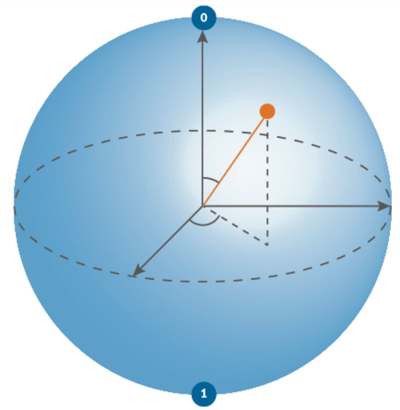
Quantum Information Science

Mathematical background

André Nies

University of Auckland, May 15



What is quantum physics?

- Framework for the construction of (physical) theories, in particular at microscopic levels.
- Example of such a theory: quantum electrodynamics, which describes the interaction of atoms and light
- Quantum physics is expressed mathematically in the language of operators on finite dimensional Hilbert spaces. So the language is linear algebra.
- Four postulates, connecting physics concepts such as state of a system, measurement with mathematical concepts
- Since the 1980s, researchers have used quantum physics as a framework for a new kind of information science

Quantum physics: timeline (1)

1900 Planck's work on black body radiation; energy is quantized

1924-27 Heisenberg, Schrödinger, Born and others formulate the principles of quantum mechanics (or quantum mechanics)

1933 Einstein, Podolsky and Rosen paper criticizing this work

MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*
(Received March 25, 1935)

1933 Niels Bohr's reply

OCTOBER 15, 1935 PHYSICAL REVIEW VOLUME 48

Can Quantum-Mechanical Description of Physical Reality be Considered Complete?

N. BOHR, *Institute for Theoretical Physics, University, Copenhagen*
(Received July 13, 1935)

Quantum physics: timeline (2)

1932 Von Neumann *Mathematische Grundlagen der Quantenmechanik,* summarising his papers from 1927 to that date.

1964 Bell's inequality, 1969 CHSH inequality: non-locality

Physics Vol. 1, No. 3, pp. 195–200, 1964 Physics Publishing Co. Printed in the United States

ON THE EINSTEIN PODOLSKY ROSEN PARADOX*

J. S. BELL†

Department of Physics, University of Wisconsin, Madison, Wisconsin

(*Received* 4 *November* 1964)

