Introduction to Quantum Computing

XII KNMF Conference
Prepared by: Dr. Philippe J.S. De Brouwer
Honorary Consul of Belgium in Kraków
guest professor at the UJ, AGH, UEK and UW
board member of AGH and ISK
SVP at HSBC in Kraków

AGH

Team:
AGH University of Krakow
Date: 2024-04-04

HSBC

Table of Contents

Introduction

HSBC

The three stages of computers: (1) Analogue

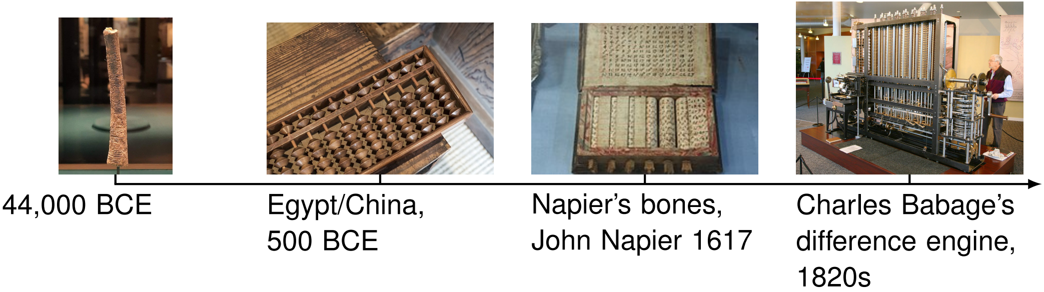


Figure: Analogue counting devices

The Analytical Engine – 1837 (concept)

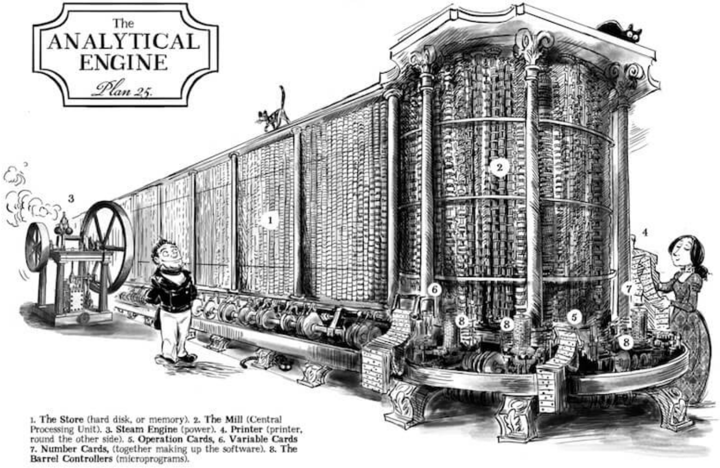


Figure: In 1837 Charles Babage proposed the first general purpose computer: the “analytical engine”. Legend: 1: memory, 2: the mill (CPU), 3: steam engine, 4: printer, 5: operation cards, 6: variable cards, 7: number cards, 8: barrel (controller)

The three stages of computers: (2) Digital

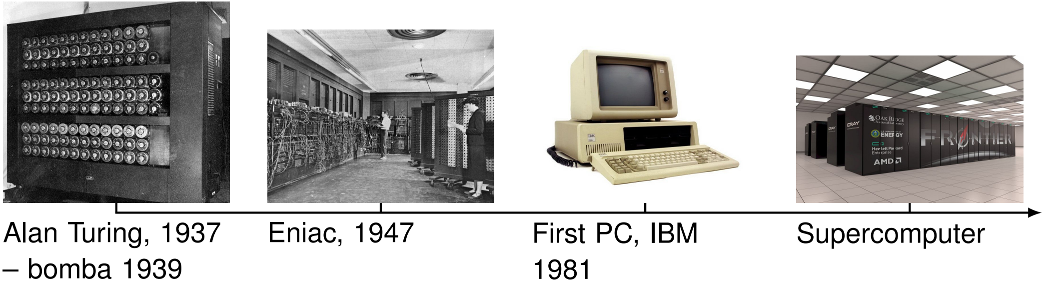


Figure: Digital Computers

The three stages of computers: (2) Digital

Figure: The fastest supercomputer in the world: Frontier, HPE CRAY EX235A, AMD OPTIMIZED 3RD GENERATION EPYC 64C 2GHZ – USA, Oakr Ridge – Rmax = 1.5 Exa Flops = 1.5×10^{18} Flops, using 21’000KwH – foto: Oak Ridge

