operators for proper duration of time.

(iv) $\hat{S} = \sqrt{\hat{Z}}$

$$\hat{S} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = e^{i\pi/4} \begin{pmatrix} e^{-i\pi/4} & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} = e^{i\pi/4} e^{-i\pi\sigma_z/4}$$

where $e^{i\pi/4} = \sqrt{\det \hat{S}}$.

(v) $\hat{T} = \sqrt{\hat{S}}$

$$\hat{T} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} = e^{i\pi/8} \begin{pmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{pmatrix} = e^{i\pi/8} e^{-i\pi\sigma_z/8}$$

where $e^{i\pi/8} = \sqrt{\det \hat{T}}$.

(vi) Hadamard gate

$$\begin{aligned}
\hat{H} &= \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} = e^{i\pi/2} \begin{pmatrix} \frac{e^{-i\pi/2}}{\sqrt{2}} & \frac{e^{-i\pi/2}}{\sqrt{2}} \\ \\ \frac{e^{-i\pi/2}}{\sqrt{2}} & -\frac{e^{i\pi/2}}{\sqrt{2}} \end{pmatrix} \\
&= e^{i\pi/2} \left[\cos\frac{\pi}{2} - i \sin\frac{\pi}{2} \left(\frac{\sigma_x + \sigma_z}{\sqrt{2}} \right) \right] \\
&= e^{i\pi/2} e^{-i\pi \left(\frac{\sigma_x + \sigma_z}{\sqrt{2}} \right)/2}
\end{aligned}$$

where $n_x = n_z = \frac{1}{\sqrt{2}}$.

Two-qubit gates are in $U(4)$

$U(4)$ is the group of unitary 4-by-4 matrices or operators. Similarly to the single-qubit gates, they can be expressed in terms of $SU(4)$

$$U(4) = U(1) \otimes SU(4)$$

where $U(1)$ is the group of complex numbers of the unit modulus, $e^{i\alpha}$, and $SU(4)$ is the group of unitary 4-by-4 matrices of the unit determinant.

$SU(4)$ Lie group and $su(4)$ algebra

The SU(4) group is 15-dimensional: $n^2 - 1 = 15$.

Each element of $SU(4)$ can be expressed as a complex exponential function of an element of the $su(4)$ algebra

$$e^{-i \sum_{ab} \theta_{ab} T_{ab}}$$

where T_{ab} are the generators of $su(4)$ algebra. They naturally split into two sets.

(i) Generators of local, single-qubit, operations

$$T_{a0} \;:\; T_{x0} = \frac{\sigma_x \otimes \hat{I}}{2},\;\; T_{y0} = \frac{\sigma_y \otimes \hat{I}}{2},\;\; T_{z0} = \frac{\sigma_z \otimes \hat{I}}{2}$$
$$T_{0a} \;:\; T_{0x} = \frac{\hat{I} \otimes \sigma_x}{2},\;\; T_{0y} = \frac{\hat{I} \otimes \sigma_y}{2},\;\; T_{0z} = \frac{\hat{I} \otimes \sigma_z}{2}$$

The generators from the first set commute with those of the second set. Each of these sets, generates a subgroup $SU(2)$, and thus together they generate the subgroup of all single qubit operations, over the first and second qubit, in the $SU(4)$ group:

$$SU(2) \otimes SU(2) \subset SU(4)$$

(ii) Generators of nonlocal operations

$$T_{ab} = \frac{\sigma_a \otimes \sigma_b}{2}$$

where $a, b = x, y, z$, giving the remaining nine generators:

$$T_{xx},\ \ T_{xy},\ \ T_{xz},\ \ T_{yx},\ \ T_{yy},\ \ T_{yz},\ \ T_{zx},\ \ T_{zy},\ \ T_{zz}$$

Physically these nonlocal generators originate from interaction between qubits. Their presence in the system Hamiltonian in general leads to time evolution that affects the state of both qubits and leads to changes of entanglement between both qubit.

The Lie brackets of all generators

$[T_{ij}, T_{kl}]$	T_{x0}	T_{y0}	T_{z0}	T_{0x}	T_{0y}	T_{0z}	T_{xx}	T_{xy}	T_{xz}	T_{yx}	T_{yy}	T_{yz}	T_{zx}	T_{zy}	T_{zz}
T_{x0}	0	T_{z0}	$-T_{y0}$	0	0	0	0	0	0	T_{zx}	T_{zy}	T_{zz}	$-T_{yx}$	$-T_{yy}$	$-T_{yz}$
T_{y0}	$-T_{z0}$	0	T_{x0}	0	0	0	$-T_{zx}$	$-T_{zy}$	$-T_{zz}$	0	0	0	T_{xx}	T_{xy}	T_{xz}
T_{z0}	T_{y0}	$-T_{x0}$	0	0	0	0	T_{yx}	T_{yy}	T_{yz}	$-T_{xx}$	$-T_{xy}$	$-T_{xz}$	0	0	0
T_{0x}	0	0	0	0	T_{0z}	$-T_{0y}$	0	T_{xz}	$-T_{xy}$	0	T_{yz}	$-T_{yy}$	0	T_{zz}	$-T_{zy}$
T_{0y}	0	0	0	$-T_{0z}$	0	T_{0x}	$-T_{xz}$	0	T_{xx}	$-T_{yz}$	0	T_{yx}	$-T_{zz}$	0	T_{zx}
T_{0y}	0	0	0	T_{0y}	$-T_{0x}$	0	T_{xy}	$-T_{xx}$	0	T_{yy}	$-T_{yx}$	0	T_{zy}	$-T_{zx}$	0
T_{xx}	0	T_{zx}	$-T_{yx}$	0	T_{xz}	$-T_{xy}$	0	T_{0z}	$-T_{0y}$	T_{z0}	0	0	$-T_{y0}$	0	0
T_{xy}	0	T_{zy}	$-T_{yy}$	$-T_{xz}$	0	T_{xx}	$-T_{0z}$	0	T_{0x}	0	T_{z0}	0	0	$-T_{y0}$	0
T_{xz}	0	T_{zz}	$-T_{yz}$	T_{xy}	$-T_{xx}$	0	T_{0y}	$-T_{0x}$	0	0	0	T_{z0}	0	0	$-T_{y0}$
T_{yx}	$-T_{zx}$	0	T_{xx}	0	T_{yz}	$-T_{yy}$	$-T_{z0}$	0	0	0	T_{0z}	$-T_{0y}$	T_{x0}	0	0
T_{yy}	$-T_{zy}$	0	T_{xy}	$-T_{yz}$	0	T_{yx}	0	$-T_{z0}$	0	$-T_{0z}$	0	T_{0x}	0	T_{x0}	0
T_{yz}	$-T_{zz}$	0	T_{xz}	T_{yy}	$-T_{yx}$	0	0	0	$-T_{z0}$	T_{0y}	$-T_{0x}$	0	0	0	T_{x0}
T_{zx}	T_{yx}	$-T_{xx}$	0	0	T_{zz}	$-T_{zy}$	T_{y0}	0	0	$-T_{x0}$	0	0	0	T_{0z}	$-T_{0y}$
T_{zy}	T_{yy}	$-T_{xy}$	0	$-T_{zz}$	0	T_{zx}	0	T_{y0}	0	0	$-T_{x0}$	0	$-T_{0z}$	0	T_{0x}
T_{zz}	T_{yz}	$-T_{xz}$	0	T_{zy}	$-T_{zx}$	0	0	0	T_{y0}	0	0	$-T_{x0}$	T_{0y}	$-T_{0x}$	0

Cartan decomposition of $SU(4)$

Every unitary operation $U \in SU(4)$ can be expressed using the Cartan decomposition

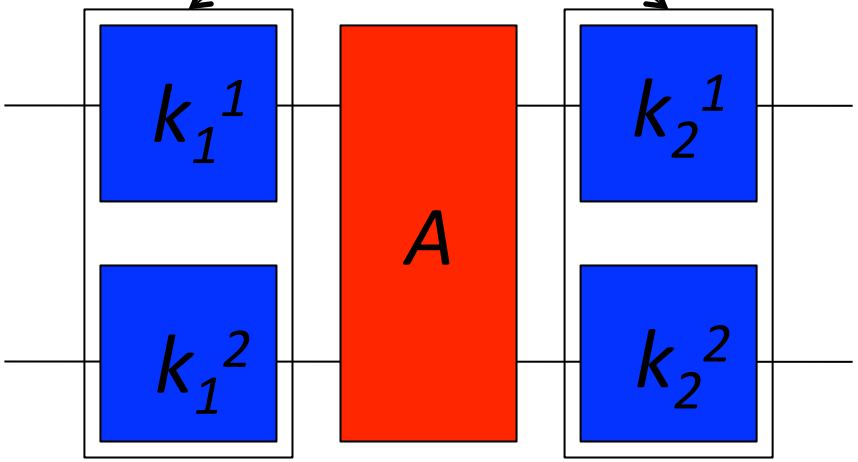
$$U \;=\; k_1\, A\, k_2 = k_1\, e^{\frac{i}{2}\left(c_1\, \sigma_x^1\sigma_x^2 + c_2\, \sigma_y^1\sigma_y^2 + c_3\, \sigma_z^1\sigma_z^2 \right)} k_2$$

where $k_1, k_2 \in SU(2) \otimes SU(2)$ are local gates. The part A embodies purely non-local content of the operation U and is generated by the maximal Abelian subalgebra of $SU(4)$ taht is spanned by the generators T_{xx}, T_{yy}, and T_{zz}.

The Cartan decomposition is indispensable in classification of the two-qubit operations according to their non-local content.

$$U \in SU(4)$$

$$U = k_1 A k_2 = k_1 e^{\frac{i}{2}\left(c_1 \sigma_x^1\sigma_x^2 + c_2 \sigma_y^1\sigma_y^2 + c_3 \sigma_z^1\sigma_z^2 \right)} k_2$$



$$k_1,\ k_2 \in SU(2) \otimes SU(2)$$

Parameter counting:

6 + 3 + 6 = 15 = $4^2 - 1$

If two gates have the same *A* in the Cartan decomposition, they are locally equivalent:

$$U_1 = k_1 U_2 k_2$$

Local equivalence classes and the Weyl chamber

The Cartan decomposition contains extra symmetries, including interchanges of c_1 c_2 and c_3 with and without sign flips. These can be removed using theory of local invariants and Weyl reflection symmetries. This allows us to classify the two-qubit operations in terms of their local equivalence classes.

We say the operations U_1 and U_2 are **locally equivalent** if U_1 and U_2 are related by local, i.e. single qubit operations: $U_1 = k_1 U_2 k_2$.

The set of all operations that are locally equivalent forms **local equivalence class**.

The set of all local equivalence classes forms the coset

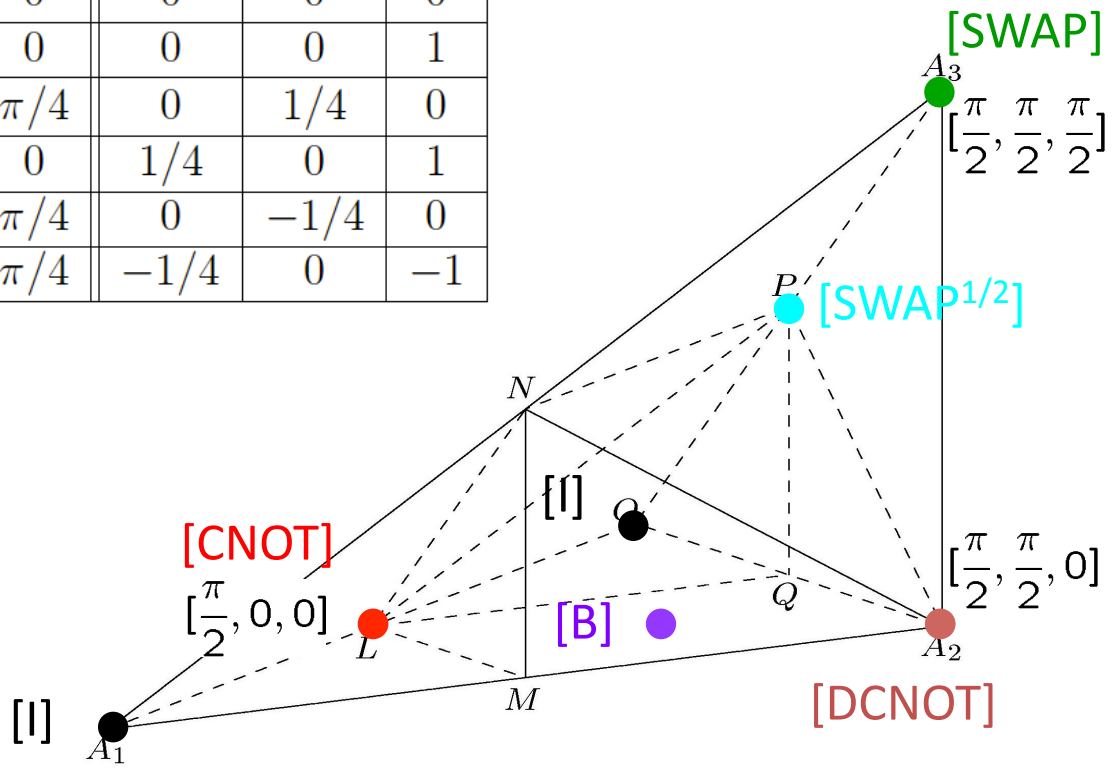
$$SU(4)/SU(2) \otimes SU(2).$$

Example: Several elements of the local equivalence class $[CNOT]$

$$U_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad U_{CPHASE} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \quad U_{Q} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & i & i & 0 \\ 0 & 1 & -1 & 0 \\ i & 0 & 0 & -i \end{pmatrix}$$

Examples:

point (gate)	c_1	c_2	c_3	g_1	g_2	g_3
O, A_1 ($[\mathbb{1}]$)	0, π	0	0	1	0	3
A_2 ([DCNOT])	$\pi/2$	$\pi/2$	0	0	0	-1
A_3 ([SWAP])	$\pi/2$	$\pi/2$	$\pi/2$	-1	0	-3
B ([B-Gate])	$\pi/2$	$\pi/4$	0	0	0	0
L ([CNOT])	$\pi/2$	0	0	0	0	1
P ($[\sqrt{\text{SWAP}}]$)	$\pi/4$	$\pi/4$	$\pi/4$	0	$1/4$	0
Q, M	$\pi/4$, $3\pi/4$	$\pi/4$	0	$1/4$	0	1
N	$3\pi/4$	$\pi/4$	$\pi/4$	0	$-1/4$	0
R	$\pi/2$	$\pi/4$	$\pi/4$	$-1/4$	0	-1



Universal set of quantum computing operations

Universal set of quantum computing gates is the set of operations that allows us to implement any computable function, i.e. any quantum computation algorithm or any unitary operation over n qubits, on a quantum computer.

