CS 593/MA 592 - Intro to Quantum Computing
Spring 2024
Tuesday, January 30 - Lecture 4.1

Today's scribe: Ralph Razzouk

Reading: Subsection 4.1-4.5.3 of Nielsen and Chuang.

Agenda:

1. Approximating unitaries and universality
2. Single qubit gates
3. "Two-level" unitaries
4. $\{H,T,CNOT\}$ universal gate set

Last time we showed the set of all 3-ary quantum gates $\mathcal{G} := U\left(2^3\right)$ was sufficient to encode all Boolean functions in quantum circuits. In fact, this was overkill. All we really needed were the 3-ary permutations of the computational basis vectors

$$U(8) \geq \mathcal{G} = \{\text{permutations of computational basis}\} \cong S_8.$$

While permutations in the computational basis are enough to encode all classical calculations "quantumly," it is not hard to convince oneself that permutation matrices will never be enough to implement all unitary transformations on qubit (even just approximately to within, say, error at most 0.01).

Our goal today will be to fix this. We will show that the gate set $\mathcal{G} = \{H,T,CNOT\}$ is enough to approximately simulate all possible unitaries on any number of qubits.

1 Approximating Unitaries and Universality

A discrete set of gates can't be used to implement an arbitrary unitary operation *exactly*, since the set of unitary operations is continuous. However, it turns out that a discrete set can be used to *approximate* any unitary operation. To understand how this works, we first need to study what it means to approximate a unitary operation. Suppose U and V are two unitary operators on any Hilbert Space $\mathcal{H}$ (e.g. $\mathcal{H} = \left(\mathbb{C}^2\right)^{\otimes k}$), where U is the target unitary operator that we wish to implement, and V is the unitary operator that is actually implemented in practice. We define the error when V is implemented instead of U by

$$E(U,V) := ||U-V|| := \sup_{|\psi\rangle \neq 0} \frac{||(U-V)|\psi\rangle||}{||\,|\psi\rangle\,||} = \sup_{|||\psi\rangle||=1} ||(U-V)|\psi\rangle||,$$

where the supremum is taken over all normalized quantum states $|\psi\rangle$ in the state space. As we will now show, this notion of error is pertinent because it bounds the difference in the outcome distributions of any projective measurement when performed on $U|\psi\rangle$ and $V|\psi\rangle$ (in the infinity norm, for those who know what this means).

Here's what I mean in detail. For any projective measurement (that is, Hermitian operator), we have a spectral decomposition $A = A^* = \sum_\lambda \lambda P_\lambda$. Then

$$\begin{aligned}
|P(\lambda|U|\psi\rangle) - P(\lambda|V|\psi\rangle)| &= |\langle\psi|U^* P_\lambda U|\psi\rangle - \langle\psi|V^* P_\lambda V|\psi\rangle| \\
&= |\langle\psi|U^* P_\lambda (U-V)|\psi\rangle - \langle\psi|(U^*-V^*)P_\lambda V|\psi\rangle| \\
&\leq ||(U-V)|\psi\rangle|| + ||(U-V)|\psi\rangle|| \qquad \text{(Cauchy-Schwarz inequality)} \\
&\leq 2E(U,V).
\end{aligned}$$

Thus, when $E(U,V)$ is small, then measurement outcomes occur with similar probabilities, regardless of whether U or V were performed.

