Quantum Computation and Information

Source: Nielsen and Chuang: Quantum Computation and Quantum Information (2000)

Definition of quantum computing: study of information processing tasks which use quantum mechanical systems

Combination of quantum mechanics, computer science, information theory

Quantum mechanics: most successful theory to describe microscopic world, but is often counterintuitive (developed in 1920s)

certain operations which are trivial in classical information are not even possible in quantum case

example: cloning of data

only imperfect cloning is possible

- complete control over quantum systems (single)
- recent developments: single atom traps
  - can observe properties of single atom isolated from surroundings
- can we do quantum information processing?
  - state-of-the-art: manipulation of a few qubits
  - some success in quantum cryptography

Computer Science

Turing - developed abstract notion of what we would call a computer (1936)

Universal Turing machine: completely captures the performance of algorithms in principle

- first computers:
  - Z3 (Konrad Zuse, 1941)
  - 1947 Bardeen, Brattain, Schockley ⇒ transistor
  - Moore's law: computer power for a given cost doubles once every two years (approximately true since 1960's up to now)

- we expect that Moore's law will not hold in the near future ⇒ size of electronic devices are smaller and smaller ⇒ are approaching the molecular/atomic length scale where quantum mechanics is important

  to maintain Moore's law ⇒ need quantum computing (or some other paradigm change)

- quantum computer - can be simulated using a classical computer ⇒ but not efficiently

  efficient: means that effort needed scales as polynomial of the size of the problem

Church - Turing hypothesis: Any algorithmic process can be simulated efficiently using a Turing machine

- hypothesis challenged by randomized algorithms
  1970s Solovay - Strassen: can determine whether a number is prime or not within some probability
  ⇓ ⇓
  uses random number generator
  → extend Church - Turing hypothesis to probabilistic case

Deutsch: can one derive a Church - Turing hypothesis based on the laws of physics?
- can one construct a device to simulate an arbitrary physical system?
  ⇓
  considered quantum analogs of devices in Turing machines
  ⇓
  ~~but~~ hypothesis is still an open issue
  but Church - Turing hypothesis has been challenged → for some cases quantum version of algorithm is more efficient
- other examples: Shor's - discrete logarithm algorithm
  - finding prime factors of an integer

quantum computers seem to be more efficient than Turing machines

Grover: quantum search algorithms
Feynmann: simulation of a quantum system
up to now an impossible task for systems
of meaningful size

- issue with quantum computing: our intuition
is rooted in the classical world
→ hard to construct quantum algorithms

information theory

- aim: quantity resources for sending
information from sender to receiver

- issues: noisy channel, error-correction

- Shannon: theorems which accomplish this

- for quantum information theory
no analogous theorem
- nevertheless: in principle possible to send
information even in the presence of
noise, error-correcting also
possible

- cryptography: transmit message which cannot be
read by third party

- quantum cryptography:
- measurement in quantum
mechanics changes state
→ third party interference detectable

Quantum Bits

bit - fundamental concept of classical computation $\Rightarrow$ 0, 1

qubit - same for quantum computing

- for now introduce conceptually $\Rightarrow$ they can also be realital

- classical bit: state $|0\rangle$ or $|1\rangle$

quantum bit: in superposition state

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

α, β - complex numbers

$|0\rangle, |1\rangle$ - known as basis states

orthonormal: $\langle 0|0\rangle = \langle 1|1\rangle = 1$

$\langle 0|1\rangle = \langle 1|0\rangle = 0$

- classical bit $\Rightarrow$ can be determined state is either 1 or 0

- quantum bit $\Rightarrow$ state can not be determined

measurement gives 0 with probability $|\alpha|^2$

or

1 with probability $|\beta|^2$

$|\alpha|^2 + |\beta|^2 = 1 \Rightarrow$ state of qubit $\Rightarrow$ a unit vector in complex space

- classical state observable / quantum state unobservable

$\Downarrow$

heart of quantum computation!!!