Universality in quantum computation means the ability to generate an arbitrary element of the group of special unitary operations over n qubits, that is, an arbitrary element of the group $SU(2^n)$.

Solovay-Kitaev theorem

Given a set of gates that is dense in $SU(2^n)$ and closed under hermitian conjugation, any gate $U \in SU(2^n)$ can be approximated to an accuracy ϵ with a sequence of poly[log(1/ϵ)] gates from the set.

Universal quantum computation can be realized by a circuit of two-qubit and single-qubit gates from a universal set.

Examples of universal sets:

(i) Continuous: $SU(2)$ over any qubit, and $CNOT$ on any pair of qubits.
(ii) Discrete (approximation): Hadamard, phase flip $\hat{Z}$, $\hat{T}$, $CNOT$.

QUANTUM MECHANICS FOUNDATIONS OF QUANTUM INFORMATION PROCESSING

MEASUREMENT

FOURTH POSTULATE
(Measurement I)

The only possible result of the measurement of a physical quantity $\mathcal{A}$ is one of the eigenvalues of the corresponding observable $\hat{A}$.

FIFTH POSTULATE
(Measurement II)

1. a discrete non-degenerate spectrum:
   When the physical quantity $\mathcal{A}$ is measured on a system in the normalized state $|\psi\rangle$, the probability $\mathcal{P}(a_n)$ of obtaining the non-degenerate eigenvalue a_n of the corresponding physical observable $\hat{A}$ is

$$\mathcal{P}(a_n) = |\langle u_n|\psi\rangle|^2$$

   where $|u_n\rangle$ is the normalised eigenvector of $\hat{A}$ associated with the eigenvalue a_n.

2. a discrete spectrum:

$$\mathcal{P}(a_n) = \sum_{i=1}^{g_n} \left|\langle u_n^i|\psi\rangle\right|^2$$

where g_n is the degree of degeneracy of a_n and $\{|u_n^i\rangle\}$ $(i = 1, \ldots, g_n)$ is an orthonormal set of vectors which forms a basis in the eigenspace $\mathcal{H}_n$ associated with the eigenvalue a_n of the observable $\hat{A}$.

3. a continuous spectrum:
   the probability $\mathrm{d}\mathcal{P}(\alpha)$ of obtaining result included between α and $\alpha + \mathrm{d}\alpha$ is

$$\mathrm{d}\mathcal{P}(\alpha) \quad = \quad |\langle v_\alpha|\psi\rangle|^2 \, \mathrm{d}\alpha$$

   where $|v_\alpha\rangle$ is the eigenvector corresponding to the eigenvalue α of the observable $\hat{A}$.

SIXTH POSTULATE
(Measurement III)

If the measurement of the physical quantity $\mathcal{A}$ on the system in the state $|\psi\rangle$ gives the result a_n, the state of the system immediately after the measurement is the mormalized projection

$$\frac{\hat{P}_n|\psi\rangle}{\sqrt{\langle\psi|\hat{P}_n|\psi\rangle}} = \frac{\hat{P}_n|\psi\rangle}{\left\|\hat{P}_n|\psi\rangle\right\|}$$

of $|\psi\rangle$ onto the eigensubspace associated with a_n.

General measurement

Measurement is defined by the set of measurement operators $\{\hat{M}_m\}$ where m refers to the measurement outcomes.

If the state of the system before the measurement is $|\phi\rangle$, then the probability that result m occurs is

$$p_m = \langle\phi|\hat{M}_m^\dagger \hat{M}_m|\phi\rangle$$

and the state after the measurement is

$$|\psi\rangle = \frac{\hat{M}_m|\phi\rangle}{||\hat{M}_m|\phi\rangle||} = \frac{\hat{M}_m|\phi\rangle}{\sqrt{\langle\phi|\hat{M}_m^\dagger \hat{M}_m|\phi\rangle}}$$

The measurement operators satisfy the completeness relation

$$\sum_m \hat{M}_m^\dagger \hat{M}_m = \hat{I}$$

which expresses the fact that the probabilities of of measurement results sum to unity

$$\sum_m \langle \phi | \hat{M}_m^\dagger \hat{M}_m | \phi \rangle = \sum_m p_m = 1$$

Distinguishing quantum states

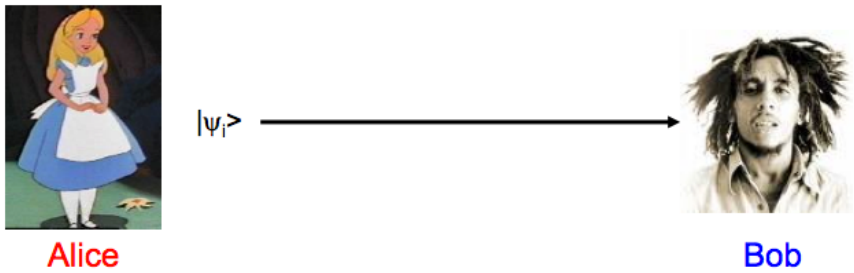
Two-parties game: Alice chooses a state $|\psi_i\rangle$, where $1 \leq i \leq n$, from some fixed set of states known to both parties, and sends it to Bob whose task is to identify it.

If the states $\{|\psi_i\rangle\}$ are **orthogonal** than Bob can perform a quantum measurement to distinguish the states: Bob has to define the measurement operators

$$\begin{aligned} \hat{M}_i &= |\psi_i\rangle\langle\psi_i| \\ \hat{M}_0 &= \sqrt{\hat{I} - \sum_{i\neq 0} |\psi_i\rangle\langle\psi_i|} \qquad \text{(positive square-root)} \end{aligned}$$

which satisfy the completeness relation and thus can be used to distinguish the state.

If the states $\{|\psi_i\rangle\}$ are **non-orthogonal** than there is no quantum measurement to reliably distinguish the states.



Projective measurement

A projective measurement is described by an observable $\hat{M}$, a self-adjoint operator on a state space of the system which is being observed. The observable has the spectral decomposition

$$\hat{M} = \sum_m \lambda_m \hat{P}_m$$

where $\hat{P}_m$ is the projector onto the eigenspace of $\hat{M}$ associated with the eigenvalue λ_m.

The possible outcomes of the measurement correspond to the eigenvalues λ_m of the observable $\hat{M}$.

If the state of the system before the measurement is $|\phi\rangle$, then the probability that the result λ_m occurs is

$$p_m = \langle\phi|\hat{P}_m^\dagger \hat{P}_m|\phi\rangle = \langle\phi|\hat{P}_m^2|\phi\rangle = \langle\phi|\hat{P}_m|\phi\rangle$$

and the state immediately after the measurement is

$$|\psi\rangle = \frac{\hat{P}_m|\phi\rangle}{||\hat{P}_m|\phi\rangle||} = \frac{\hat{P}_m|\phi\rangle}{\sqrt{\langle\phi|\hat{P}_m^\dagger \hat{P}_m|\phi\rangle}} = \frac{\hat{P}_m|\phi\rangle}{\sqrt{\langle\phi|\hat{P}_m|\phi\rangle}} = \frac{\hat{P}_m|\phi\rangle}{\sqrt{p_m}}$$

Projective measurement allows us to easily calculate the expectation value of an observable $\hat{M}$ for the system in the state $|\phi\rangle$

$$< \hat{M} >= \langle\phi|\hat{M}|\phi\rangle = \langle\phi|\left(\sum_m \lambda_m \hat{P}_m\right)|\phi\rangle = \sum_m \lambda_m \langle\phi|\hat{P}_m|\phi\rangle = \sum_m \lambda_m p_m$$

Heisenberg uncertainty relation

Let $\hat{A}$ and $\hat{B}$ be self-adjoint operators, and $|\phi\rangle$ be a quantum state.
Suppose $\langle\phi|\hat{A}\hat{B}|\phi\rangle = x + iy$, where $x, y \in \mathbb{R}$ and note that

$$\begin{aligned} \langle\phi|\left[\hat{A},\hat{B}\right]|\phi\rangle &= 2iy \\ \langle\phi|\left\{\hat{A},\hat{B}\right\}|\phi\rangle &= 2x \end{aligned}$$

This implies

$$\left|\langle\phi|\left[\hat{A},\hat{B}\right]|\phi\rangle\right|^2 + \left|\langle\phi|\left\{\hat{A},\hat{B}\right\}|\phi\rangle\right|^2 = 4\left|\langle\phi|\hat{A}\hat{B}|\phi\rangle\right|^2$$

By Cauchy-Schwarz inequality

$$\left|\langle\phi|\hat{A}\hat{B}|\phi\rangle\right|^2 \leq \langle\phi|\hat{A}^2|\phi\rangle\langle\phi|\hat{B}^2|\phi\rangle$$

and using the previous relation and dropping negative terms we get

$$\left|\langle\phi|\left[\hat{A},\hat{B}\right]|\phi\rangle\right|^2 \leq 4\langle\phi|\hat{A}^2|\phi\rangle\langle\phi|\hat{B}^2|\phi\rangle$$

Suppose $\hat{C}$ and $\hat{D}$ are two observables. Substituting $\hat{A} = \hat{C} - <\hat{C}>$ and $\hat{B} = \hat{D} - <\hat{D}>$ into the last equation, we obtain the Heisenberg uncertainty relation

$$\Delta(\hat{C})\Delta(\hat{D}) \geq \frac{\left|\langle\phi|\left[\hat{C},\hat{D}\right]|\phi\rangle\right|}{2}$$

where $\Delta(\hat{C}) = \sqrt{<\hat{C}^2> - <\hat{C}>^2} = \sqrt{\langle\phi|\hat{C}^2|\phi\rangle - \langle\phi|\hat{C}|\phi\rangle^2}$ and $\Delta(\hat{D})$ is define similarly.

Example:

Consider the observables $\hat{X} = \sigma_x$ and $\hat{Y} = \sigma_y$ when measured for the qubit state $|0\rangle$.

We know, or we can easily calculate, that $\left[\hat{X}, \hat{Y}\right] = 2i\hat{Z}$, where $\hat{Z} = \sigma_z$, so the uncertainty relation is

$$\Delta(\hat{X})\Delta(\hat{Y}) \geq \frac{\left|\langle 0| \left[\hat{X}, \hat{Y}\right] |0\rangle\right|}{2} = \langle 0|\hat{Z}|0\rangle = 1$$

POVM measurements

Suppose a measurement described by the set of measurement operators $\{\hat{M}_m\}$ is performed upon a quantum system in the state $|\phi\rangle$.

Then the probability that result m occurs is $p_m = \langle\phi|\hat{M}^\dagger \hat{M}_m|\phi\rangle$.

Let us define

$$\hat{E}_m = \hat{M}_m^\dagger \hat{M}_m$$

then E_m is a positive operator such that

$$\sum_m \hat{E}_m = 1 \quad \text{and} \quad p_m = \langle\phi|\hat{E}_m|\phi\rangle$$

The set $\{E_m\}$ is known as a Positive Operator-Valued Measure or POVM.

The set of operators $\hat{E}_m$ which are known as POVM elements associated with the measurement, are sufficient to determine the probabilities of different measurement outcomes.

Example: Projective measurement

$$\hat{E}_m = \hat{P}_m$$

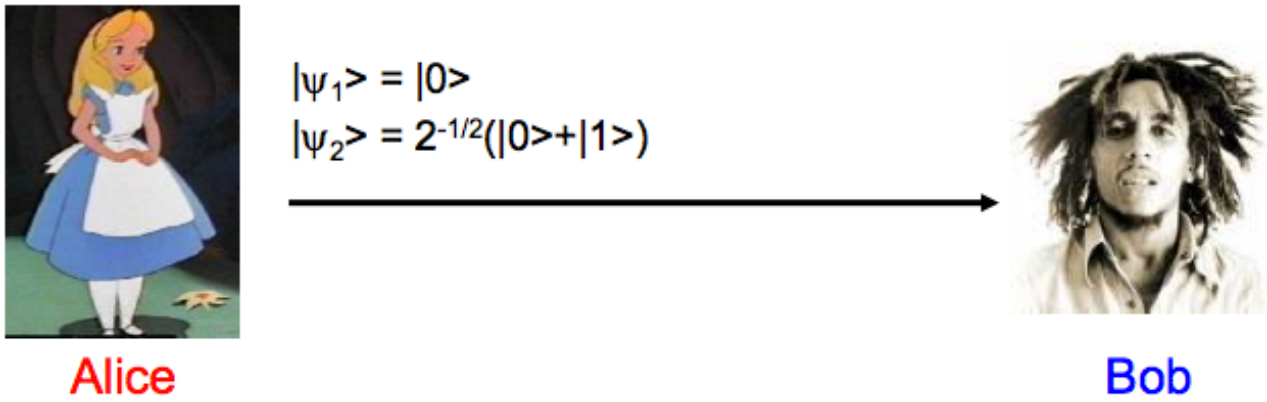
POVM measurement: example

Alice sends one of the states below

$$\begin{aligned} |\psi_1\rangle &= |0\rangle \\ |\psi_2\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \end{aligned}$$

to Bob who however can not distinguish them reliably as they are not orthogonal.

However, he can perform a measurement that distinguishes the states some of the time, and never makes an error of mis-identification.



