S. KIMMEL

Universality

Classically

OR, AND, NOT,
↓
can combine to create any Boolean function

Quantumly

Small set of ≤ 2 qubit unitaries
↓
can combine to create any unitary?

Universal Discrete Gate Set

For fault tolerant computing, need a discrete set of gates:

$G_1, G_2 \cdots G_t$

$\underbrace{R_z(\theta)}$ uncountably ∞ set of unitaries

Problem: can form countably ∞ unitaries

Can't hope to do many unitaries exactly, but if approximate, is OK.

Approximate?

- Want: $\underset{\text{Ideal } U}{U}|0\rangle^{\otimes n} = |\psi\rangle$, $\underset{\text{Approximate } U}{U'}|0\rangle^{\otimes n} = |\psi'\rangle \Rightarrow |\psi\rangle \approx |\psi'\rangle$?

$\approx$?

- Want: $|\psi\rangle \approx |\psi'\rangle \Rightarrow$ Small probability that any measurement can distinguish $|\psi\rangle$ from $|\psi'\rangle$

S.KIMMEL

def: Given $|\psi\rangle$ and $|\psi'\rangle$, their $\underline{l_2\text{-distance}}$ is

$$\| |\psi\rangle - |\psi'\rangle \| = \sqrt{(\langle\psi| - \langle\psi'|)(|\psi\rangle - |\psi'\rangle)} \qquad \text{where } \underset{l_2\text{-norm}}{\| |v\rangle \|} = \sqrt{\langle v|v\rangle}$$

$$= \sqrt{2 - 2\,\mathrm{Re}(\langle\psi|\psi'\rangle)}$$

Properties of trace distance

- Probability that any measurement can distinguish $|\psi\rangle$ from $|\psi'\rangle$ is $\leq \| |\psi\rangle - |\psi'\rangle \|$
- Metric: Δ inequality, symmetry, $\| |\psi\rangle - |\psi\rangle \| = 0$
- If $|\psi\rangle, |\psi'\rangle$ orthogonal $\rightarrow \| |\psi\rangle - |\psi'\rangle \| = \sqrt{2}$
- $\| |\psi\rangle - (-|\psi\rangle) \| = 2$ ... weird

Now can be precise about a unitary approximating another:

def: $E(U, U') = \max_{|\psi\rangle} \| U|\psi\rangle - U'|\psi\rangle \|$ discuss why good def

$= \max_{|\psi\rangle} \| (U - U')|\psi\rangle \|$

$\underline{E(U,V) \text{ properties}}$

(a) Metric: Δ inequality

(b) $E(U, U') = E(VU, VU') = E(UV, U'V)$

- Using (a), (b) can show $E(UV, U'V') \leq E(U, U') + E(V, V')$

"composition" $\quad E\left(\prod_{i=1}^{k} U_k, \prod_{i=1}^{k} U_k'\right) \leq \sum_i E(U_i, U_i')$

Exercise: $\max_{|\psi\rangle}$ Important? Find $\max_{|\psi\rangle} \| R_z(\frac{-\pi}{2})|\psi\rangle - R_z(\frac{\pi}{2})|\psi\rangle \|$

$\min_{|\psi\rangle}$ " "

Maybe seemed like max over all measurements was overkill, but important for composition

S. KIMMEL

def: A gate set is universal if for any unitary U (on any # of qubits), and any $\varepsilon > 0$, $\exists$ gates $V_1, \dots, V_k$ from the set s.t.

$E(U, V_k^{A_k} \dots V_2^{A_2} V_1^{A_1}) < \varepsilon$ $\quad V_i^{A_i} = V_{A_i} \otimes I_{\text{elsewhere}}$

ex: $\left\{ H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \; T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}, \; CNOT \right\}$ are universal

"$\pi/8$-gate"

In this case

Sufficient condition: Gate Set is universal $\Longleftarrow$
- universal for single qubit (H, T)
- contains an entangling gate $(CNOT)$

def: U is entangling if $U|\psi_1\rangle_A|\psi_2\rangle_B$ is entangled b/t A, B.

Sufficient condition: Universal for single qubit $\Longleftarrow$
- Bloch sphere rotation by irrational multiple of π (HT)
- Bloch sphere rotations about 2 axes (H, T)

Efficiency

Not every unitary can be implemented efficiently. (Countable vs uncountable!)

Maybe some gate sets are better than others? ... No!

Thm: Given a universal single qubit gate set S s.t. if $G \in S$ then $G^\dagger \in S$, gates from S can approximate any single qubit gate to error ε using $\leq \text{poly}(\log(\frac{1}{\varepsilon}))$ gates. [Solovay-Kitaev]

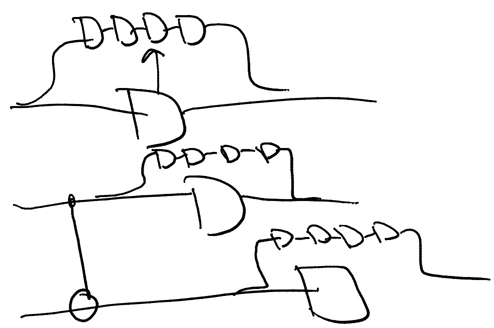
S.KIMMEL

Ex: • Let U be a circuit with m single qubit gates $U_1, U_2, \ldots U_m$. & some CNOTS.

• You have access to perfect CNOTS & universal single qubit gate set S.

• Suppose you want to create V, and approximation to U, by approximating each U_i with a set of gates from S.

• If we want $E(U,V) \leq \varepsilon$, how many single qubit gates are sufficient to create V?



$$E\left(\prod U_i, \prod U_i'\right) \leq \sum_i E(U_i, U_i')$$