בית ספר הלן דילר לחישוב קוואנטי, אוקטובר 2020

הרצאות 3

פרופסור איתי ארז, טכניון

TECHNION | Helen Diller Quantum Center

Outline:

1. Definition of quantum algorithms
2. Universal set of gates
3. The powers and limitations of quantum algorithms
   - Quantum vs. classical algorithms
   - Entanglement
   - Interference

Quantum algorithms

$$U = U_k \cdot U_{k-1} \cdots U_1$$

$$U = \begin{pmatrix} y_1 & \cdots & \cdots & \cdots \\ \vdots & \ddots & & \\ \vdots & & \ddots & \\ y_{2^n} & & & \end{pmatrix}$$

Alternatively:

$$g_i^{\text{NZ}}(x_1, x_2, \ldots, x_n)$$

- **Input:** $x_1, x_2, \ldots, x_n$
- **"Running time":** L = number of gates
- **Initial state:** $|x_1\rangle \otimes |x_2\rangle \cdots |x_n\rangle \otimes |0\rangle^{poly}$
- **Efficient Alg:** $L = poly(n)$
- **Final state:** $|x_1\rangle \cdots U_k \cdots U_1 |x_1\rangle = c_{00\ldots0}|00\cdots0\rangle + \cdots + c_{11\ldots1}|11\cdots1\rangle$
- **Output:** $y_1, y_2, \ldots$ $\quad \Pr(b|x_1, y_1, \ldots) = p_{y_1,y_2,\ldots}$

Quantum algorithms are probabilistic algorithms!

- For a YES/NO problems

Assume:

$\Pr(\text{Outcome} = \text{"YES"}|\text{YES}) \geq 2/3$

$\Pr(\text{Outcome} = \text{"NO"}|\text{NO}) \geq 2/3$

repeat k times + majority voting

$\Pr(\text{Outcome} = \text{"YES"}|\text{YES}) \geq 1 - 2^{-O(k)}$

$\Pr(\text{Outcome} = \text{"NO"}|\text{NO}) \geq 1 - 2^{-O(k)}$

- Find a solution $F(y) = 0$

Assume:

$\text{Prob}[F(y) = 0] > \frac{1}{1000}$

repeat ~ 1000 times

Find a satisfying y with Prob ≥ 0.9

- Sometimes we just want to **sample** $\text{Prob}[y]$ (example: VQE)

Universal sets of gates

(1) Problem: there is an **infinite** number possible 1-qubit and 2-qubits gates

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \qquad \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix}$$

but any realistic physical device can only implement a small subset of them.

? Can we use any 1,2-qubit gates in our algorithm design?

? Can an algorithm that was written using a gate set of QC can be run on QC B, which has a different gate set?

Definition: A universal set of gate is a set of unitaries that can be used to generate (or approximate) any 1,2-qubits gates.

Idea: Assume we want to generate the set $\begin{pmatrix} e^{i\theta} & 0 \\ 0 & 1 \end{pmatrix}$ for all θ using a single gate

Pick:

$U_\pi \equiv \begin{pmatrix} e^{i\pi} & 0 \\ 0 & 1 \end{pmatrix}$ $\quad \theta_0$ is irrational w. respect to π $\quad (U_\pi)^k = \begin{pmatrix} e^{ik\pi} & 0 \\ 0 & 1 \end{pmatrix}$

Examples:

- All 1-qubit gates are generated by: Hadamard gate H and T gate.

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad T = \begin{pmatrix} 1 & \\ & e^{i\pi/4} \end{pmatrix}$$

- 2-qubit gates are generated by CNOT + all one-qubit gates
- n 2-qubit gates are generated by CNOT + H + T gates.
- IBM: H, X, Y, Z, T, S = T^2, $R_x(\theta)$, $R_y(\theta)$, $R_z(\theta)$, SWAP, CNOT, CZ, CRX, CRY, CRZ, etc...
- Many, many more examples...

The power of quantum computers

In principle, they are as strong as classical computers

AND	$a \wedge b$	
OR	$a \vee b$	non-reversible
COPY	$a \to a\,a$	
NOT	$\neg a$	

Use ancilla qubits:

Classical gates can be simulated by quantum gates

Evolution:

$$|x_1\rangle \to |x_1^{(1)}\rangle \otimes |x_2^{(1)}\rangle \otimes |x_3^{(1)}\rangle \cdots$$
$$|x_2\rangle \to |x_1^{(2)}\rangle \otimes |x_2^{(2)}\rangle \otimes |x_3^{(2)}\rangle \cdots$$
$$\vdots$$
$$|x_3\rangle \to |x_1^{(3)}\rangle \otimes |x_2^{(3)}\rangle \otimes |x_3^{(3)}\rangle \cdots$$

But quantum computers can do so much more...

