An elementary introduction to quantum entanglement and its applications in physics and quantum computer science

Eric CANCES

EMC2 seminar - February 22, 2019

Aspect's experiment ('82)

143 km quantum teleportation ('12)

D-Wave 2000Q ('17)

Hot topic with massive investment decisions made in 2018

Europe: *Quantum Flagship was launched as one of the largest and most ambitious research initiatives of the European Union. With a budget of 1 billion euros and a duration of 10 years, the flagship brings together research institutions, academia, industry, enterprises, and policy makers, in a joint and collaborative initiative on an unprecedented scale.*

USA: *National Quantum Initiative Act (H.R. 6227) authorizes $1.2 billion over five years for federal activities aimed at boosting investment in quantum information science, or QIS, and supporting a quantum-smart workforce*

China: *is building the world's largest quantum research facility to develop a quantum computer (National Laboratory for Quantum Information Science, Hefei, budget: $10 billions)*

+ Google, Microsoft, Amazon, IBM, Huawei...

Outline of the talk

1. Basics of quantum mechanics
2. Qubits
3. Using quantum entanglement

   (a) quantum communication

   dense coding and quantum teleportation for secure communication

   (b) quantum computing

   quantum parallelism, Deustch problem, Grover's search algorithm

... and maybe next time

Shor's factorization algorithm (breaking RSA)
Harrow, Hassidim, Lloyd quantum algorithm for linear systems

(c) resolving Einstein-Podolsky-Rosen (EPR) paradox

local hidden variable theories vs quantum mechanics, Bell's inequalities, Aspect's experiments

1 - Basics of quantum mechanics

Fundamental postulates of quantum mechanics

- **1st postulate.** To any closed quantum system can be associated a separable complex Hilbert space $\mathcal{H}$ such that the set of the pure states of the system is diffeomorphic to the projective space $P\mathcal{H} := (\mathcal{H} \setminus \{0\})/\mathbb{C}^*$.

  In practice, the state of the system at time t is described by a normalized wavefunction $\Psi(t) \in \mathcal{H}$ (Dirac's notation $|\Psi(t)\rangle$), keeping in mind that $\Psi(t)$ and $e^{i\alpha}\Psi(t)$, $\alpha \in \mathbb{R}$, are two representations of the same state.

  Examples:

  – particle of spin s in the position representation: $\mathcal{H} = L^2(\mathbb{R}^3; \mathbb{C}^{2s+1})$

  $|\psi(t;x)|^2$: probability density of observing the particle at point $x \in \mathbb{R}^3$ at time t

  – 1 qubit: $\mathcal{H} = \mathbb{C}^2$

  – n qubits $\mathcal{H} = \underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n \text{ times}} \equiv \mathbb{C}^{2^n}$

Fundamental postulates of quantum mechanics

- **1st postulate.** To any closed quantum system can be associated a separable complex Hilbert space $\mathcal{H}$ such that the set of the pure states of the system is diffeomorphic to the projective space $P\mathcal{H} := (\mathcal{H} \setminus \{0\})/\mathbb{C}^*$.

  In practice, the state of the system at time t is described by a normalized wavefunction $\Psi(t) \in \mathcal{H}$ (Dirac's notation $|\Psi(t)\rangle$), keeping in mind that $\Psi(t)$ and $e^{i\alpha}\Psi(t)$, $\alpha \in \mathbb{R}$, are two representations of the same state.

- **2nd postulate.** To any scalar physical quantity $\widetilde{A}$ is associated an observable A (i.e. a self-adjoint operator on $\mathcal{H}$).

  Example: spinless particle of mass m in a bounded external potential V

  – Hilbert space: $\mathcal{H} = L^2(\mathbb{R}^3; \mathbb{C})$

  – physical quantity: energy

  – observable: quantum Hamiltonian $H = -\dfrac{\hbar^2}{2m}\Delta + V$

Fundamental postulates of quantum mechanics

- **1st postulate.** To any closed quantum system can be associated a separable complex Hilbert space $\mathcal{H}$ such that the set of the pure states of the system is diffeomorphic to the projective space $P\mathcal{H} := (\mathcal{H} \setminus \{0\})/\mathbb{C}^*$.

  In practice, the state of the system at time t is described by a normalized wavefunction $\Psi(t) \in \mathcal{H}$ (**Dirac's notation** $|\Psi(t)\rangle$), keeping in mind that $\Psi(t)$ and $e^{i\alpha}\Psi(t)$, $\alpha \in \mathbb{R}$, are two representations of the same state.

- **2nd postulate.** To any scalar physical quantity $\widetilde{A}$ is associated an observable A (i.e. a self-adjoint operator on $\mathcal{H}$).

- **3rd postulate.** Between two measures, the dynamics of the system is given by

  $$\Psi(t) = U(t;t_0)\Psi(t_0)$$

  where $(U(t;t_0))_{t,t_0 \in \mathbb{R}}$ is a strongly continuous family of unitary operators on $\mathcal{H}$ called the propagator. For an isolated system, $U(t;t_0) = e^{-i(t-t_0)H/\hbar}$, where H is the Hamiltonian of the system, i.e. the observable associated with the energy.