- even though α, β cannot be measured directly, manipulations on qubits (gates) are possible

⇓

consequences experimentally verifiable

- classical bit: exists in state 0 or 1

qubit: exists in superposition state until observed!

example: $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

before measurement:	50%	0	after measurement: 0 or 1 (100%)
	50%	1	

- qubits have a number of experimental realizations
  - Stern-Gerlach → spin of individual atoms
  - → ground/excited state of atom/molecule

- geometric representation of qubit

$$|\psi\rangle = e^{i\delta}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right)$$

α, β - 4 unknowns ⟶ 3 after normalization

δ, θ, φ - 3 unknowns

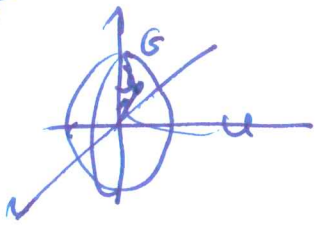
- turns out δ is (usually) inconsequential

θ, φ - point on unit 3D sphere

⇓

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$$

Bloch sphere: visualization of state of single qubit



gates (operations on qubits) ⇒ operations on unit vector ⇒ rotations

information stored in qubit?

- in principle: surface of sphere ⇒ ∞ - points
- problem: can not easily be recovered
  - measurement/observation: qubit falls into specific state $|0\rangle$ or $|1\rangle$ and qubit stays there ~~ever after~~ (until next nontrivial operation)
- "collapse" → one of fundamental postulates of quantum mechanics
- to reconstruct state $\alpha|\beta$ ⇒ need an ensemble of identically prepared states with an infinite number of members

- if we do not measure qubit: remains in state α, β until further operations:
  then $\alpha\beta \rightarrow \alpha'\beta' \rightarrow \alpha''\beta''$ according to propagation

⇒ α, β - coefficients of hidden information

Multiple qubits

- two qubits: four states: $|00\rangle, |01\rangle, |10\rangle, |11\rangle$

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

- One can measure 1st qubit, 2nd qubit or both simultaneously

- $|x\,y\rangle$ (y ← second qubit; x ↑ 1st qubit)

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

measurement on first qubit ⇒

~~suppose~~	probability
result 0	$\lvert\alpha_{00}\rvert^2 + \lvert\alpha_{01}\rvert^2$
result 1	$\lvert\alpha_{10}\rvert^2 + \lvert\alpha_{11}\rvert^2$

state after measurement:

result 0: $$\frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

result 1: $$\frac{\alpha_{10}|10\rangle + \alpha_{11}|11\rangle}{\sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2}}$$

- important qubit state:

Bell state ⇒ $$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

(EPR pair)

particularity of qubit state:

suppose measurement on 1st qubit is made ⇒ result of measurement on 2nd qubit is then determined with 100% certainty

→ outcomes are correlated!

outcomes are correlated even if particles are infinitely apart ⇒ what Einstein did not like about quantum mechanics

⇓ ⇓

particularity of quantum mechanics

- in general n qubits: $|x_1, \dots, x_n\rangle$

state $\sum_{x_1 \dots x_n} \alpha(x_1, \dots, x_n) |x_1, \dots, x_n\rangle$

one single n-qubit state stores 2^n bits of information $x_1 = 0,1, \dots, x_n = 0,1$

Quantum Computation

quantum computation: uses quantum gates in quantum circuits to carry out tasks

Single qubit gates

classical computers: wires, logic gates

single bit classical gates are trivial

NOT gate $0 \to 1$, $1 \to 0$

quantum NOT gate

$$\alpha|0\rangle + \beta|1\rangle \longrightarrow \alpha|1\rangle + \beta|0\rangle$$

linear transformation

can be written as a matrix $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

state of system, vector $\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$

$$\times \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$$

in general quantum gates acting on single qubits can be represented as 2×2 matrices

- condition on matrices: must preserve norm!

$$\begin{bmatrix} \alpha' \\ \beta' \end{bmatrix} = \tilde{X} \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

$$|\alpha'|^2 + |\beta'|^2 \stackrel{!}{=} |\alpha|^2 + |\beta|^2$$

→ matrix which preserves norm: unitary matrix $\tilde{X}^\dagger \tilde{X} = I$

$$\Downarrow$$

$$[\alpha' \ \beta'] \begin{bmatrix} \alpha' \\ \beta' \end{bmatrix} = [\alpha \ \beta] \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

$$\Downarrow$$

$$[\alpha \ \beta] \underbrace{\tilde{X}^\dagger \tilde{X}} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = [\alpha \ \beta] \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

$$\tilde{X}^\dagger \tilde{X} = \tilde{I}$$

NOT gate $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

- in classical computing: only NOT gate is not entirely trivial
- in quantum computing:

only condition is unitarity on 2×2 matrix

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad (Z\text{-gate})$$

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad (\text{Hadamard-gate})$$

action of Hadamard gate:

examples: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

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

$H|1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \Longrightarrow \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$

