CS59200-PRS: Pseudorandomness Oct 27, 2025

Lecture 17: Basics of quantum information

Lecturer: Wei Zhan *Scribe: Kyle Asbury*

1 Quantum States

Before introducing quantum computing, we first review the models of classical computing. We use states to describe the current configuration of the machine, and computation on the machine is essentially a series of transition of states.

For classical deterministic computing on a computer with n-bit memory, the state is an n-bit string, or just an element in $[N]$ for $N = 2^n$. The transition is thus just a function $M\colon [N] \to [N]$. We can also use matrix representation and represent each state with a basis vector, while the transition is now a $\{0,1\}$-matrix with exactly one 1 in each column.

The matrix representation naturally generalizes to classical randomized computation, where the state is a distribution over $[N]$ represented by a non-negative vector with unit ℓ_1-norm, and the transition $p \mapsto Mp$ is performed with a stochastic matrix M (so that it preserves non-negativity and ℓ_1-norm).

Now quantum computing, is based on *qubits* instead of classical bits. To describe the states of n qubits, we use complex vectors of dimension $N = 2^n$ with unit ℓ_2-norms, and the transition $q \mapsto Mq$ is performed with a unitary matrix M (so that it preserves ℓ_2-norm). We list the correspondence in the table below.

	n-(qu)bit state	State transition
Classical deterministic	$i \in [2^n = N]$	$M : [N] \to [N]$
	$e_i = (0, \dots, 0, 1, 0, \dots, 0)^\intercal$	$M \in \{0,1\}^{N\times N}$, one 1 in each column
Classical randomized	$p \in \mathbb{R}^N_{\geq 0}$, $\lvert p\rvert_1 = 1$	$M \in \mathbb{R}^{N\times N}_{\geq 0}$, M stochastic
Quantum	$q \in \mathbb{C}^N$, $\lVert q\rVert_2 = 1$	$M \in \mathbb{C}^{N\times N}$, M unitary

It seems a bit arbitrary that we just define another computation model by changing ℓ_1-norm to ℓ_2-norm, but it is actually just how nature works. The Schrödinger equation decides how a physical system, described by the wave function Ψ (i.e. the state) evolves over time:

$$i\hbar\frac{\partial \Psi}{\partial t} = H\Psi,$$

where $\hbar$ is the Planck constant, and H is a Hermitian matrix called Hamiltonian that describes the system. When H is time invariant we can solve the equation to get

$$\Psi(t) = e^{-iHt/\hbar}\Psi(0),$$

which yields unitaries since a matrix M is unitary if and only if $M = e^{-iH/\hbar}$ for some Hermitian matrix H.

Example. When $n = 1$, single-qubit states are of the form

$$(\alpha, \beta) \text{ s.t. } \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1,$$

which we say is a superposition over the basis states $(1, 0)$ and $(0, 1)$ as

$$(\alpha, \beta) = \alpha \cdot (1, 0) + \beta \cdot (0, 1).$$

1.1 Bra-ket notation

Writing quantum states as vectors can be inconvenient, so we use the bra-ket notation to denote them.

- (ket) We use $|i\rangle$ to denote the basis vector e_i, and in general $|\psi\rangle$ is a unit column vector in $\mathbb{C}^N$.
- (bra) We use $\langle\psi|$ to denote $|\psi\rangle^\dagger$, which is unit row vector. Here $\dagger$ is the conjugate transpose.

Example. For single-qubit states we have $|0\rangle = (1, 0)^\intercal$ and $|1\rangle = (0, 1)^\intercal$. We also define notation for another useful orthonormal basis over $\mathbb{C}^2$:

$$|+\rangle = \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right)^\intercal = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$
$$|-\rangle = \left(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}\right)^\intercal = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.$$

Inner Product We use $\langle\psi|\phi\rangle$ to denote the inner product of $|\psi\rangle$ and $|\phi\rangle$, which is simply a shorthand for $\langle\psi|\,|\phi\rangle$. For instance, $\langle\psi|\psi\rangle = 1$ for every state $|\psi\rangle$, and $\langle 0|1\rangle = \langle +|-\rangle = 0$.

Product State Classically, the joint distribution of two independent states is represented by their tensor product $p_1 \otimes p_2$. For quantum states, the tensor product $|\psi\rangle \otimes |\phi\rangle$ also describes the joint system of two non-interactive states $|\psi\rangle$ and $|\phi\rangle$. For short we also write $|\psi\rangle\,|\phi\rangle$ or $|\psi, \phi\rangle$.

The tensor product states are call *unentangled* states. Not all states of a joint system are unentangled. For instance, the EPR state on two qubits

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle = \left(\frac{1}{\sqrt{2}}, 0, 0, \frac{1}{\sqrt{2}}\right)^\intercal$$

is entangled, as it cannot be written as a tensor product.

2 Measurement

In classical computing, we get the output by reading the bits from the final state. To compute a classical function using a quantum computer, we also need a way to read classical information from the quantum states, and that is by measurements.

For instance, if we measure the single-qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ in the computational basis $\{|0\rangle, |1\rangle\}$:

- With probability $|\alpha|^2 = |\langle\psi|0\rangle|^2$, we get outcome 0, and the state collapses to $|0\rangle$,
- With probability $|\beta|^2 = |\langle\psi|1\rangle|^2$, we get outcome 1, and the state collapses to $|1\rangle$.