Consider the POVM

$$\begin{aligned}
\hat{E}_1 &= \frac{\sqrt{2}}{1+\sqrt{2}}|1\rangle\langle 1| \\
\hat{E}_2 &= \frac{\sqrt{2}}{\left(1+\sqrt{2}\right)}\,\frac{|0\rangle - |1\rangle}{\sqrt{2}}\,\frac{\langle 0| - \langle 1|}{\sqrt{2}} \\
\hat{E}_3 &= \hat{I} - \hat{E}_1 - \hat{E}_2
\end{aligned}$$

If the result of the measurement is E_1, then the state was $|\psi_2\rangle$, and if the result E_2 occurs then the state was $|\psi_1\rangle$. Some of the time however, Bob will obtain the result E_3 from which he can infer nothing about the state.

Measurement and quantum circuit

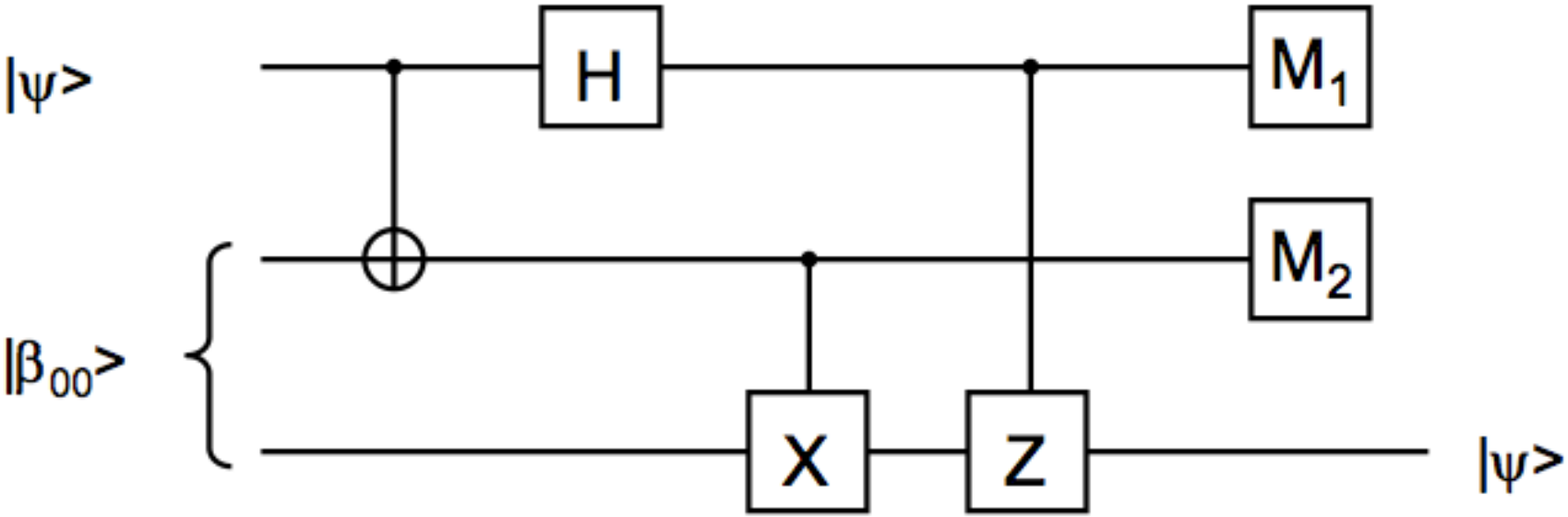
Principle of deferred measurement

Measurement can always be moved from an intermediate stage of a quantum circuit to the end of the circuit; if the measurement results are used at any stage of the circuit then the classically controlled operations can be replaced by conditional quantum operations.

Principle of implicit measurement

Without loss of generality, any unterminated quantum wires, that is, qubits that are not measured, at the end of a quantum circuit may be assumed to be measured.

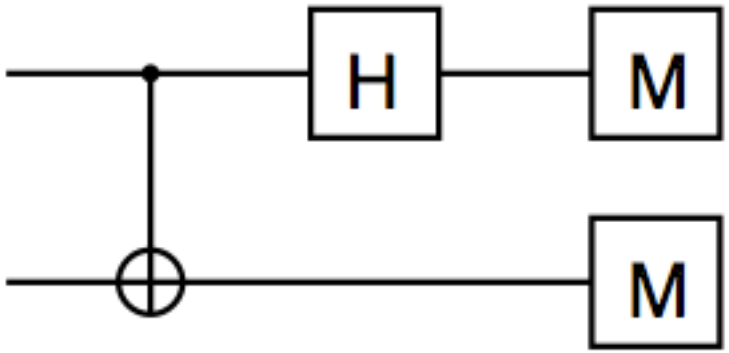
Example: Principle of deferred measurement in quantum teleportation circuit



Measurement in other then computational basis

Recipe:
first unitarily transform from the basis you wish to perform a measurement in to the computational basis, and then measure qubits in the computational basis.

Example: Measurement in the Bell basis in the superdense coding protocol



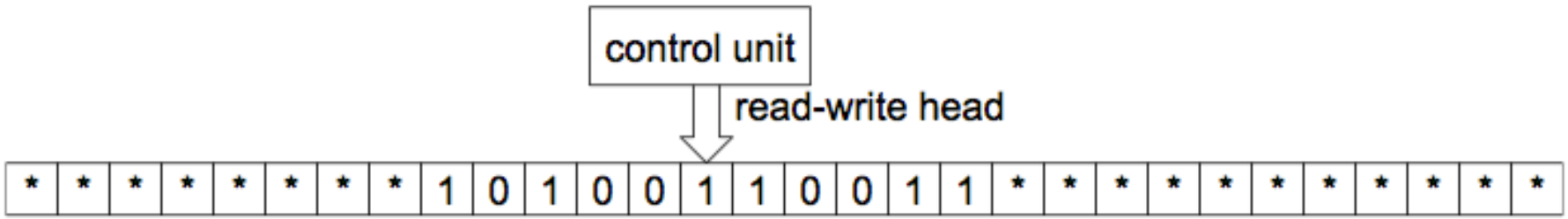
CLASSICAL AND QUANTUM COMPUTATION

COMPUTATIONAL COMPLEXITY CLASSES

Deterministic computation and deterministic Turing machine

Turing machine consists of

1. a finite *alphabet* Σ containing the blank symbol $*$;
2. a 2-way infinite tape divided into cells, one of which is a special *starting cell*. Each cell contains a symbol from the alphabet Σ. All but a finite number of cells contain the special blank symbol $*$, denoting an empty cell;
3. *read-write head* that examines a single cell at a time and can move left $(\leftarrow)$ or right $(\rightarrow)$;
4. a *control unit* along with a finite set of states Γ including a distinguished starting state, γ_0, and a set of *halting states*.



The computation of a Turing machine is controlled by a *transition function*:

$$\delta : \quad \Gamma \times \Sigma \quad \rightarrow \quad \Gamma \times \Sigma \times \{\leftarrow, \rightarrow\}$$

Example: Unary addition Turing machine

States: $\Gamma = \{\gamma_0, \gamma_1, \gamma_2, \gamma_3\}$ with the starting state γ_0 and the halting state γ_3;

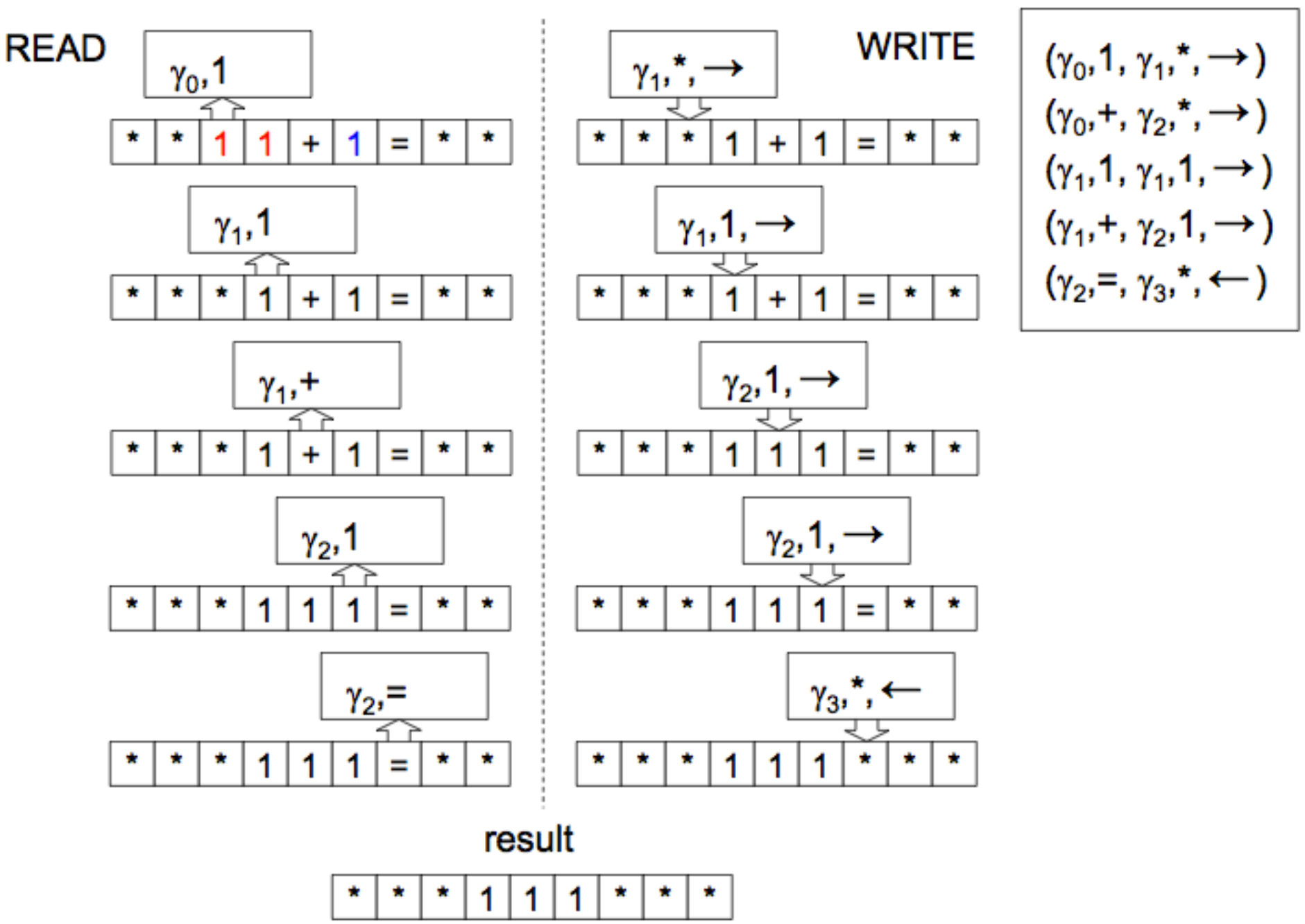
Alphabet: $\Sigma = \{*, 1, +, =\} = \Sigma_0 \cup \{*\}$ where Σ_0 is called external alphabet;

Input: integers $a, b \leq 0$ with the symbol + and =
(e.g. $2 + 1$ is written as '$11 + 1 =$' on the tape with the leftmost input symbol in the starting square);

Output: $a + b$ unary

Transition function:

$(\gamma_0, 1, \gamma_1, *, \rightarrow)$	$a \neq 0$, reading a
$(\gamma_0, +, \gamma_2, *, \rightarrow)$	$a = 0$, erase +, read b
$(\gamma_1, 1, \gamma_1, 1, \rightarrow)$	reading a
$(\gamma_1, +, \gamma_2, 1, \rightarrow)$	replace + by 1, read b
$(\gamma_2, =, \gamma_3, *, \leftarrow)$	finish reading b, erase =, halt


READ
WRITE
γ_0,1
γ_1,1
γ_1,+
γ_2,1
γ_2,=
γ_1,*,→
γ_1,1,→
γ_2,1,→
γ_2,1,→
γ_3,*,←
* * 1 1 + 1 = * *
* * * 1 + 1 = * *
* * * 1 1 1 = * *
* * * 1 1 1 * * *
(γ_0,1, γ_1,*, →)
(γ_0,+, γ_2,*, →)
(γ_1,1, γ_1,1, →)
(γ_1,+, γ_2,1, →)
(γ_2,=, γ_3,*, ←)
result
* * * 1 1 1 * * *

Computable functions and decidable predicates

Every Turing machine M computes a function

$$\phi_M : \Sigma_0^* \to \Sigma_0^*$$

where Σ_0^* is the set of all strings over Σ_0 (external alphabet). $\phi_M(x)$ is the output string for input x. The value of $\phi_M(x)$ is undefined if the computation never terminates.

A function $f : \Sigma_0^* \to \Sigma_0^*$ is *computable* if there exists a Turing machine M such that $\phi_M = f$. In this case we say f is computed by M.

A predicate is a function $L : \Sigma_0^* \to \{0.1\}$, a function with a Boolean value. A predicate is called *decidable* if this function is computable.

Church-Turing thesis

Any algorithm can be realized by a Turing machine.

A Turing machine is a finite object, so it can be encoded by a string. Then for any fixed alphabet Σ_0^*, we can consider a *universal Turing machine* U which computes the function

$$u([M], x) = \phi_M(x)$$

where $[M]$ is the encoding of a Turing machine M.

Complexity

A TM works in time $T(n)$ if it performs *at most* $T(n)$ steps for any input of size n.

A function/predicate F on $\mathbb{B}^*$, that is on binary strings, is *computable/decidable in polynomial time* if there exists a TM that computes it in time $T(n) = poly(n)$, where n is the input length.

A class of all functions (predicates) computable (decidable) in polynomial time is called P.

We say that these functions are efficiently solvable or tractable on deterministic Turing machine.