The three stages of computers: (3) Quantum

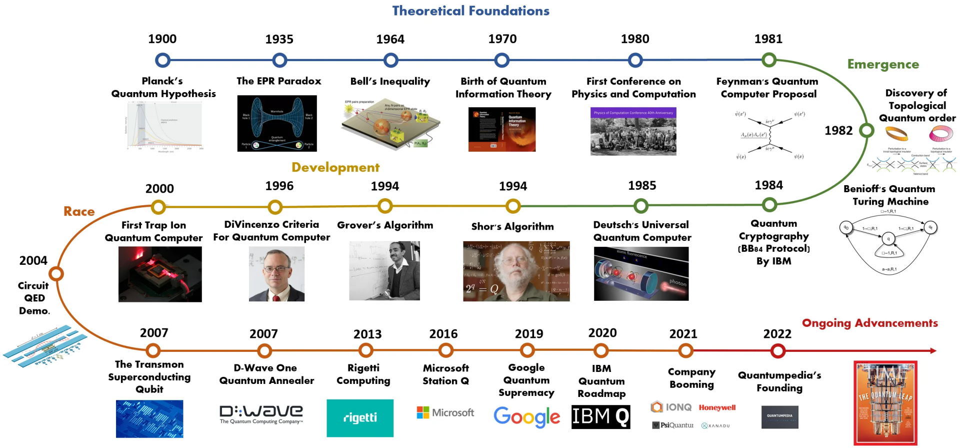


Figure: The timeline for quantum computers

Basics of Quantum Physics

HSBC

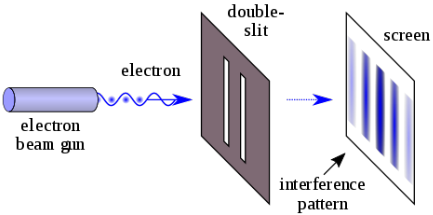
The quantum world

Imagine a world where

- things are largely empty space (much more than 99.9999999999996% empty)
- things are waves and waves are things
- things can be in an infinite amount of places at the same time
- it is not possible to observe anything without changing what we observe forever and everywhere
  - so and event on one planet can influence reality in another galaxy, and
  - this influencing happens faster than the speed of light
- it is possible to get through walls even without sufficient energy to do so
- where no properties like color, softness, compassion, intelligence, cold, wet, etc. exists
- things have only mathematical properties
- vacuum is not empty

Could this world underlie our familiar and logical world?

Thomas Young’s double slit experiment (1801)



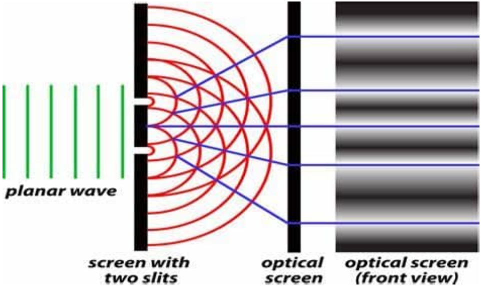


Figure: The double slit experiment. — (images licensed under Creative Commons CC0 1.0 Universal Public Domain Dedication and Creative Commons Attribution-Share Alike 3.0 Unported (author Fu-Kwun Hwang))

Schrödinger's Equation

Quantum entities are described by the Schödinger equation:

$$i\hbar\frac{\partial}{\partial t}\Psi(\mathbf{r},t) = \hat{H}\Psi(\mathbf{r},t)$$

The probabilities to find the entity are then given by

$$P(\mathbf{r},t) = |\Psi(\mathbf{r},t)|^2$$

Schrödinger's Equation

Quantum entities are described by the Schödinger equation:

$$i\hbar\frac{\partial}{\partial t}\Psi(\mathbf{r},t) = \hat{H}\Psi(\mathbf{r},t)$$

The probabilities to find the entity are then given by

$$P(\mathbf{r},t) = |\Psi(\mathbf{r},t)|^2$$

Superposition

The equation is linear, hence linear combinations of solutions are also solutions.

Schrödinger's Equation

Quantum entities are described by the Schödinger equation:

$$i\hbar\frac{\partial}{\partial t}\Psi(\mathbf{r},t) = \hat{H}\Psi(\mathbf{r},t)$$

The probabilities to find the entity are then given by

$$P(\mathbf{r},t) = |\Psi(\mathbf{r},t)|^2$$

Superposition

The equation is linear, hence linear combinations of solutions are also solutions.

Example: Qubit

If an object can have a quantum state "up" or "down" with equal probabilities, then it is described by $\Psi = \frac{1}{\sqrt{2}}|up\rangle + \frac{1}{\sqrt{2}}|down\rangle$. When measured one state is observed.

