CMSC 657: Introduction to Quantum Information Processing
Lecture 6

Instructor: Daniel Gottesman

Fall 2024

1 Universal Gate Sets

We would like to be able to do any kind of computation by starting with only a few basic types of gates. A gate set that lets us put together the fundamental gates into any allowed function or unitary is called *universal*.

Universal classical gate sets: The goal here is to compute an arbitrary function $f(x_0, x_1, x_2, \ldots, x_{n-1})$ on n bits. We can write f as a polynomial of total degree at most n (since $x^2 = x$ for bits).

- **Irreversible:** $\{\text{NOT}, \text{AND}\}$ is a universal gate set. (a AND $b = ab$, NOT $a = a \oplus 1$, NOT [(NOT a) AND (NOT b)] = a OR $b = ab \oplus a \oplus b$, a XOR b = (a AND NOT b) OR (NOT a AND b) = $a \oplus b$. XOR lets us add terms in the polynomial, NOT gives us constant terms, AND lets us build up higher-degree terms. For instance, (a AND b AND c) XOR (a AND c) XOR $b = abc \oplus ac \oplus b$.
- **Reversible:** $\{\text{Tof}, 0 \text{ and } 1 \text{ ancilla preparation}\}$ form a universal gate set. (Tof with first two inputs 11 is the NOT, Tof with last input 0 is the AND.)

Universal quantum gate sets: The goal is now to perform arbitrary unitaries, elements of $SU(2^n)$ (since we do not care about global phase). We can talk about *exact* universality (getting any unitary exactly), or *approximate* universality (creating unitaries which are arbitrarily close to any unitary – i.e., set of possible unitaries is dense in $SU(2^n)$).

- **Exact:** $\{\text{CNOT}, \text{single-qubit unitaries}\}$
- **Approximate:** $\{H, R_{\pi/2}, \text{Tof}\}$, $\{\text{CNOT}, H, R_{\pi/4}\}$.

For exact universality, we need an infinite family of gates because there is an infinite (uncountable) set of unitaries. But for approximate universality, it turns out that only a finite set of gates can be enough.

1.1 Distance Measures

How do we measure whether two quantum states are close to each other? There is not a unique answer to this question, and in fact there are multiple good ones, useful in different circumstances.

For pure states, the most natural measure is the inner product between two states. This can involve complex numbers, so we actually use the *fidelity*, the absolute value of the inner product:

$$F(|\phi\rangle, |\psi\rangle) = |\langle\phi|\psi\rangle|. \tag{1}$$

There is also a notion of fidelity between mixed states which is generalization of this definition. The point of the fidelity is that it is 1 when the states are identical and close to 1 when they are very close together.

There are other useful measures of closeness between mixed states, for instance the *trace distance.*. This is defined as

$$d(\rho, \sigma) = \frac{1}{2} \operatorname{Tr} |\rho - \sigma|. \tag{2}$$

For the purposes of approximate universality, we also need a measure of distance on unitary operators. Again, there are various possible choices. One common operator norm goes by a few names, such as the sup norm or the infinity norm. The sup norm is applied to linear operators acting on the Hilbert space, and it is defined as

$$\|A\|_{\sup} = \sup_{|\psi\rangle} \|A|\psi\rangle\|. \tag{3}$$

Here, the supremum is taken over normalized states. The sup norm is the maximum amount the operator can stretch (or the least amount it can shrink) a vector and is equal to the largest eigenvalue of the matrix.

We can also measure closeness bewteen CPTP maps using various ideas. We will discuss them and revisit the above notions of distance in more detail later in the course.

1.2 Efficiency of Gate Approximation

Just because we can get arbitrary functions or unitaries exactly or approximately does not mean we can do so *efficiently*. On the contrary, most functions or unitaries require exponentially many gates (in the number of bits/qubits). It is an important question in general to determine which functions/unitaries do not need so many and how to write them as smaller circuits. This is the topic of (quantum) algorithms and complexity, which we will discuss more next week.

However, if we have a fixed qubit dimension, approximately universal gate sets allow us to rapidly approximate unitaries to high accuracy.

Theorem 1 (Solovay-Kitaev theorem)**.** *Given any approximately universal gate set for n qubits that generates the exact inverses of all the gates in the gate set, then there is a classical algorithm that takes as input $\epsilon > 0$, unitary U, runs in time polynomial in $\log 1/\epsilon$, and outputs a circuit $V = V_1 V_2 \dots V_k$, with k polynomial in $\log 1/\epsilon$ and $\|V - U\|_{\sup} < \epsilon$.*

This theorem means we can get very good approximations with a modest cost. Do note, though, that the algorithm and number of gates needed is exponential in the number of qubits n; it is only efficient in terms of $1/\epsilon$.