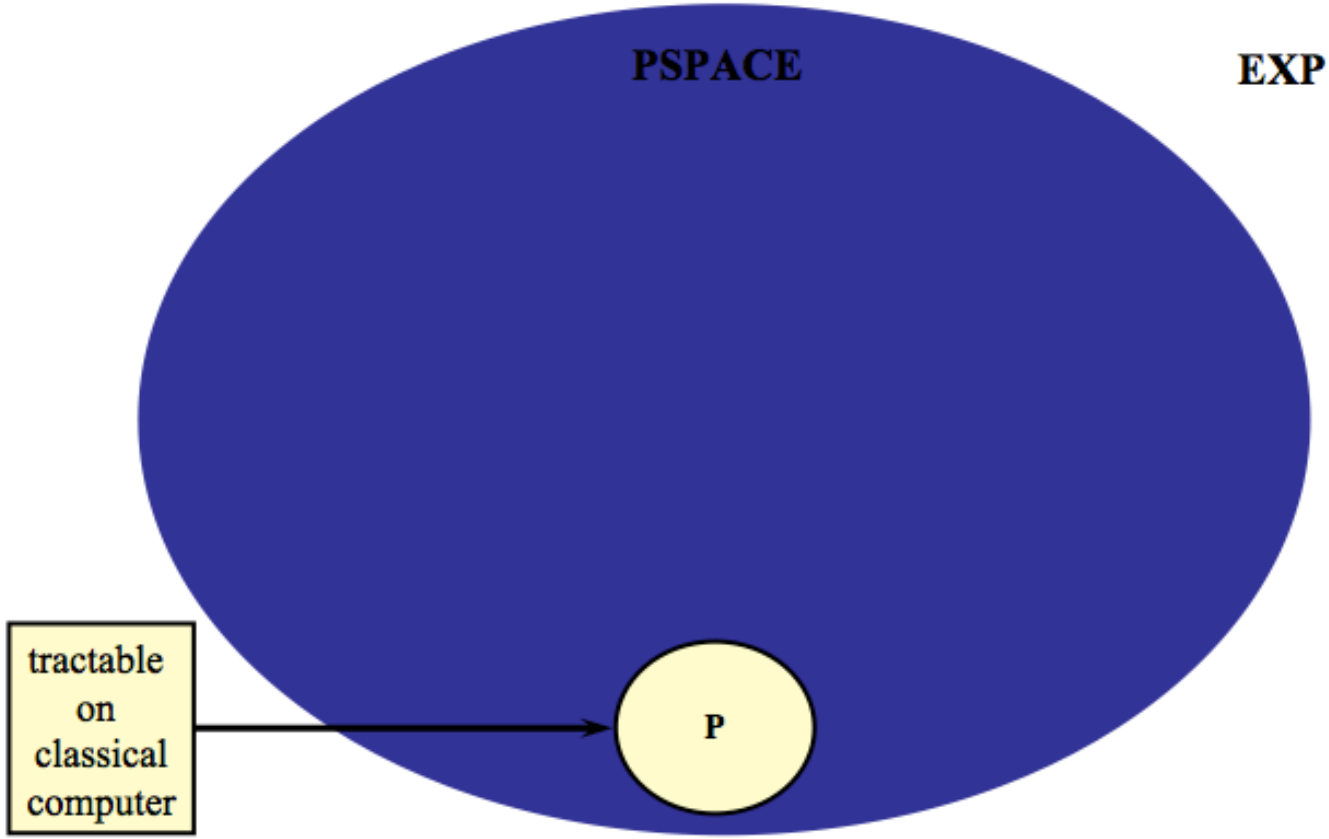
A TM works in space $s(n)$ if it visits at most $s(n)$ cells for any computation on inputs of size n.

A function (predicate) F on $\mathbb{B}^*$ is *computable (decidable) in polynomial space* if there exists a TM that computes F and runs in space $s(n) = poly(n)$ where n is the input length.

A class of all functions (predicates) computable (decidable) in polynomial space is called PSPACE.

P ⊆ PSPACE

It is generally believed that this inclusion is strict though this is an open question.



Non-deterministic computation

A non-deterministic Turing machine is a hypothetical machine that resembles a deterministic Turing machine but can non-deterministically choose one of several actions possible in a given configuration. **Its transition function is multivalued.**

A predicate L belongs to the **class NP, Non-deterministic Polynomial**, if there exist a non-deterministic Turing machine M and a polynomial $p(n)$ such that

$L(x) = 1 \quad \Rightarrow \quad$ there exists a computational path that gives the answer 'yes' in time $p(|x|)$, where $|x|$ is the size of the input;

$L(x) = 0 \quad \Rightarrow \quad$ there is no path with this property.

Alternative definition of the complexity class NP (Kitaev)

Imagine two persons: King Arthur (with polynomially bounded mental capabilities) and a wizard Merlin (intellectually omnipotent). Arthur is interested in $L(x)$. Merlin wants to convince Arthur that $L(x)$ is true, but Arthur does not trust Merlin (he is too smart to be loyal) and wants to make sure that $L(x)$ is true.

So Arthur arranges that, after both he and Merlin see input string x, Merlin writes a note to Arthur where he proves that $L(x)$ is true. Then Arthur verifies this proof by some polynomial proof-checking predicate (procedure)

$$R(x, y) = \text{"}y \text{ is a proof of } L(x)\text{"}$$

where $L(x) = 1$ if Merlin can convince Arthur that $L(x)$ is true by presenting some proof y such that $R(x, y)$, and $L(x) = 0$ whenever Merlin says that Arthur is not convinced: $R(x, y)$ is false for any y.

NP, NP hardness and NP completeness

A predicate L_1 is *reducible* to a predicate L_2 if there exists a function $f \in$ P such that $L_1(x) = L_2(x)$ for any input string x. We say $L_1 \propto L_2$.

Lemma: Let $L_1 \propto L_2$, then

(a) $L_2 \in$ P $\Rightarrow$ $L_1 \in$ P

(a) $L_2 \notin$ P $\Rightarrow$ $L_1 \notin$ P

(a) $L_2 \in$ NP $\Rightarrow$ $L_1 \in$ NP

Predicate L is NP-*hard* if any predicate in NP is reducible to it.

Predicate L is NP-*complete* if it is NP-hard and $L \in$ NP.

Example: SAT (satisfiability)

SAT(x) means that x is a propositional formula, containing Boolean variables and operations (negation, disjunction, conjunction) that is satisfiable, that is "true" for some values of the variables.

Cook-Levin Theorem:

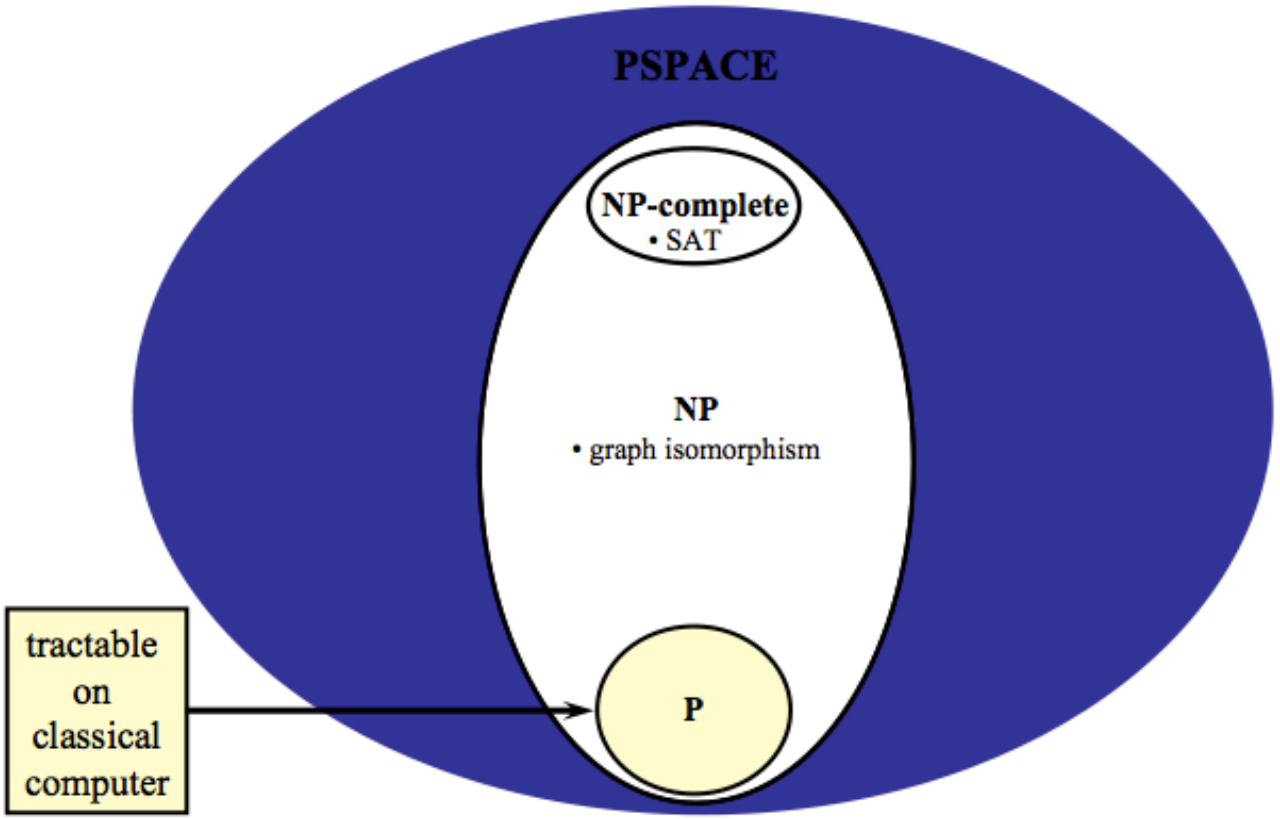
$$\text{SAT} \in \text{NP}$$
$$\text{SAT} \in \text{NP-complete}$$

Other examples: 3-COLORING, CLIQUE, ...

$P \subseteq NP \subseteq PSPACE$

Again it is believed that the inclusions are strict though this is an open question.

If you could prove that SAT $\in$ P, then you would resolve the problem P vs. NP which is one of the Millenium problems of the Clay Mathematics Institute with a prize of $ 1,000,000.



Probabilistic computation

A probabilistic Turing machine can probabilistically choose one of several actions possible in a given configuration. This is similar to a non-deterministic TM but the choice is made by coin tossing rather than guessing. PTM is in principle physical.

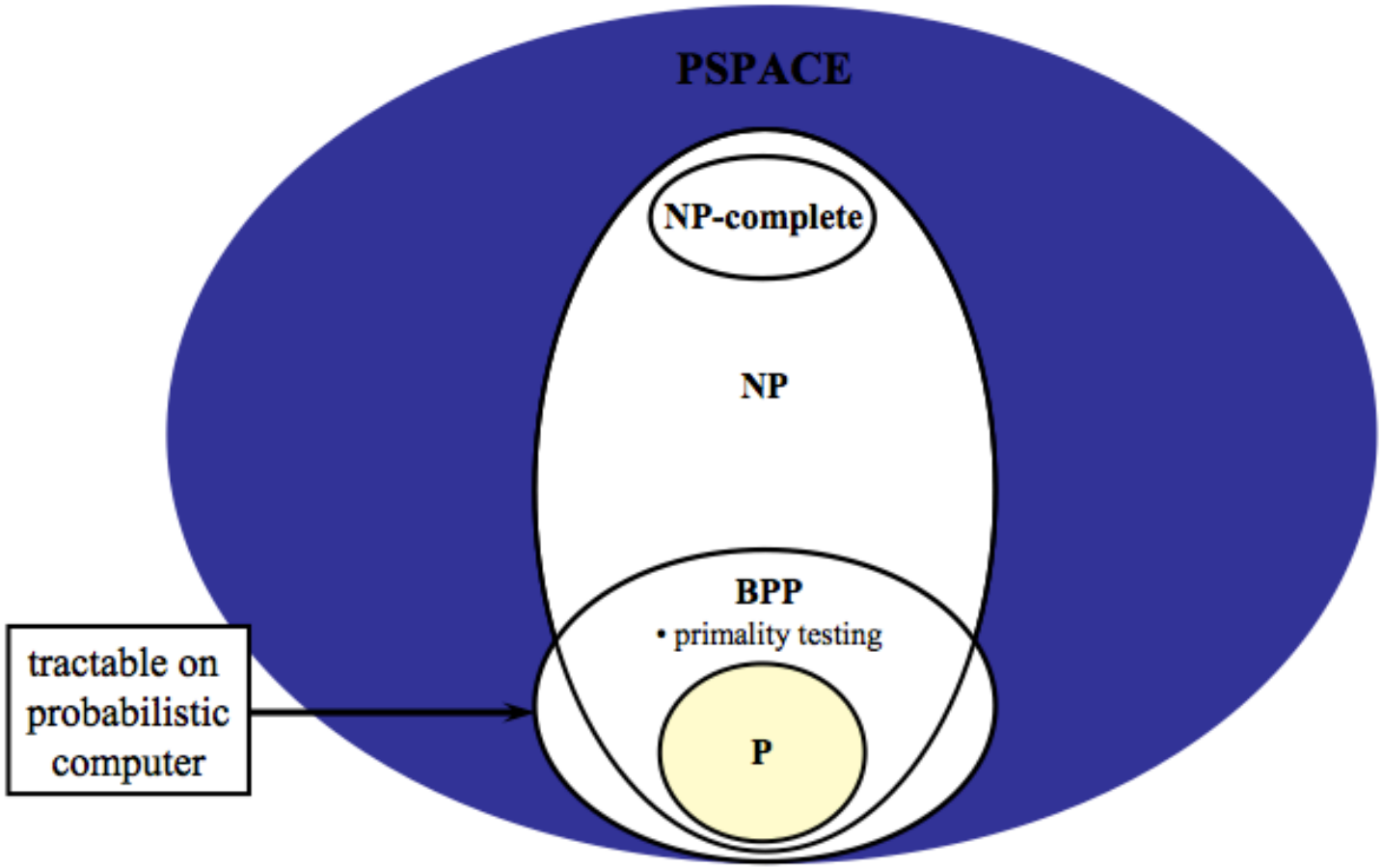
Let ϵ be a constant such that $0 < \epsilon < \frac{1}{2}$. A predicate L belongs to the **class BPP, Bounded-error Probabilistic Polynomial,** if there exists a probabilistic Turing machine M and a polynomial $p(n)$ such that the machine M running on input string x always terminates at most $p(|x|)$ steps, and

$L(x) = 1 \quad \Rightarrow \quad M$ gives the answer 'yes' with probability $\geq 1 - \epsilon$;

$L(x) = 0 \quad \Rightarrow \quad M$ gives the answer 'no' with probability $\leq \epsilon$.