1982- Alain Aspect and others confirm entanglement experimentally

2015 Loophole free experiments, Henson et al., Giustina et al.

Theory of (quantum) computation: timeline

1936 Turing: a theoretical machine that can simulate all computations

1982 R. Feynman: suggests to build computers based on quantum mechanics

1985 D. Deutsch: challenges polynomial time Church-Turing thesis

1994 P. Shor: quantum algorithms for factoring and discrete logarithm

1995 Shor, Steane independently: quantum error correction, leads to threshold theorem (Aharonov and Ben-Or)

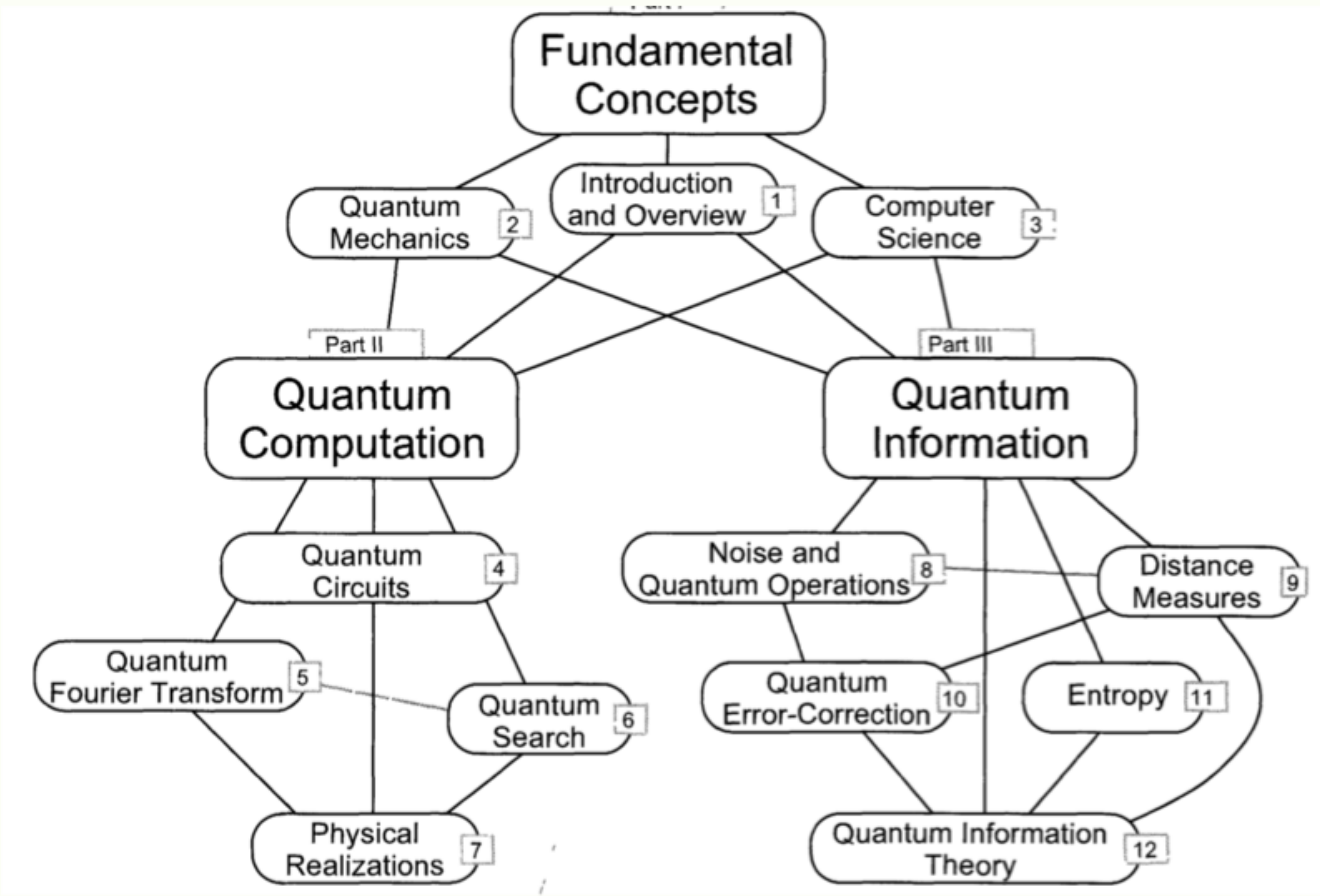
1995 quantum circuits, Solovay-Kitaev theorem

1997 Bernstein-Vazirani: universal quantum Turing machine

2013 Aaronson, Arkhipov: boson sampling as a way to show “quantum supremacy”.

2016 Bremner, Montanaro, Sheperd: random circuit sampling, IQP

Structure of Nielsen and Chuang's 2000 book (2010 second edition)



Hilbert space

- Finite-dimensional vector space A over the complex numbers $\mathbb{C}$
- Vectors are denoted $|\varphi\rangle$, $|\psi\rangle$ etc
- Inner product $\langle\varphi|\psi\rangle$
- linear in the second, antilinear in the first component
- Value 0 means orthogonal; value 1 means equal (for unit vectors)
- Length of a vector $|\varphi\rangle$ is $\sqrt{\langle\varphi|\varphi\rangle}$; Cauchy-Schwartz inequality
- Operators are linear maps between Hilbert spaces; given by matrices
- Hermitian operator: equals the conjugate transpose
- Unitary operator: the inverse equals the conjugate transpose

States and their time evolution

Postulate 1: A physical system is represented by an n-dimensional Hilbert space A. The state of the system is a unit vector in A, written $|\psi\rangle$

- For instance, to represent a single qubit we let n=2.
- The vectors $|0\rangle$ and $|1\rangle$ form a basis of the Hilbert space.
- A qubit is a vector $a|0\rangle + b\,|1\rangle$ where a,b are complex numbers and $|a|^2 + |b|^2 = 1.$
- When measured, $|a|^2$ is the probability to get 0, and $|b|^2$ the probability to get 1.