Schrödinger’s Cat thought experiment

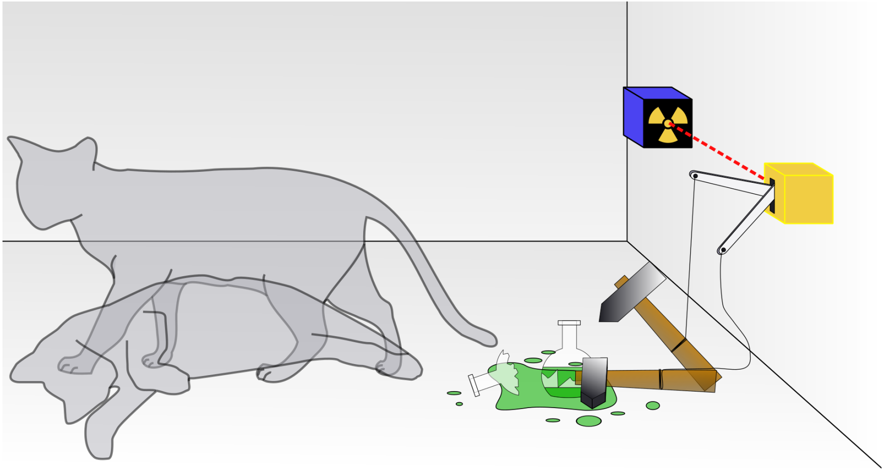


Figure: Poison is released when the radioactive atom decayes. As long as the box is not opened the radioactive atom is in superposition $\Psi_{atom} = \alpha_1 \, |decayed\rangle + \alpha_2 \, |not\ decayed\rangle$, and hence the cat must be $\Psi_{cat} = \alpha_1 \, |dead\rangle + \alpha_2 \, |alive\rangle$.

Entanglement

A system of two qubits can be characterized by

$$\alpha_1 \left|00\right\rangle + \alpha_2 \left|01\right\rangle + \alpha_3 \left|10\right\rangle + \alpha_4 \left|11\right\rangle$$

where

- $\left|01\right\rangle$ means: the first qubit is $\left|0\right\rangle$ and the second $\left|1\right\rangle$
- $\sum_{i=1}^{4} |\alpha_i|^2 = 1$, with $\forall i : \alpha_i \in \mathbb{C}$

Figure: AI's interpretation of wedding rings in entanglement. Microsoft's copilot

Entanglement

If two or more of α_i are non-zero, qubits are entangled if knowing one determines the state of the other.

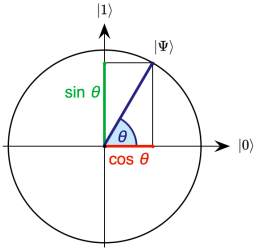
Example

$\frac{\sqrt{2}}{2} \left|11\right\rangle + \frac{\sqrt{2}}{2} \left|10\right\rangle$ is not entangled

$\frac{\sqrt{2}}{2} \left|01\right\rangle + \frac{\sqrt{2}}{2} \left|10\right\rangle$ is entangled

Figure: AI's interpretation of entanglement. Microsoft's copilot

Amplitudes and Probabilities

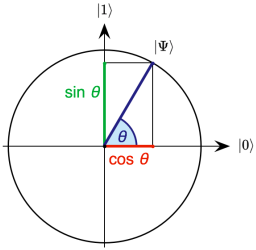


For a single qubit: unit sphere in $\mathbb{C}^2$ with the quantum state $\alpha_1|0\rangle + \alpha_2|1\rangle$ such that $|\alpha_1|^2 + |\alpha_2|^2 = 1$.

Notes

- The state can be re-written as $|\cos\theta|^2 + |\sin\theta|^2 = 1$, or $|\alpha_1|^2 = \cos^2\theta$ and $|\alpha_2|^2 = \sin^2\theta$.
- $|\alpha_1|^2$ is the probability of measuring $|0\rangle$ and $|\alpha_2|^2$ is the probability of measuring $|1\rangle$.

Amplitudes and Probabilities



For a single qubit: unit sphere in $\mathbb{C}^2$ with the quantum state $\alpha_1|0\rangle + \alpha_2|1\rangle$ such that $|\alpha_1|^2 + |\alpha_2|^2 = 1$.

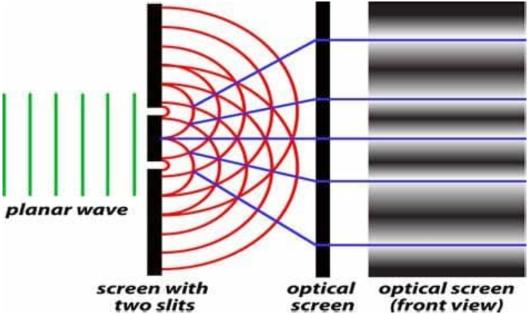
Notes

- The state can be re-written as $|\cos\theta|^2 + |\sin\theta|^2 = 1$, or $|\alpha_1|^2 = \cos^2\theta$ and $|\alpha_2|^2 = \sin^2\theta$.
- $|\alpha_1|^2$ is the probability of measuring $|0\rangle$ and $|\alpha_2|^2$ is the probability of measuring $|1\rangle$.

Amplitudes are Complex

Probabilities are real numbers and add up to 1, amplitudes are complex and the sum of absolute values adds up to 1. This allows for wave-like behaviour: interference.

Quantum Interference



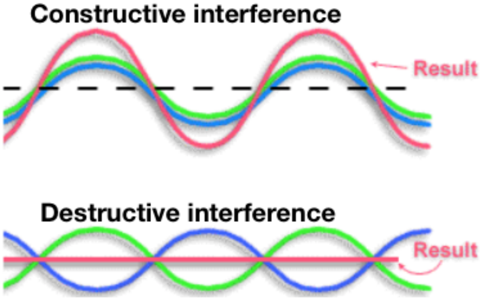


Figure: Quantum particles can influence others or themselves (via superposition) and disappear in certain places.

Well . . .

Is the universe local and real?