Example: PRIMALITY, i.e. checking whether a given integer is a prime number.

P ⊆ BPP ⊆ PSPACE


PSPACE
NP-complete
NP
BPP
• primality testing
P
tractable on probabilistic computer

Quantum computation

A quantum Turing machine can choose a superposition of several actions in a given configuration. This is somewhat similar to a probabilistic TM.

Let ϵ be a constant such that $0 < \epsilon < \frac{1}{2}$. A predicate L belongs to the **class BQP, Bounded-error Quantum Polynomial,** if there exists a quantum Turing machine M and a polynomial $p(n)$ such that the machine M running on input string x always terminates at most $p(|x|)$ steps, and

$L(x) = 1 \quad \Rightarrow \quad M$ gives the answer 'yes' with probability $\geq 1 - \epsilon$;

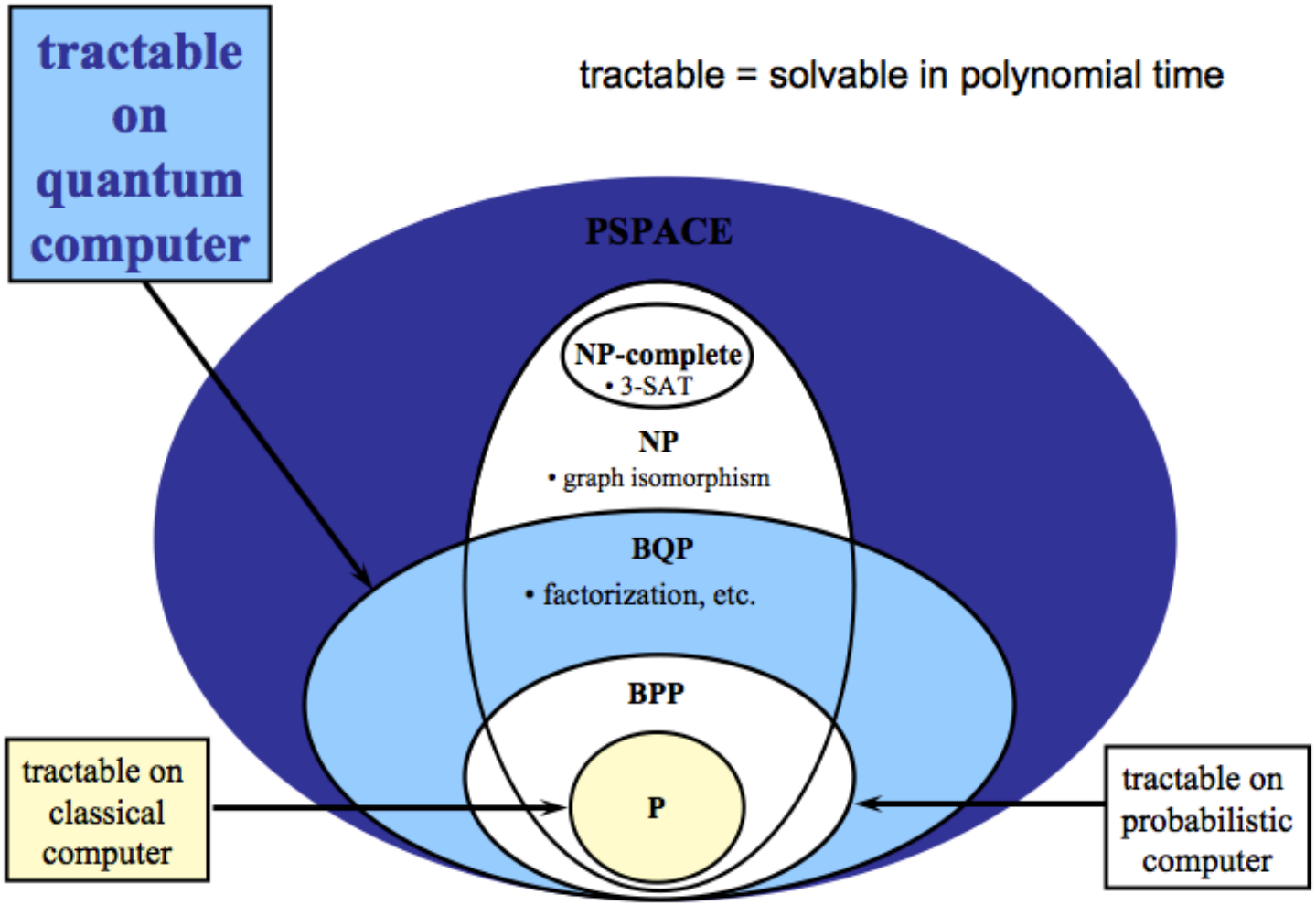
$L(x) = 0 \quad \Rightarrow \quad M$ gives the answer 'no' with probability $\leq \epsilon$.

Alternatively using quantum circuit:

A *quantum algorithm* for the computation of a function $F : \mathbb{B}^* \to \mathbb{B}^*$ is a classical algorithm, that is, a deterministic Turing machine, that computes a function of the form $x \mapsto Z(x)$ where $Z(x)$ is a description of a *quantum circuit* which computes $F(x)$ on empty input.

The function F is said to belong to the class BQP if there is a quantum algorithm that computes F in time $poly(n)$.

P ⊆ BPP ⊆ BQP ⊆ PSPACE



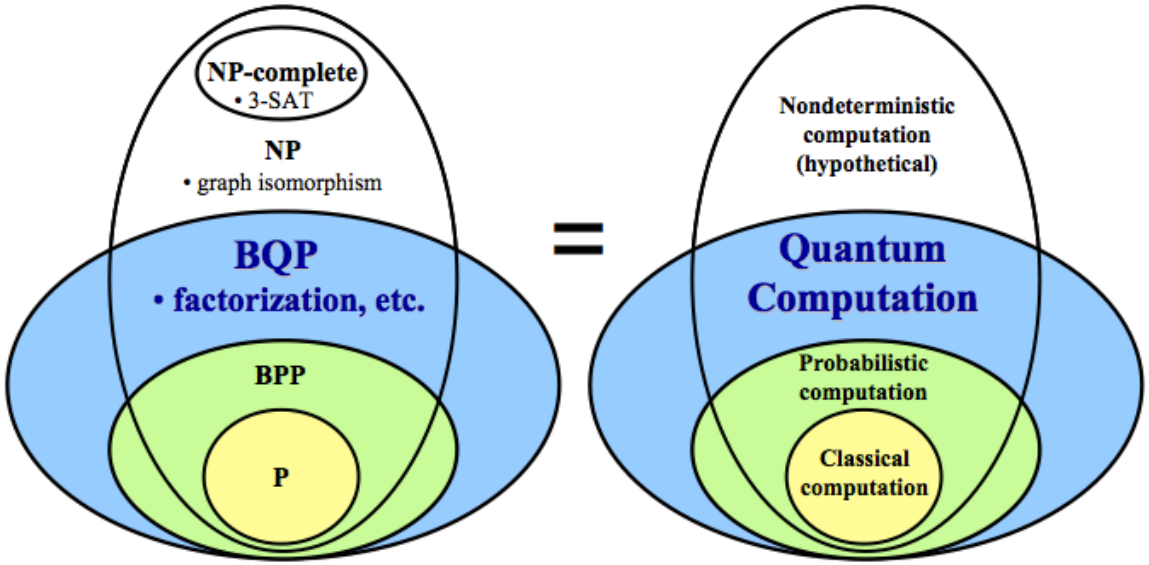
CLASSICAL AND QUANTUM COMPUTATION

QUANTUM ALGORITHMS

P ⊆ BPP ⊆ BQP ⊆ PSPACE

Complexity classes provide classification of computational problems according to their tractability using certain computational models, either conceptual or physical.

Quantum computation can efficiently solve problems that are not known to be tractable on a classical computer. It appears to be **fundamentally more powerful** than any classical computation.



Deutsch-Jozsa algorithm

It computes whether a Boolean function F over n variables is constant or balanced.
A Boolean function F over n variables is said to be

- *constant* if it gives the same output to all possible inputs;
- *balanced* if it outputs 0 for half of all possible inputs and 1 to the other half.

Examples:

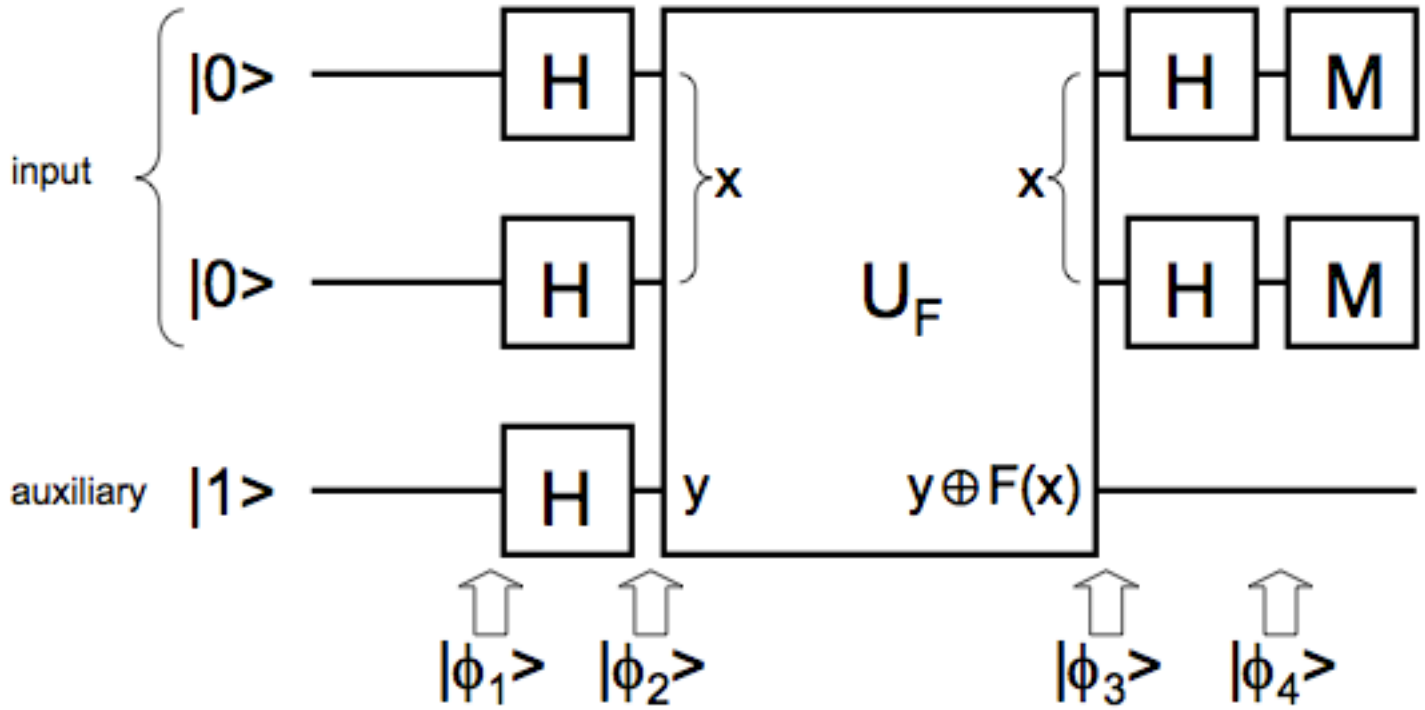
		Constant:		Balanced:					
x_1	x_2	$F(x_1,x_2)$		$F(x_1,x_2)$					
0	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	0	1	1	0
1	0	1	0	0	1	1	0	1	0
1	1	1	0	0	1	0	1	0	1

Classical complexity is exponential: in the worst case, the function needs to be applied $2^{n-1}+1$ times to check its output for more than a half of all inputs.