Postulate 2 describes the time evolution of a closed physical system via some form of Schrödinger's equation.

Composite systems

- The tensor product $A \otimes B$ consists of linear combinations of vectors

$$|\psi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$$

- Inner product is defined by looking at components.
- The operation $\otimes$ is bilinear.

Postulate 4: If two systems are represented by Hilbert spaces A, B, then the composite system is represented by the tensor product $A \otimes B$.

- A system of two qubits is represented by Hilbert space $\mathbb{C}^2 \otimes \mathbb{C}^2$, which has dimension 4.
- For bits x,y write $|xy\rangle = |x\rangle \otimes |y\rangle$.
- The state is a unit vector $a|00\rangle + b\,|01\rangle + c|10\rangle + d\,|11\rangle$.

No-cloning theorem

Informally, no quantum machine can copy an unknown state.

Formally, there is no unitary operator U on $A \otimes B$ and state $|s\rangle$ in B such that $U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$ for each state $|\psi\rangle$ in A.

Proof. Assume otherwise. Then

$$\langle \varphi | \psi \rangle = \langle |\varphi\rangle \otimes |s\rangle \mid |\psi\rangle \otimes |s\rangle \rangle$$

because $\langle s|s \rangle = 1.$

We can apply U to $|\varphi\rangle \otimes |s\rangle$ and $|\psi\rangle \otimes |s\rangle$ without changing the value of the inner product. This yields

$$\langle \varphi | \psi \rangle = \langle |\varphi\rangle \otimes |\varphi\rangle \mid |\psi\rangle \otimes |\psi\rangle \rangle = \langle \varphi | \psi \rangle \, \langle \varphi | \psi \rangle$$

So either $\langle \varphi | \psi \rangle = 0$ (orthogonal) or $\langle \varphi | \psi \rangle = 1$ (equal).

Measurements on system given by a Hilbert space

Postulate 3

- A measurement is a sequence $P_0, \dots, P_{r-1}$ where the P_k's are projections on A (Hermitian, $P_k P_k = P_k$) and $\sum P_k = 1_A$.
- The probability that result m occurs when state $|\psi\rangle$ is measured is $p(m) = \langle\psi|P_m|\psi\rangle$ i.e., the inner product of $|\psi\rangle$ with P_m ($|\psi\rangle$).
- After measurement outcome m, the system is in the state $\frac{1}{\sqrt{p(m)}} P_m|\psi\rangle$.

Example

In system $\mathbb{C}^2 \otimes \mathbb{C}^2$ of two qubits, we measure the second qubit by

- P_0 $\quad |a0\rangle \longrightarrow |0\rangle,\ |a1\rangle \longrightarrow \emptyset$ (zero vector) $\quad a = 0,1$
- P_1 $\quad |a1\rangle \longrightarrow |1\rangle,\ |a0\rangle \longrightarrow \emptyset$ $\quad a = 0,1$