Moreover,

$$\begin{aligned}
E(U_2U_1,V_1V_2) &= \sup_{|||\psi\rangle||=1} ||(U_2U_1 - V_1V_2)\,|\psi\rangle\,|| \\
&= \sup_{|||\psi\rangle||=1} ||(U_2U_1 - V_2U_1)\,|\psi\rangle + (V_2U_1 - V_1V_2)\,|\psi\rangle\,|| \\
&\leq \sup_{|||\psi\rangle||=1} ||(U_2U_1 - V_2U_1)\,|\psi\rangle\,|| + \sup_{|||\psi\rangle||=1} ||(V_2U_1 - V_1V_2)\,|\psi\rangle\,|| \\
&= E(U_2,V_2) + E(U_1,V_1).
\end{aligned}$$

Inductively, we have

$$E(U_mU_{m-1}\cdots U_2U_1, V_mV_{m-1}\cdots V_2V_1) \leq \sum_{i=1}^{m} E(U_i,V_i).$$

The take-away from this is that if we want to approximate unitaries that are a composition of gates over a "big" gate set using a "small" gate set, it suffices to approximate the gates individually.

Definition. *A gate set $\mathcal{G}$ is universal if, for all natural numbers k, unitaries $U \in U(2^k)$, and all $\varepsilon > 0$, we can find a circuit C over the gate set $\mathcal{G}$ on $k+\ell$ qubits (where the ℓ extra qubits are ancillas), such that*

- *The circuit C, when restricted to the subspace where all the ancillas are set to 0, sends that subspace back to itself.*

$$C|_{(\mathbb{C}^2)^{\otimes k}\otimes|0\cdots0\rangle}\left((\mathbb{C}^2)^{\otimes k}\otimes|0\cdots0\rangle\right) = (\mathbb{C}^2)^{\otimes k}\otimes|0\cdots0\rangle \cong (\mathbb{C}^2)^{\otimes k}$$

- *When the circuit C, restricted to the subspace where all the ancillas are set to 0, is implemented instead of the target unitary operator U, then the error is smaller than ε.*

$$E\left(U, C|_{(\mathbb{C}^2)^{\otimes k}\otimes|0\cdots0\rangle}\right) < \varepsilon$$

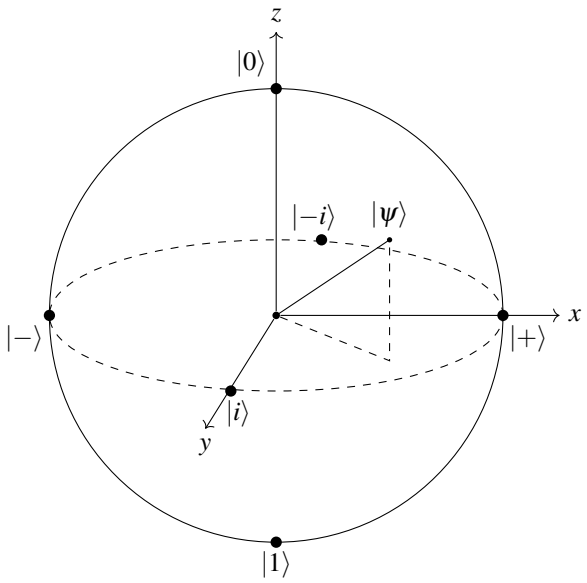
Our goal will be to show that $\mathcal{G} = \{H,T,CNOT\}$ is universal, even without any ancillas.

2 Single Qubit States

$$U(2) \to U(2)/\text{global phases} \equiv PU(2) \cong SO(3)$$

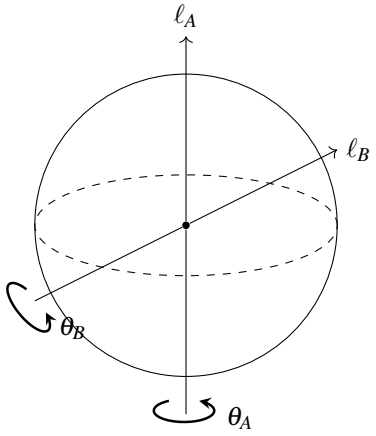
$$\mathbb{C}^2 - \{0\} \to \mathbb{C}^2 - \{0\}/\text{global phases} \equiv \mathbb{CP}^1 \simeq S^2 \quad \text{(Fubiny study metric)}$$

In other words, up to unimportant global phases, single qubit gates act like rotations of S^2, which we call the Bloch sphere.