- **4th postulate. The result of the measure of the quantity $\widetilde{A}$ is necessarily a point of $\sigma(A)$, the spectrum of A.**

  Example: particle in a single well / in a double well

- **4th postulate. The result of the measure of the quantity $\widetilde{A}$ is necessarily a point of $\sigma(A)$, the spectrum of A.**

- **5th postulate. If at time $t_0 - 0$, the system is in the state $\Psi(t_0 - 0)$, the probability that the result of the measure of $\widetilde{A}$ lays in the Borel set B is $\|\Pi_B^A \Psi(t_0 - 0)\|^2$, where $\Pi_\bullet^A$ is the spectral measure associated with A.**

  If the operator A is has a pure-point spectrum

$$A = \sum_n \alpha_n \, |e_n\rangle\langle e_n| \quad \textbf{and} \quad \Pi_B^A = \sum_{n \,|\, \alpha_n \in B} |e_n\rangle\langle e_n|$$

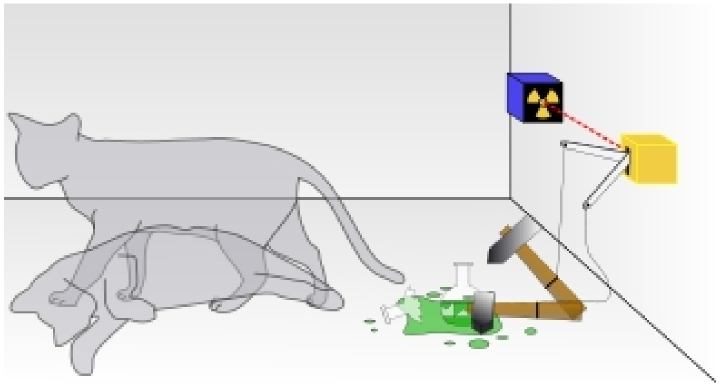
$$0 \leq \|\Pi_B^A \Psi(t_0 - 0)\|^2 = \sum_{n \,|\, \alpha_n \in B} |\langle e_n | \Psi(t_0 - 0)\rangle|^2 \leq \|\Psi(t_0 - 0)\|^2 = 1$$

- **4th postulate.** **The result of the measure of the quantity $\widetilde{A}$ is necessarily a point of $\sigma(A)$, the spectrum of A.**

- **5th postulate.** **If at time $t_0 - 0$, the system is in the state $\Psi(t_0 - 0)$, the probability that the result of the measure of $\widetilde{A}$ lays in the Borel set B is $\|\Pi_B^A \Psi(t_0 - 0)\|^2$, where $\Pi_\bullet^A$ is the spectral measure associated with A.**

- **6th postulate (wave function collapse in the Copenhagen interpretation).** **If the result of the measure is known to lay in the Borel set B (with no additional information), then the state of the system at time $t_0 + 0$ is a.s.**

$$\Psi(t_0 + 0) = \frac{\Pi_B^A \Psi(t_0 - 0)}{\|\Pi_B^A \Psi(t_0 - 0)\|}.$$



Measurements and preparation of a quantum state

Consider a quantum system with state space $\mathcal{H}$ and a collection of observables $(A_k)_{1\leq k\leq K}$ such that

1. **the spectra of each A_k is pure point;**
2. **the operators A_k commute with one another;**
3. **the joint eigenspaces of all the A_k all are of dimension 1;**

$\rightarrow$ **complete set of commuting observables (CSCO).**

If one successively measures each of the physical quantities $\widetilde{A}_1, \cdots, \widetilde{A}_K$ and obtain the values $\alpha_1, \cdots, \alpha_K$, then we know for sure that after these measurements, the system is in the unique pure state associated with the 1D subspace

$$\bigcap_{k=1}^{K} \mathbf{Ker}(A_k - \alpha_k \mathbb{1}_{\mathcal{H}})$$

of $\mathcal{H}$. The state of the system after the measurement then is completely characterized, and can be transformed into the desired state by applying unitary transforms (that is by acting on the system in a controlled way).

Composite quantum system

If a system can be decomposed into two *distinguishable* quantum subsystems A and B, then the state space of this system is

$$\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B,$$

where $\mathcal{H}_A$ and $\mathcal{H}_B$ are the state spaces of A and B respectively.

Factored and entangled states

Consider a composite quantum system with state space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$.

Definition. **A pure state $\psi_{AB} \in \mathcal{H}_{AB}$ is called factored if there exist $\psi_A \in \mathcal{H}_A$ and $\psi_B \in \mathcal{H}_B$ such that**

$$\psi_{AB} = \psi_A \otimes \psi_B.$$

Otherwise, it is called entangled.

