quantum information

foundations and entanglement

radu ionicioiu

roqnet

IFIN-HH

outline

- I. the future is quantum
  overview of quantum technologies

- II. quantum information: foundations and entanglement
  qubit, quantum gates, entanglement

- III. quantum mechanics: protocols and applications
  teleportation, entanglement swapping, quantum cryptography

what is quantum information?

q. info: paradigm change of how we view and process information

information is physical

Landauer

store & process with:

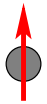
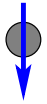
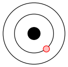
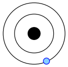
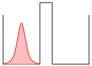
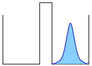
- classical devices $\Rightarrow$ classical information science
- quantum devices $\Rightarrow$ quantum information science

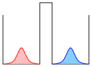
quantum is a resource

bit vs. qubit

0	1	
low	high	voltage
open	closed	MOSFET

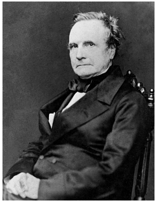
no classical analogue !

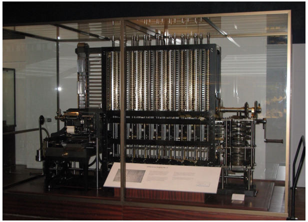
	$\|0\rangle$	$\|1\rangle$
spin	 up	 down
ion	 ground	 excited
e in 2QD	 L	 R

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

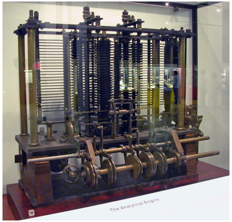
computing pioneers

Babbage & Ada





difference engine (1823): tabulate polynomials



analytical engine (1835): general-purpose computer

Turing machine

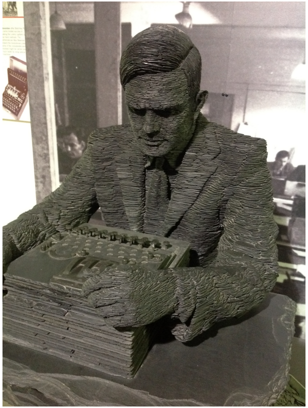
Proc. London Math. Soc. s2 **42**, 230 (1937)

230 A. M. TURING [Nov. 12,

ON COMPUTABLE NUMBERS, WITH AN APPLICATION TO THE ENTSCHEIDUNGSPROBLEM

By A. M. TURING.

[Received 28 May, 1936.—Read 12 November, 1936.]

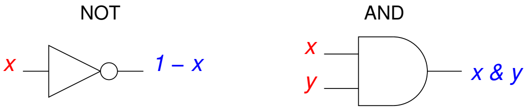


- universal Turing machine
- Turing complete (computational universal)

boolean logic

Boolean operations (gates)

NOT, AND, OR, NAND



universal set of gates:

$$\{NOT, AND\}, \quad \{NOT, OR\}, \quad \{NAND\}$$

quantum Turing machines

Proc. R. Soc. Lond. A **400**, 97–117 (1985)
Printed in Great Britain

Quantum theory, the Church–Turing principle and the universal quantum computer

BY D. DEUTSCH
Department of Astrophysics, South Parks Road, Oxford OX1 3RQ, U.K.

(*Communicated by R. Penrose, F.R.S. – Received* 13 *July* 1984)

Proc. R. Soc. Lond. A **425**, 73–90 (1989)
Printed in Great Britain

Quantum computational networks

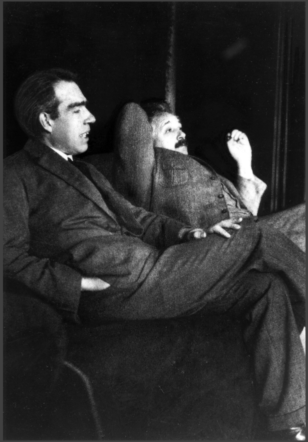
BY D. DEUTSCH
Oxford University Mathematical Institute, 24–29 St Giles, Oxford OX1 3LB, U.K.

