# The Circuit Model

Bei Zeng

University of Guelph

# What is computation?

To compute a function

$$x \to f(x)$$

$x = x_{n-1}x_{n-2}\dots x_1x_0, \quad x_i = 0, 1$

Example

$$f(x) = x_1 \oplus x_2 \oplus \cdots \oplus x_n$$

where the exclusive OR (XOR) gate:

$$\begin{array}{ccccc} 0 & \oplus & 0 & = & 0 \\ 0 & \oplus & 1 & = & 1 \\ 1 & \oplus & 0 & = & 1 \\ 1 & \oplus & 1 & = & 0 \end{array}$$

And a function with multi-bit output $x \oplus y$, where

$$\begin{aligned} x &= x_{n-1}x_{n-2}\dots x_1x_0 \\ y &= y_{n-1}y_{n-2}\dots y_1y_0 \end{aligned}$$

# More gates

| NOT | OR | AND | NAND |
|---|---|---|---|
| | $00 \to 0$ | $00 \to 0$ | $00 \to 1$ |
| $0 \to 1$ | $01 \to 1$ | $01 \to 0$ | $01 \to 1$ |
| $1 \to 0$ | $10 \to 1$ | $10 \to 0$ | $10 \to 1$ |
| | $11 \to 1$ | $11 \to 1$ | $11 \to 0$ |

$$\mathbf{NAND} = \mathbf{NOT} \circ \mathbf{AND}$$

# Circuit Diagrams

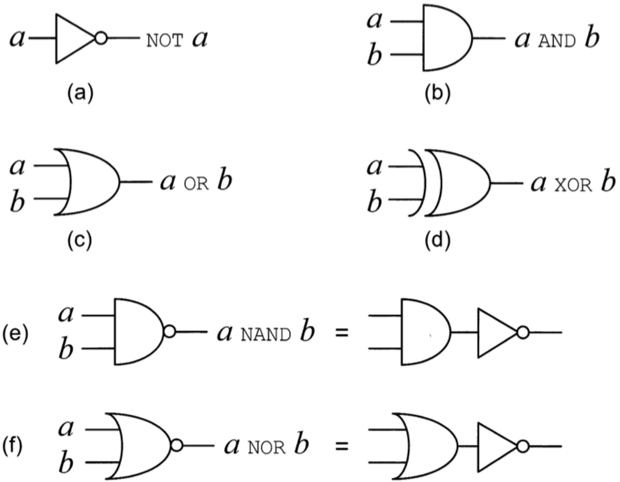


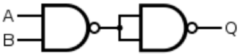

Figure 3.4. Elementary circuits performing the AND, OR, XOR, NAND, and NOR gates.

# Circuits

## Example

Build **AND** from **NAND**

| **NAND** | | | **AND** | | |
|---|---|---|---|---|---|
| 00 | $\rightarrow$ | 1 | 00 | $\rightarrow$ | 0 |
| 01 | $\rightarrow$ | 1 | 01 | $\rightarrow$ | 0 |
| 10 | $\rightarrow$ | 1 | 10 | $\rightarrow$ | 0 |
| 11 | $\rightarrow$ | 0 | 11 | $\rightarrow$ | 1 |




Universal Gates

Any function on bits can be computed from the composition of NAND gates alone.

# Circuits

Size of a circuit: # of gates in the circuit

Example $f(x) = x_1 \oplus x_2 \oplus \cdots \oplus x_n, \quad \text{size } n-1$

Measure of complexity:
Polynomial: $Size(f) \sim p(n)$
Exponential: $Size(f) \sim e^{\alpha n}$

Strong Church-Turing Thesis
Any model of computation can be simulated on a probabilistic Turing machine at most a polynomial increase in the number of elementary operation required

# How to compute quantum mechanically

Consider the following unitary operator

$$\mathbf{U}_f(|x\rangle_n|y\rangle_m) = |x\rangle_n|y \oplus f(x)\rangle_m$$

note that

$$\mathbf{U}_f\mathbf{U}_f(|x\rangle_n|y\rangle_m) = \mathbf{U}_f(|x\rangle|y \oplus f(x) \oplus f(x)\rangle = |x\rangle_n|y\rangle_m$$

i.e. $\mathbf{U}_f^\dagger = \mathbf{U}_f$.
For $y = 0$, we have

$$\mathbf{U}_f(|x\rangle_n|0\rangle_m) = |x\rangle_n|f(x)\rangle_m$$

# The Hadamard Transform

For a single qubit:

$$\begin{aligned}\mathbf{H}|0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \equiv |+\rangle \\ \mathbf{H}|1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \equiv |-\rangle\end{aligned}$$