2 Example Quantum Circuits

2.1 Bell Measurement

The Bell measurement is an entangled projective measurement on two qubits with 2 classical bits xz as the outcome:

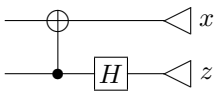
$$\Pi_{00} = |\Phi^+\rangle\langle\Phi^+|, \quad |\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{4}$$

$$\Pi_{01} = |\Phi^-\rangle\langle\Phi^-|, \quad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{5}$$

$$\Pi_{10} = |\Psi^+\rangle\langle\Psi^+|, \quad |\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{6}$$

$$\Pi_{11} = |\Psi^-\rangle\langle\Psi^-|, \quad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{7}$$

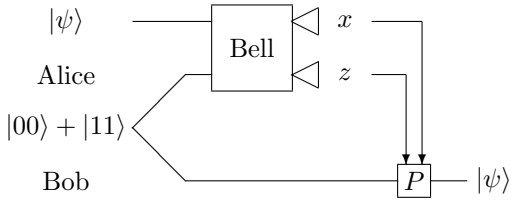
We can do the Bell measurement with the following circuit:



If we have the input state $|\Phi^+\rangle$, we always get the measurement outcome $xz = 00$. If we have $|\Phi^-\rangle$, we get the outcome 01. If we have $|\Psi^+\rangle$, we get 10, and if we have $|\Psi^-\rangle$, we get the outcome 11, as desired.

2.2 Quantum Teleportation

One interesting example of a quantum circuit is quantum teleportation. This is a simple quantum protocol. It usually is phrased in terms of two people, Alice and Bob. Alice has a qubit which she wants to send to Bob, who is far away. If they only have a classical communications channel, there is no way to do this. Measuring will destroy the state and lose some information about superpositions. However, if Alice and Bob have previously shared an entangled state, there is a way to do it. In particular, let us assume that Alice and Bob were together in the past, or used to have a quantum channel, or in some other way acquired the entangled state $|00\rangle + |11\rangle$, with the first qubit held by Alice and the second qubit held by Bob. Now Alice wants to send a state $|\psi\rangle$ to Bob. Alice is going to make a measurement on the qubit she wants to send and her qubit from the entangled state, then send 2 classical bits to Bob, who, based on those two bits, will do a unitary operation on his qubit from the entangled state. This unitary takes Bob's qubit into exactly the state of Alice's original qubit!



The initial entangled state is $|\Phi^+\rangle$, one of the Bell states. The Bell states are "maximally" entangled states and are also called *EPR pairs* due to the Einstein-Podalsky-Rosen argument which highlighted the non-local nature of quantum mechanics. Based on the 2-bit outcome of Alice's measurement, Bob does P, which is one of the 4 Pauli matrices.

$$xz = 00, \quad P = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{8}$$

$$xz = 01, \quad P = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{9}$$

$$xz = 10, \quad P = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{10}$$

$$xz = 11, \quad P = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{11}$$

Here are a few observations about this protocol:

1. Alice's I qubit was destroyed and replaced by part of a Bell state. It had to be this way because the No-Cloning Theorem prohibits us from leaving a copy behind with Alice when Bob gets one.

2. The entangled state is also used up in the process. We need a new entangled state every time we want to teleport a qubit.

3. Because entanglement with reference systems is preserved, we can teleport multiple qubits by repeating this protocol. To teleport n qubits, we need n entangled pairs plus $2n$ classical bits transmitted.

4. The amplitudes α and β are complex numbers, with arbitrary precision. Despite this, with the aid of the entanglement, we can transmit them to Bob by just sending 2 classical bits.

5. The probability of each measurement outcome is $1/4$, irrespective of the state $|\psi\rangle$. This means that the classical bits being sent are completely random, with no information about the input state.

6. Before applying P, the density matrix of Bob's qubit is $I/2$, the completely mixed state. Thus, Bob's qubit before receiving the classical bits from Alice is also completely random, with no information about the input state.

7. Despite the previous two points, the classical bits and Bob's qubit together can be put together to exaclty reconstruct Alice's input qubit.

Teleportation breaks the task of "quantum communication" into a "quantum" part — the entangled state — and a "communication" part — the classical bits.