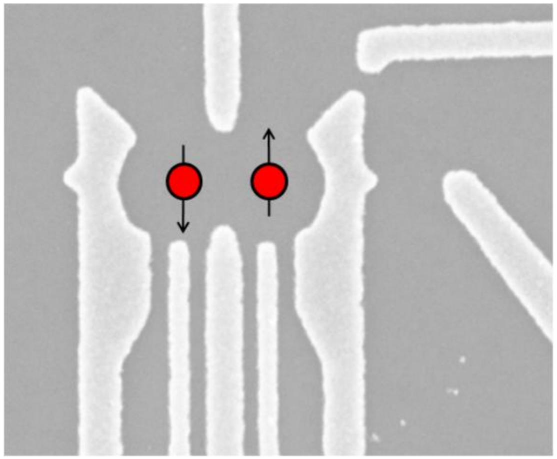
Entangled states exhibit correlations that have no classical analogue. For this reason, they can be used to certify the principles of quantum mechanics, and also play key roles in quantum communication and quantum computing.

2 - Qubits

Bit: a classical system with two possible sates, 0 or 1.

Qubit (or Qbit): a quantum system with state space $\mathcal{H} = \mathbb{C}^2$.

Several possible physical realizations of qubits (ex: double quantum dot).



Singlet-triplet qubit

Scanning electronic microscope image
+ cartoon of the trapped electrons
(Harvard 2012)

Google 72-qubit processor

(March 2018)

Physical realization of qubits

Physical support	Name	Information support	$\vert 0\rangle$	$\vert 1\rangle$
Photon	Polarization encoding Number of photons Time-bin encoding	Polarization of light Fock state Time of arrival	Horizontal Vacuum Early	Vertical Single photon state Late
Coherent state of light	Squeezed light	Quadrature	Amplitude-squeezed	Phase-squeezed
Electrons	Electronic spin Electron number	Spin Charge	Spin up No electron	Spin down One electron
Nucleus	Nuclear spin (addressed through NMR)	Spin	Spin up	Spin down
Optical lattices	Atomic spin	Spin	Spin up	Spin down
Josephson junction	Superconducting charge qubit Superconducting flux qubit Superconducting phase qubit	Charge Current Energy	$Q = 0$ Clockwise current Ground state	$Q = 2e$ (extra Cooper pair) Counterclockwise current First excited state
Singly charged quantum dot pair	Electron localization	Charge	Electron on left dot	Electron on right dot
Doubly charged quantum dot pair	Singlet-triplet	Spin state	$\frac{\vert\uparrow\downarrow\rangle+\vert\downarrow\uparrow\rangle}{\sqrt{2}}$	$\frac{\vert\uparrow\downarrow\rangle-\vert\downarrow\uparrow\rangle}{\sqrt{2}}$
Quantum dot	Dot spin	Spin	Spin down	Spin up
Gapped topological systems	Non-abelian anyons	Braiding of excitations	Depends on system	Depends on system

Lemma. **The set of the pure states of a qubit is diffeormorphic to the unit sphere $\mathbb{S}^2 \subset \mathbb{R}^3$.**

Proof. **To any $\vec{n} = \begin{pmatrix} \sin\theta\cos\phi \\ \sin\theta\sin\phi \\ \cos\theta \end{pmatrix} \in \mathbb{S}^2$, we can associate the normalized vector of $\mathbb{C}^2$ defined by**

$$\psi_{\vec{n}} := \begin{pmatrix} e^{-i\phi/2}\cos(\theta/2) \\ e^{i\phi/2}\sin(\theta/2) \end{pmatrix}.$$

It is easily checked that

$$\begin{array}{rcl} \mathbb{S}^2 & \to & P^2(\mathbb{C}) := \left(\mathbb{C}^2 \setminus \{0\}\right)/\mathbb{C}^* \\ \vec{n} & \mapsto & \mathbb{C}^*\psi_{\vec{n}} \end{array}$$

is a smooth diffeomorphism.

Single qubit observables

Any observable on $\mathcal{H} = \mathbb{C}^2$ is of the form

$$A = a_0 \mathbb{1}_{\mathbb{C}^2} + \sum_{j=1}^{3} a_j \sigma_j, \quad (a_0, a_1, a_2, a_3) \in \mathbb{R}^4,$$

where $\mathbb{1}_{\mathbb{C}^2}$ is the rank-2 identity matrix and where

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

are the Pauli matrices.

Any observable on $\mathcal{H} = \mathbb{C}^2$ therefore is of the form

$$A = a_0 \mathbb{1}_2 + b A_{\vec{p}}, \quad \textbf{with} \quad (a_0, b) \in \mathbb{R} \times \mathbb{R}_+, \quad \vec{p} \in \mathbb{S}^2, \quad A_{\vec{p}} = \vec{p} \cdot \vec{\sigma}.$$

For $\vec{p} \in \mathbb{S}^2$, we call $A_{\vec{p}}$ the polarization observable along $\vec{p}$.