For two qubits:

$$\begin{aligned}\mathbf{H} \otimes \mathbf{H}(|0\rangle \otimes |0\rangle) &= \mathbf{H}(|0\rangle)(\mathbf{H}|0\rangle) \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{2}(|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle) \\ &= \frac{1}{2}(|0\rangle_2 + |1\rangle_2 + |2\rangle_2 + |3\rangle_2)\end{aligned}$$

# The Hadamard Transform

For $n$ qubits:

$$\mathbf{H}^{\otimes n}|0\rangle_n = \frac{1}{2^{n/2}} \sum_{0 \le x < 2^n} |x\rangle_n,$$

where

$$\mathbf{H}^{\otimes n} = \mathbf{H} \otimes \mathbf{H} \otimes \cdots \otimes \mathbf{H}$$

Now consider the following operations on $n + m$ qubits:

$$\begin{aligned} & \mathbf{U}_f(\mathbf{H}^{\otimes n} \otimes \mathbf{I}_m)(|0\rangle_n |0\rangle_m) \\ = \quad & \frac{1}{2^{n/2}} \sum_{0 \le x < 2^n} \mathbf{U}_f(|x\rangle_n |0\rangle_m) \\ = \quad & \frac{1}{2^{n/2}} \sum_{0 \le x < 2^n} |x\rangle_n |f(x)\rangle_m \end{aligned}$$

# Quantum Circuits

Single qubit unitary:
Important single-qubit unitaries are the $\mathbf{X}, \mathbf{Y}, \mathbf{Z}$ rotations:

$$\mathbf{X}_\theta = \exp(-i\theta\mathbf{X}/2) = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}\mathbf{X} = \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix},$$

and

$$\mathbf{Y}_\theta = \exp(-i\theta\mathbf{Y}/2) = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}\mathbf{Y} = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix},$$

and

$$\mathbf{Z}_\theta = \exp(-i\theta\mathbf{Z}/2) = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}\mathbf{Z} = \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix}.$$

# Circuit Diagram

**Single-qubit Unitary**

For any unitary operation $\mathbf{U}$ on a single qubit, there exist real numbers $\alpha, \beta, \gamma, \delta$ such that $\mathbf{U} = e^{i\alpha}\mathbf{Z}_\beta \mathbf{Y}_\gamma \mathbf{Z}_\delta$.

For any $2 \times 2$ unitary matrix $\mathbf{U}$, the rows and columns of $\mathbf{U}$ are orthogonal plus that each row or column is a normalized vector. This then follows that therethere exist real numbers $\alpha, \beta, \gamma, \delta$ such that

$$\mathbf{U} = \begin{pmatrix} e^{i(\alpha-\beta/2-\delta/2)} \cos\frac{\gamma}{2} & -e^{-i(\alpha-\beta/2+\delta/2)} \sin\frac{\gamma}{2} \\ e^{i(\alpha+\beta/2-\delta/2)} \sin\frac{\gamma}{2} & e^{i(\alpha+\beta/2+\delta/2)} \cos\frac{\gamma}{2} \end{pmatrix}.$$

$$|\psi\rangle \;—\; \boxed{\mathbf{Z}_\delta} \;—\; \boxed{\mathbf{Y}_\gamma} \;—\; \boxed{\mathbf{Z}_\beta} \;—\quad \mathbf{Z}_\delta \mathbf{Y}_\gamma \mathbf{Z}_\beta |\psi\rangle$$

$$|\psi\rangle \;—\; \boxed{\mathbf{V}} \;—\; \boxed{\mathbf{W}} \;—\quad \mathbf{W}\mathbf{V}|\psi\rangle$$

# Two-qubit Unitary

Controlled-NOT:

$$|x\rangle \otimes |y\rangle \to |x\rangle \otimes |y \oplus x\rangle$$

In the basis of $\{|00\rangle,\ |01\rangle,\ |10\rangle,\ |11\rangle\}$ the matrix:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Similarly, a controlled-NOT gate with the second qubit as the control qubit takes $|x\rangle \otimes |y\rangle$ to $|x \oplus y\rangle \otimes |y\rangle$.

