Architecture

Reversible Gates

Quantum Gates

Lecture 6

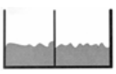
Reversible Gates

- In quantum world all operations that are not measurements:
  - reversible
  - represented by unitary matrices
  - e.g., AND gate are not reversible
    NOT gate and identity gate are reversible
- Today's computers lose energy and generate heat. In 1960s Rolf Landauer showed:
  - Erasing information causes energy loss and heat
  - Writing information not

Landauer's principle

Landauer's principle (I)

Intuition (not completely correct): tub of water

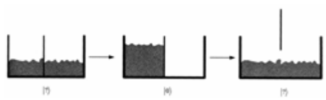


No state

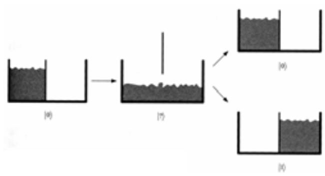
In state |0> and in state |1>

State |0> dissipating and creating energy

Landauer's principle (II)



Reversibility of writing



Irreversibility of erasing

Landauer's principle (III)

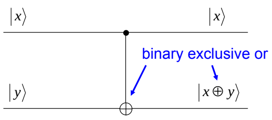
- Intuition with two people, Alice and Bob
- Writing
  - Alice writes letter on empty blackboard
  - Bob walks into the room
  - Bob erases the letter
  - Blackboard in its original state
  - Writing is reversible
- Erasing
  - Blackboard with writing on it
  - Alice erases the board
  - Bob walks into the room
  - Bob cannot write what was on the board
  - Erasing not reversible

Landauer's principle (IV)

- Erasing information is an irreversible, energy-dissipating operation.
- Charles H. Bennett in 1970s: if erasing information is the only operation that uses energy, then a computer that is reversible and does not erase would not use any energy → reversible circuits and programs.

Reversible gates: controlled-NOT gate

- Identity gate
- NOT gate
- Controlled-NOT gate:



$$\begin{array}{c|cccc} & 00 & 01 & 10 & 11 \\ \hline 00 & 1 & 0 & 0 & 0 \\ 01 & 0 & 1 & 0 & 0 \\ 10 & 0 & 0 & 0 & 1 \\ 11 & 0 & 0 & 1 & 0 \end{array}$$

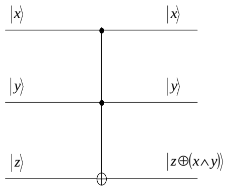
Top input is control bit:

• if |x›=0 then bottom output of |y› will be the same as the input

• if |x› =1 then the bottom output will be the opposite

Controlled-NOT gate can be reversed by itself

Reversible gates: Toffoli gate



	000	001	010	011	100	101	110	111
000	1	0	0	0	0	0	0	0
001	0	1	0	0	0	0	0	0
010	0	0	1	0	0	0	0	0
011	0	0	0	1	0	0	0	0
100	0	0	0	0	1	0	0	0
101	0	0	0	0	0	1	0	0
110	0	0	0	0	0	0	0	1
111	0	0	0	0	0	0	1	0

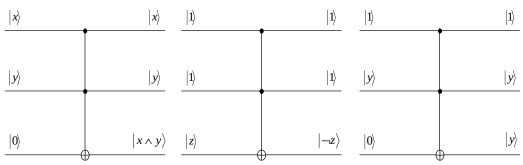
Similar to the controlled-NOT gate, but with two controlling bits:

• the bottom bit flips only when *both* of the two top bits are in state |1›.

• can be written as $|z \oplus (x \wedge y)\rangle$

Toffoli gate (cont'd)

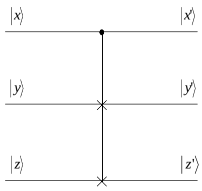
- Toffoli gate is universal: with copies one can make any logical gate.
- You can make a reversible computer using only Toffoli gates.
- In theory this computer will neither use any energy nor give off any heat.



AND gate NOT gate fanout gate

Fredkin gate

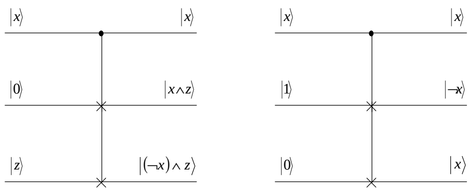
- Fredkin gate is also universal:
  - the top input is the control input
  - |0, *y*, *z* › → |0, *y*, *z* › and |1, *y*, *z* › → |1, *z*, *y*›



	000	001	010	011	100	101	110	111
000	1	0	0	0	0	0	0	0
001	0	1	0	0	0	0	0	0
010	0	0	1	0	0	0	0	0
011	0	0	0	1	0	0	0	0
100	0	0	0	0	1	0	0	0
101	0	0	0	0	0	0	1	0
110	0	0	0	0	0	1	0	0
111	0	0	0	0	0	0	0	1

Fredkin gate (cont'd)

Universal:



AND gate NOT gate

Both the Toffoli and the Fredkin gates are universal.
Not only are both reversible gates, their matrices are also unitary.

