4.1 Basic set up of Quantum computing

(1) Prepare a set of registers (qubits).

(2) Apply some unitary transforms to carry out quantum algorithms.

(3) Measure the outcome to derive conclusion.

Mathematically, qubit is a vector in $|x\rangle = a|0\rangle + b|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{C}^2$ with $|a|^2 + |b|^2 = 1$ realized by physical quantum states such as the vertically and horizontally polarized photons, or spin 1/2 in NMR system.
One often starts with a pure state $|psi\rangle = |0 \dots 0\rangle$ and apply a series of quantum gate $U_1, U_2, \dots,$ to the initial states so that a careful measurement of the resulting state will provide us the needed information.

4.2 Quantum gates

Mathematically, quantum gates are realized as unitary transformations/maps. For example, we can use the Pauli matrices:

$$X = \sigma_x, \quad Y = -i\sigma_y, \quad Z = \sigma_z$$

There are other quantum gates involving states represented by multiple qubits:

Walsh-Hadamard gate: $U_H = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\langle 0| + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\langle 1|$.

The matrix form is:

CNOT (controlled-NOT) gate:

$$U_{\text{CNOT}} : |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11| = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X.$$

The matrix form is:

The circuit diagram is:

CCNOT (controlled-controlled-NOT) gate (a.k.a. Toffoli gate):

$$U_{CCNOT} = (|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I + |11\rangle\langle 11| \otimes X.$$

The matrix form is:

The circuit diagram is:

Extension: Walsh-Hadamard transformation $H \otimes H \otimes H \cdots$ to a quantum gate on n qubits.

There are other basic quantum gates: SWAP gate adn Frdkin gate.

4.3 Comparison with Classical logical gates

It is interesting to compare their actions on qubits to the classical Boolean gates.

NOT, AND, XOR, OR, NAND gates.

4.4 No-Cloning Theorem

Theorem An unknown quantum system cannot be cloned by unitary transformations.
That is, there is no unitary $U \in M_n$ and $|y\rangle \in \mathbb{C}^n$ such that $U|x\rangle|y\rangle = |x\rangle|x\rangle$ for any given $|x\rangle \in \mathbb{C}^n$.

4.5 Dense Coding and Teleportation

1. Using an entangled pair (Bell state), one can send two binary bit information using one quantum bit.
2. Using an entangled pair (Bell state), one can use two classical bit information to transmit a qubit.

4.6 Universal quantum gates

Theorem The set of single qubit gates and the CNOT gate from a universal set.

Example for 2-qubit gates.

In general, we use the grey code to realize a two-level unitary gate as a the product of CNOT gates and a controlled qubit gate.

Every controlled qubit gate is a product of at most two CNOT gates and three single qubit gates. (Lemma 4.4)

4.7 Quantum parallelism and entanglement

Given x and f, construct unitary U such that

$$U_f : |x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle,$$

where U_f is unitary. If x is a superposition of $x_1, \ldots, x_n$, then $|x\rangle|f(x)\rangle$ may provide information of $f(x_1), \ldots, f(x_n)$ simultaneously in the process. So, we often use

$$|x\rangle = H_n|0\cdots0\rangle = \frac{1}{\sqrt{2^n}}(|00\cdots0\rangle + |00\cdots1\rangle + \cdots + |11\cdots1\rangle).$$