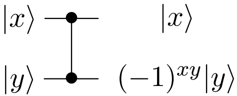
# Two-qubit Unitary

Controlled-**Z**:

$$|00\rangle \to |00\rangle, \ |01\rangle \to |01\rangle, \ |10\rangle \to |10\rangle, \ |11\rangle \to -|11\rangle.$$

Given that the controlled-**Z** operation is symmetric between the two qubits, it is not necessary to specify which one is the control qubit and which one is the target qubit. In the basis of $\{|00\rangle, \ |01\rangle, \ |10\rangle, \ |11\rangle\}$ the matrix:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$



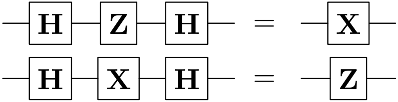
# Controlled-$\mathbf{Z}$ from Controlled-NOT

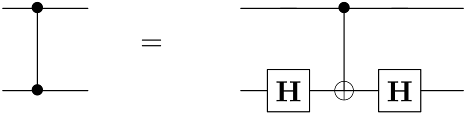
The Hadamard Transform

$$\mathbf{H}|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$$

In the basis of $\{|0\rangle,\ |1\rangle\}$ the matrix:

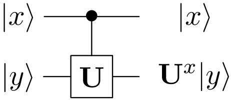
$$\mathbf{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$



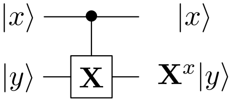



# Controlled-$\mathbf{U}$

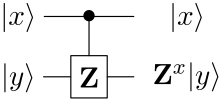
Controlled-$\mathbf{U}$:




Controlled-NOT is in fact controlled-$\mathbf{X}$.

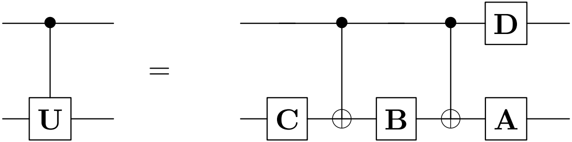



Controlled-$\mathbf{Z}$:



# Controlled-$\mathbf{U}$ from Controlled-NOT

Controlled-$\mathbf{U}$ from single-qubit unitaries and controlled-NOT:




where

$$\mathbf{D} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix},$$

and $\mathbf{U}, \alpha, \mathbf{A}, \mathbf{B}, \mathbf{C}$ satisfy

$$\begin{aligned} \mathbf{U} &= e^{i\alpha}\mathbf{AXBXC} \\ \mathbf{I} &= \mathbf{ABC}. \end{aligned}$$

# Universal Gates

Universal Gates

Any unitary on qubits can be built from single-qubit unitaries and controlled-NOT.

Size of a quantum circuit:

# of single-qubit and controlled-NOT gates in the circuit

Measure of complexity:

Polynomial: $\mathrm{S}ize(f) \sim p(n)$

Exponential: $\mathrm{S}ize(f) \sim e^{\alpha n}$

# Unitary Evolution

The Ising-type interaction Hamiltonian:

$$H_{in} = J\mathbf{Z} \otimes \mathbf{Z}.$$

Observe that

$$\begin{aligned} & \exp -i\frac{\pi}{4}(\mathbf{I} \otimes \mathbf{I} - \mathbf{Z} \otimes \mathbf{I} - \mathbf{I} \otimes \mathbf{Z} + \mathbf{Z} \otimes \mathbf{Z}) \\ = \quad & e^{-i\frac{\pi}{4}} e^{i\frac{\mathbf{Z}\otimes\mathbf{I}}{4}\pi} e^{i\frac{\mathbf{I}\otimes\mathbf{Z}}{4}\pi} e^{-i\frac{\mathbf{Z}\otimes\mathbf{Z}}{4}\pi} \end{aligned}$$

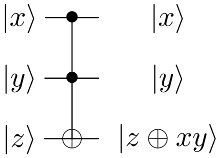
which gives the controlled-$\mathbf{Z}$ operation.

Unitary Evolutions from Single- and Two-qubit Ones

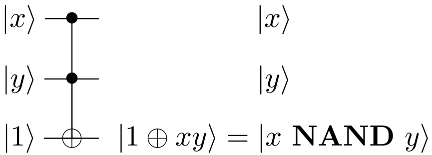
Single qubit terms and any non-trivial two-qubit interaction can generate an arbitrary $n$-qubit unitary evolution.

