MP 472 Quantum Information and Computation

http://www.thphys.may.ie/staff/jvala/MP472.htm

Outline

Quantum bits

Quantum operations
- postulate of quantum mechanics regarding quantum (unitary) dynamics
- single-qubit and two-qubit gates
- universality of quantum computing operations and Solovay-Kitaev theorem
- quantum circuit model of quantum computation

Quantum measurement

Tensor products of operators

Suppose |v> and |w> are vectors in V and W, and A and B are linear operators on V and W respectively. Then we can define a linear operator $A\otimes B$ on $V\otimes W$ by the equation:

$$A\otimes B\,(|v\rangle\otimes|w\rangle) = A|v\rangle\otimes B|w\rangle$$

And we can extend this definition to all elements of $V\otimes W$ in the natural way to ensure linearity of $A\otimes B$

$$A\otimes B\,(\Sigma_i a_i|v_i\rangle\otimes|w_i\rangle) = \Sigma_i a_i A|v_i\rangle\otimes B|w_i\rangle$$

In matrix representation:

$$A\otimes B = \begin{pmatrix} A_{11}B & A_{12}B & \ldots & A_{1n}B \\ A_{21}B & A_{22}B & \ldots & A_{2n}B \\ \ldots & & & \\ A_{m1}B & A_{m2}B & \ldots & A_{mn}B \end{pmatrix}$$

Example:

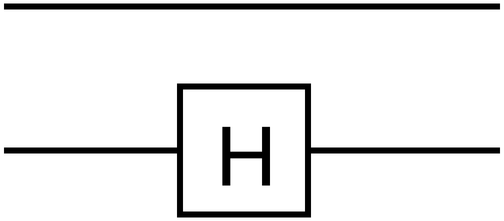
$$X\otimes Y = \begin{pmatrix} 0.Y & 1.Y \\ 1.Y & 0.Y \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \\ 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \end{pmatrix}$$

More examples

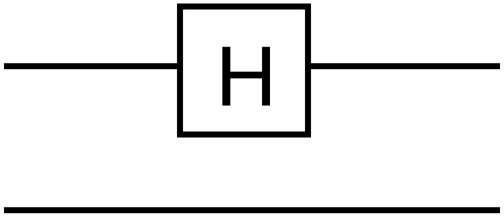
In matrix representation:

$$A \otimes B = \begin{pmatrix} A_{11}B & A_{12}B & \dots & A_{1n}B \\ A_{21}B & A_{22}B & \dots & A_{2n}B \\ \dots & & & \\ A_{m1}B & A_{m2}B & \dots & A_{mn}B \end{pmatrix}$$

Example:



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



$$H \otimes I = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$$

Matrix functions

Recall spectral decomposition: $A = \sum_a a|a\rangle\langle a|$

then a function of an operator can be defined as:

$$f(A) = \sum_a f(a)|a\rangle\langle a|$$

Example:

- square root: $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ $\quad Z^{1/2} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
- exponential: $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ $\quad e^{-iZ} = \begin{pmatrix} e^{-it} & 0 \\ 0 & e^{it} \end{pmatrix}$

Trace: $\mathrm{tr}(A) = \sum_i A_{ii}$

$\mathrm{tr}(AB) = \mathrm{tr}(BA)$	cyclic permutation invariance
$\mathrm{tr}(A+B) = \mathrm{tr}(A)+\mathrm{tr}(B)$	linearity
$\mathrm{tr}(zA) = z\,\mathrm{tr}(A)$	$z \in \mathbb{C}$
$\mathrm{tr}(UAU^+) = \mathrm{tr}(A)$	$U \in U(N)$ (set of all unitary N-by-N matrices)

Commutator and Anti-commutator

Commutator:

$$[A,B] = AB - BA$$

Homework: show the commutation relations between the Pauli matrices

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Simultaneous diagonalization theorem:

Let A and B be hermitian operators. Then $[A,B]=0$ iff there exists an orthonormal basis s.t. both A and B are diagonal with respect to that basis. We say that A and B are *simultaneously diagonalizable*.