Entanglement, mathematically

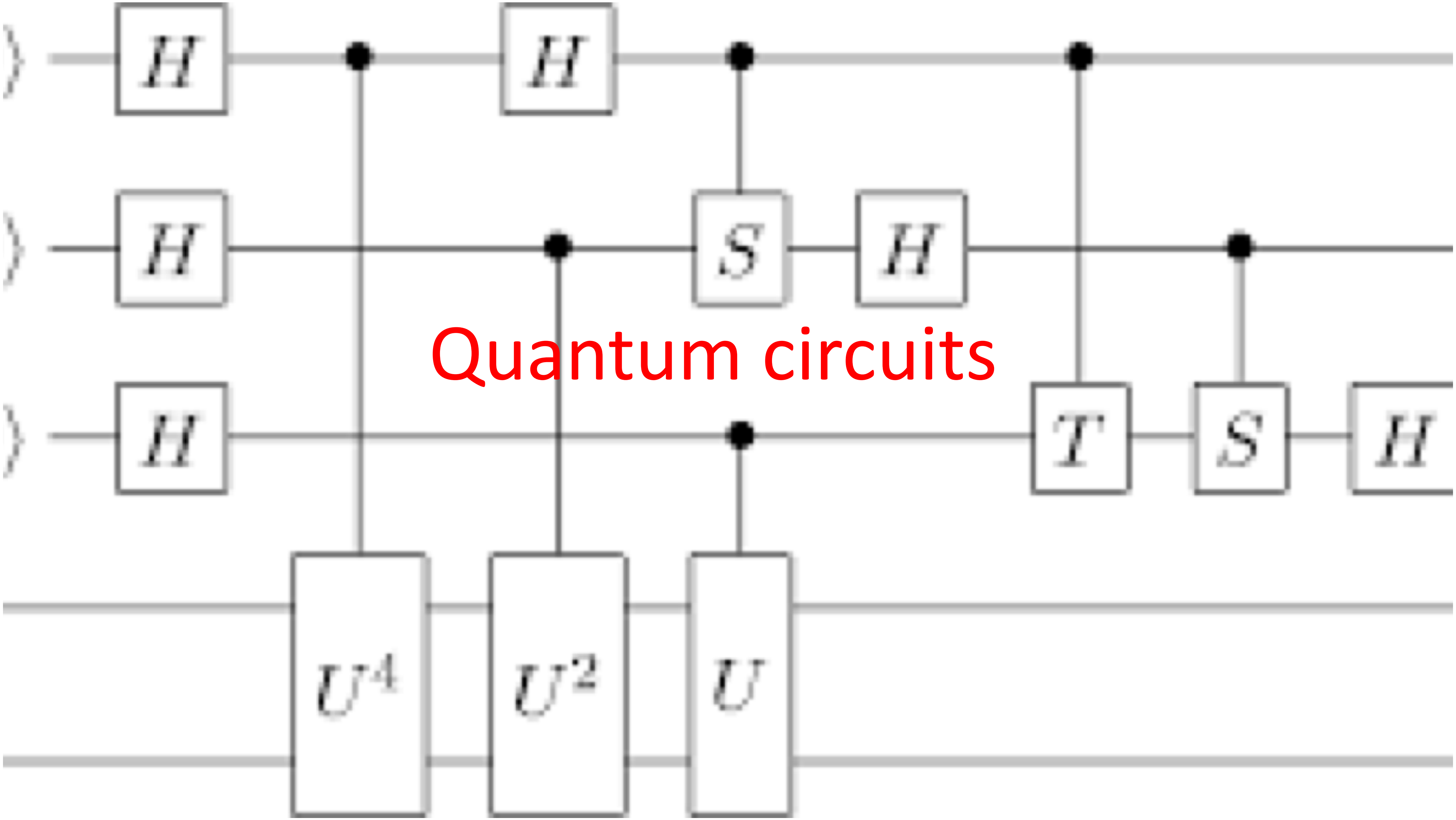
- We have a composite system $A \otimes B$
- Consider a state $|\psi\rangle \in A \otimes B$, where
  A has basis $|j\rangle$; $j = 0,1, \ldots, r-1$ and B has basis $|k\rangle$; $j = 0,1, \ldots, s-1$.
- The most general form of such $|\psi\rangle$ is $|\psi\rangle = \sum c_{jk} \, |jk\rangle$.
- $|\psi\rangle$ is called separable if $|\psi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$ for states

  $$|\psi_A\rangle = \sum a_j |j\rangle, \, |\psi_B\rangle = \sum b_k |k\rangle.$$

  i.e. $c_{jk} = a_j b_k$.
- Otherwise $|\psi\rangle$ is called entangled (verschränkt).

Example $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is entangled:
If we have $|\psi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$ then $c_{00} \neq 0$, so $a_0, b_0 \neq 0$.
$c_{11} \neq 0$, so $a_1, b_1 \neq 0$. Then also $c_{01} = a_0 b_1 \neq 0$, which is not the case.

