2. Universal gate set, quantum circuit

Isaac H. Kim (UC Davis)

Universal quantum gates

- The goal is to generate an arbitrary unitary in $U(2^n)$.
- The Lie algebra of $U(2^n)$ consists of $2^n \times 2^n$ anti-Hermitian matrices.
- Claim: Single- and two-qubit gates generate the universal gate set.

$$\mathcal{H} = \bigotimes_{i=1}^{n} \mathcal{H}_i$$

Single-qubit gates

- Basis: $|0\rangle, |1\rangle$
- General form: $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, UU^\dagger = U^\dagger U = I.$
- Examples
  - Paulis: $X = \overset{\sigma_x}{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}, Y = \overset{\sigma_y}{\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}}, Z = \overset{\sigma_z}{\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}}.$

  - $\exp(i\theta X), \exp(i\theta Y), \exp(i\theta Z), \ldots$

Two-qubit gates

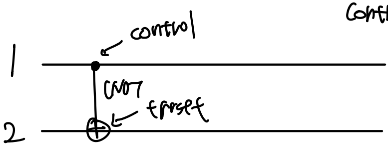
- Basis: $|00\rangle, |01\rangle, |10\rangle, |11\rangle$
- Examples: CNOT, CZ

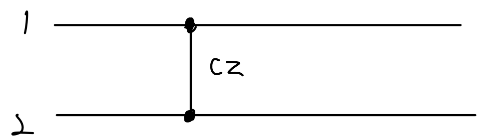
$$\begin{matrix} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{matrix} \xrightarrow{CNOT_{1,2}} \begin{matrix} |00\rangle \\ |01\rangle \\ |11\rangle \\ |10\rangle \end{matrix}$$

$$\begin{matrix} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{matrix} \xrightarrow{CZ_{2,1} = CZ_{1,2}} \begin{matrix} |00\rangle \\ |01\rangle \\ |10\rangle \\ -|11\rangle \end{matrix}$$

$CNOT_{1,2}$: CNOT from 1 to 2

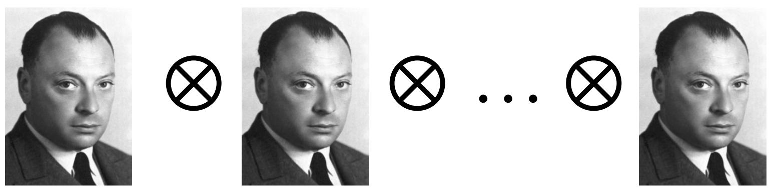
Control Target





n-qubit gates

- Basis: $|x\rangle$, where x is a n-bit string.
- Examples: Pauli product operators: $P_1 \otimes P_2 \otimes \ldots \otimes P_n$. $P_1, \ldots P_n \in \{I, X, Y, Z\}$



Universality

- To prove universality, it suffices to show that one can generate $\exp(iH\delta t)$ for any Hermitian operator H, with $\delta t \ll 1$.
- Basic idea: Decompose H into the canonical *Pauli basis* and apply infinitesimal rotation generated by each Pauli Product operators.

$$U = \left(\exp(iH\delta t)\right)^{\frac{T}{\delta t}}$$ → integer

$$H = \sum_P \alpha_P P$$ → Pauli Product operator

$\alpha_P \in \mathbb{R}$ why? Because Pauli Product operators form a basis of the set of operators

$$\exp(iH\delta t) \approx \prod_P \exp(i\alpha_P \delta t P)$$

$\exp(i\alpha_P \delta t P)$ $P = U(Z \otimes I \cdots \otimes I)U^\dagger$ U: sequence of CNOT, $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, $S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$

Experiments

As of now (Year 2021), the one and two-qubit gates have been implemented successfully in superconducting qubits, ion traps, neutral atoms, NV-centers, … (=pretty much any quantum technology)

Noise

- In real experiments, no gate is implemented perfectly.
- Current noise rate: $10^{-3} \sim 10^{-2}$, depending on the technology.
- This means that we cannot run a long computation and hope to get a correct result.

State-of-the-art quantum algorithms

- As of now, quantum algorithms with commercial applications which are (almost) guaranteed to work requires at least $10^8 \sim 10^9$ gates.
- To get a correct result with high probability, the error rate must be much smaller than $10^{-8} \sim 10^{-9}$.
- Current consensus is that we won't be able to achieve that without quantum error correction.

