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

Remark. *3-ary quantum gates $g = U\left(2^3\right)$ were sufficient to encode all Boolean functions in quantum circuits. This is an overkill. In fact*

$$g = \{\textit{permutations of computational basis}\} \simeq S_8.$$

Permutations in the computational basis are enough to encode all classical calculations 'quantumly', but not all unitaries, even just approximately.

Our goal today will be to fix this system, showing that the gate set $g = \{H, T, CNOT\}$ is enough.

1 Approximating Unitaries and Universality

If U and V are two unitary operators on any Hilbert Space $\mathcal{H}$ (e.g. $\mathcal{H} = \left(\mathbb{C}^2\right)^{\otimes k}$), then the error is given by

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

For any projective measurement, we have $A = A^* = \sum_\lambda \lambda P_\lambda$. Then

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

Thus, when $E(U,V)$
Moreover,

$$\begin{aligned}
E(U_2U_1, W_1W_2) &= \sup_{|||\psi\rangle||=1} ||(U_2U_1 - W_1W_2)|\psi\rangle|| \\
&= \sup_{|||\psi\rangle||=1} ||(U_2U_1 - W_2U_1)|\psi\rangle + (W_2U_1 - W_1W_2)|\psi\rangle|| \\
&\leq \sup_{|||\psi\rangle||=1} ||(U_2U_1 - W_2U_1)|\psi\rangle|| + \sup_{|||\psi\rangle||=1} ||(W_2U_1 - W_1W_2)|\psi\rangle|| \\
&= E(U_2, W_2) + E(U_1, W_1).
\end{aligned}$$

Inductively, we have

$$E(U_m U_{m-1} \cdots U_2 U_1, W_m W_{m-1} \cdots W_2 W_1) \leq \sum_{i=1}^{m} E(U_i, W_i).$$

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 them individually.

Definition. *A gate set g is universal if*

$$\forall k \in \mathbb{N}, \forall U \in U\left(2^k\right) \wedge \forall \varepsilon > 0, \exists \text{ circuit } C \text{ over } g \text{ on } k+\ell \text{ qubits } (\ell \text{ ancillas})$$

such that:

- $$C\big|_{\left(\mathbb{C}^2\right)^{\otimes k} \otimes |0\cdots 0\rangle} = \left(\mathbb{C}^2\right)^{\otimes k} \otimes |0\cdots 0\rangle \simeq \left(\mathbb{C}^2\right)^{\otimes k}$$
- $$E\left(U_1, C\big|_{\left(\mathbb{C}^2\right)^{\otimes k} \otimes |0\cdots 0\rangle}\right) < \varepsilon$$

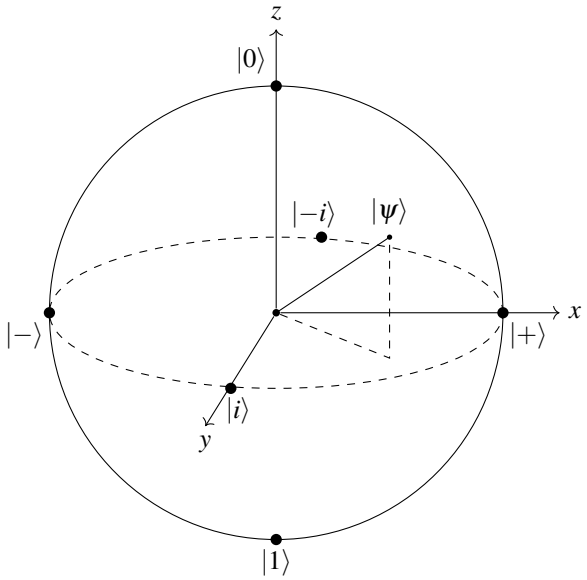
Our goal will be to show that $g = \{H, T, CNOT\}$ is universal, even without any ancillas.

2 Single Qubit States

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

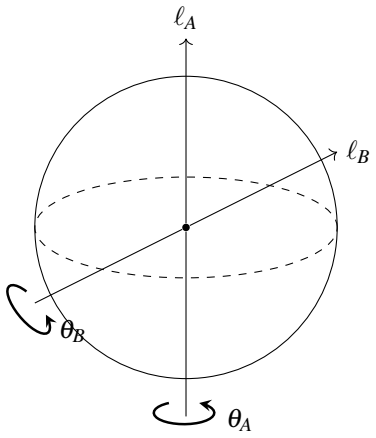
$$\mathbb{C}^2 - \{0\} \to \mathbb{C}^2 - \{0\}/\text{global phases} \equiv \mathbb{CP}^1 \simeq S^2 \quad \text{(Fubiny study metric)}$$

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 $|A| = |B| = \infty$ (i.e. $A^k \neq Id$ for any $k > 0$, similar for B). We want $[A, B] \neq 0$ so that we do not have redundancies. Then the subgroup of $SO(3)$ generated by A and B, denoted by $\langle A, B\rangle \leq SO(3)$ is dense.*

Proof. Idea of proof: 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. Moreover, since $[A,B] \neq 0$, then ℓ_A and ℓ_B are distinct. □



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

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

This, 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. In fact, the only two-generated subgroups of $SO(3)$ that are infinite and not dense are abelian with a constant rotation axis or "infinite dihedral" (i.e. 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. □

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.*

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

A high-brow explanation is as follows. We need to key facts:

- Every unitary can be written as $U = \exp iH$, where H is Hermitian.
- 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 $H : \left(\mathbb{C}^2\right)^{\otimes n} \to \left(\mathbb{C}^2\right)^{\otimes n}$. Define, for all $0 \le \ell \le k \le 2^n - 1$

$$E_{\ell,k} = \begin{pmatrix} 0 & & 1 \\ & \ddots & \\ 1 & & 0 \end{pmatrix}, \text{ if } \ell < k,$$

$$E_\ell = E_{\ell,\ell} = \begin{pmatrix} 0 & & \\ & \ddots & \\ & & 0 \end{pmatrix},$$

$$F_{\ell,k} = \begin{pmatrix} 0 & & -i \\ & \ddots & \\ i & & 0 \end{pmatrix}.$$

noticing that $\operatorname{span}_{\mathbb{R}}\{E_{\ell,k}, F_{\ell,k}\} = \{\text{all Hermitians}\}$. We now 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.

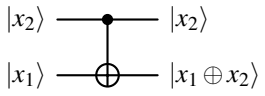
Inductively, we can see that, to implement U approximately, it suffices to implement $\exp\left(i\frac{r_{\ell,k}E_{\ell,k}}{n}\right)$ and $\exp\left(i\frac{s_{\ell,k}f_{\ell,k}}{n}\right)$ (exactly) for all n by two-level unitaries. Well, these two **are** two-level unitary matrices. □

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

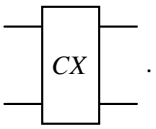
Claim. *$g = \{H, T, CNOT\}$ is universal.*

Proof. By our previous work, 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). □

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



also written as



.

More generally, for any unitary $U : \mathbb{C}^2 \to \mathbb{C}^2$,

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

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.

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