Anti-commutator:

$$\{A,B\} = AB + BA$$

Homework:

- show the anti-commutation relations between the Pauli matrices
- show $[A,B]^+ = [B^+,A^+]$
- show $[A,B] = - [B,A]$

Postulates of quantum mechanics

Quantum state

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

Quantum observable

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

Quantum Dynamics

- The time evolution of the state vector $|\psi\ (t)>$ is governed by the Schroedinger equation $i\hbar\ d|\psi(t)>/dt = \mathbf{H}(t)|\psi(t)>$ where **H**(t) is the observable associated with the total energy of the system.

Measurement

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

- When the physical quantity $\mathscr{A}$ is measured on a system in the normalized state $|\psi>$, the probability $p(a_n)$ of obtaining the (non-degenerate) eigenvalue a_n of the corresponding observable **A** is: $P(a_n) = |<u_n|\psi>|^2$, where $|u_n>$ is the normalized eigenvector of **A** with the eigenvalue a_n.

- If the measurement of the physical quantity $\mathscr{A}$ on the system in the state $|\psi>$ gives the result a_n, the state of the system immediately after the measurement is the normalized projection, $P_n|\psi>/(<\psi|\psi>)^{1/2}$, of $|\psi>$ onto the eigenspace associated with a_n.

Schroedinger equation

$$i\hbar \, d|\psi(t)\rangle/dt = \mathbf{H}(t)|\psi(t)\rangle$$

where **H**(t) is the observable (i.e. a Hermitian operator) associated with the total energy of the system. This operator is called the Hamiltonian.

Formal solution is: $$|\psi(t)\rangle = \exp[-i\int dt\mathbf{H}(t)/\hbar]\, |\psi(0)\rangle$$

or if the Hamiltonian is time independent, it is:

$$|\psi(t)\rangle = \exp[-it\mathbf{H}/\hbar]\, |\psi(0)\rangle$$

Because the Hamiltonian is hermitian, the evolution operator which is generated by the Hamiltonian is unitary:

$$|\psi(t)\rangle = U_t(\mathbf{H})\, |\psi(0)\rangle$$

$$U_t(\mathbf{H})^+ = U_{-t}(\mathbf{H}^+) = U_{-t}(\mathbf{H}) \qquad U^+U = UU^+ = 1$$

Unitary evolution

Examples:

Hamiltonian: Dynamics:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad U_X = e^{-iXt/2} = \cos(t/2).I - i\sin(t/2).X = \begin{pmatrix} \cos(t/2) & -i\sin(t/2) \\ -i\sin(t/2) & \cos(t/2) \end{pmatrix}$$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad U_Y = e^{-iYt/2} = \cos(t/2).I - i\sin(t/2).Y = \begin{pmatrix} \cos(t/2) & -\sin(t/2) \\ \sin(t/2) & \cos(t/2) \end{pmatrix}$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad U_Z = e^{-iZt/2} = \cos(t/2).I - i\sin(t/2).Z = \begin{pmatrix} e^{-it/2} & 0 \\ 0 & e^{it/2} \end{pmatrix}$$

Let $n = (n_x,n_y,n_z)$ be a real unit vector in three dimensions then a rotation by an angle t about the n axis is defined as

$$U_n(t) = e^{\mathbf{-i\ n.\sigma\ t/2}} = \cos(t/2).I - i\sin(t/2).(n_xX + n_yY + n_zZ)$$