For example: $\quad |x_1\rangle = 0.2200000 \cdots 0.3100001 + 0.8100000 \cdots 0.4795101|0\rangle$

Generally: $\quad |x_1\rangle = \sum_{x_1 \cdots x_n} \overbrace{c_{x_1 \cdots x_n}}^{2^{2^{\cdots}} \text{terms}} |x_1\rangle \otimes |x_2\rangle \cdots$

States in a Q.C. can be highly **entangled**!

Reminder:

- **Product state:** $|0\rangle \otimes |1\rangle, \quad |+\rangle \otimes |0\rangle, \quad |+\rangle \otimes |\phi\rangle$
- **Entangled states:** $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \quad 0.2200 \cdots + 0.3101 + 0.8101 \cdots + 0.4795|11\rangle$

(cannot be written as a product state)

Hard to simulate classically (seems to need exponential resources)

States in a Q.C. **must** be highly entangled for speedup

Assume we have no entanglement at all:

$$|\psi_1\rangle = |\phi_1^{(1)}\rangle \otimes |\phi_2^{(1)}\rangle \cdots \otimes |\phi_n^{(1)}\rangle$$
$$|\phi_1^{(1)}\rangle = \alpha_0^{(1)}|0\rangle + \alpha_1^{(1)}|1\rangle$$

$|\psi_1\rangle$ is represented using only $2n$ complex numbers

- Also easy to update:

$|\phi_1^{(2)}\rangle = |\phi_1^{(1)}\rangle$

$|\phi_2^{(2)}\rangle = A|\phi_2^{(1)}\rangle$ $\quad$ 4×4 matrix calculation

$|\phi_3^{(2)}\rangle = |\phi_3^{(1)}\rangle$

$|\phi_4^{(2)}\rangle = |\phi_4^{(1)}\rangle$

Algorithms with no entanglement have no speedup over classical algorithms

Quantum speedups are tricky

Entanglement is necessary but not sufficient.
We also need clever **interference**

Example of a hard problem: **constraint satisfaction**

- $x_1, x_2, \ldots, x_n \in \{0, 1\}$ boolean variables
- $C_1(x_1, x_2, x_3), \ldots, x_n$ set of boolean constraints over γ variables
- $F(x_1, \ldots, x_n) = C_1(x_1, x_2, x_3) \wedge C_2(x_2, x_3, x_4) \wedge C_3(x_1, x_2, x_4) \wedge \ldots$

Is there a satisfying $(x_1, x_2, \ldots, x_n)$ assignment?

A naive quantum algorithm (doesn't really work)

$$U_F(|0\rangle \otimes |x\rangle) = (F(x))|0\rangle \otimes |x\rangle$$

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \text{Hadamard gate} \qquad H|0\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$(H|0\rangle) \otimes (H|0\rangle) = (H|0\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) = (|00\rangle + |01\rangle)$$
$$= \frac{1}{2^{n/2}}(|00\cdots0\rangle + |00\cdots1\rangle + \ldots + |11\cdots1\rangle)$$
$$= \frac{1}{2^{n/2}}\sum_x |x\rangle \quad \text{uniform superposition of all strings}$$

What about:

$$|\psi_0\rangle = H^{\otimes n}|0\rangle$$

$$|\psi_1\rangle = H|0\rangle \otimes \frac{1}{2^{n/2}}\left(\sum_x |x\rangle - \frac{1}{2^{n/2}}\sum_x |0\rangle \otimes |x\rangle\right)$$
$$|\psi_2\rangle = \frac{1}{2^{n/2}}\sum_x U_F(|0\rangle \otimes |x\rangle)$$
$$|\psi_3\rangle = \frac{1}{2^{n/2}}\sum_x (F(x))|0\rangle \otimes |x\rangle$$

Can we find the solution by repeatably running the algorithm until we find x in the first register $(F(x))$?

Yes, but... $\quad \Pr(\text{Pick } x) = \left(\frac{1}{2^{n/2}}\right)^2 = \frac{1}{2^n}$

No quantum advantage

We need non-trivial **interference**

$$|\psi_0\rangle = |0\rangle \otimes H^{\otimes n} \qquad |\psi_1\rangle = \frac{1}{2^{n/2}}\sum_x |0\rangle \otimes |x\rangle \qquad |\psi_2\rangle = \frac{1}{2^{n/2}}\sum_x (F(x)) \otimes |x\rangle$$

Example of non-trivial interference:

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$H^2|0\rangle = \frac{1}{\sqrt{2}}H|0\rangle + \frac{1}{\sqrt{2}}H|1\rangle$$
$$= \frac{1}{2}(|0\rangle + |1\rangle) + \frac{1}{2}(|0\rangle - |1\rangle)$$
$$= |0\rangle$$

Constructive interference

Destructive interference

Summary

- Quantum speedups are tricky
- Necessary condition I: **entanglement**
- Necessary condition II: **non-trivial interference**