# Reversible Classical Computer

The Toffoli Gate: $\mathbf{T}|x\rangle|y\rangle|z\rangle = |x\rangle|y\rangle|z \oplus xy\rangle$

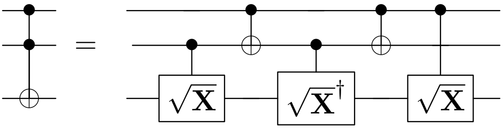



To implement **NAND**:

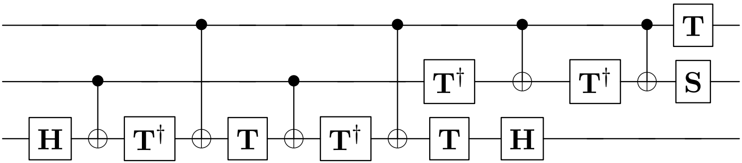


# Toffoli Gate from Two-Qubit Gates

Implementation of Toffoli gate using two-qubit controlled gates.

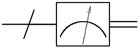



Implementation of Toffoli gate using Hadamard, phase, controlled-NOT and $\pi/8$ gates.



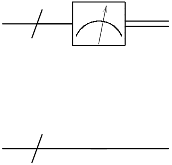
# Measurements (the Born rule)

For $|\psi\rangle = \sum \alpha_x |x\rangle_n$, measure in the basis of $\{|x\rangle_n\}$ returns $|x\rangle_n$ with probability $p_x = |\alpha_x|^2$.

$|\psi\rangle = \sum \alpha_x |x\rangle_n$  $|x\rangle_n$

For $|\psi\rangle = \sum \alpha_x |x\rangle_n |\phi_x\rangle_m$, measure the first register in the basis of $\{|x\rangle_n\}$ returns $|x\rangle_n |\phi_x\rangle_m$ with probability $p_x = |\alpha_x|^2$.

$|\psi\rangle = \sum \alpha_x |x\rangle_n |\phi_x\rangle_m$



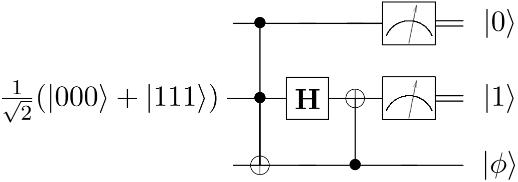
$|x\rangle_n$

$|\phi_x\rangle_m$

Measurements in different basis

## Example

Find the output state $|\phi\rangle$ of the following circuit:




$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \xrightarrow{\text{Toffoli}} \frac{1}{\sqrt{2}}(|000\rangle + |110\rangle)$$

$$\xrightarrow{\mathbf{H}_2} \frac{1}{\sqrt{2}}\left[|0\rangle\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle + |1\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|0\rangle\right]$$

$$= \frac{1}{2}(|000\rangle + |010\rangle + |100\rangle - |110\rangle) \xrightarrow{\text{CNOT}_{32}}$$

$$= \frac{1}{2}(|000\rangle + |010\rangle + |110\rangle - |100\rangle) \to |\phi\rangle = |0\rangle$$

# A Quantum Computer: The Circuit Model

**DiVincenzo Criteria**

- a scalable physical system of well-characterized qubits;
- the ability to initialize the state of the qubits to a simple fiducial state;
- long (relative) decoherence times, much longer than the gate-operation time;
- a universal set of quantum gates;
- a qubit-specific measurement capability.

# $n$-Qubit Unitary

Question: how 'efficient' this realization is?

A simple counting: an arbitrary $n$-qubit unitary may be written as $\sim 4^n$ two-level unitary operations, and implementing a two-level operation needs $\sim n^2$ single particle and controlled-$U$ operations, which gives $\sim n^2 4^n$ single particle and controlled-$U$ operations to realize an arbitrary $n$-qubit unitary.

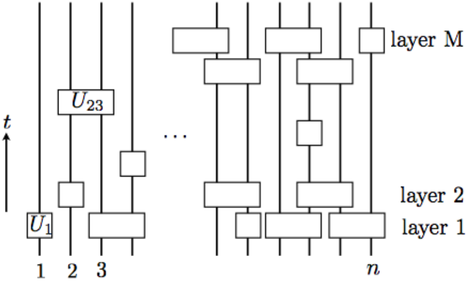
In general, exponentially many single and two-qubit unitaries are needed for generating an $n$-qubit unitary evolution.