Claim. *Let $A, B \in SO(3)$ with infinite order $|A| = |B| = \infty$ (i.e. $A^k \neq Id$ for any $k > 0$, similar for B) and $[A,B] \neq 0$ (i.e. A and B don't commute). Then the subgroup of $SO(3)$ generated by A and B, denoted by $\langle A,B \rangle \leq SO(3)$ is dense in $SO(3) \cong PU(2)$.*

Proof. This is really a problem in geometry, so we'll just sketch the general idea. Since $|A| = |B| = \infty$, A, B are rotations of infinite order. Let ℓ_A and ℓ_B be their rotation axes. Since $|A| = |B| = \infty$, then their rotation angles θ_A and θ_B must be irrational multiples of 2π. Note that the set of all integer multiples of either of these two angles is dense in the interval $[0, 2\pi]$. Thus, we can approximately implement any rotation around the two axes ℓ_A and ℓ_B. Moreover, since $[A,B] \neq 0$, then ℓ_A and ℓ_B are distinct. From here, one can further argue that we can aproximately implement any rotation around *any* axis ℓ. □



Theorem 4.1 in the book shows that every element of $SO(3)$ can be written as

$$R_y(\theta_3) R_z(\theta_2) R_y(\theta_1).$$

Thus, it suffices to show that, for any $\varepsilon > 0$, we can find $w \in \langle A,B \rangle$ such that the axis of w is within ε of being orthogonal to ℓ_A and w has infinite order. A similar statement holds for any two rotation axes that are orthogonal. For non-orthogonal rotation axes, we have to alternate between the two axes (see the announcement I sent about HW3).

In fact, the only two-generated subgroups of $SO(3)$ that are infinite and not dense are either abelian with a constant rotation axis or "infinite dihedral." In other words, any non-dense infinite subgroup preserves a plane.

Corollary 1. *$\langle H, T\rangle$ is dense in $PU(2) \approx SO(3)$.*

Proof. Let $A = THTH$ and $B = HTHT$, then read the book to learn why A and B satisfy the conditions of the previous Claim. □

Note. *1-qubit gates will never be universal.*

3 Two-Level Unitaries

Definition. *A two-level unitary on k qubits is a unitary*

$$U : \left(\mathbb{C}^2\right)^{\otimes k} \to \left(\mathbb{C}^2\right)^{\otimes k}$$

that acts non-trivially on at most two computational basis vectors (i.e. up to permuting rows and columns by the same permutations)

$$U = \begin{pmatrix} \tilde{U} & 0 \\ 0 & \mathbb{I}_{2^n-1} \end{pmatrix}.$$

Example.

$$U = \begin{pmatrix} a & 0 & \cdots & 0 & c \\ 0 & & & & 0 \\ 0 & & \mathbb{I} & & 0 \\ 0 & & & & 0 \\ b & 0 & \cdots & 0 & d \end{pmatrix}$$

where $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ *is unitary.*

Note that two-level unitaries are *not* 2-qubit gates. Rather, a two-level unitary is like a *single* qubit gate, but on a "logical qubit" that is "mixed up" in the state space of n qubits.

Claim. *$\mathcal{G} = \{$ all k-qubit 2-level unitaries $/k \in \mathbb{N}\}$ is universal.*

The book gives a very hands-on but somewhat opaque proof of this claim. I will give a high-brow conceptual explanation that depends on two key facts:[1]

- Every unitary can be written as $U = \exp(iH)$, where H is Hermitian.
- The Trotter product formula

$$\exp(i(A+B)) = \lim_{n\to\infty}\left[\exp\left(\frac{iA}{n}\right) + \exp\left(\frac{iB}{n}\right)\right].$$

Proof. Let U be a unitary on n-qubits, i.e. $U \in U(2^n)$. Write $U = \exp(iH)$ for some Hermitian $H : \left(\mathbb{C}^2\right)^{\otimes n} \to \left(\mathbb{C}^2\right)^{\otimes n}$. For all $0 \le \ell \le k \le 2^n - 1$, define the following three types of matrices:

1. $E_{l,k}$, the matrix with a 1 in the (l,k) and (k,l) entry, and 0's elsewhere
2. $E_{l,l}$, them matrix with a 1 in the (l,l) spot and 0's elsewhere.
3. $F_{l,k}$, the matrix with an i in the (l,k) spot, a $-i$ in the (k,l) spot and 0's elsewhere.