Properties of polarization observables

$$\sigma(A_{\vec{p}}) = \{-1, 1\}\,, \quad A_{\vec{p}}\psi_{\vec{p}} = \psi_{\vec{p}}, \quad A_{\vec{p}}\psi_{-\vec{p}} = -\psi_{-\vec{p}},$$
$$\Pi^{A_{\vec{p}}}_{\{\pm 1\}} = |\psi_{\pm\vec{p}}\rangle\langle\psi_{\pm\vec{p}}| = \frac{1}{2}\left(\mathbb{1}_{\mathbb{C}^2} \pm \vec{p}\cdot\vec{\sigma}\right).$$

If a qubit is in the state $\psi_{\vec{n}}$ and if one measures the polarization along $\vec{p}$, the result will be

- $+1$ **with probability** $p = \cos^2\left(\frac{1}{2}\arccos(\vec{p}\cdot\vec{n})\right)$**;**
- -1 **with probability** $1 - p = \sin^2\left(\frac{1}{2}\arccos(\vec{p}\cdot\vec{n})\right)$**.**

Qubit states $|0\rangle$ and $|1\rangle$

We denote by

$$|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \psi_{\vec{e}_3} = |{\uparrow}\rangle \qquad \textbf{and} \qquad |1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \psi_{-\vec{e}_3} = |{\downarrow}\rangle.$$

We have

$$A_{\vec{e}_3}|0\rangle = \sigma_3|0\rangle = |0\rangle \qquad \textbf{and} \qquad A_{\vec{e}_3}|1\rangle = \sigma_3|1\rangle = -|1\rangle.$$

System of two (distinguishable) qubits ($\mathcal{H}_{AB} = \mathbb{C}^2 \otimes \mathbb{C}^2$)

Canonical basis of factored states (eigenstates of the CSCO $(\sigma_3 \otimes \mathbb{1}_2, \mathbb{1}_2 \otimes \sigma_3)$)

$$|00\rangle = |0\rangle\otimes|0\rangle, \qquad |10\rangle = |1\rangle\otimes|0\rangle, \qquad |01\rangle = |0\rangle\otimes|1\rangle, \qquad |11\rangle = |1\rangle\otimes|1\rangle.$$

Some useful maximally entangled states

$$\phi^{\pm}_{AB} = \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right) = \frac{1}{\sqrt{2}}\left(|\uparrow\uparrow\rangle \pm |\downarrow\downarrow\rangle\right),$$
$$\psi^{\pm}_{AB} = \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right) = \frac{1}{\sqrt{2}}\left(|\uparrow\downarrow\rangle \pm |\downarrow\uparrow\rangle\right).$$

System of n (distinguishable) qubits = quantum register ($\mathcal{H}_n = (\mathbb{C}^2)^{\otimes n}$)

Canonical basis of factored states (eigenstates of the CSCO $(\mathbb{1}_2^{\otimes(n-1-j)} \otimes \sigma_3 \otimes \mathbb{1}_2^{\otimes j})$)

$|k\rangle_n = |$**binary exp. of** $k\rangle$, **i.e.** $|0\rangle_n = |0\cdots000\rangle,\ |1\rangle_n = |0\cdots001\rangle,\ |2\rangle_n = |0\cdots010\rangle, \ldots$

Uniform state:
$$|\psi_0\rangle = \left(\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)\right)^{\otimes n} = \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}|k\rangle_n.$$

Acting on (systems of) qubits:

- reversible transformations by means of unitary operators ;
- irreversible transformations by measurement.

Common structure of a quantum experiment and a quantum algorithm:

1. prepare an initial pure state $\psi_i \in \mathcal{H}_n := (\mathbb{C}^2)^{\otimes n}$;
2. apply to ψ_i a sequence of unitary operators - play with entanglement - (sometimes together with intermediate measurements);
3. make measurements on the so-obtained final state ψ_f.

No-cloning theorem: there is no unitary transform U on $\mathcal{H} \otimes \mathcal{H}$ satisfying

$$\exists \psi_0 \in \mathcal{H} \text{ s.t . } \forall \psi \in \mathcal{H}, \quad U(|\psi\rangle \otimes |\psi_0\rangle) = |\psi\rangle \otimes |\psi\rangle.$$

Entanglement and factored unitary operators: for any unitary operator U on $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ of the form $U = U_A \otimes U_B$ with U_A and U_B unitary on $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively, we have

$$|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \text{ factored} \quad \Rightarrow \quad U|\Psi\rangle \text{ factored}.$$

Any unitary operator on $\mathcal{H}_n = (\mathbb{C}^2)^{\otimes n}$ can be constructed with 1-qubit gates and 2-qubit controlled NOT (cNOT) gates (Barenco et al '95).

1-qubit gate = unitary operator acting on a single qubit, i.e.

$$U_j = \mathbb{1}_{\mathbb{C}^2}^{\otimes(n-j-1)} \otimes u \otimes \mathbb{1}_{\mathbb{C}^2}^{\otimes j}$$

Commonly used 1-qubit gate operators u:

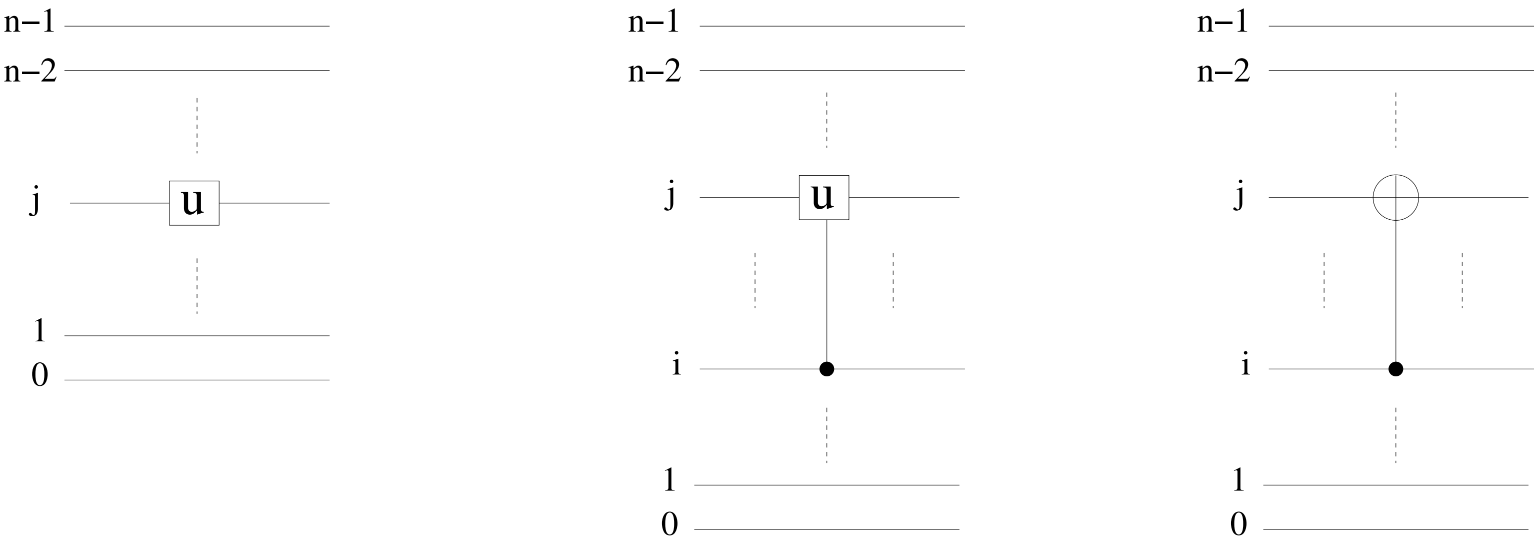
- **the Pauli matrices $X := A_{\vec{e}_1} = \sigma_1$ =NOT gate, $Y := A_{\vec{e}_2} = \sigma_2$, $Z = A_{\vec{e}_3} := \sigma_3$;**
- **the Hadamard transform defined by**

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,,\ H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\,, \quad H := \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}}(X+Z)\,.$$

Controlled 2-qubit gate = unitary operator acting on two qubits, one qubit being the control, the second qubit being the target, i.e. for u unitary of $\mathbb{C}^2$

$$C_{ij}^u\left(|k\rangle_{n-1-j} \otimes |\phi\rangle \otimes |l\rangle_{j-i-1} \otimes |0\rangle \otimes |m\rangle_i\right) = |k\rangle_{n-1-j} \otimes |\phi\rangle \otimes |l\rangle_{j-i-1} \otimes |0\rangle \otimes |m\rangle_i$$
$$C_{ij}^u\left(|k\rangle_{n-1-j} \otimes |\phi\rangle \otimes |l\rangle_{j-i-1} \otimes |1\rangle \otimes |m\rangle_i\right) = |k\rangle_{n-1-j} \otimes (u|\phi\rangle) \otimes |l\rangle_{j-i-1} \otimes |1\rangle \otimes |m\rangle_i.$$

Graphical representation of 1-qubit and controlled 2-qubit logic gates



(cNOT gate)

Controlled NOT (cNOT) gate $C_{13} := C_{13}^X$ on $\mathcal{H}_4$:

$$C_{13}|0x_2 0x_0\rangle := |0x_2 0x_0\rangle, \qquad C_{13}|1x_2 0x_0\rangle := |1x_2 0x_0\rangle,$$
$$C_{13}|0x_2 1x_0\rangle := |1x_2 1x_0\rangle, \qquad C_{13}|1x_2 1x_0\rangle := |0x_2 1x_0\rangle.$$

The first 2-qubit silicon logic gate was developed in 2015.

3 - Using entanglement:
quantum communication and quantum computing

Some historical milestones:

- **Quantum computing:**

  R.P. Feynman, *Simulating physics with computers*, Int. J. Theor. Phys. 21 (1982) 467–488

  Deutsch's problem ('85): particular vs relational information

  Shor algorithm ('94): polynomial time integer factorization
  (the quantum factorization of 56,153 was performed in 2014)

  Grover's algorithm ('96): unstructured search with complexity $\sqrt{N}$

- **Quantum communication:**

  – teleportation (Bennett et al., PRL '83)
  – dense coding (Bennett and Wiesner, PRL '92)

Reference: N.D. Mermin, *Quantum computer science. An introduction*, Cambridge University Press 2007.

If Alice sends to Bob a qubit off the shell, she can only send one bit of information (e.g. DHL a qubit in state $|0\rangle$ or $|1\rangle$), with a risk of eavesdropping.