(*Communicated by R. Penrose, F.R.S. – Received* 8 *July* 1988)

quantum mechanics

anyone who is not shocked by quantum mechanics has not understood it

Bohr



i think i can safely say that nobody understands quantum mechanics

Feynman

qm: successful, but strange

wave-particle duality, superposition, entanglement, nonlocality

counterintuitive quantum features:

- have no classical analogue
- resources for quantum technologies

QM postulates

rules of engagement

- Q1, Hilbert space

$$\mathcal{S} \to \mathcal{H}, \qquad |\psi\rangle \in \mathcal{H}, \qquad \langle\psi|\psi\rangle = 1$$

- Q2, tensor product

$$\mathcal{S}_1 + \mathcal{S}_2 \to \mathcal{H}_1 \otimes \mathcal{H}_2$$

- Q3, unitary evolution

$$|\psi\rangle \to U|\psi\rangle$$

- Q4, measurement

$$|\psi\rangle \to \Pi_k|\psi\rangle$$

observable: $\mathcal{A} \to A$, hermitian

we measure: $a_0, a_1, \ldots, a_{n-1}$ eigenvals of A

Born rule: $p(a_k) = |\langle a_k|\psi\rangle|^2 = \langle\psi|\Pi_k|\psi\rangle$

state collapse: $|\psi\rangle \to \Pi_k|\psi\rangle = |a_k\rangle$

mathematical interlude

vectors and matrices

$$|ket\rangle = \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{d-1} \end{bmatrix}$$

$$\langle bra| = \begin{bmatrix} \overline{\alpha}_0 & \overline{\alpha}_1 & \dots & \overline{\alpha}_{d-1} \end{bmatrix}$$

$\alpha_i \in \mathbb{C}$

$$\langle bra|ket\rangle = c, \quad number \in \mathbb{C}$$

$$|ket\rangle\langle bra| = M, \quad matrix \in \mathcal{M}_n(\mathbb{C})$$

postulate Q1

Hilbert space

- a quantum system $\mathcal{S}$ has associated a Hilbert space $\mathcal{H}$
- the state of a (closed) system is completely described by a unit vector $|\psi\rangle \in \mathcal{H}$

$$\langle\psi|\psi\rangle = 1$$

Q1: examples

- qubit: 2-dim quantum system
- qudit: *d*-dim quantum system

$$|\psi\rangle = \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{d-1} \end{bmatrix} = \alpha_0|0\rangle + \ldots + \alpha_{d-1}|d-1\rangle = \sum_i \alpha_i\,|i\rangle$$

$\alpha_i \in \mathbb{C}$

$$\langle\psi|\psi\rangle = \sum_i |\alpha_i|^2 = 1$$

qubit

two-level quantum system

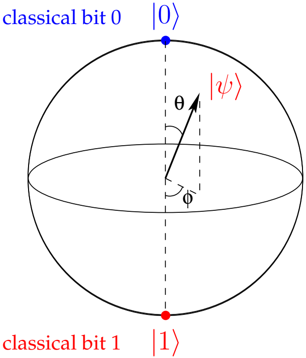
$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha|0\rangle + \beta|1\rangle$$

$\alpha, \beta \in \mathbb{C}$

$$\begin{aligned} ||\psi||^2 &= \langle\psi|\psi\rangle = \begin{bmatrix} \overline{\alpha} & \overline{\beta} \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \\ &= |\alpha|^2 + |\beta|^2 \\ &= 1 \end{aligned}$$

qubit states have norm 1

$|\psi\rangle \sim e^{i\alpha}|\psi\rangle$: *same state*



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

postulate Q2

tensor product

two quantum systems $\mathcal{S}_1, \mathcal{S}_2$: $\mathcal{H}_1, \mathcal{H}_2$

what is the Hilbert space of $\mathcal{S}_1 + \mathcal{S}_2$?

the Hilbert space of the composite system is

$$\mathcal{S}_1 + \mathcal{S}_2 : \quad \mathcal{H}_{12} = \mathcal{H}_1 \otimes \mathcal{H}_2$$

state of the composite system

$$|\psi\rangle_{12} \in \mathcal{H}_1 \otimes \mathcal{H}_2$$

basis

$\mathcal{H}_1$: basis $\{|i\rangle_1\}$; $\mathcal{H}_2$: basis $\{|j\rangle_2\}$

basis in $\mathcal{H}_1 \otimes \mathcal{H}_2$

$$\{|i\rangle_1 \otimes |j\rangle_2\}$$

$$\dim \mathcal{H}_{12} = \dim \mathcal{H}_1 \cdot \dim \mathcal{H}_2 = d_1 \cdot d_2$$

shortcut notations

$$|i\rangle_1 \otimes |j\rangle_2 := |i\rangle_1 |j\rangle_2 = |i\rangle|j\rangle = |ij\rangle$$

general state:

$$|\psi\rangle_{12} = \sum_{i,j} a_{ij}\, |i\rangle_1 \otimes |j\rangle_2 := \sum_{i,j} a_{ij}\, |i\rangle|j\rangle$$

entanglement!!