Quantum Error Correction

- Using quantum error correction, we can reduce the error.
- However, once we start using quantum error correction, the set of gates we can use becomes more restrictive.
- In fact, any reasonably continuous gate set, e.g., $\{\exp(i\theta Z) : \theta \in \mathbb{R}\}$ is incompatible with quantum error correction. [Eastin and Knill (2009)]

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Universal *Fault-tolerant* quantum gates

- Fortunately, there is a discrete set of universal gate set which is compatible with quantum error correction.
- There are different choices, but the following two is the standard.
  - Clifford + T
  - Hadamard + Toffoli

single-qubit unitary

$\{H, T\}$ $\quad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, $\quad T = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{i} \end{pmatrix}$

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

Any 2×2 unitary U can be approximated w. error $\leq \varepsilon$ using $O(\log \frac{1}{\varepsilon})$ H and T-gates.

Solovay-Kitaev theorem

[Solovay (1995), Kitaev (1997)] Given a universal gate set, one can find a gate sequence of length $O(\log^c(1/\epsilon))$ to approximate arbitrary unitary with an error of ϵ .

So, being restricted to a discrete gate set is not a problem.

Cliffords

- Clifford gates are unitaries U such that for every Pauli Product operator P, $UPU^\dagger$, is again a Pauli Product Operator.
- The Clifford group (consisting of Clifford gates) is generated by H, S, and $CNOT$.
- Clifford gates are cheap, compared to non-Clifford gates. (Fault-tolerant QC)

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

"Hadamard" gate   "phase" gate

Clifford

$$\exp(iP\theta) = \exp(i\, U (Z \otimes I \otimes \cdots \otimes I) U^\dagger \theta)$$

$$= U \exp(i (Z \otimes I \otimes \cdots \otimes I)\theta)\, U^\dagger$$

Non-Clifford gates

- A quantum computation consisting of Clifford gates can be efficiently simulated on a classical computer. [Gottesman-Knill theorem]
- To utilize the full power of quantum computation, we need gates outside of the Clifford group. These are called as non-Clifford gates.

  $T = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{i} \end{pmatrix}$

  ex) T-gate, Toffoli gate
- Non-Clifford gates are more expensive than Clifford gates. They are slower and requires more qubits to implement.
- Most of the time, the cost of a quantum algorithm is determined by the number of non-Clifford gates.

Rotations

- Rotations like $\exp(i\theta Z)$ may seem like the easiest gate you can implement.
- However, in a fault-tolerant quantum computer, this is even more expensive than non-Clifford gates.
- At this point, the (near-)optimal gate sequence can be efficiently computed on a classical computer. For precision ϵ, for general angle, we can implement this using $3\log_2(1/\epsilon) + O(\log\log(1/\epsilon))$ T-gates. This is optimal. [Ross and Selinger (2012)].
- For $\epsilon \approx 10^{-10}$, we need ≈ 100 T-gates.

$3\log_2(1/\epsilon) + O(\log(1/\epsilon))$

Cost analysis of different gates

(Fault-tolerant QC world)

Using the current best known fault-tolerant gate implementations, the number of qubits needed x time is (roughly):

- Clifford: 1 CNOT, CZ, H, S
- T-gate: 100 2-qubit gates
- Rotation: 10,000

Summary

- One- and two-qubit gates are universal.
- Fault-tolerant universal gate set: Clifford + non-Clifford(T-gate or Toffoli)
- Clifford ≪ non-Clifford ≪ Arbitrary rotation

X Z · · · · · Z X

Y Z · · · · Z Y

$|x\rangle \longrightarrow e^{i\tilde{x}}|x\rangle$

↓

n-bit number

$x = 11$

↓

$0.11 = \frac{1}{2} + \frac{1}{4} = 0.75$

$U|x\rangle|y\rangle = |x\rangle|y+x\rangle$

$|x\rangle|QFT\rangle \xrightarrow{U} |x\rangle|QFT\rangle e^{\frac{2\pi i x}{N}}$

$|QFT\rangle = \sum e^{\frac{2\pi i y}{N}} |y\rangle$