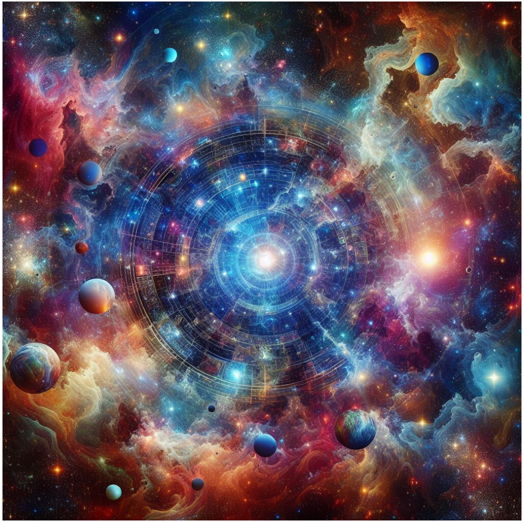


Figure: AI's interpretation of a universe that is not local nor real. Microsoft's copilot

Quantum Bits (Qubits)

HSBC

The QuBit

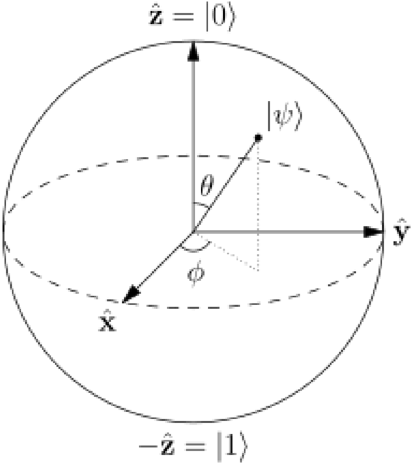


Figure: The qubit can be visualized on the Bloch-Sphere.
Image licensed under Creative Commons

The QuBit

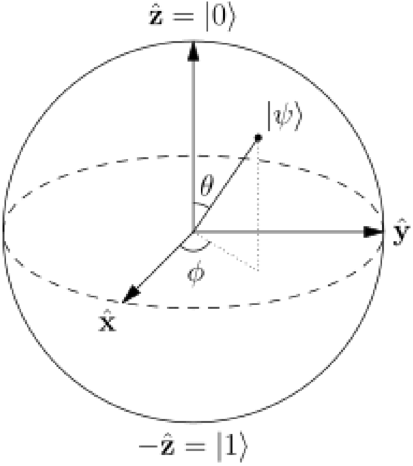


Figure: The qubit can be visualized on the Bloch-Sphere. Image licensed under Creative Commons

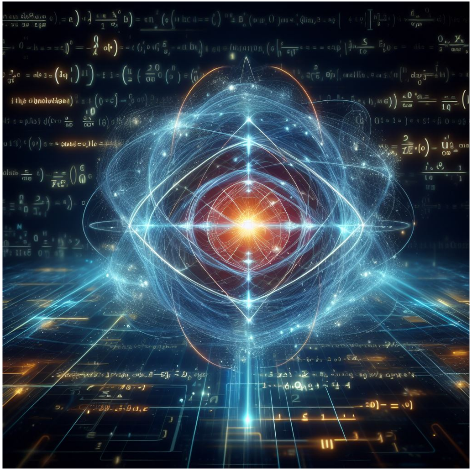


Figure: AI's interpretation of a qubit. Microsoft's copilot

Quantum Gates and Circuits

Classical Computers

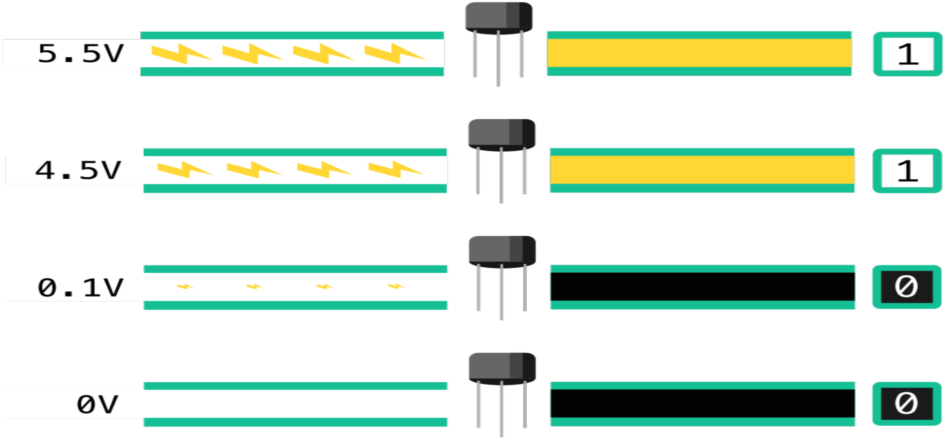


Figure: We use transistors to create logical states of 1 and 0.