On the other hand, if Alice and Bob share a 2-qubit in the entangled state

$$\phi^+_{AB} = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right),$$

then Alice can send to Bob two bits of information safe from eavesdroppers.

- **Step 1: depending on whether she wants to send 00, 10, 01 or 11, she applies $\mathbb{1}_{\mathbb{C}^2}$, X, Z or XZ to her qubit. The 2-qubit system then is in state**

$$(\mathbb{1}_{\mathbb{C}^2} \otimes \mathbb{1}_{\mathbb{C}^2})\phi^+_{AB} = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right), \quad (X \otimes \mathbb{1}_{\mathbb{C}^2})\phi^+_{AB} = \frac{1}{\sqrt{2}}\left(|10\rangle + |01\rangle\right)$$

$$(Z\otimes\mathbb{1}_{\mathbb{C}^2})\phi^+_{AB} = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right), \quad \textbf{or} \quad ((XZ)\otimes\mathbb{1}_{\mathbb{C}^2})\phi^+_{AB} = \frac{1}{\sqrt{2}}\left(|10\rangle - |01\rangle\right).$$

- **Step 2: Alice sends her qubit to Bob;**
- **Step 3: Bob applies the unitary transform $U := (H \otimes \mathbb{1}_{\mathbb{C}^2})C_{10}$ and gets**

$$|00\rangle, \quad |10\rangle, \quad |01\rangle, \quad \textbf{or} \quad |11\rangle.$$

No-cloning theorem: there is no unitary transform U on $\mathbb{C}^2 \otimes \mathbb{C}^2$ satisfying

$$\forall \psi \in \mathbb{C}^2, \quad U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle.$$

Quantum teleportation of a 1-qubit state

Suppose that

- Alice has a qubit in a state

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad (\alpha \text{ and } \beta \text{ unknown to Alice});$$

- Alice and Bob share a 2-qubit system in the entangled state

$$\phi_{AB}^{+} = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right);$$

- Alice wants to reassign the state $|\psi\rangle$ to the qubit belonging to Bob;
- Alice and Bob are allowed to share classical information.

The global 3-qubit system is in the state

$$|\Psi_{AAB}\rangle = |\psi\rangle \otimes \phi_{AB}^{+} = \frac{1}{\sqrt{2}}\left(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle\right).$$

- **Step 1: Alice applies a cNOT gate using her first qubit as the control and her second qubit as the target. The result is**

$$|\Psi^{(1)}_{AAB}\rangle = \frac{1}{\sqrt{2}}\left(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle\right).$$

- **Step 2: Alice then applies a Hadamard transform to her first qubit. The result is**

$$|\Psi^{(2)}_{AAB}\rangle = \frac{1}{2}\left(\alpha|000\rangle + \alpha|100\rangle + \alpha|011\rangle + \alpha|111\rangle + \beta|010\rangle - \beta|110\rangle + \beta|001\rangle - \beta|101\rangle\right)$$

$$= \frac{1}{2}|00\rangle\otimes(\alpha|0\rangle+\beta|1\rangle) + \frac{1}{2}|10\rangle\otimes(\alpha|0\rangle-\beta|1\rangle) + \frac{1}{2}|01\rangle\otimes(\alpha|1\rangle+\beta|0\rangle) + \frac{1}{2}|11\rangle\otimes(\alpha|1\rangle-\beta|0\rangle).$$

- **Step 3: Alice measures the observables $Z \otimes \mathbb{1}_{\mathbb{C}^2}$ and $\mathbb{1}_{\mathbb{C}^2} \otimes Z$ for the two qubits in her possession and sends the result to Bob, who gets**

$$\left\{\begin{array}{l}(+1,+1)\\ \alpha|0\rangle+\beta|1\rangle\end{array}\right. \quad \textbf{OR} \quad \left\{\begin{array}{l}(-1,+1)\\ \alpha|0\rangle-\beta|1\rangle\end{array}\right. \quad \textbf{OR} \quad \left\{\begin{array}{l}(+1,-1)\\ \alpha|1\rangle+\beta|0\rangle\end{array}\right. \quad \textbf{OR} \quad \left\{\begin{array}{l}(-1,-1)\\ \alpha|1\rangle-\beta|0\rangle\end{array}\right.$$

- **Step 4: in order to recover the state $|\psi\rangle$ Bob applies to his qubit a unitary transform which depends on the classical message sent by Alice**

$$(+1,+1) \to \mathbb{1}_{\mathbb{C}^2}, \qquad (-1,+1) \to Z, \qquad (+1,-1) \to X, \qquad (-1,+1) \to ZX.$$

Experimental achievements:

- **1997: quantum teleportation between photons;**
- **2006: quantum teleportation between photons and atoms;**
- **2012: quantum teleportation over 143 km;**
- **2012: quantum teleportation between two remote "macroscopic objects" (quantum memory nodes, each composed of 10^8 rubidium atoms and connected by a 150-meter optical fiber);**
- **2014: quantum teleportation over a distance of 10 feet (3.048 meters) with zero percent error rate (a vital step towards a quantum Internet);**
- **2015: quantum teleportation of multiple degrees of freedom of a quantum particle;**
- **2017: ground-to-satellite quantum teleportation (1,400 km).**

Unitary operators associated with a function $f : |[0, N-1]| \to |[0, M-1]|$

Consider a function $f : |[0, N-1]| \to |[0, M-1]|$ and denote by n and m the smallest integers such that $N \leq 2^n$ and $M \leq 2^m$.