examples

- 2 qubits: $\mathcal{H}_1 = \mathcal{H}_2 = span\{|0\rangle, |1\rangle\}$

  basis in $\mathcal{H}_1 \otimes \mathcal{H}_2$: $\{|0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|0\rangle, |1\rangle|1\rangle\} = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ dim $= 4$

- n qubits: $\mathcal{H} = \mathcal{H}_1^{\otimes n} = \mathcal{H}_1 \otimes \ldots \otimes \mathcal{H}_1$

  basis in $\mathcal{H}$: $\{|0...0\rangle, |0...1\rangle, \ldots, |1...1\rangle\}$ dim $= 2^n$

- 2 qudits: $\mathcal{H}_1 = \mathcal{H}_2 = span\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$

  basis in $\mathcal{H}_1 \otimes \mathcal{H}_2$: $\{|0\rangle|0\rangle, |0\rangle|1\rangle, \ldots, |d-1\rangle|d-1\rangle\}$ dim $= d^2$

postulate Q3

unitary evolution

the evolution of a closed system is unitary

$$|\psi'\rangle = U|\psi\rangle$$

$$UU^\dagger = U^\dagger U = \mathbb{I}$$

- reversible: $|\psi\rangle = U^\dagger|\psi'\rangle$

$$|\psi\rangle \xrightarrow{U} |\psi'\rangle$$
$$|\psi'\rangle \xrightarrow{U^\dagger} |\psi\rangle$$

Schrödinger eqn.: $i\hbar\frac{d}{dt}|\psi\rangle = \mathbf{H}|\psi\rangle, \quad U_t = e^{-\frac{i}{\hbar}\mathbf{H}t}, \quad |\psi(t)\rangle = U_t|\psi_0\rangle$

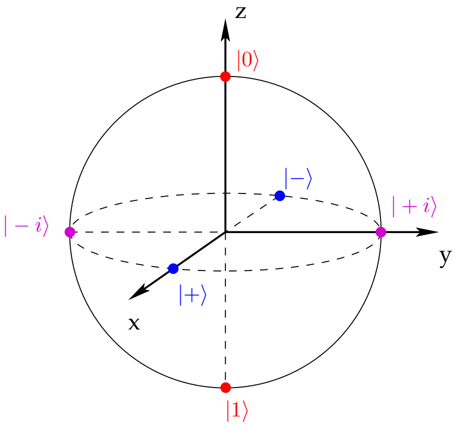
examples

$$X: \quad |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$Y: \quad |+i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \quad |-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$$

$$H|0\rangle = |+\rangle$$
$$H|1\rangle = |-\rangle$$
$$H|+i\rangle = |-i\rangle$$
$$H|-i\rangle = |+i\rangle$$

$$Z|+\rangle = |-\rangle$$
$$Z|-\rangle = |+\rangle$$



postulate Q4

observables & measurement

observable $\mathcal{A}$: hermitian operator $A = A^\dagger$ acting on $\mathcal{H}$

1. *what values can I experimentally measure?*

   eigenvals a_k of A

   $$a_0, \ldots, a_{n-1} \in \mathbb{R}$$

2. *with what probability?*

   $$p(a_k) = |\langle a_k|\psi\rangle|^2 = \langle\psi|\Pi_k|\psi\rangle$$

   Born rule

3. *what's the state after the measurement?*

   $$|\psi'\rangle = |a_k\rangle$$

basis of eigenvectors of A: $\{|a_k\rangle\}$; $A|a_k\rangle = a_k|a_k\rangle$

$$|\psi\rangle = \sum_i c_i|a_k\rangle \quad , \qquad c_i \in \mathbb{C}$$

consistency

$$\sum_k p(a_k) = \sum_k \langle\psi|\Pi_k|\psi\rangle = \langle\psi|\sum_k \Pi_k|\psi\rangle = \langle\psi|\mathbb{I}|\psi\rangle = \langle\psi|\psi\rangle = 1$$