Logical Gates

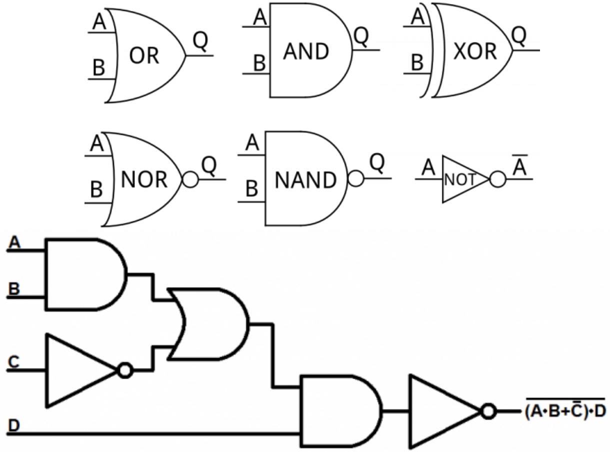


Figure: Those transistors are used to create logical gates that are in turn building blocks for logical circuits.

Quantum Gates

quantum gate

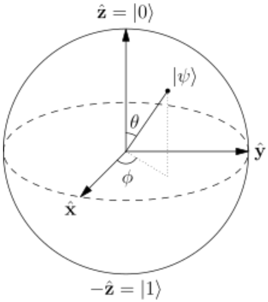
a quantum logic gate (or quantum gate) is a basic quantum circuit operating on a small number of qubits.

Examples of Quantum Gates

Operator	Gate(s)	Matrix
Pauli-X (X)	$\boxed{X}$	$\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$
Pauli-Y (Y)	$\boxed{Y}$	$\begin{bmatrix}0 & -i\\i & 0\end{bmatrix}$
Pauli-Z (Z)	$\boxed{Z}$	$\begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}$
Hadamard (H)	$\boxed{H}$	$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}$
Phase (S, P)	$\boxed{S}$	$\begin{bmatrix}1 & 0\\0 & i\end{bmatrix}$
$\pi/8$ (T)	$\boxed{T}$	$\begin{bmatrix}1 & 0\\0 & e^{i\pi/4}\end{bmatrix}$
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)	$\boxed{Z}$	$\begin{bmatrix}1 & 0 & 0 & 0\\0 & 1 & 0 & 0\\0 & 0 & 1 & 0\\0 & 0 & 0 & -1\end{bmatrix}$
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)		$\begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0\end{bmatrix}$

Figure: Examples of popular quantum gates. There are in fact an uncountable infinity of quantum gates.

Examples of quantum gates on one qubit



The vector representation of $|a\rangle = \alpha_1|1\rangle + \alpha_2|0\rangle$ is $\begin{bmatrix} \alpha_1 \\ \alpha_2 \end{bmatrix}$

Examples acting on one qubit:

1. Identity gate: $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
2. Pauli X-gate (rotation around X axis):
   $X = \sigma_x = \text{NOT} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
3. Pauli Y-gate: $Y = \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
4. Pauli Z-gate: $Z = \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

Example of quantum gates: creating superposition

Hadamard Gate acts on a single qubit. It maps the basis states$|0\rangle \mapsto \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|1\rangle \mapsto \frac{|0\rangle-|1\rangle}{\sqrt{2}}$ (an equal superposition state if given a computational basis state).
The two states $(|0\rangle + |1\rangle)/\sqrt{2}$ and $(|0\rangle - |1\rangle)/\sqrt{2}$ are sometimes written $|+\rangle$ and $|-\rangle$ respectively. The Hadamard gate performs a rotation of π about the axis $(\hat{x} + \hat{z})/\sqrt{2}$ at the Bloch sphere, and is therefore involutory.

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

Example of a quantum gate on 2 qubits and entanglement

Controlled gates act on 2 or more qubits, where one or more qubits act as a control for some operation.

controlled NOT gate (or CNOT or CX)

acts on 2 qubits, and performs the NOT operation on the second qubit only when the first qubit is $|1\rangle$ (otherwise leaves it unchanged). With respect to the basis $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ it is represented by the Hermitian unitary matrix:

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Measuring Qubits

Measurement = reduce the quantum states to a classical state.
Therefore, measurement is irreversible and not a quantum gate.

The probability of finding a state is the modulus of its amplitude[1]

$$\textit{if } \Psi = \alpha|x\rangle + \ldots, \textit{ then } P[|x\rangle] = |\alpha|^2$$

For example, measuring a qubit with the quantum state $\frac{|0\rangle - i|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -i \end{bmatrix}$ will yield with equal probability either $|0\rangle$ or $|1\rangle$

[1] This is known as the Born rule and appears as a stochastic non-reversible operation as it sets with a given probability the quantum state equal to the basis vector that represents the measured state.

Building your first quantum circuit

See the presentation of IBM later today ;-)

What is a quantum computer?