W.L.O.G., we can assume that $f : \mathbb{X}_n \to \mathbb{X}_m$ with $\mathbb{X}_l = \left\{|k\rangle_l,\ 0 \leq k \leq 2^l - 1\right\}$.

The function f can be encoded using $n+m$ qubits, by introducing the unitary operator U_f on

$$\mathcal{H}_{n+m} = \underbrace{\mathcal{H}_n}_{\text{input register}} \otimes \underbrace{\mathcal{H}_m}_{\text{output register}}$$

defined by

$$U_f\left(|x\rangle_n \otimes |y\rangle_m\right) := |x\rangle_n \otimes |y \oplus f(x)\rangle_m,$$

where $\oplus$ denotes the modulo 2 bitwise addition:

$$|y \oplus z\rangle_m = |(y_{m-1} + z_{m-1}) \textbf{ (mod 2)}\rangle \otimes \cdots \otimes |(y_0 + z_0) \textbf{ (mod 2)}\rangle.$$

It is necessary to encode f on $n+m$ bits in order to preserve reversibility ($U_f^2 = \mathbb{1}_{\mathcal{H}_{n+m}}$).

Quantum parallelism (what it really means)

Suppose that we have at hand a black box U_f corresponding to an (unknown) function $f : \mathbb{X}_n \to \mathbb{X}_m$.

- **Prepare the state $|0\rangle_{n+m}$ and apply the unitary transform $H^{\otimes n} \otimes \mathbb{1}_{\mathbb{C}^2}^{\otimes m}$:**

$$\left(H^{\otimes n} \otimes \mathbb{1}_{\mathbb{C}^2}^{\otimes m}\right) |0\rangle_{n+m} = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle_n \otimes |0\rangle_m .$$

- **Apply U_f to the resulting state and get**

$$|\Psi\rangle := U_f \left(H^{\otimes n} \otimes \mathbb{1}_{\mathbb{C}^2}^{\otimes m}\right) |0\rangle_{n+m} = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle_n \otimes |f(k)\rangle_m .$$

It seems that applying U_f a single time, we have computed all the 2^n values $f(k)$ at once → quantum parallelism.

However, this information is hidden in the state $|\Psi\rangle$. The only way to extract information from $|\Psi\rangle$ is to make a measurement on it (which will destroy it). Only a tiny bit of information can be extracted in this way .

Deutsch problem ('85) (extracting relational information)

Suppose that we have at hand a black box U_f (a unitary operator on $\mathbb{C}^2 \otimes \mathbb{C}^2$) corresponding to an (unknown) function $f : \mathbb{X}_1 \to \mathbb{X}_1$ (with $\mathbb{X}_1 = \{0, 1\}$).

The question we want to answer is: are $f(0)$ and $f(1)$ equal?

- If we use a classical computer, the only way to answer the question is to apply f first to 0, then to 1, and check if the two results are equal.

- If we use a quantum computer, we can answer the question by applying U_f only once! Indeed,

$$(H \otimes \mathbb{1}_{\mathbb{C}^2}) U_f (H \otimes H)(X \otimes X)|00\rangle = \left| \begin{array}{ll} |1\rangle \otimes \left(\frac{1}{\sqrt{2}} |f(0)\rangle - |f(0)+1\rangle \right) & \textbf{if } f(0) = f(1), \\ |0\rangle \otimes \left(\frac{1}{\sqrt{2}} |f(0)\rangle - |f(0)+1\rangle \right) & \textbf{if } f(0) \neq f(1), \end{array} \right.$$

Measuring the observable $Z \otimes \mathbb{1}_{\mathbb{C}^2}$ in the above state, we obtain

-1 **if** $f(0) = f(1)$,
$+1$ **if** $f(0) \neq f(1)$.

Grover's search algorithm ('96)

Suppose that we have at hand a black box U_f corresponding to an (unknown) function $f : \mathbb{X}_n \to \mathbb{X}_1$ such that there exists $k_0 \in X_n$ for which

$$f(k) = 0 \textbf{ if } k \neq k_0 \quad \textbf{and} \quad f(k_0) = 1.$$

How many times do we need to apply U_f to find out k_0?