Quantum circuits



Quantum circuits

- Quantum analog of Boolean circuits
- Unlike Boolean circuits, they are made up of unitary operations, and hence reversible
- Can be used to create an entangled pair of qubits
- Used to implement the discrete Fourier transform
- We also allow measurement at the end, or even in between (though it’s not a reversible operation)
- The symbol for measurement w.r.t. standard basis is 

Important unary quantum gates

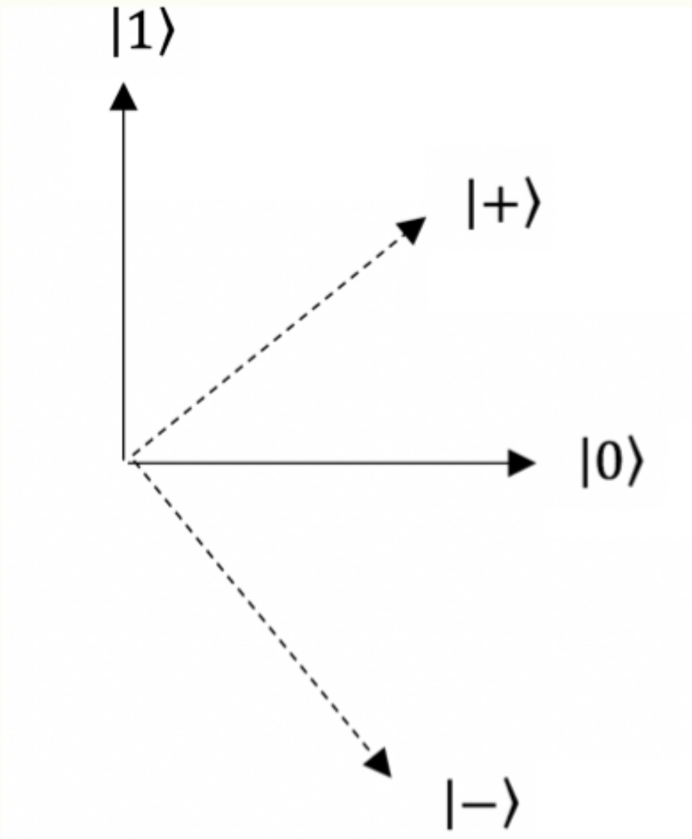
- Pauli X,Y and Z gates

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

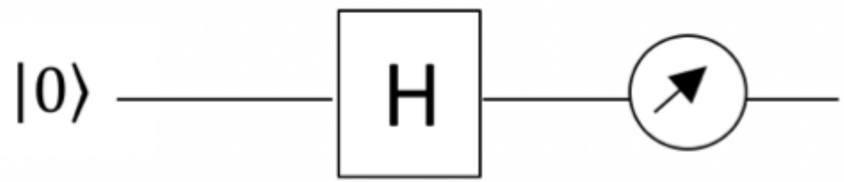
- $\frac{\pi}{8}$ – gate $T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix}$

Hadamard gate

- $|0\rangle \longrightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|1\rangle \longrightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- So, $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.
- $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ is written $|+\rangle$
- $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ is written $|-\rangle$.



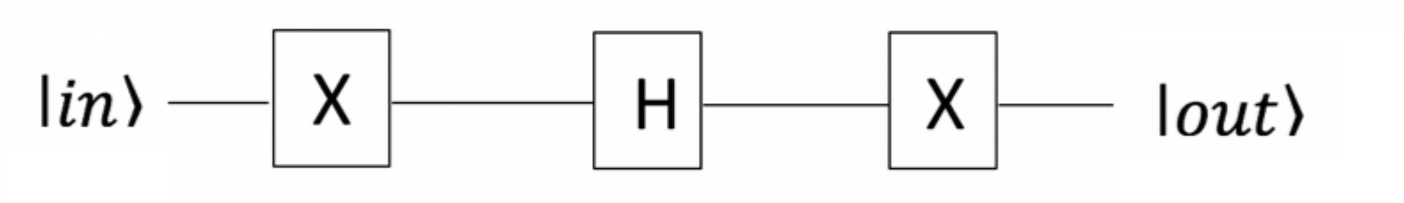
The following circuit produces a random bit, i.e. 0 and 1 each with probability 1/2.



Making circuits from gates

Circuits are formed by putting gates together. No cycles, no splitting of wires.