Figure: Photosynthesis is possible thanks to quantum mechanics. – own photo 2014

An example of a simulation: the Fermiac

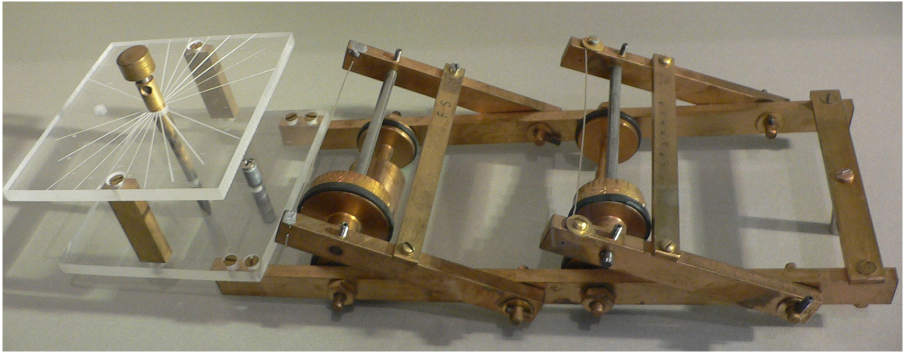


Figure: The FERMIAC, or Monte Carlo trolley, was an analog device invented by Enrico Fermi to implement studies of neutron transport. — image under Creative Commons Attribution-Share Alike 1.0

Aspects of Quantum Computing: Exponential Power

- qubit $\rightarrow$ 2 quantum states dimensions: $\alpha |0\rangle + \beta |1\rangle$

Aspects of Quantum Computing: Exponential Power

- qubit $\rightarrow$ 2 quantum states dimensions: $\alpha \left|0\right\rangle + \beta \left|1\right\rangle$
- 2 qubits $\rightarrow$ 4 states: $\alpha_1 \left|00\right\rangle + \alpha_2 \left|01\right\rangle + \alpha_3 \left|10\right\rangle + \alpha_4 \left|11\right\rangle$

Aspects of Quantum Computing: Exponential Power

- qubit $\rightarrow$ 2 quantum states dimensions: $\alpha\,|0\rangle + \beta\,|1\rangle$
- 2 qubits $\rightarrow$ 4 states: $\alpha_1\,|00\rangle + \alpha_2\,|01\rangle + \alpha_3\,|10\rangle + \alpha_4\,|11\rangle$
- 3 qubits $\rightarrow$ 8 quantum state dimensions

Aspects of Quantum Computing: Exponential Power

- qubit $\rightarrow$ 2 quantum states dimensions: $\alpha\,|0\rangle + \beta\,|1\rangle$
- 2 qubits $\rightarrow$ 4 states: $\alpha_1\,|00\rangle + \alpha_2\,|01\rangle + \alpha_3\,|10\rangle + \alpha_4\,|11\rangle$
- 3 qubits $\rightarrow$ 8 quantum state dimensions
- 6 qubits $\rightarrow$ 64 quantum state dimensions (card deck)

Aspects of Quantum Computing: Exponential Power

- qubit $\rightarrow$ 2 quantum states dimensions: $\alpha \left|0\right\rangle + \beta \left|1\right\rangle$
- 2 qubits $\rightarrow$ 4 states: $\alpha_1 \left|00\right\rangle + \alpha_2 \left|01\right\rangle + \alpha_3 \left|10\right\rangle + \alpha_4 \left|11\right\rangle$
- 3 qubits $\rightarrow$ 8 quantum state dimensions
- 6 qubits $\rightarrow$ 64 quantum state dimensions (card deck)
- 10 qubits $\rightarrow$ 1024 quantum state dimensions (810 listed companies on WSE)

Aspects of Quantum Computing: Exponential Power

- qubit $\rightarrow$ 2 quantum states dimensions: $\alpha \left|0\right\rangle + \beta \left|1\right\rangle$
- 2 qubits $\rightarrow$ 4 states: $\alpha_1 \left|00\right\rangle + \alpha_2 \left|01\right\rangle + \alpha_3 \left|10\right\rangle + \alpha_4 \left|11\right\rangle$
- 3 qubits $\rightarrow$ 8 quantum state dimensions
- 6 qubits $\rightarrow$ 64 quantum state dimensions (card deck)
- 10 qubits $\rightarrow$ 1024 quantum state dimensions (810 listed companies on WSE)
- 20 qubits $\rightarrow$ 1.048576×10^6 quantum state dimensions (ca. number of all possible liquid investments)

Aspects of Quantum Computing: Exponential Power

- qubit $\rightarrow$ 2 quantum states dimensions: $\alpha\left|0\right\rangle + \beta\left|1\right\rangle$
- 2 qubits $\rightarrow$ 4 states: $\alpha_1\left|00\right\rangle + \alpha_2\left|01\right\rangle + \alpha_3\left|10\right\rangle + \alpha_4\left|11\right\rangle$
- 3 qubits $\rightarrow$ 8 quantum state dimensions
- 6 qubits $\rightarrow$ 64 quantum state dimensions (card deck)
- 10 qubits $\rightarrow$ 1024 quantum state dimensions (810 listed companies on WSE)
- 20 qubits $\rightarrow$ 1.048576×10^6 quantum state dimensions (ca. number of all possible liquid investments)
- 60 qubits $\rightarrow$ 1.1529215×10^{18} states (ca. 10^{19} grains of sand on earth)