- **classical algorithm: $\sim N = 2^n$ times;**
- **quantum Grover's algorithm: $\sim \sqrt{N}$ times (which is optimal, Zalka '99).**

Let $|\phi\rangle = H^{\otimes n}|0\rangle_n = \frac{1}{\sqrt{N}} \sum_{k \in \mathbb{X}_n} |k\rangle_n, \quad V = \mathbb{1} - 2|k_0\rangle_{nn}\langle k_0|, \quad W = \mathbb{1} - 2|\phi\rangle\langle\phi|.$

We have

$$|\phi\rangle = \sin(\theta)|k_0\rangle_n + \cos(\theta)|\psi\rangle, \quad \textbf{with } |\psi\rangle \in |k_0\rangle_n^\perp \textbf{ and } \sin(\theta) = \frac{1}{\sqrt{N}}$$

and

$$(WV)^j|\phi\rangle = \sin((2j+1)\theta)|k_0\rangle_n + \cos((2j+1)\theta)|\psi\rangle.$$

Grover's algorithm:

1. prepare the state $|0\rangle_n$ and construct $|\phi\rangle = H^{\otimes n}|0\rangle_n$;
2. apply $j = \left[\frac{\pi}{4}\sqrt{N}\right]$ times the unitary operator WV;
3. measure the n observables $\mathbb{1}^{\otimes(n-1-i)} \otimes Z \otimes \mathbb{1}^{\otimes i}$.

The results will give the binary expansion of k_0 with probability

$$p_n = 1 - \sin^2\left(\left[\frac{\pi}{2}\sqrt{N} + 1\right] \arcsin\left(\frac{1}{\sqrt{N}}\right)\right) = 1 - O\left(\frac{1}{2^{n/2}}\right).$$

Practical question: how to apply V and W to a given state $|\chi\rangle \in \mathcal{H}_n$?

- Applying V to $|\chi\rangle$ amounts to applying U_f to $|\chi\rangle \otimes (H|1\rangle)$ since

$$\forall k \in \mathbb{X}_n, \quad U_f\left(|k\rangle_n \otimes (H|1\rangle)\right) = (V|k\rangle_n) \otimes (H|1\rangle).$$

- W (in fact $-W$, which does not change anything in the argument) can be applied using a few 1 and 2-qubit gates (see Mermin '07).

Conclusion

Conclusion

Entanglement is a purely quantum property, which no classical analogue

- which was successfully used to strengthen the quantum theory of matter
  → Bell's inequalities and Aspect's experiments;
- and leads to very promising applications in the fields of secured communications (quantum teleportation) and quantum computing.

Main technological bottleneck: a qubit register is not an isolated system: it interacts with its environment. It is extremely difficult to isolate a qubit register well-enough to prevent or control quantum decoherence.

Google 72-qubit processor

D-Wave 2000Q (T=0.02 K)

Entanglement is a purely quantum property, which no classical analogue

- **which was successfully used to strengthen the quantum theory of matter**

  → **Bell's inequalities and Aspect's experiments;**

- **and leads to very promising applications in the fields of secured communications (quantum teleportation) and quantum computing.**

Main technological bottleneck: a qubit register is not an isolated system: it interacts with its environment. It is extremely difficult to isolate a qubit register well-enough to prevent or control quantum decoherence.

D-Wave computers are quantum annealers dedicated to solving

$$\min \left\{ C(x_1, \cdots, x_N) := \sum_{i,j=1}^{N} a_{ij} x_i x_j + \sum_{i=1}^{N} b_i x_i, \quad x_i \in \{0,1\} \right\}$$

They can be build with imperfect qubits

$\#$ logical qubits $\ll$ $\#$ physical qubits (quantum error correction)

Entanglement is a purely quantum property, which no classical analogue

- which was successfully used to strengthen the quantum theory of matter
  → Bell's inequalities and Aspect's experiments;
- and leads to very promising applications in the fields of secured communications (quantum teleportation) and quantum computing.

Main technological bottleneck: a qubit register is not an isolated system: it interacts with its environment. It is extremely difficult to isolate a qubit register well-enough to prevent or control quantum decoherence.

Fast progress is being made though:

https://en.wikipedia.org/wiki/Timeline_of_quantum_computing

Entanglement is a purely quantum property, which no classical analogue

- which was successfully used to strengthen the quantum theory of matter
  → Bell's inequalities and Aspect's experiments;
- and leads to very promising applications in the fields of secured communications (quantum teleportation) and quantum computing.

Main technological bottleneck: a qubit register is not an isolated system: it interacts with its environment. It is extremely difficult to isolate a qubit register well-enough to prevent or control quantum decoherence.

Massive investments announced in 2018

- Europe: Quantum Flagship (1 billion euros over 10 years)
- USA: National Quantum Initiative ($1.2 biilions over 5 years)
- China: National Laboratory for Quantum Information Science ($10 billions)
- + Google, Microscoft, Amazon, IBM, Huawei...

https://quantumcomputingreport.com/news/

Conclusion

Quantum communication

- break widely used public key inscriptions (not so interesting though)

  RSA-2048 with 4100 qubits, EEC (bitcoins) with 2330 qubits

- entanglement-based secure communication (very interesting)

Quantum computing (see http://quantumalgorithmzoo.org $\sim$ 400 refs.)

- search and optimization, machine learning, quantum clustering algorithms
- linear systems and PDEs
- Monte Carlo simulations

- applications to physics: computation of propagators and partition functions
- applications to quantum chemistry (quantum computing killer's app?)

  M. Reiher, N. Wiebe, K.M. Svore, D. Wecker, and M. Troyer, *Elucidating reaction mechanisms on quantum computers*, PNAS '17

- think quantum, act classical: quantum inspired algorithms