Example:



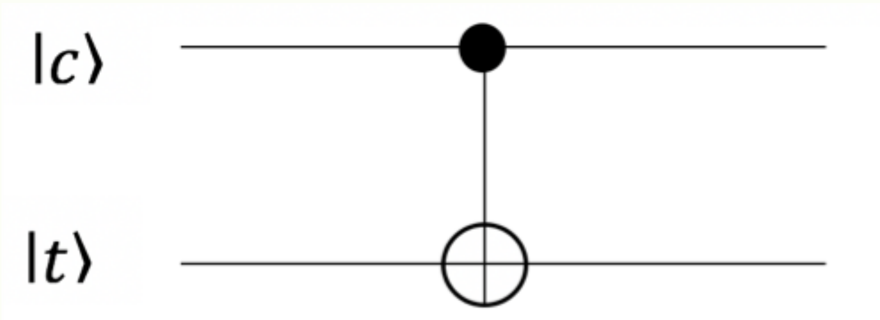
Controlled "Not'' binary gate

CNOT acts as follows for $c = 0,1$, $t = 0,1$

$$\underset{\substack{\uparrow\\ \text{control}}}{|c\rangle}\ \underset{\substack{\uparrow\\ \text{target}}}{|t\rangle} \longrightarrow |c\rangle|t\underset{\substack{\uparrow\\ \text{addition modulo 2}}}{\oplus} c\rangle$$

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

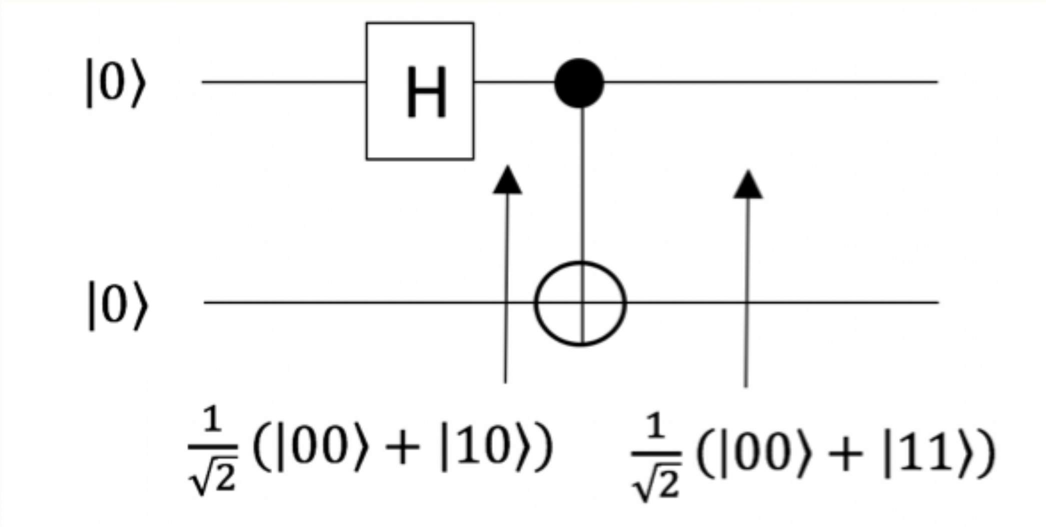
I.e., if control bit is $|1\rangle$ then the target bit is flipped.



Circuit notation for controlled-not

Creating an EPR state

We can use H and CNOT gates to create a pair of entangled qubits, the EPR state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.



This works because CNOT turns a linear combination $a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ into $a|00\rangle + b|01\rangle + d|10\rangle + c|11\rangle$.

Here, $a = c = \frac{1}{\sqrt{2}}$, $b = d = 0$.