Deutsch-Jozsa algorithm for a two-qubit function

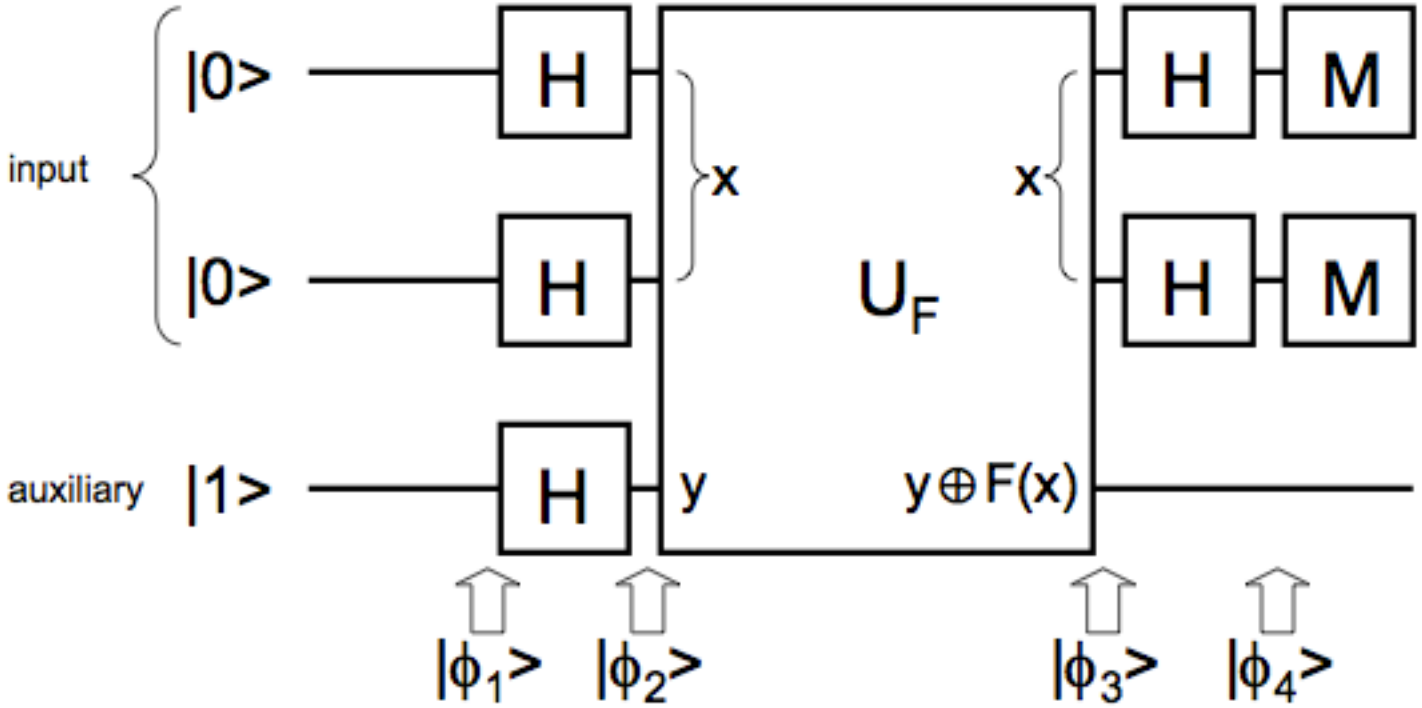
The initial state:

$$|\phi_1\rangle = |0\rangle \otimes |0\rangle \otimes |1\rangle = |001\rangle$$



Deutsch-Jozsa algorithm for a two-qubit function: Hadamard gates

$$
\begin{aligned}
|\phi_2\rangle &= \left(\hat{H}\otimes\hat{H}\otimes\hat{H}\right)(|0\rangle\otimes|0\rangle\otimes|1\rangle) = \hat{H}|0\rangle\otimes\hat{H}|0\rangle\otimes\hat{H}|1\rangle \\
&= \left[\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\right]\otimes\left[\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\right]\otimes\left[\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\right] \\
&= \frac{1}{2}(|00\rangle+|01\rangle+|10\rangle+|11\rangle)\otimes\left[\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\right]
\end{aligned}
$$



Hadamard gates: general n-qubit input

General n-qubit input state in the computational basis

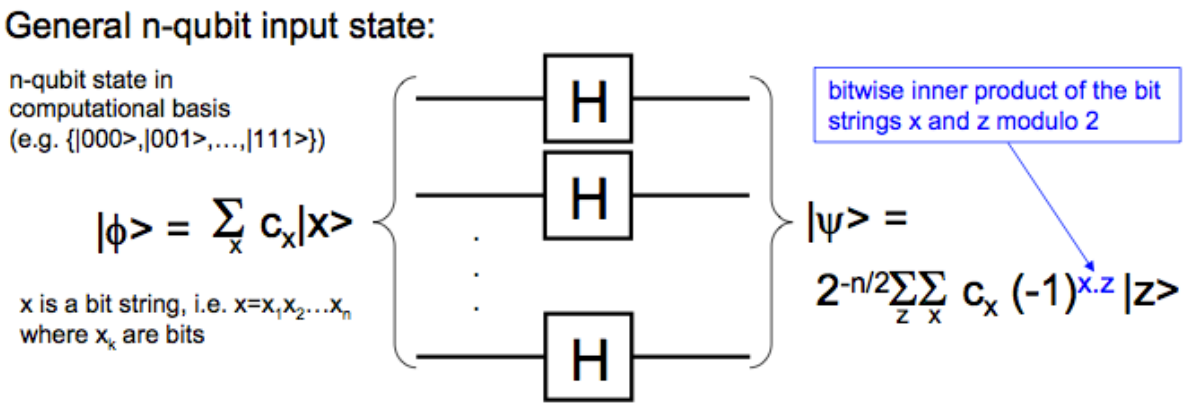
$$|\phi\rangle = \sum_{\mathbf{x}} c_{\mathbf{x}} |\mathbf{x}\rangle$$

where **x** is a bit string, $\mathbf{x} = x_1 x_2 \ldots x_n$, with the bits x_k.

The Hadamard rotations on each qubit transform the state as follows

$$|\psi\rangle = \hat{H}^{\otimes n} |\phi\rangle = \frac{1}{2^{n/2}} \sum_{\mathbf{z}} \sum_{\mathbf{x}} c_{\mathbf{x}} (-1)^{\mathbf{z}.\mathbf{x}} |\mathbf{z}\rangle$$

where $\mathbf{z}.\mathbf{x}$ is the bitwise inner product of the bit strings **z** and **x** modulo 2.



Example:

$$
\begin{aligned}
|\phi\rangle &= |001\rangle \\
|\psi\rangle &= \hat{H}^{\otimes 3} = \frac{1}{2^{3/2}} \sum_{\mathbf{z}} (-1)^{(0.z_1+0.z_2+1.z_3)(\mathrm{mod}\ 2)} |\mathbf{z} = z_1 z_2 z_3\rangle \\
&= \frac{1}{2^{3/2}} (|000\rangle - |001\rangle + |010\rangle - |011\rangle + |100\rangle - |101\rangle + |110\rangle - |111\rangle \\
&= \frac{1}{2} (|0\rangle + |01\rangle + |10\rangle + |11\rangle) \otimes \left[\frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right]
\end{aligned}
$$

Deutsch-Jozsa algorithm for a two-qubit function

$$\begin{aligned} |\phi_2\rangle &= \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right) \otimes \left[\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)\right] \\ &= \mathbf{x} \otimes \mathbf{y} \end{aligned}$$

For our example, let us choose the function F to be balanced:

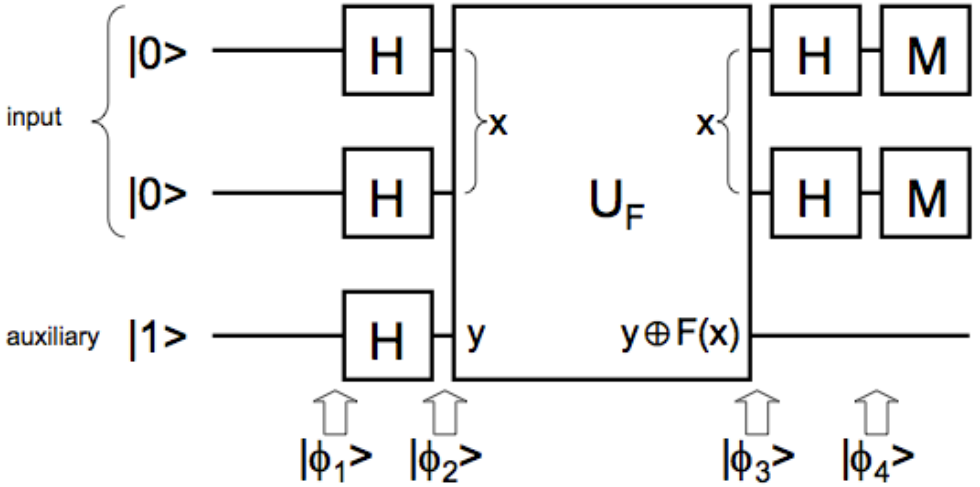
x_1	x_2	$F(x_1, x_2)$
0	0	0
0	1	1
1	0	0
1	1	1

Deutsch-Jozsa algorithm for a two-qubit function: $\mathbf{y} \oplus F(\mathbf{x})$

The function is implemented by one unitary operation that reads the input qubits $\mathbf{x}$ and transforms the auxiliary qubit $\mathbf{y}$ into $\mathbf{y} \oplus F(\mathbf{x})$, that is, it adds $\mathbf{y}$ and $F(\mathbf{x})$ mod 2.
In our example:

x_1	x_2	$F(x_1, x_2)$	$\mathbf{y}$	$\mathbf{y} \oplus F(\mathbf{x})$
0	0	0	0	0
0	1	1	0	1
1	0	0	1	1
1	1	1	1	0

The qubit $\mathbf{y}$ is flipped whenever $F = 1$.



Deutsch-Jozsa algorithm for a two-qubit function: $\hat{U}_F$

$$
\begin{aligned}
|\phi_3\rangle &= \hat{U}_F\,|\phi_2\rangle = \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right) \otimes \left[\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)\right] \\
&= \hat{U}_F\left\{\frac{1}{2}|00\rangle \otimes \left[\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)\right]\right\} + \hat{U}_F\left\{\frac{1}{2}|01\rangle \otimes \left[\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)\right]\right\} \\
&\quad + \hat{U}_F\left\{\frac{1}{2}|10\rangle \otimes \left[\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)\right]\right\} + \hat{U}_F\left\{\frac{1}{2}|11\rangle \otimes \left[\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)\right]\right\} \\
&= \frac{1}{2}\left(|00\rangle \otimes \left[\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)\right] + |01\rangle \otimes \left[\frac{1}{\sqrt{2}}\left(|1\rangle - |0\rangle\right)\right]\right. \\
&\quad \left. + \ |10\rangle \otimes \left[\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)\right] + |11\rangle \otimes \left[\frac{1}{\sqrt{2}}\left(|1\rangle - |0\rangle\right)\right]\right) \\
&= \frac{1}{2}\left(|00\rangle - |01\rangle + |10\rangle - |11\rangle\right) \otimes \left[\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)\right]
\end{aligned}
$$

Deutsch-Jozsa algorithm for a two-qubit function: readout

Now, we can disregard the auxiliary qubit and focus on the first factor of $|\phi_3\rangle$ above. We first rewrite it as

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

and then perform the Hadamard rotations

$$\begin{aligned} |\phi_4\rangle &= \hat{H}\left[\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)\right] \otimes \hat{H}\left[\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)\right] \\ &= |0\rangle \otimes |1\rangle = |01\rangle \end{aligned}$$

The measurement of each qubit reveals that the function is balanced.

The function is constant if the measurement of each input qubit at the end of the computation yields 0. Otherwise the function is balanced.

Deutsch-Jozsa algorithm

Inputs:
A black box $\hat{U}_F$ which performs the transformation $|\mathbf{x}\rangle|\mathbf{y}\rangle \rightarrow |\mathbf{x}\rangle|\mathbf{y} \oplus F(\mathbf{x})\rangle$ for $\mathbf{x} \in \{0, 1, \ldots, 2^{n-1}\}$ and $F(\mathbf{x}) \in \{0, 1\}$. It is promised that the function $F(\mathbf{x})$ is either constant or balanced.

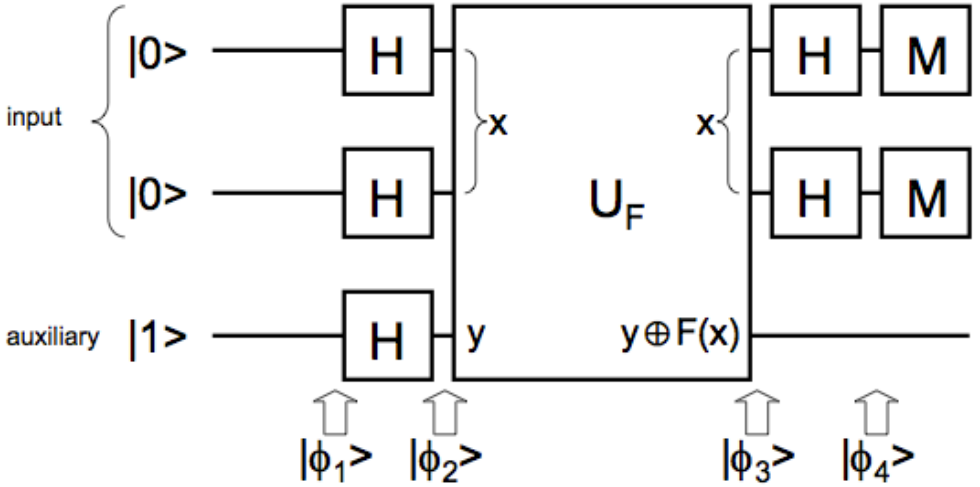
Outputs:
0 iff F is constant.

Complexity/Runtime:
One evaluation of $\hat{U}_F$. Always succeeds.

Exponential speed-up compared to classical algorithm

Procedure:

1. $|\phi_1\rangle = |0\rangle^{\otimes n}|1\rangle$
2. $\rightarrow \quad |\phi_2\rangle = \frac{1}{2^{n/2}} \sum_{\mathbf{x}=0}^{2^n-1} |\mathbf{x}\rangle \left[\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right]$
3. $\rightarrow \quad |\phi_3\rangle = \frac{1}{2^{n/2}} \sum_{\mathbf{x}=0}^{2^n-1} (-1)^{F(\mathbf{x})} |\mathbf{x}\rangle \left[\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right]$
4. $\rightarrow \quad |\phi_4\rangle = \frac{1}{2^n} \sum_{\mathbf{z}} \sum_{\mathbf{x}} (-1)^{\mathbf{x}.\mathbf{z}+F(\mathbf{x})} |\mathbf{z}\rangle \left[\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right]$
5. $\rightarrow \quad \mathbf{z}$



CLASSICAL AND QUANTUM COMPUTATION

QUANTUM ALGORITHMS

Quantum Fourier transform

Quantum Fourier transform is an efficient way of performing a Fourier transform of quantum mechanical amplitudes.

It does not speed up classical task of performing a Fourier transform of classical data but it enables *phase estimation*, the approximation of the eigenvalues of a unitary operator under certain circumstances.

Phase estimation allows to solve other interesting problems including quantum computation of *molecular electronic structure* and *factorization*.

Discrete Fourier transform

Input:

a vector of N complex numbers $x_0, x_1, \ldots, x_{N-1}$;

Output:

a vector of N complex numbers $y_0, y_1, \ldots, y_{N-1}$ defined by

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \, e^{2\pi i jk/N}$$

Quantum Fourier transform

Quantum Fourier transform on an orthonormal basis $|0\rangle, |1\rangle, \ldots, |N-1\rangle$ is defined to be a linear operator

$$|j\rangle \quad \rightarrow \quad \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i jk/N} \, |k\rangle$$

Equivalently, the quantum Fourier transform on an arbitrary quantum state is given as

$$\sum_{j=0}^{N-1} x_j \, |j\rangle \quad \rightarrow \quad \sum_{k=0}^{N-1} y_k \, |k\rangle$$

where the amplitudes y_k are the discrete Fourier transform of the amplitudes x_j.