[1] Let me note that my construction shows universality, whereas the book shows something stronger about 2-level unitaries: every unitary can be *exactly* implemented by a composition of two-level unitaries. I will just show they can be *approximately* implemented.

Notice that $\text{span}_{\mathbb{R}}\{E_{\ell,k}, F_{\ell,k}\} = \{\text{all Hermitians}\}$. We can thus write

$$H = \sum_{0\le\ell\le k\le 2^k-1} r_{\ell,k}E_{\ell,k} + \sum_{0\le\ell\le k\le 2^k-1} s_{\ell,k}F_{\ell,k},$$

where $r_{\ell,k}, s_{\ell,k} \in \mathbb{R}$.

Trotter's formula shows that we can approximately implement $\exp(i(A+B))$ any time we can (exactly) implement $\exp\left(\frac{iA}{n}\right)$ and $\exp\left(\frac{iB}{n}\right)$, for all n.

Inductively, we can see that, to implement U approximately, it suffices to exactly implement

$$\exp\left(i\frac{r_{\ell,k}E_{\ell,k}}{n}\right) \qquad \text{and} \qquad \exp\left(i\frac{s_{\ell,k}f_{\ell,k}}{n}\right)$$

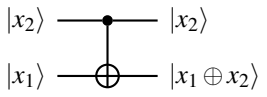
for all n by two-level unitaries. Well, these kinds of matrices **are** two-level unitary matrices, so we're done. □

4 $\{H, T, CNOT\}$ Universal Gate Set

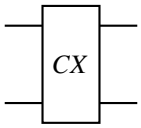
Claim. *$\mathcal{G} = \{H, T, CNOT\}$ is universal.*

Proof. By our previous results, it suffices to approximate every two-level unitary by a quantum circuit built out of arbitrary 1-qubit gates and CNOT. §4.3, §4.4 are mostly about this, so I will refer you there for full details. Let me give you the basic idea.

Recall that CNOT (a.k.a C-X) is



also occasionally written as



but this isn't ideal, because it's unclear which input is the control.

More generally, for any single qubit unitary $U : \mathbb{C}^2 \to \mathbb{C}^2$, we define the two qubit controlled CU operation by

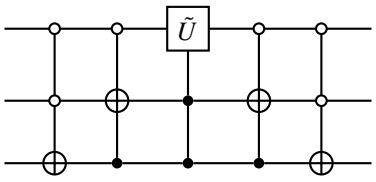
$$\begin{aligned} CU : \mathbb{C}^2 \otimes \mathbb{C}^2 &\to \mathbb{C}^2 \otimes \mathbb{C}^2 \\ |0\rangle \otimes |x\rangle &\mapsto |0\rangle \otimes |x\rangle \\ |1\rangle \otimes |x\rangle &\mapsto |1\rangle \otimes (U|x\rangle). \end{aligned}$$

Example.

$$U = \begin{pmatrix} a & & c \\ & \mathbb{I} & \\ b & & d \end{pmatrix} \qquad \textit{on 3-qubits } (8\times 8 \textit{ matrix})$$

U acts non-trivially only on $|000\rangle$ and $|111\rangle$. So, we should build a circuit (over 1-qubit gates and CNOTs) that approximates U. Let $\tilde{U}$ be the 1-qubit gate

$$\tilde{U} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$


$\tilde{U}$

□