expectation value (=average value) of observable A

$$\langle A\rangle = \sum_k a_k\, p(a_k) = \langle\psi|A|\psi\rangle$$

examples

	measure Z			measure X		
$\lvert\psi\rangle$	$p(+1)$	$p(-1)$	$\langle Z\rangle$	$p(+1)$	$p(-1)$	$\langle X\rangle$
$\lvert 0\rangle$	1	0	1			
$\lvert 1\rangle$	0	1	-1			
$\lvert +\rangle$	0.5	0.5	0			
$\lvert -\rangle$	0.5	0.5	0			

$$p(a_k) = |\langle a_k|\psi\rangle|^2 = \langle\psi|\Pi_k|\psi\rangle$$

$$\langle A\rangle = \sum_k a_k\, p(a_k) = \langle\psi|A|\psi\rangle$$

qubit

qubit = quantum two-level system

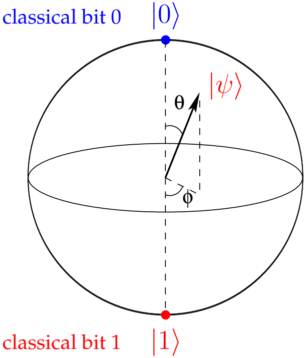
$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha|0\rangle + \beta|1\rangle$$

$\alpha, \beta \in \mathbb{C}$

$$\langle\psi|\psi\rangle = |\alpha|^2 + |\beta|^2 = 1$$

quantum states have norm 1

$|\psi\rangle \sim e^{i\alpha}|\psi\rangle$: *same state*

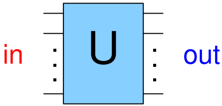


$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

quantum gates

quantum gate = *unitary U acting on* $|\psi\rangle$

$$|\psi_{out}\rangle = U\,|\psi_{in}\rangle$$



universality (functional completeness)

which gates are sufficient to do ANY computation?

on any number of (qu)bits

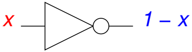
classical

$\{NOT, AND\}; \ \{NAND\}$

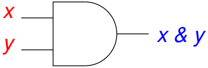
quantum

$\{H, P_\varphi, CNOT\}$

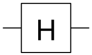
NOT



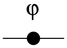
AND



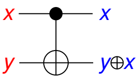
Hadamard



Phase



CNOT



Theorem

Any quantum algorithm can be build out of the following gates

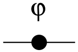
$$H, P_{\varphi}, CNOT$$

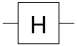
A. Barenco *et al.*, *Elementary gates for quantum computation*, Phys. Rev. A **52**, 3457 (1995)

single-qubit gates

$$I = \mathbb{I}_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, \quad T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}, \quad P_\varphi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}, \quad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$





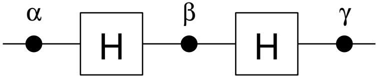
$$R_z(\varphi) = e^{-i\frac{\varphi}{2}Z} = \begin{bmatrix} e^{-i\frac{\varphi}{2}} & 0 \\ 0 & e^{i\frac{\varphi}{2}} \end{bmatrix} = e^{-i\frac{\varphi}{2}} P_\varphi$$

universality: single-qubit

$\forall U$, single-qubit gate

$$U = e^{i\theta_0} e^{i\theta_1 Z} e^{i\theta_2 X} e^{i\theta_3 Z}$$

equivalently

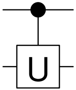


$$U = e^{i\varphi} P_\gamma \; H \; P_\beta \; H \; P_\alpha$$

$$e^{i\alpha M} = \cos\alpha \mathbb{I} + i \sin\alpha M, \quad \forall M, \; M^2 = \mathbb{I}$$

two-qubit gates: entangling

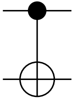
$$C(U) = \begin{bmatrix} I & 0 \\ 0 & U \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{bmatrix}$$



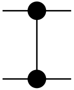
$$C(U)\,|x\rangle|y\rangle = |x\rangle U^{x}|y\rangle$$

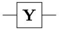
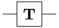
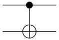
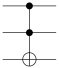
examples

$$CNOT = C(X) = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$



$$C(Z) = \begin{bmatrix} I & 0 \\ 0 & Z \end{bmatrix} = \mathrm{diag}(1, 1, 1, -1)$$