Quantum Fourier transform circuit

We consider $N = 2^n$, $n \in \mathbb{Z}$ and the computational basis $|0\rangle, |1\rangle, \ldots, |2^n - 1\rangle$.

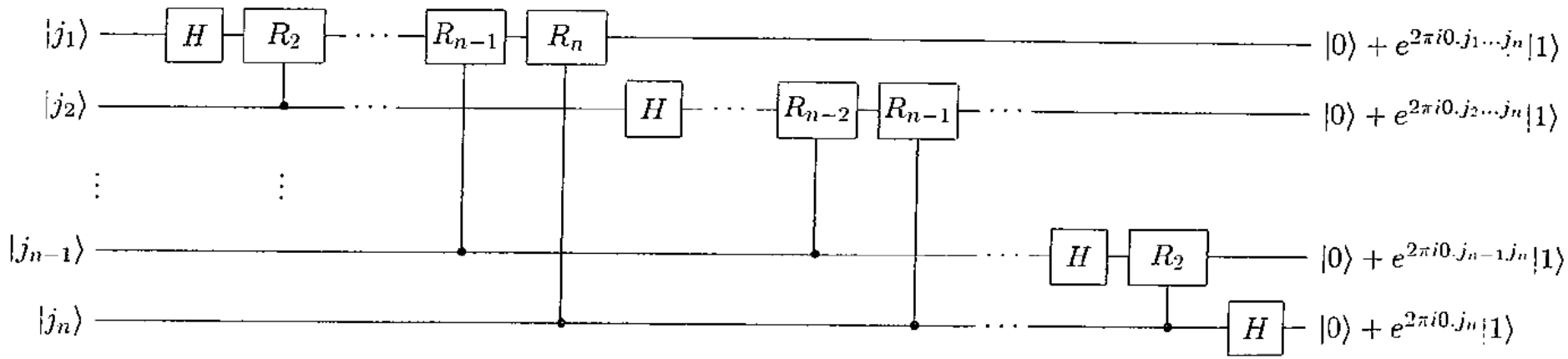
We write the state $|j\rangle$ in binary representation $j = j_1 j_2 \ldots j_n$, or more formally $j = j_1 2^{n-1} + j_2 2^{n-2} + \ldots + j_n 2^0$.

Also, we adopt the notation $0.j_l j_{l+1} \ldots j_m$ to represent the *binary fraction* $j_l/2 + j_{l+1}/4 + \ldots + j_m/2^{m-l+1}$.

The new notation allows us to represent quantum Fourier transform in a *product* form that is well suited for construction of an efficient quantum circuit computing the transform. It will also provide insights into the algorithms based upon QFT.

The quantum Fourier transform can be rewritten as follows

$$
\begin{aligned}
|j\rangle \quad &\rightarrow \quad \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi i jk/2^n} \, |k\rangle \\
&= \quad \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} e^{2\pi i j \left(\sum_{l=1}^{n} \, k_l \, 2^{-l}\right)} \, |k_1 \ldots k_n\rangle \\
&= \quad \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} e^{2\pi i j k_l \, 2^{-l}} \, |k_l\rangle \\
&= \quad \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[\sum_{k_l=0}^{1} e^{2\pi i j k_l \, 2^{-l}} \, |k_l\rangle \right] = \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[|0\rangle + e^{2\pi i j \, 2^{-l}} |1\rangle \right] \\
&= \quad \frac{\left(|0\rangle + e^{2\pi i \, 0.j_n} \, |1\rangle\right) \left(|0\rangle + e^{2\pi i \, 0.j_{n-1} j_n} \, |1\rangle\right) \ldots \left(|0\rangle + e^{2\pi i \, 0.j_1 j_2 \ldots j_n} \, |1\rangle\right)}{2^{n/2}}
\end{aligned}
$$


$|j_1\rangle$
$|j_2\rangle$
$|j_{n-1}\rangle$
$|j_n\rangle$
H
R_2
R_{n-1}
R_n
H
R_{n-2}
R_{n-1}
H
R_2
H
$|0\rangle + e^{2\pi i 0.j_1 \cdots j_n}|1\rangle$
$|0\rangle + e^{2\pi i 0.j_2 \cdots j_n}|1\rangle$
$|0\rangle + e^{2\pi i 0.j_{n-1} j_n}|1\rangle$
$|0\rangle + e^{2\pi i 0.j_n}|1\rangle$

Applying the Hadamard gate to the first qubit of the input state $|j_1 \dots j_n\rangle$ gives

$$\frac{1}{2^{1/2}}\left(|0\rangle + e^{2\pi i\ 0.j_1}|1\rangle\right)|j_2 \dots j_n\rangle$$

since $e^{2\pi i\ 0.j_1}$ equals $+1$ when $j_1 = 0$ and equals -1 when $j_1 = 1$.
We define a unitary gate R_k as

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix}$$

The controlled-R_2 gate applied on the first qubit, conditional on j_2, now gives

$$\frac{1}{2^{1/2}}\left(|0\rangle + e^{2\pi i\ 0.j_1 j_2}|1\rangle\right)|j_2 \dots j_n\rangle$$

Applying further the controlled-R_3, R_4 ... R_n gates, conditional on j_3, j_4 etc., we get

$$\frac{1}{2^{1/2}}\left(|0\rangle + e^{2\pi i\ 0.j_1 j_2 \dots j_n}|1\rangle\right)|j_2 \dots j_n\rangle$$

Next we perform a similar procedure onto the second qubit. The Hadamard gate produces the state

$$\frac{1}{2^{2/2}}\left(|0\rangle + e^{2\pi i\ 0.j_1 j_2 \ldots j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i\ 0.j_2}|1\rangle\right)|j_3 \ldots j_n\rangle$$

and the controlled-R_2 through R_n gates yield the state

$$\frac{1}{2^{2/2}}\left(|0\rangle + e^{2\pi i\ 0.j_1 j_2 \ldots j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i\ 0.j_2 \ldots j_n}|1\rangle\right)|j_3 \ldots j_n\rangle$$

We continue this procedure for each qubit, obtaining a final state

$$\frac{1}{2^{n/2}}\left(|0\rangle + e^{2\pi i\ 0.j_1 j_2 \ldots j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i\ 0.j_2 \ldots j_n}|1\rangle\right)\ldots\left(|0\rangle + e^{2\pi i\ 0.j_n}|1\rangle\right)$$

Eventually, we use the $SWAP$ operations to reverse the order of the qubits to obtain the state in the desired product form

$$\frac{1}{2^{n/2}}\left(|0\rangle + e^{2\pi i\ 0.j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i\ 0.j_{n-1} j_n}|1\rangle\right)\ldots\left(|0\rangle + e^{2\pi i\ 0.j_1 j_2 \ldots j_n}|1\rangle\right)$$

Complexity of quantum Fourier transform

How many gates the circuit use?

qubit	# of Hadamard gates	# of controlled-R gates	total # of gates
1	1	$n-1$	n
2	1	$n-2$	$n-1$
...			
$n-1$	1	1	2
n	1	0	1
Total			$n(n+1)/2$ plus $\frac{n}{2}$ $SWAP$ gates

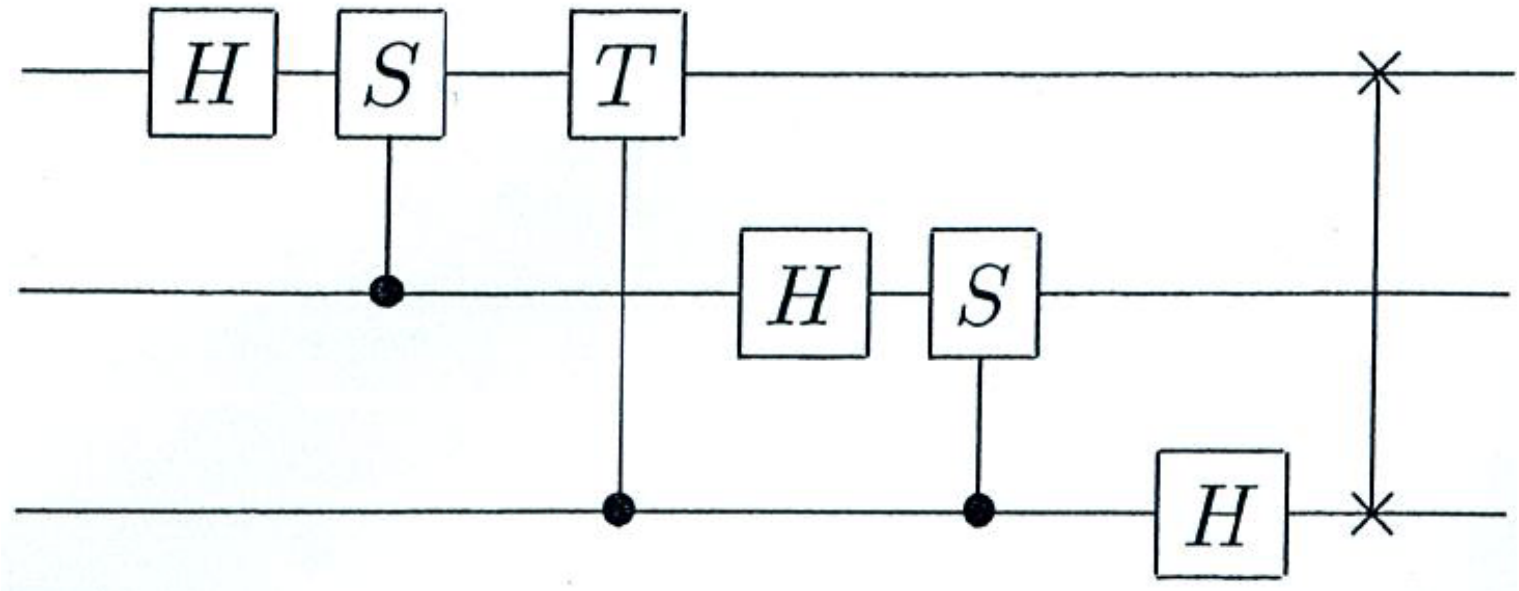
The circuit provides $\Theta(n^2)$ algorithm for performing quantum Fourier transform.

The best classical algorithms for the discrete Fourier transform, such as the Fast Fourier Transform, require $\Theta(n2^n)$ gates to perform the transform on 2^n elements.

Example: Three qubit QFT

In this case, we will need only the controlled R_2 and R_3 gates. Note that

$$R_2 = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{\pi i/2} \end{pmatrix} = \hat{S} \qquad R_3 = \begin{pmatrix} 1 & 0 \\ 0 & e^{\pi i/4} \end{pmatrix} = \hat{T}$$



The quantum Fourier transform can in this case be written explicitly as a matrix

$$QFT_3 = \frac{1}{\sqrt{8}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^1 & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega^1 & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{pmatrix}$$

where $\omega = e^{2\pi i/8} = \sqrt{i}$.

Quantum phase estimation subroutine

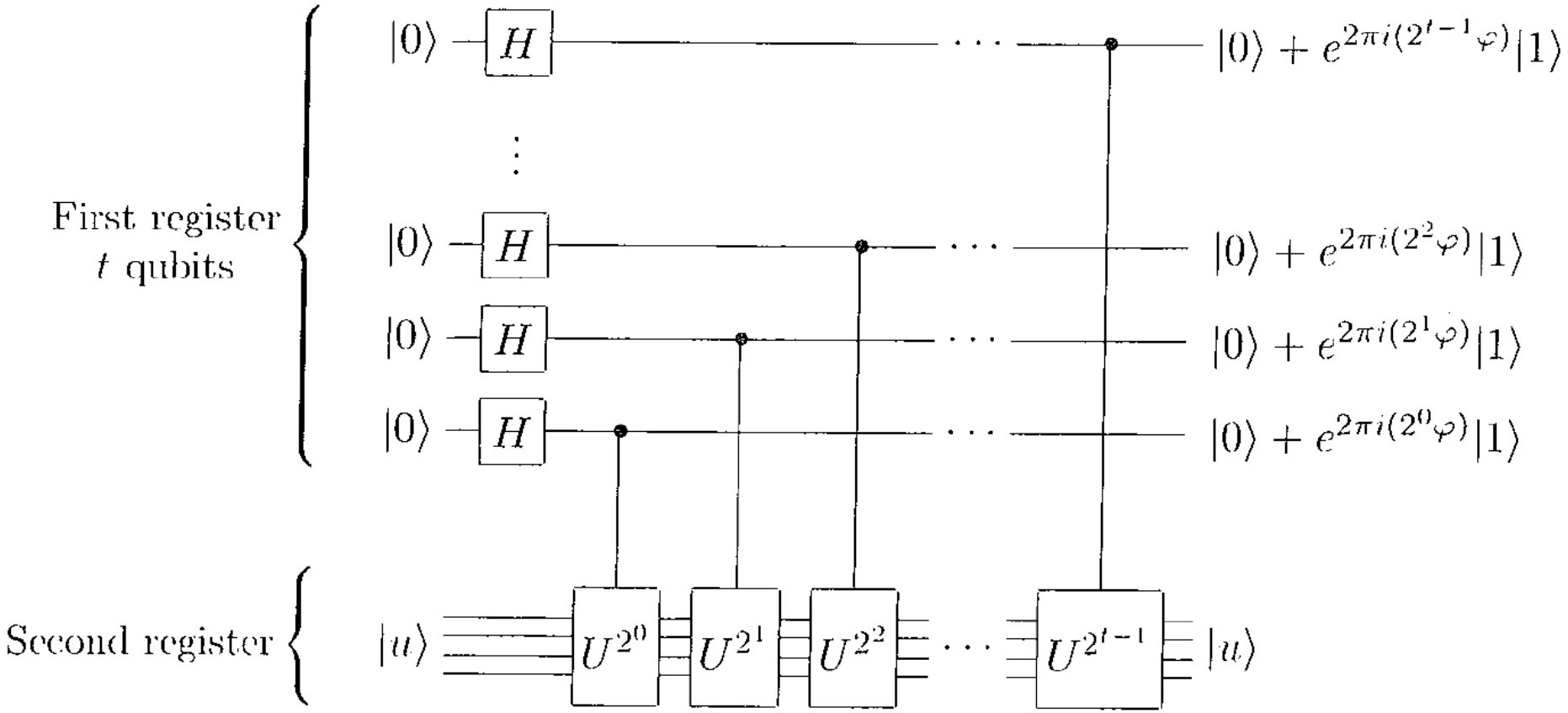
Suppose a unitary operator U has an eigenvector $|u\rangle$ with eigenvalue $e^{2\pi i\varphi}$ where the value of φ is unknown. The goal of the phase estimation algorithm is to estimate φ.