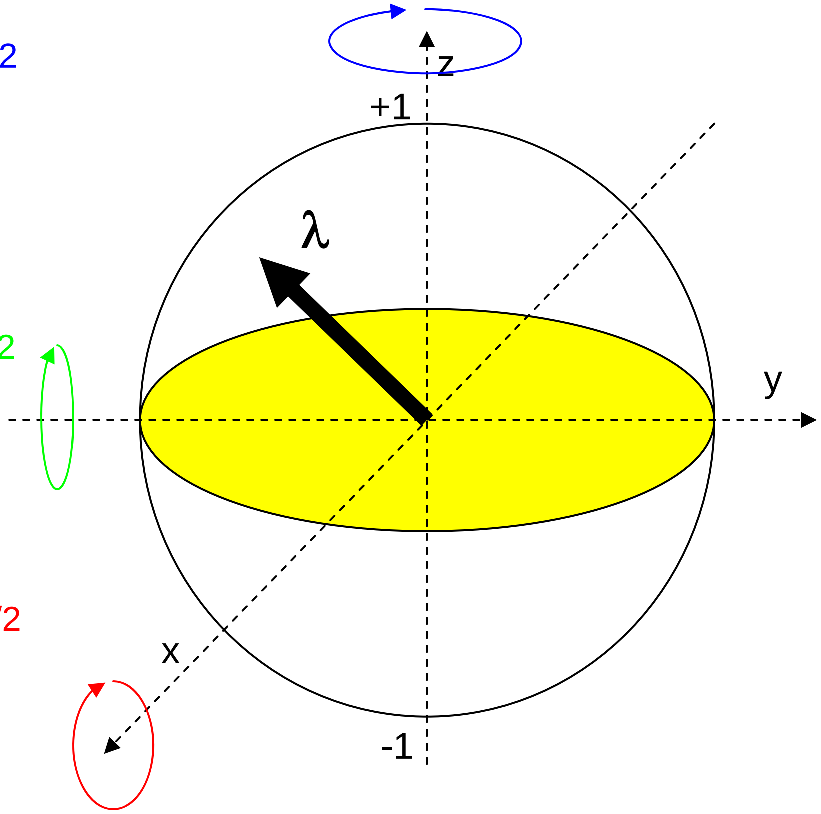
where σ denotes three component vector (X,Y,Z) of Pauli matrices.

Bloch sphere interpretation of rotations

Suppose a single qubit gate has a state represented by the Bloch vector λ. Then the effect of the rotation $U_n(t)$ on the state is to rotate it by an angle t about the n axis of the Bloch sphere.

Bloch representation

$x = 2\mathrm{Re}(c_0 c_1^*)$ $\quad$ $y = 2\mathrm{Im}(c_0 c_1^*)$ $\quad$ $z = |c_1|^2 - |c_0|^2$

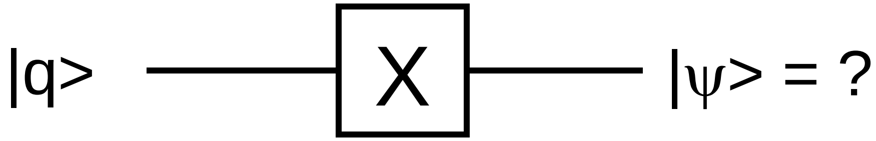


$U_Z = e^{-iZt/2}$

$U_y = e^{-iYt/2}$

$U_X = e^{-iXt/2}$

Quantum computing gates: X



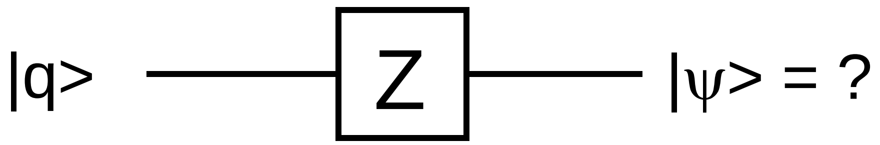
|0> → |1>

|1> → |0>

in the computational {|0>,|1>} basis:

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

Z



|q>

Z

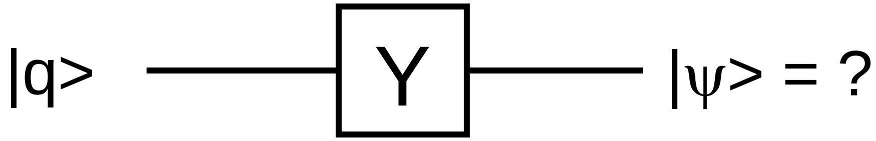
|ψ> = ?