# Quantum Circuit

The circuit model of quantum computing

$$|\psi_f\rangle = U_K U_{K-1} \dots U_2 U_1 |0\rangle^{\otimes n},$$

each $U_i$ is a single- or two-qubit unitary.




Circuit size: the number of unitaries $K$.
Circuit depth: the number of layers $M$.

# Quantum Simulation

The evolution of few-body Hamiltonians can be simulated efficiently by single qubit $Y, Z$ terms and any non-trivial two-qubit interaction.

The Hamiltonian $H = \sum_{j=1}^{L} H_j$. Shrödinger's equation:

$$i\frac{\partial|\psi(t)\rangle}{\partial t} = H|\psi(t)\rangle$$

For time independent Hamiltonian $H$, $|\psi(t)\rangle = \exp[-iH(t-t_0)]$. In the simplest case, if $[H_j, H_k] = 0$ for all $j, k$, i.e. all the terms $H_j$ commute, then the evolution $\exp -iHt$ is given by

$$\exp[-iHt] = \exp[-it\sum_{j=1}^{L} H_j] = \prod_{j=1}^{L} \exp[-iH_j t].$$

This directly gives an efficient quantum circuit, as each $\exp[-iH_j t]$ is a unitary acting on only a few number of particles.

# Quantum Simulation

$H = \sum_{j=1}^{L} H_j$, when $H_i$s do not commute.

Trotter Product Formula

$$\lim_{s\to\infty} (e^{iAt/s} e^{iBt/s})^s = e^{i(A+B)t}.$$

Taylor expansion for $e^{iAt/s}$:

$$e^{iAt/s} = I + \frac{1}{s}(iAt) + O(\frac{1}{s^2}).$$

$$\to e^{iAt/s} e^{iBt/s} = I + \frac{1}{s} i(A+B)t + O(\frac{1}{s^2}),$$

$$\to \left(e^{iAt/s} e^{iBt/s}\right)^s = \left(I + \frac{1}{s} i(A+B)t + O(\frac{1}{s^2})\right)$$

$$\to = I + \sum_{k=1}^{s} \binom{s}{k} \frac{1}{s^k} \left[i(A+B)t\right]^k + O(\frac{1}{s^2}).$$

# Quantum Simulation

Since
$$\binom{s}{k}\frac{1}{s^k} = \frac{1}{k!}\left[1 + O(\frac{1}{s})\right],$$
taking the limit $s \to \infty$ gives
$$\lim_{s\to\infty}\left(e^{iAt/s}e^{iBt/s}\right)^s$$
$$= \lim_{s\to\infty}\sum_{k=0}^{s}\frac{[i(A+B)t]^k}{k!}(1 + O(\frac{1}{s})) + O(\frac{1}{s^2}) = e^{i(A+B)t}.$$

The idea for quantum simulation is similar.
$$e^{i(A+B)\Delta t} = e^{iA\Delta t}e^{iB\Delta t} + O(\Delta t^2),$$

similarly
$$e^{i(A+B)\Delta t} = e^{iA\Delta t/2}e^{iB\Delta t}e^{iA\Delta t/2} + O(\Delta t^3).$$

# Quantum Simulation

For $H = \sum_{j=1}^{L} H_j$, one can further show that

$$e^{-2iH\Delta t} = \left[e^{-iH_1\Delta t}e^{-iH_2\Delta t}\dots e^{-iH_L\Delta t}\right]$$
$$\times \left[e^{-iH_L\Delta t}e^{-iH_{L-1}\Delta t}\dots e^{-iH_1\Delta t}\right] + O(\Delta t^3),$$

A more detailed analysis will show that in order to achieve the precision $\epsilon$ for the simulation, in a sense that the output of the simulation is $|\psi'(t)\rangle$ such that

$$|\langle\psi'(t)|e^{-iHt}|\psi(0)\rangle|^2 \geq 1 - \epsilon,$$

then one would need a quantum circuit with poly$(\frac{1}{\epsilon})$ (i.e. polynomial in $\frac{1}{\epsilon}$) number of single and two-particle unitary operations.