Chapter 16

Quantum Computer

A quantum computer is a classical computer whose resources (tape, register, gates) obey the laws of quantum mechanics. Most popular is the quantum circuit model which is a "quantizied" version of the classical circuit model. In the quantum circuit model the collection of input bits can exist in any superposition state, and the circuit's gates are realized in terms of unitary operators.

16.1 Single qubit gates

Single-qubit gates are realized in terms of a unitary operator, $\hat{U} \in U(2)$, an element of the group of unitary 2×2 matrices. Every such element can be written in the form

$$\text{U:} \quad \sim\!\!\sim\boxed{U}\sim\!\!\sim \ , \quad \hat{U} = e^{i\delta}\hat{R}_n(\theta) \tag{16.1}$$

with $\delta \in \mathbb{R}$, and $\hat{R}_n$ and special unitary

$$\hat{R}_n(\theta) = \exp\{-i\tfrac{\theta}{2}\vec{n}\cdot\hat{\vec{\sigma}}\}\,. \tag{16.2}$$

In quantum computation, one usually deals with a discrete set of unitaries. Of some importance are the HADAMARD and the $\pi/8$ gate,

HADAMARD: , $\hat{H} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, (16.3)

$\pi/8$, $\hat{T} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$, (16.4)

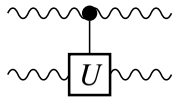
Theorem The Hadamard and the $\pi/8$ gate can be used to approximate any given unitary on a single qubit with arbitrary accuracy.

On the Bloch sphere, $\hat{T}$ and $\hat{H}\hat{T}\hat{H}$ are rotations by an angle $\pi/4$ radians around the $\vec{e}_z$- and $\vec{e}_x$-axis, respectively. The composition of these two operations gives a rotation by an angle θ, which is defined by $\cos\frac{\theta}{2} = \cos^2\frac{\pi}{8}$, around an axis $\vec{n}$, which is defined by $\vec{n} = (\cos\frac{\pi}{8}, \sin\frac{\pi}{8}, \cos\frac{\pi}{8})$. Since θ is irrational, any rotation around the $\vec{n}$-axis can be build, to arbitrary precision, from $\hat{T}$ and $\hat{H}\hat{T}\hat{H}$. Furhtermore, since for α arbirary $\hat{H}\hat{R}_n(\alpha)\hat{H} = \hat{R}_m(\alpha)$ with $\vec{m} = (\cos\frac{\pi}{8}, -\sin\frac{\pi}{8}, \cos\frac{\pi}{8})$ not collinear $\vec{n}$, there are angles α, β, γ such that any given $\hat{U}$ can be written $\hat{U} = \hat{R}_n(\alpha)\hat{R}_m(\beta)\hat{R}_n(\gamma)$.

16.2 Two-qubit gates

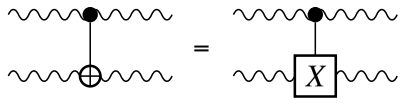
Two-qubit gates are realized in terms of a unitary operator, $\hat{U} \in U(4)$, an element of the group of unitary 4×4 matrices.

Two-qubit gates can be used for controlled operations: one of the qubits, called the target, is manipulated in a manner which is conditioned on the other qubit, called the control. The prototype is the CONTROLLED-U, or CU for short. The CU maps the target $|t\rangle \mapsto \hat{U}|t\rangle$, with $\hat{U}$ unitary, if the control bit is set, otherwise it is left unchanged. In the computational basis, the gate's unitary reads

$cU:$  , $\hat{U}_{cu} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{bmatrix}$ (16.5)

where the 2×2 matrix in the lower right corner is the single qubit unitary $\hat{U}$.

Most popular is the CONTROLLED-NOT, or CNOT for short. In the computational basis the gate operation reads $|c\rangle|t\rangle \to |c\rangle|t \oplus c\rangle$, the unitary matrix given by

$cnot:$  , $\hat{U}_{cnot} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ (16.6)

The CNOT can be used to swap two qubits and generate entangled states, see Fig. 17.1.

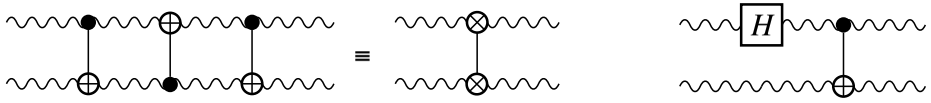


Figure 16.1: Configuration of the CNOT for the SWAP (left) and Bell-state maker (right).

Most important is the following theorem.

Theorem Any given 2-qubit gate can be composed from CNOT and a single qubit gate.

16.3 Quantum circuit

Mathematically, a quantum circuit for l qubits is a unitary operator which acts in a 2^l dimensional Hilbert space. As it is fundamental to the notion of "mechanical computation" that programming and computation occur by finite means, we cannot just assume that U may be efficiently implemented. Instead, U must be constructed using some finite basis set of transformations. However, since the unitaries form a continuum, we are able to construct them only approximately in general. This approximation my be carried to any derired degree of accuracy, though, using sufficiently large circuits.

Theorem [DEUTSCH 1985] Let U be any d-dimensional unitary matrix. Then U may be written as a product of $2d^2 - d$ unitary matrices, each of which acts only within a two-dimensional subspace spanned by a pair of computational basis states.

For a proof see "Quantum computation and Shor's factoring algorithm" by A. Ekert and R. Josza, Rev. Mod. Phys. **68**, 733 (1996). *End-of-proof*

Using () we see that, for any d-dimensional unitary U, there exists a circuit of size poly(d/ϵ) which approximates U to within accuracy ϵ.

An algorithm which involves at most k unitary transformations U_i, one after the other, may be approximated to any desired accuracy ϵ by approximating each U_i to accuracy ϵ/k. This requires at most $k$poly(dk/ϵ) elementary steps, where d is the

maximum size of the U_i's. If $\mathcal{A}$ is an efficient algorithm, i.e. $k = \text{poly}(\text{ld}N)$ for input N, and each U_i has size $\text{poly}(\text{ld}n)$, then, for each fixed accuracy ϵ, we will have an efficient approximating algorithm.