$$|0\rangle \longrightarrow |0\rangle$$

$$|1\rangle \longrightarrow -|1\rangle$$

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

Y=iZX

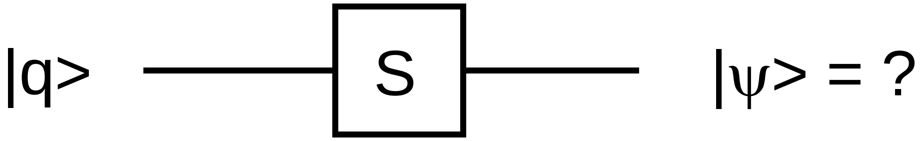


$|0\rangle \longrightarrow i|0\rangle$

$|1\rangle \longrightarrow -\,i|1\rangle$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$\underline{S=(Z)^{1/2}}$

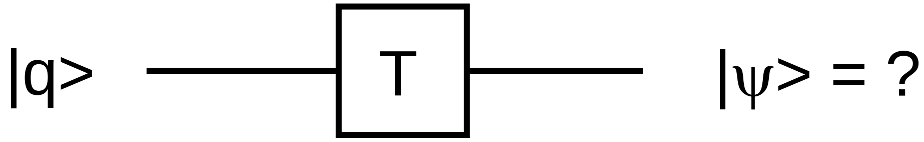


$|0\rangle \longrightarrow |0\rangle$

$|1\rangle \longrightarrow i|1\rangle$

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

T=?

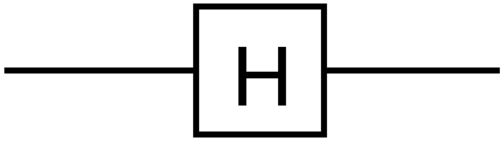


$$|0> \longrightarrow |0>$$

$$|1> \longrightarrow e^{i\pi/4}|1>$$

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

Hadamard gate $H=2^{-1/2}(X+Z)$



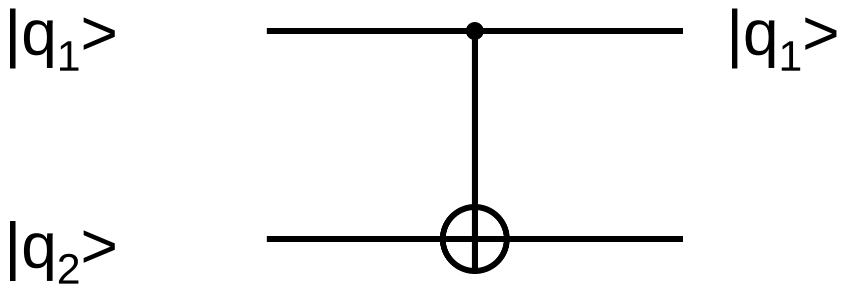
$|q>$ $\quad$ $|\psi> = ?$

$$|0> \longrightarrow 2^{-1/2}\,(|0> + |1>)$$

$$|1> \longrightarrow 2^{-1/2}\,(|0> - |1>)$$

$$H = 2^{-1/2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Two-qubit operation: CNOT gate



$|q_1q_2>$

|00> → |00>
|01> → |01>
|10> → |11>
|11> → |10>

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Universal set of quantum computing gates

The universal set of quantum computing gates is the set of operations that allows 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 ability to generate an arbitrary element of the group of special unitary matrices over n qubits; this group s called SU(2^n) and Is spanned by all 2^n-by2^n unitary matrices of unit determinant.

Good news: only single qubit and two-qubit operations are needed for universality.

Examples of universal sets:

- Continuous:
  SU(2) over any qubit, and CNOT between any pair of qubits

- Discrete (approximating):
  {Hadamard, Z, T, CNOT}

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