Operator	Gate(s)	Matrix
Pauli-X (X)		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)		$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

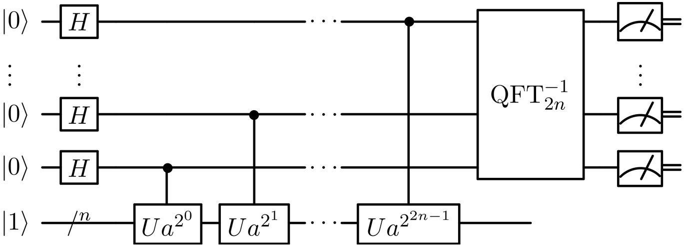
source: wiki

quantum circuits

standard computational model

q. circuit = sequence of quantum gates on *n* qubits

any quantum algorithm = circuit of 1- and 2- qubit gates



source: wiki, Shor's algorithm

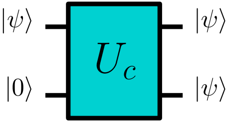
Theorem

An ***unknown*** *quantum state cannot be cloned* *(= copied perfectly)*

Proof.

$$|\psi\rangle \otimes |0\rangle \xrightarrow{U_c} |\psi\rangle \otimes |\psi\rangle = U_c\, |\psi\rangle \otimes |0\rangle$$

$$|\phi\rangle \otimes |0\rangle \xrightarrow{U_c} |\phi\rangle \otimes |\phi\rangle = U_c\, |\phi\rangle \otimes |0\rangle$$



$$\langle\psi|\phi\rangle \cdot \langle\psi|\phi\rangle = \langle\psi|\phi\rangle \cdot \langle 0|0\rangle$$

$$\Rightarrow \langle\psi|\phi\rangle = 0 \;\; \text{or} \;\; \langle\psi|\phi\rangle = 1$$

$$|\phi\rangle \perp |\psi\rangle \;\; \text{or} \;\; |\phi\rangle = |\psi\rangle$$

$\Rightarrow$ contradiction, cannot clone non-orthogonal states

$\square$

no-cloning

- a known quantum state can be copied perfectly (=cloned)
- an unknown quantum state can be copied imperfectly

but

an unknown quantum state cannot be copied perfectly

crucial for quantum communications

entanglement

what is entanglement?

entangled = not separable

$$|\psi\rangle_{AB} \neq |\phi_1\rangle_A \otimes |\phi_2\rangle_B$$

- cannot describe it as states of separate particles
- quantum correlations - stronger than classical

the whole is more than the sum of its parts

Schrödinger

on entanglement

entanglement is not one but rather the characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought

the best possible knowledge of a whole does not necessarily include the best possible knowledge of all its parts

E. Schrödinger, *Discussion of Probability Relations Between Separated Systems*, Proc. Camb. Philos. Soc. **31**, 555 (1935); **32**, 446 (1936)

EPR-Bell states

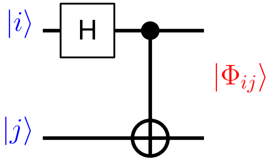
Bell basis for two qubits

$$|\Phi^+\rangle \equiv |\Phi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|\Phi^-\rangle \equiv |\Phi_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\Psi^+\rangle \equiv |\Phi_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\Psi^-\rangle \equiv |\Phi_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$



- orthogonality:

$$\langle\Phi_{ij}|\Phi_{kl}\rangle = \delta_{ik}\delta_{jl}$$

- maps the computational basis to the Bell basis: $|i\rangle|j\rangle \mapsto |\Phi_{ij}\rangle$

entanglement

two questions

- given $|\psi\rangle$, can we decide if it's entangled or not?

  if yes, how much entanglement does it have?