- general representation of a single qubit quantum gates:

$$U = e^{i\alpha} \begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix} \begin{bmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{bmatrix} \times \begin{bmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{bmatrix}$$

Multiple qubit gates

classical two bit gates: AND, OR, XOR (exclusive or)

NAND, NOR

AND: $00 \rightarrow$

	0	1
0	0	0
1	0	1

OR:

	0	1
0	0	1
1	1	1

XOR:

	0	1
0	0	1
1	1	0

NAND:

	0	1
0	1	1
1	1	0

NOR

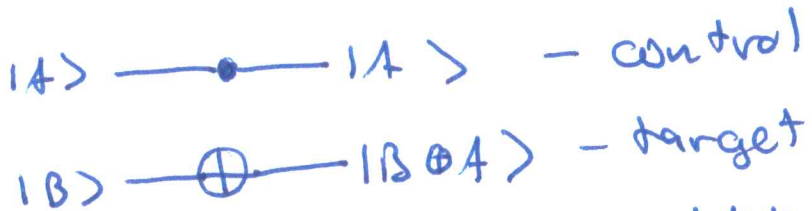
	0	1
0	1	0
1	0	0

- NAND - universal gate any operation can be produced as a sequence of NANDs

- example of multi-qubit quantum gate:

controlled-NOT => CNOT

- one-qubit = control qubit
- other-qubit = target qubit



⊕ - addition modulo 2 (NOT)

$|00\rangle \to |00\rangle$
$|01\rangle \to |01\rangle$
$|10\rangle \to |11\rangle$
$|11\rangle \to |10\rangle$

=> matrix representation

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

- two qubit gates: 4×4 matrices

constraint: conserve norm - unitarity

- not all classical gates can be generalized to quantum gates

XOR and NAND gates are not <u>invertible</u> or <u>irreversible</u>

if given output of a classical NAND or XOR => not possible to say what the input was

- quantum gates are always reversible: unitary matrices always have inverses and the inverse is also a unitary matrix
- any multiple qubit gate can be produced from CNOT and single qubit gates
- change of basis: $|\Phi\rangle$

quantum computing can be performed in alternative bases

example: $|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$, $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ $\Rightarrow$ Obey

$\langle +|+\rangle = \langle -|-\rangle = 1$

$\langle +|-\rangle = \langle -|+\rangle = 0$

in general $|a\rangle$ & $|b\rangle$ $\Rightarrow$ form good bases

$\langle a|\alpha\rangle = \langle b|\beta\rangle = 1$

$\langle a|b\rangle = \langle b|\alpha\rangle = 0$

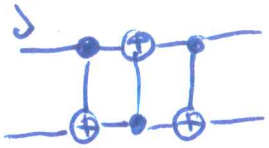
rewrite $|0\rangle$, $|1\rangle$ state in new basis

$$\alpha|0\rangle + \beta|1\rangle = \alpha\left(\frac{|+\rangle + |-\rangle}{\sqrt{2}}\right) + \beta\left(\frac{|+\rangle - |-\rangle}{\sqrt{2}}\right)$$

$$= \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle$$

Quantum circuits

example: "wire" –



wire - not necessarily physical wire

can also indicate passage of time (chronology of gates)

what does this circuit do?

$$|a,b\rangle \to |a, a\oplus b\rangle \longrightarrow |a\oplus(a\oplus b),\ a\oplus b\rangle$$

$$|b,\ a\oplus b\rangle$$

$$\to |b,\ b\oplus(a\oplus b)\rangle$$

$$|b,a\rangle$$

Since $a\oplus(a\oplus b) = b$

proof: calculate explicitly:

a	b	$a\oplus b$	$a\oplus(a\oplus b)$
0	0	0	0
0	1	1	1
1	0	1	0
1	1	0	1

circuit switches a with b

$$|a,b\rangle \to |b\ a\rangle$$

in quantum circuits: - loops not allowed

- wires can not join (FANIN) (OR) ⇒ not reversible
- spreading out of wires (FANOUT)

bits copied ⇒ not allowed in quantum circuits