Aspects of Quantum Computing: Exponential Power

- qubit $\rightarrow$ 2 quantum states dimensions: $\alpha \left|0\right\rangle + \beta \left|1\right\rangle$
- 2 qubits $\rightarrow$ 4 states: $\alpha_1 \left|00\right\rangle + \alpha_2 \left|01\right\rangle + \alpha_3 \left|10\right\rangle + \alpha_4 \left|11\right\rangle$
- 3 qubits $\rightarrow$ 8 quantum state dimensions
- 6 qubits $\rightarrow$ 64 quantum state dimensions (card deck)
- 10 qubits $\rightarrow$ 1024 quantum state dimensions (810 listed companies on WSE)
- 20 qubits $\rightarrow$ 1.048576×10^6 quantum state dimensions (ca. number of all possible liquid investments)
- 60 qubits $\rightarrow$ 1.1529215×10^{18} states (ca. 10^{19} grains of sand on earth)
- 175 qubits $\rightarrow$ 4.7890486×10^{52} states (ca. 10^{50} atoms on earth)

Aspects of Quantum Computing: Exponential Power

- qubit $\rightarrow$ 2 quantum states dimensions: $\alpha\,|0\rangle + \beta\,|1\rangle$
- 2 qubits $\rightarrow$ 4 states: $\alpha_1\,|00\rangle + \alpha_2\,|01\rangle + \alpha_3\,|10\rangle + \alpha_4\,|11\rangle$
- 3 qubits $\rightarrow$ 8 quantum state dimensions
- 6 qubits $\rightarrow$ 64 quantum state dimensions (card deck)
- 10 qubits $\rightarrow$ 1024 quantum state dimensions (810 listed companies on WSE)
- 20 qubits $\rightarrow$ 1.048576×10^6 quantum state dimensions (ca. number of all possible liquid investments)
- 60 qubits $\rightarrow$ 1.1529215×10^{18} states (ca. 10^{19} grains of sand on earth)
- 175 qubits $\rightarrow$ 4.7890486×10^{52} states (ca. 10^{50} atoms on earth)
- 275 qubits $\rightarrow$ 6.0708403×10^{82} quantum states (ca. 10^{82} atoms in the visible universe)

Note: entanglement

To simulate quantum states on a Turing machine, we need to encode all possible entangled states too. The number of states in a quantum processor is 2^N, the complexity with entanglement scales as follows:

1. 10 qubits $\rightarrow$ 1,024 quantum states $\xrightarrow{\text{entanglement}}$ 16,000 Bits = 16 KB
2. 500 qubits $\rightarrow$ more quantum states than atoms in the visible universe $\xrightarrow{\text{entanglement}}$ not enough atoms in the visible universe

Quantum Algorithms

HSBC

Factoring

PGP relies on factoring large numbers

1 7 0 1 4 1 1 8 3 4 6 0
4 6 9 2 3 1 7 3 1 6 8 7
3 0 3 7 1 5 8 8 4 1 0 5
7 2 7

X

2 0 9 8 8 9 3 6 6 5 7 4
4 0 5 8 6 4 8 6 1 5 1 2
6 4 2 5 6 6 1 0 2 2 2 5
9 3 8 6 3 9 2 1

=

3 5 7 1 0 8 2 5 2 2 4 7 3 7 6 6 7 4
4 8 4 3 0 4 9 7 5 7 7 8 5 2 7 4 0 1 8
9 5 2 0 0 1 1 5 7 2 6 1 2 0 7 9 5 8 4
2 5 7 6 3 5 5 5 0 9 7 4 6 4 0 2 6 1 4
7 7 5 5 6 7

Factoring

PGP relies on factoring large numbers

1 7 0 1 4 1 1 8 3 4 6 0
4 6 9 2 3 1 7 3 1 6 8 7
3 0 3 7 1 5 8 8 4 1 0 5
7 2 7

X

2 0 9 8 8 9 3 6 6 5 7 4
4 0 5 8 6 4 8 6 1 5 1 2
6 4 2 5 6 6 1 0 2 2 2 5
9 3 8 6 3 9 2 1

=

3 5 7 1 0 8 2 5 2 2 4 7 3 7 6 6 6 7 4
4 8 4 3 0 4 9 7 5 7 7 8 5 2 7 4 0 1 8
9 5 2 0 0 1 1 5 7 2 6 1 2 0 7 9 5 8 4
2 5 7 6 3 5 5 5 0 9 7 4 6 4 0 2 6 1 4
7 7 5 5 6 7

# digits	Supercomputer

Factoring

PGP relies on factoring large numbers

1 7 0 1 4 1 1 8 3 4 6 0 4 6 9 2 3 1 7 3 1 6 8 7 3 0 3 7 1 5 8 8 4 1 0 5 7 2 7 X 2 0 9 8 8 9 3 6 6 5 7 4 4 0 5 8 6 4 8 6 1 5 1 2 6 4 2 5 6 6 1 0 2 2 2 5 9 3 8 6 3 9 2 1 = 3 5 7 1 0 8 2 5 2 2 4 7 3 7 6 6 7 4 4 8 4 3 0 4 9 7 5 7 7 8 5 2 7 4 0 1 8 9 5 2 0 0 1 1 5 7 2 6 1 2 0 7 9 5 8 4 2 5 7 6 3 5 5 5 0 9 7 4 6 4 0 2 6 1 4 7 7 5 5 6 7