Deutsch's algorithm (1985)

Problem:

Given a function $f: \{0,1\} \rightarrow \{0,1\}$. Is f

- constant: $f(0) = f(1)$

or

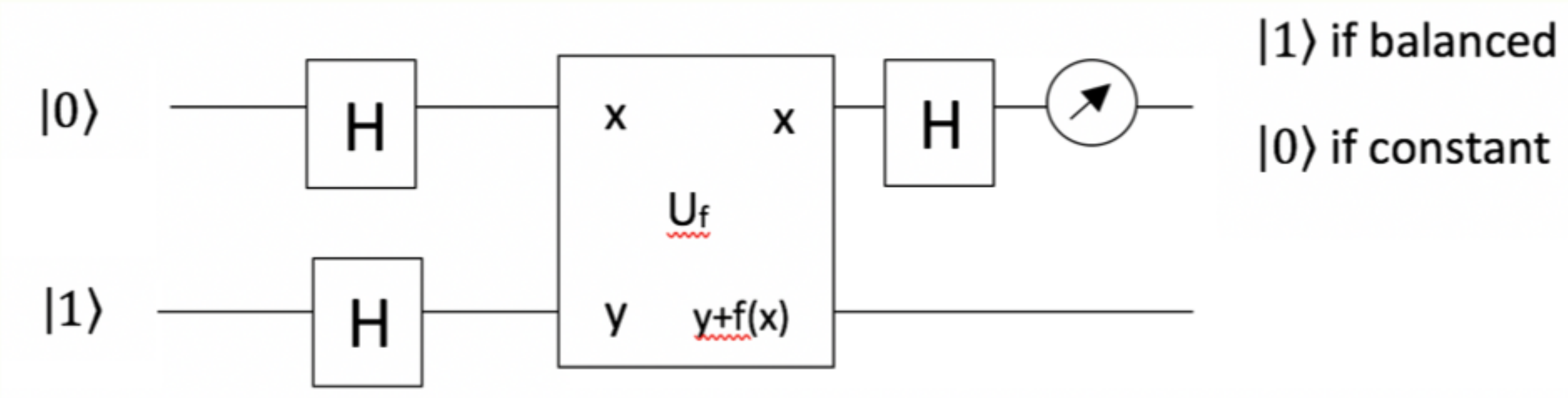
- balanced: $f(0) \neq f(1)$?

In 'quantum way', we can solve this with one application of f:

A quantum circuit determines if f is balanced

Encode f into unitary operator: $U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$

The following circuit decides which case we have:



Shor’s algorithm (1994)

Problem: Given a number N that is not prime,
find a nontrivial factorization N=ab.

Shor’s algorithm does that in polynomial time on a quantum computer.

This means one needs circuit of poly(log N) quantum gates.

It only finds the answer with high probability.

Shor was ICM speaker in 1998 and got Nevanlinna Prize for this

Reduction of factoring to period-finding

Let N be odd, not prime, not a prime power. E.g. N= 15.

- Choose random $x < N$ such that gcd(x, n)=1. E.g. x=7
- Let p be a period of $x \; mod \; N$. i.e. $x^p \equiv 1 \; mod \; N$. If p is odd, try other x. p=4
- Else $\left(x^{p/2}+1\right)\left(x^{p/2}-1\right) \equiv x^p - 1 \equiv 0 \; mod \; N$. i.e. N divides this product.
- So gcd($x^{p/2}+1, N$) gcd($x^{p/2}-1, N$)= N is a factoring.

E.g. $(7^2+1)(7^2-1) \equiv 7^4 - 1 \equiv$ 0 mod 15, and the factoring is 5 . 3 = 15

If one of the factors is 1, try another x. One can show that the chance of x being useless is $\leq 2^{-m}$, where N has m prime factors.

Preparing data (1)

Two quantum registers, called IR (input register) and OR.

- Choose an integer q such that $N^2 < q < 2N^2$ **let's pick 256**
- Choose a random integer x such that GCD(x, N) = 1 **let's pick 7**

  - Input register: must contain enough qubits to represent numbers as large as q-1. **Up to 255, so we need 8 qubits**

  - Output register: must contain enough qubits to represent numbers as large as N-1. **Up to 14, so we need 4 qubits**

Preparing Data (2)

Load the input register with an equally weighted superposition of all the integers from 0 to q-1. 0 to 255

Load the output register with zeros.

The state of the system at this point is:

$$\underbrace{\frac{1}{\sqrt{256}}\sum_{a=0}^{255}|a>}_{\text{IN}}\ \underbrace{|0000>}_{\text{OUT}}$$

The two registers make a composite system.