Quantum gates

- A quantum gate is an operator that acts on qubits. Such operators will be represented by unitary matrices.
- Examples: identity operator *I*, the Hadamard gate $H\left(\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\right)$, the NOT gate, the controlled-NOT gate, the Toffoli gate, and the Fredkin gate.
- Pauli matrices:

$$X = \sigma_x = \mathrm{NOT} = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} \qquad Y = \sigma_y = \begin{bmatrix}0 & -i\\ i & 0\end{bmatrix} \qquad Z = \sigma_z = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$$

- Other important matrices:

$$S = \begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix} \qquad T = \begin{bmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{bmatrix}$$

- Several relations between these operators (see book)

Square root of NOT gate

- Matrix representation: $\sqrt{\text{NOT}} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$
- Not its own inverse: √NOT ≠ √NOT†
- Reason for name:
  - Put qubits |0> and |1> through √NOT gate twice:

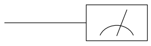
$$\sqrt{\text{NOT}} * \sqrt{\text{NOT}} = \left(\sqrt{\text{NOT}}\right)^2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

$$|0\rangle = [1,0]^T \mapsto \left[\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right]^T \mapsto [0,1]^T = |1\rangle$$

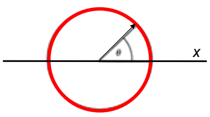
$$|1\rangle = [0,1]^T \mapsto \left[-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right]^T \mapsto [-1,0]^T = -1|0\rangle, \text{represent same state as } |0\rangle$$

  - Performs same operation as the NOT gate.

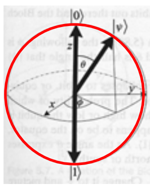
Measurement operation

- Not unitary
- Not reversible
- Usually performed at the end of a computation
- Denoted as 

Geometric representation of qubit states and operations

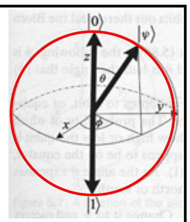


Complex numbers *c* with $|c|^2 = 1$, only identified by one number, the angle *θ* between vector and *x*-axis



Qubits $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$, where $|c_0|^2 + |c_1|^2 = 1$ can be identified by two numbers, the latitude *θ* and the longitude *φ* on a three-dimensional sphere of radius1, known as the Bloch sphere.

Bloch sphere



Qubit: $|\psi\rangle = \cos(\theta)|0\rangle + e^{i\varphi}\sin(\theta)|1\rangle$

$$0 \le \phi < 2\pi \text{ and } 0 \le \theta \le \tfrac{\pi}{2}$$

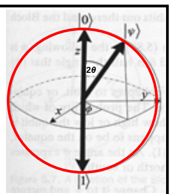
Standard parametrization of the unit sphere:

$$x = \cos\phi \sin\theta$$
$$y = \sin\phi \sin\theta$$
$$z = \cos\theta$$

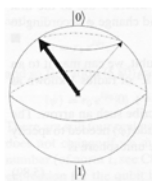
(θ,ϕ) and $(\pi - \theta, \phi + \pi)$ represent the same bit (up to the factor -1)

$$x = \cos\phi \sin 2\theta$$
$$y = \sin\phi \sin 2\theta$$
$$z = \cos\theta$$

Bloch sphere (cont'd)

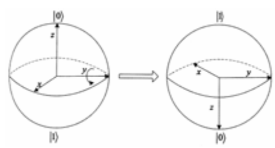


- North pole corresponds to state |0>and south pole to |1>.
- Angle *φ* is the angle that |*ψ*> makes from *x* along the equator (*longitude*) and *θ* is half the angle that |*ψ*> makes with the *z* axis (*latitude*).
- When a qubit is measured in the standard basis, it collapses to the north or south pole of the Bloch sphere. The probability depends on the latitude, so on *θ*.
- Rotation around the *z* axis, changing the longitude: does not affect the probability to which classical state it will collapse. It is called a phase change, altering the phase parameter $e^{i\varphi}$.