- why is entanglement useful?
  - quantum computation/algorithms: Shor, Grover etc
  - quantum protocols: teleportation, entanglement swapping
  - quantum repeaters

entanglement

separability criterion: 2 qubits

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

Theorem

$$|\psi\rangle \text{ is separable } \Leftrightarrow C = 0$$

concurrence

$$C = 2\left|a_{00}a_{11} - a_{01}a_{10}\right|$$

Proof

$$\begin{aligned} |\phi_1\rangle \otimes |\phi_2\rangle &= (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) \\ &= ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle \end{aligned}$$

etc

entanglement

properties

- $0 \leqslant C \leqslant 1$
- $C = 1$ maximally entangled states
- entanglement is invariant under local unitaries

$$C(U_1 \otimes U_2 \left|\psi\right\rangle) = C(\left|\psi\right\rangle)$$

Corollary: cannot create entanglement by acting locally on a separable state

entanglement requires an interaction between qubits

concurrence

examples

compute C for the states

1. $|\psi_1\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$ $\quad C =$
2. $|\psi_2\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)$ $\quad C =$
3. $|\psi_3\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$ $\quad C =$
4. $|\psi_4\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ $\quad C =$
5. $|\psi_5\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ $\quad C =$
6. $|\psi_6\rangle = \cos\alpha|00\rangle + \sin\alpha|11\rangle$ $\quad C =$

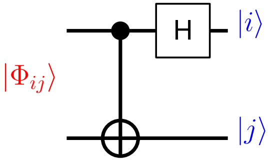
Bell state measurement (BSM)

$$|00\rangle = \frac{1}{\sqrt{2}}(|\Phi^+\rangle + |\Phi^-\rangle)$$

$$|01\rangle = \frac{1}{\sqrt{2}}(|\Psi^+\rangle + |\Psi^-\rangle)$$

$$|10\rangle = \frac{1}{\sqrt{2}}(|\Psi^+\rangle - |\Psi^-\rangle)$$

$$|11\rangle = \frac{1}{\sqrt{2}}(|\Phi^+\rangle - |\Phi^-\rangle)$$



- maps the Bell basis to the computational basis: $|\Phi_{ij}\rangle \mapsto |i\rangle|j\rangle$
- crucial for teleportation

entanglement: generalization

can we generalize the Bell states?

yes

1. more qubits
2. more dimensions (qudits)

entanglement: more qubits

3 qubits

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

$$|W\rangle = \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle)$$

n qubits

$$|GHZ_n\rangle = \frac{1}{\sqrt{2}}(|00\ldots0\rangle + |11\ldots1\rangle)$$

$$|W_n\rangle = \frac{1}{\sqrt{n}}(|10\ldots0\rangle + |01\ldots0\rangle + \ldots + |00\ldots1\rangle)$$

GHZ $\neq$ W

$$|GHZ\rangle \neq_{LOCC} U_1 \otimes U_2 \otimes U_3 \, |W\rangle$$

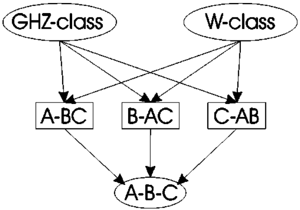


FIG. 1. Different local classes of tripartite pure states. The direction of the arrows indicates which noninvertible transformations between classes are possible.

Dür, Vidal, Cirac, *Three qubits can be entangled in two inequivalent ways*, Phys. Rev. A **62**, 062314 (2000); quant-ph/0005115

entanglement: more dimensions

two qudits

$$|\Phi_d\rangle = \frac{1}{\sqrt{d}}(|00\rangle + |11\rangle + \cdots + |d-1\ d-1\rangle) = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle|i\rangle$$

there are d^2 maximally-entangled states for two qudits

hint: apply $Z_d^i X_d^j |\Phi_d\rangle$, $i, j = 0 \ldots d-1$

Z_d, X_d generalized Pauli matrices for qudits

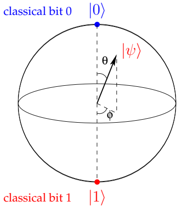
$Z_d|i\rangle = \omega^i|i\rangle$, $\omega^n = 1$

$X_d|i\rangle = |i \oplus 1\rangle$

summary

- qubit: 2-dim complex vector

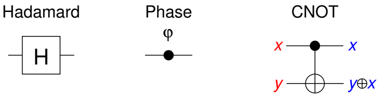
$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$



- quantum gates: unitary U acting on $|\psi\rangle$

- universality: any q. algorithm can be build from 1- and 2-qubit gates

$$\{H, P_\varphi, CNOT\}$$



- no-cloning:
  an unknown q. state cannot be cloned

$$|\psi\rangle|0\rangle \overset{U}{\nrightarrow} |\psi\rangle|\psi\rangle$$

Thank you!