We assume that we have *black boxes*, also called *oracles*, capable of preparing the state $|u\rangle$ and performing the controlled-U^{2^j} operation for suitable nonnegative $j \in \mathbb{Z}$.

The phase estimation procedure will use two *registers*:

- the first containing t qubits in the state $|0\rangle$; t depends on the desired accuracy of the phase estimation and on the probability of it being successful.

- the second register begins in the state $|u\rangle$ and contains as many qubits as necessary to store it.


First register
t qubits
Second register
$|0\rangle$
H
$|u\rangle$
U^{2^0}
U^{2^1}
U^{2^2}
$U^{2^{t-1}}$
$|0\rangle + e^{2\pi i(2^{t-1}\varphi)}|1\rangle$
$|0\rangle + e^{2\pi i(2^2\varphi)}|1\rangle$
$|0\rangle + e^{2\pi i(2^1\varphi)}|1\rangle$
$|0\rangle + e^{2\pi i(2^0\varphi)}|1\rangle$
$|u\rangle$

Quantum phase estimation circuit

The circuit begins by applying a Hadamard gates to the first register followed by the application of controlled-U operations on the second register, with U raised to successive powers of two.

The final state of the first register is

$$\frac{1}{2^{t/2}}\left(|0\rangle + e^{2\pi i\ 2^{t-1}\varphi}\ |1\rangle\right)\left(|0\rangle + e^{2\pi i\ 2^{t-2}\varphi}\ |1\rangle\right)\ \ \ldots\ \ \left(|0\rangle + e^{2\pi i\ 2^{0}\varphi}\ |1\rangle\right)$$

$$= \frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1} e^{2\pi i\varphi k}\ |k\rangle$$

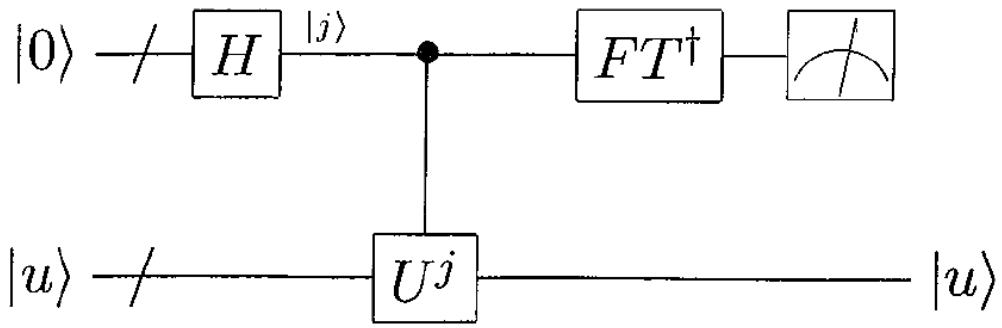
Suppose that φ can be expressed exactly in t bits as $\varphi = 0.\varphi_1 \ldots \varphi_t$. Then the final state of the first stage may be written as

$$\frac{1}{2^{t/2}}\left(|0\rangle + e^{2\pi i\, 0.\varphi_t}\,|1\rangle\right)\left(|0\rangle + e^{2\pi i\, 0.\varphi_{t-1}\varphi_t}\,|1\rangle\right) \quad \ldots \quad \left(|0\rangle + e^{2\pi i\, 0.\varphi_1\varphi_2\ldots\varphi_t}\,|1\rangle\right)$$

The second stage of the algorithm is to apply the **inverse** Fourier transform, obtained by reversing the QFT circuit, on the first register:

$$\frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1} e^{2\pi i\varphi k}\,|k\rangle\,|u\rangle \quad \rightarrow \quad |\varphi_1\varphi_2\ldots\varphi_t\rangle\,|u\rangle = |\tilde{\varphi}\rangle\,|u\rangle$$

This step can be done in $\Theta(t^2)$ steps.



The third stage is the measurement of the first register in the standard computational basis.

If φ was expressed exactly in t qubits, the measurement would give us φ exactly.
In general, $|\tilde{\varphi}\rangle$ is a good estimate of the phase φ of an eigenvalue of the unitary operator U.

To successfully obtain φ accurate to n bits with probability of success at least $1-\epsilon$, the algorithm requires

$$t = n + \left\lceil \log\left(2 + \frac{1}{2\epsilon}\right) \right\rceil$$

Applications

1. Order-finding algorithm

The order of x modulo N is the least positive integer r such that $x^r \mathrm{mod} N = 1$. This number can be computed in $O(L^3)$ operations using the quantum phase estimation algorithm, for L-bit integers x and N.

2. **Factoring** (Shor)

The prime factors of an L-bit integer N can be determined in $O(L^3)$ operations by reducing this problem to finding the order of a random number x co-prime with N.

3. Hidden subgroup problem

All the known fast quantum algorithms can be described as solving the following problem:

Let f be a function from a finitely generated group G to a finite set X such that f is constant on the cosets of a subgroup K, and distinct on each coset. Given a quantum black box for performing the unitary transform $U|g\rangle|h\rangle = |g\rangle|h \oplus f(g)\rangle$, for $g \in G$ and $h \in X$, find a generating set for K.

3. Hidden subgroup problem

If we are given a periodic function, even when the structure of the periodicity is quite complicated, we can often use a quantum algorithm to determine the periodicity.

All the known fast quantum algorithms can be described as solving the following problem:

Let f be a function from a finitely generated group G to a finite set X such that f is constant on the cosets of a subgroup K, and distinct on each coset. Given a quantum black box for performing the unitary transform $U|g\rangle|h\rangle = |g\rangle|h \oplus f(g)\rangle$, for $g \in G$ and $h \in X$, find a generating set for K.

Quantum search algorithm (Grover)

Consider an unsorted database with $N = 2^n$ entries. The algorithm requires an N-dimensional state space $\mathcal{H}$, which can be supplied by $n = \log_2 N$ qubits.

Consider the problem of determining the index of the database entry which satisfies some search criterion.

Let f be the function which maps database entries to 0 or 1, where $f(\omega) = 1$ if and only if ω satisfies the search criterion. We are provided with oracle access to a subroutine in the form of a unitary operator, U_ω, which acts as follows (for the ω for which $f(\omega) = 1$):

$$\begin{aligned} U_\omega|\omega\rangle &= -|\omega\rangle \\ U_\omega|x\rangle &= |x\rangle, \text{ for all } x \neq \omega \end{aligned}$$

Our goal is to identfy the index $|\omega\rangle$.

Algorithm

Let $|s\rangle$ denote the uniform superposition over all states

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

We introduce the operator

$$U_s = 2|s\rangle\langle s| - 1$$

known as the Grover diffusion operator.

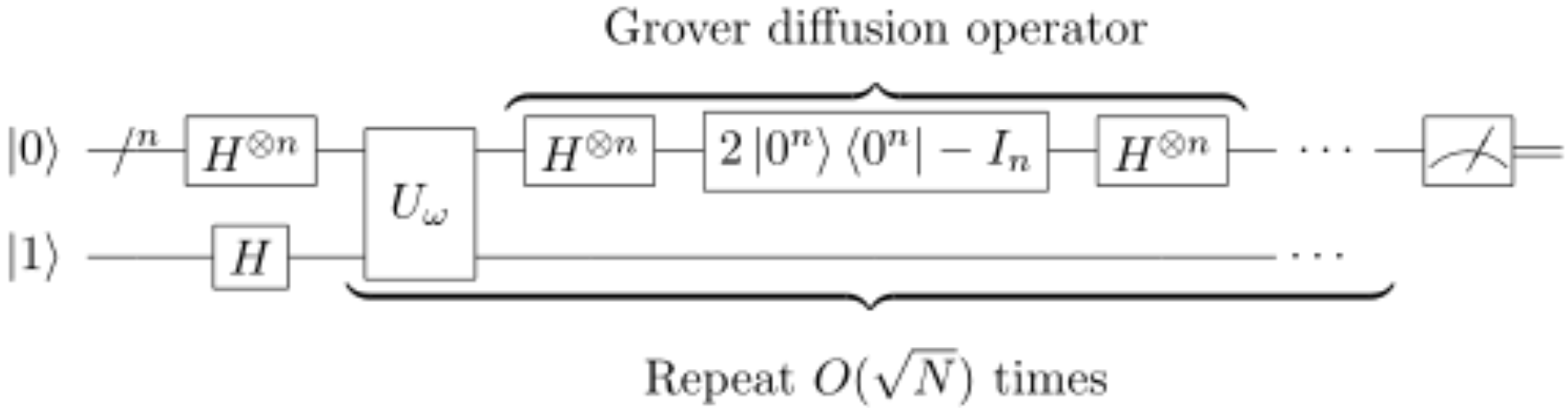
1. Initialize the system to the state

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

2. Perform the following Grover iteration $r(N)$ times where $r(N)$ is asymptotically $O(\sqrt{N})$:

   a) apply the operator U_ω;
   b) apply the operator U_s.

3. Perform the measurement Ω. The measurement result will be λ_ω with the probability approaching 1 for $N >> 1$. From λ_ω, ω may be obtained.

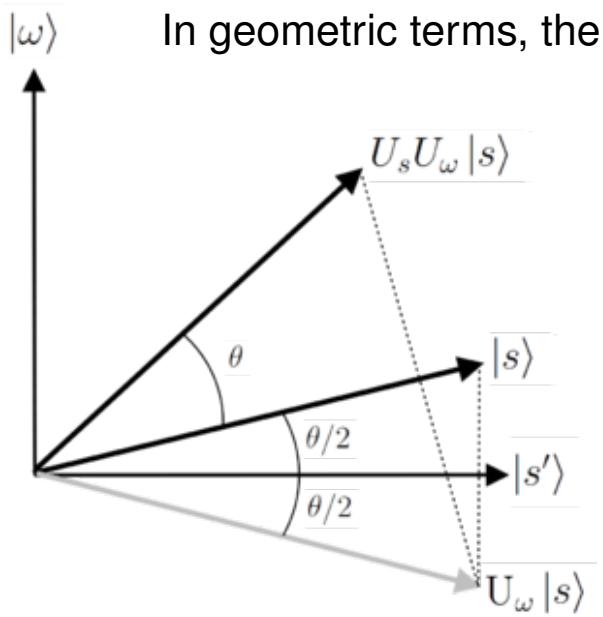

Grover diffusion operator
$|0\rangle$
$|1\rangle$
$/^n$
$H^{\otimes n}$
H
U_ω
$H^{\otimes n}$
$2\,|0^n\rangle\,\langle 0^n| - I_n$
$H^{\otimes n}$
$\cdots$
$\cdots$
Repeat $O(\sqrt{N})$ times

Consider the plane spanned by $|s\rangle$ and $|\omega\rangle$, or equivalently the plane spanned by $|\omega\rangle$ and

$$|s'\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq \omega} |x\rangle$$

We will consider the first iteration, acting on the initial ket $|s\rangle$. Since $|\omega\rangle$ is one of the basis vectors in $|s\rangle$ the overlap

$$\langle s'|s\rangle = \sqrt{\frac{N-1}{N}}$$



In geometric terms, the angle between $|s\rangle$ and $|s'\rangle$ is given as

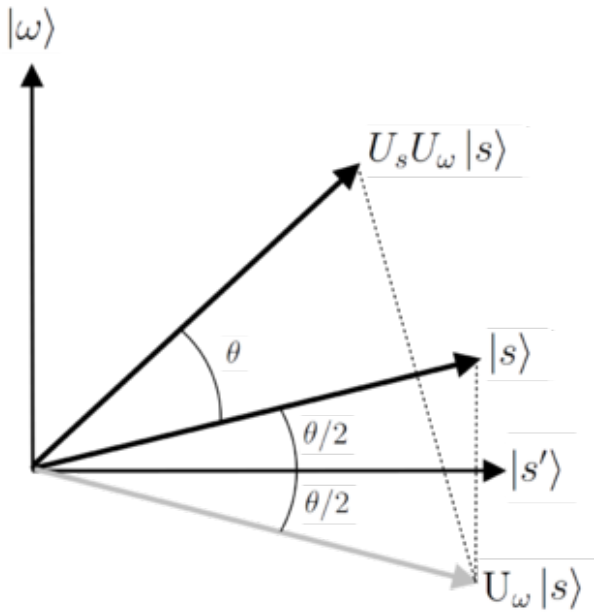
$$\sin \theta/2 = \frac{1}{\sqrt{N}}$$

The operator U_ω is a reflection at the hyperplane orthogonal to $|\omega\rangle$ for vectors in the plane spanned by $|\omega\rangle$ and $|s'\rangle$, that is it acts as a reflection across $|s'\rangle$.

The operator U_s is a reflection through $|s\rangle$. Therefore, the state vector remains in the plane spanned by $|\omega\rangle$ and $|s'\rangle$ after each application of the operators U_s and U_ω.

The operator $U_s U_\omega$ of each iteration rotates the state vector by an angle

$$\theta = 2 \arcsin \frac{1}{\sqrt{N}}$$



We need to stop when the state vector passes close to $|\omega\rangle$; after this, subsequent iterations rotate the state vector away from $|\omega\rangle$, reducing the probability of obtaining the correct answer.

The exact probability of measuring the correct answer is:

$$\sin^2\left(\left(r+\frac{1}{2}\right)\theta\right)$$

where r is the number of Grover iterations.

The earliest time we get the near-optimal measurement is $r \approx \pi\sqrt{N}/4$.