Bloch sphere: dynamics

- Every unitary 2-by-2 matrix will 'manipulate' the sphere.
- The *X*, *Y*, and *Z* Pauli matrices "flip" the Bloch sphere 180° about the *x*, *y*, and *z* axes, resp.:
  - *X* is a NOT gate taking |0> to |1> and vice versa, and even more: it takes everything above the equator to below the equator. Similar for the other Pauli matrices: e.g., *Y* operation



Bloch sphere: dynamics/rotations

- Phase shift gates: $R(\theta) = \begin{bmatrix} 1 & 0 \\ 0 & e^{\theta} \end{bmatrix}$
- Following operation on an arbitrary qubit:

$$\cos(\theta')|0\rangle + e^{i\phi}\sin(\theta')|1\rangle = \begin{bmatrix} \cos(\theta') \\ e^{i\phi}\sin(\theta') \end{bmatrix} \mapsto \begin{bmatrix} \cos(\theta') \\ e^{\theta}e^{i\phi}\sin(\theta') \end{bmatrix}$$

Leaves the latitude alone and just changes the longitude. New state will remain unchanged, only the phase will change.

Bloch sphere: dynamics/rotations

- Rotation of θ degrees around x, y, or z axis:

$$R_x(\theta) = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} X = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$

$$R_y(\theta) = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} Y = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$

$$R_z(\theta) = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} Z = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}$$

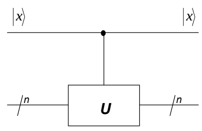
- General rotation around vector $D=(D_x,D_y,D_z)$ with size 1 from the origin:

$$R_D(\theta) = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2}(D_x X + D_y Y + D_z Z)$$

Bloch sphere: higher dimensions

- Valuable tool for understanding qubits and one-qubit operations.
- For *n*-qubits there is a higher-dimensional analog of the sphere.
- Research challenge: visualizing what happens when we manipulate several bits at once.
- Entanglement lies beyond the scope of the Bloch sphere.

controlled-*U* or ^{C}U



This operation will perform the *U* operation if the top |*x*> is a |1> and will perform the identity operation if |*x*> is |0>. Equivalent to an IF-THEN statement.

For the simple case of

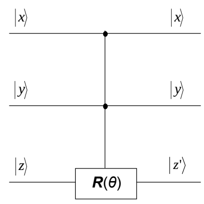
$$U = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \qquad {}^{C}U = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{bmatrix}$$

Universal quantum gates

- Universal logical gates can simulate every logical circuit:
  - {AND, NOT} gates
  - NAND gate
- Universal reversible gates:
  - Toffoli gate
  - Fredkin gate
- Universal quantum gates:
  - {*H*, ^{C}NOT, *R*($\cos^{-1}(3/5)$)}

Universal quantum gates (cont'd)

- Deutsch gate *D*(θ)



If the inputs |*x*> and |*y*> are both |1>, then the phase shift operation *R*(θ) will act on the |*z*> input. Otherwise, |*z*'> will be the same as |*z*>.

No-Cloning Theorem

- It is impossible to clone an exact quantum state.
- In other words, it is impossible to make a copy of an arbitrary quantum state without first destroying the original.
- We can "cut" and "paste" a quantum state, we cannot "copy" and "paste".
- Move is possible, copy is impossible.
- Transporting arbitrary quantum states from one system to another is no problem.
- See book for "proofs".

No-Cloning Theorem (cont'd)

- What about the fanout gate? The Toffoli and Fredkin quantum gates can mimic the fanout gate.
- Fredkin gate: $(x, 1, 0) \mapsto (x, \neg x, x)$ Cloning?
- Assume *x* input is superposition $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$, while leaving *y* = 1 and *z* = 0.
- This corresponds to the state

$$\begin{bmatrix} 0 & 0 & \frac{1}{\sqrt{2}} & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & 0 \end{bmatrix}^T$$

No-Cloning Theorem (cont'd)

Multiply with Fredkin state:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \\ 0 \end{bmatrix}$$

Resulting state: $\frac{|0,1,0\rangle + |1,0,1\rangle}{\sqrt{2}}$

So for a classical bit x the Fredkin gate performs the fanout operation, but for a superposition:

$$\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}, 1, 0\right) \mapsto \frac{|0,1,0\rangle + |1,0,1\rangle}{\sqrt{2}}$$

Not a fanout operation, no-cloning theorem safely stands.

Reading

- This lecture: Ch 5.3-5.4.
- Next lecture: Ch 6.1-??.