Exponentiation mod N, and measuring OR

Apply the transformation $x^{a} \bmod N$ to each number in IR, storing the result of each computation in OR. (Quantum parallelism)

Take a measurement on the output register. This will collapse the superposition to represent just one of the possible results of the transformation; let's call this value d.

Shor's Algorithm – Entanglement and QFT

The IR and OR registers are entangled after the modulo operation.

Thus, measuring the OR will have the effect of partially collapsing the IR into an **equal superposition** of each state between 0 and q-1 that yielded d (the value of the collapsed output register.)

If e.g. d=1 we have

$$\text{IR}= \frac{1}{\sqrt{64}}\,\mathbf{(|0> + \quad |4> + \quad |8> + \quad |12> + ...+ |252>)}$$

Now apply inverse discrete Fourier transform to the partially collapsed IR.

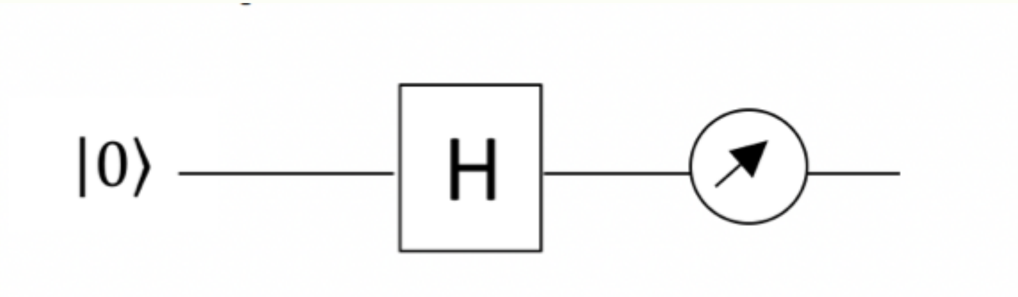
This transform turns each |a> into

$$\frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} |c> \; exp(2\pi i\, ac \,/\, q)$$

Measurement of this transform gives **|c>** the probability 0 for non-integer values of 4c/ q. From this distribution we can determine the period p=4.

Randomness for qubits

Recall that the circuit below produces a random classical bit, i.e. 0 and 1 both with probability 1/2.



This is not what we study.
The qubit H|0> is determined, it's just not accessible to us.

We want to define randomness for sequences of qubits.

Finite sequences of qubits

For finite bitstrings (in the classical setting), randomness means incompressibility. The decompressor is a universal Turing machine.

Length of a shortest description is descriptive (or Kolmogorov) complexity of a string.

A string of n qubits is a unit vector in an n-fold tensor power of $\mathbb{C}^2$.

1997 Bernstein and Vazirani's universal quantum Turing machine

2001 -2008 Vitanyi; Berthiaume et al.; Markus Müller's thesis gave various versions of descriptive complexity for qubit strings, based on this model.

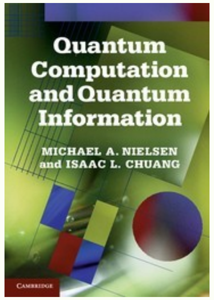
Infinite sequences of qubits?

- They have some physical relevance, e.g. spin chains.
- Mathematically they are complicated objects (states in a certain C*-algebra, which are certain sequences of density matrices).
- The reason is that if we ``delete” the second bit from the entangled pair $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, we get a statistical superposition of $|0\rangle$ and $|1\rangle$, called a mixed state.
- Nies and Scholz (2018, on arXiv) introduced a quantum version of Martin-Löf randomness for such sequences.
- They have obtained a universal test, law of large numbers, and a weak quantum version of Levin-Schnorr theorem (which says roughly: random sequence means that all initial segments are incompressible).

Some references

Peter Shor , *Quantum computing,* ICM proceedings, Documenta Mathematica, 1998

Chuang and Nielsen, Quantum Computation and Quantum Information CUP 2000/2010



Nies and Scholz, Martin-Löf random quantum states, arXiv preprint, 2018.