More generally, given a set of projections $\{\Pi_i\}$ with $\sum \Pi_i = I_N$, the projective measurement on an n-qubit state $|\psi\rangle$ has outcome i with probability $\langle\psi|\Pi_i|\psi\rangle$, and the state collapses to

$$\frac{\Pi_i|\psi\rangle}{\sqrt{\langle\psi|\Pi_i|\psi\rangle}}.$$

Example. Measuring either qubit of the EPR state in the computational basis gives 0 or 1 with probability 1/2 each, and the state collapses to $|00\rangle$ or $|11\rangle$ respectively.

3 Quantum Circuit

With unitary operators and measurements, we can now describe every quantum computation process using quantum circuits. We assume that a quantum circuit starts with n qubits set to $|0\rangle$. Then we apply unitary operators from a fixed set of gates G, and finally we measure selected qubits to get a classical output.

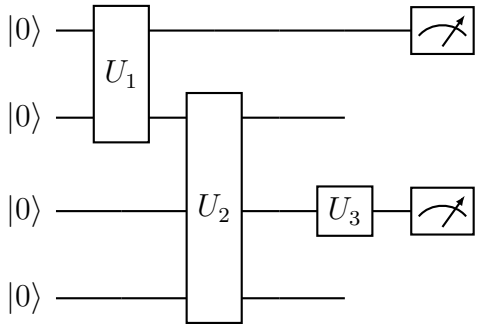

Figure 1: An example quantum circuit. Here U_1, U_2, U_3 are unitaries, and the first and third qubits are measured. Notice that a gate can be applied on a subset of qubits, and the effect of the unitary on the entire system can be described by the tensor product with identity, e.g. $U_1 \otimes I \otimes I$.

Similar to classical circuits, there are different ways to choose the gate set G, and are all equivalent as long as the set is *universal*: they generate a dense subset of the unitary group, i.e. every unitary operator can be arbitrarily closely approximated.

Theorem 1 (Bravyi-Kitaev)**.** *Given any two finite universal gate sets G_1, G_2, there exists a poly-time classical algorithm $A_{G_1 \to G_2}$ such that for every circuit C using G_1 gates, $A_{G_1 \to G_2}(C)$ is a circuit using G_2 gates, and $\left\| A_{G_1 \to G_2}(C) - C \right\|_2 \leq \frac{1}{n}$.*

4 Uniform Circuit Complexity Classes

We give alternate definitions of P and BPP using circuits, and define BQP in a similar way.

P = class of languages decidable by P-uniform poly-size classical circuits (with gates `AND`, `OR`, and `NOT`). Here P-uniform means that a poly-time Turing machine can output the description of the circuit given the input.

BPP = class of languages decidable with bounded error by P-uniform poly-size classical circuits with `COIN-FLIP` gates. These gates effectively ignore the input bits and generate random bits:

$$\texttt{COIN-FLIP}(b) = \begin{cases} 1 & \text{w.p. } 1/2 \\ 0 & \text{w.p. } 1/2. \end{cases}$$

And as usual, bounded error means that the probability of being incorrect is at most $1/3$.

BQP = class of languages decidable with bounded error by P-uniform poly-size quantum circuits (with arbitrary finite gate set due to Theorem 1).

The definitions here avoids the complication of quantum Turing machines, and allows us to easily prove the containment between the above classes.

Theorem 2. $\mathsf{P} \subseteq \mathsf{BQP}$

Proof. Note that the `NOT` gate

$$\texttt{NOT} : \begin{cases} |0\rangle \mapsto |1\rangle \\ |1\rangle \mapsto |0\rangle \end{cases}$$

is unitary. The `AND` gate can be made to be unitary by adding a qubit (called *ancilla*) to record the output:

$$\texttt{AND} : \begin{cases} |a\rangle |b\rangle |0\rangle \mapsto |a\rangle |b\rangle |a \wedge b\rangle , \\ |a\rangle |b\rangle |1\rangle \mapsto |a\rangle |b\rangle |1 - a \wedge b\rangle , \end{cases} \qquad a, b \in \{0, 1\}.$$

We will also need a unitary `FAN-OUT` gate to copy the classical bit, since in classical circuits we allow wires splitting and feeding into multiple gates:

$$\texttt{FAN-OUT} : \begin{cases} |x\rangle |0\rangle \mapsto |x\rangle |x\rangle \\ |x\rangle |1\rangle \mapsto |x\rangle |1 - x\rangle , \end{cases} \qquad x \in \{0, 1\}$$

These allows us to simulate every classical circuit with a unitary quantum circuit. Notice that all the gates are permutations over the computational basis, so the quantum state at any time is a basis state, and the final measurement is the same as simply reading the classical bit. □

Theorem 3. $\mathsf{BPP} \subseteq \mathsf{BQP}$

Proof. Since BPP is just P enhanced with random bits, we only need to simulate `COIN-FLIP` with a quantum circuit. This can be done first applying the Hadamard gate:

$$H : \begin{cases} |0\rangle \mapsto |+\rangle \\ |1\rangle \mapsto |-\rangle \end{cases}$$

and measure the result in $\{|0\rangle, |1\rangle\}$, which always gives 0 or 1 with $1/2$ probability each regardless of the state being $|+\rangle$ or $|-\rangle$. □

The proof here is not complete as in our definition of quantum circuits we only allow measurements at the end, while here we have intermediate measurements in the circuit. We will show how to resolve this problem in the next lecture.