# **digits**	**Supercomputer**
10,000	0 s
100,000	0.6 year
200,000	78,254 yrs
300,000	449 mln. yrs
400,000	72 x age of universe

Factoring

PGP relies on factoring large numbers

1 7 0 1 4 1 1 8 3 4 6 0 4 6 9 2 3 1 7 3 1 6 8 7 3 0 3 7 1 5 8 8 4 1 0 5 7 2 7	X	2 0 9 8 8 9 3 6 6 5 7 4 4 0 5 8 6 4 8 6 1 5 1 2 6 4 2 5 6 6 1 0 2 2 2 5 9 3 8 6 3 9 2 1	=	3 5 7 1 0 8 2 5 2 2 4 7 3 7 6 6 7 4 4 8 4 3 0 4 9 7 5 7 7 8 5 2 7 4 0 1 8 9 5 2 0 0 1 1 5 7 2 6 1 2 0 7 9 5 8 4 2 5 7 6 3 5 5 5 0 9 7 4 6 4 0 2 6 1 4 7 7 5 5 6 7

# **digits**	**Supercomputer**	**Quantum comp.**
10,000	0 s	56 s
100,000	0.6 year	2 min.
200,000	78,254 yrs	2 min.
300,000	449 mln. yrs	2 min.
400,000	72 x age of universe	3 min.

Factoring

Shor's Algorythm in quantum computers does not scale exponentially

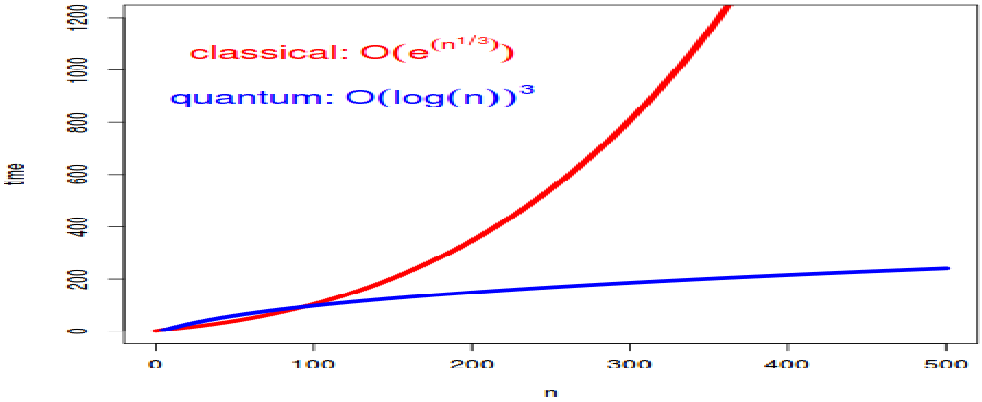


Figure: Time needed to factor large numbers in classical approach and with quantum computers

Programming a Universal Quantum Computer

Lov Grover's Algorithm

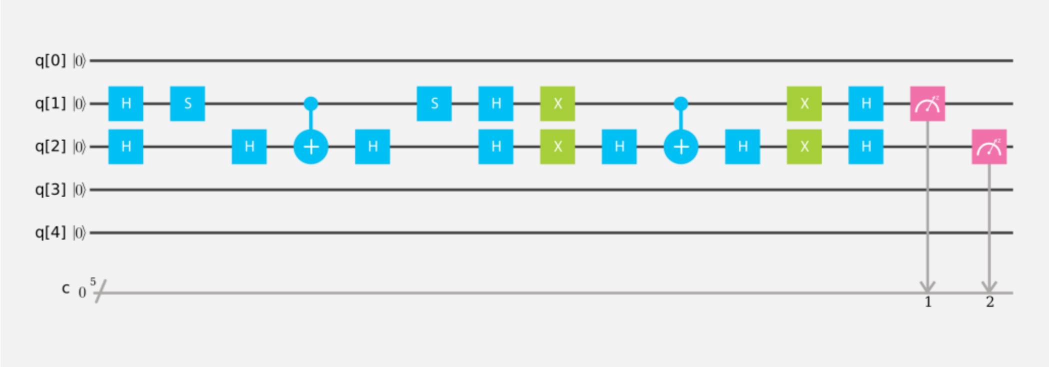


Figure: Grover's algorithm only needs $O(\sqrt{N})$ steps to find matching entry in unstructured data.

Breaking Codes and Passwords

Shor's Alogorithm to factor numbers

$$
\begin{tikzcd}
 & integer\ factorization \arrow[dr] & \\
public - key\ algorithms \arrow[ur] \arrow[r] \arrow[dr] & discrete\ logarithm \arrow[r] & Shor's\ algo \\
 & elliptic - curve\ discrete\ logarithm \arrow[ur] & \\
symmetric\ key\ algorithms \arrow[dr] & & \\
 & brute\ force\ attack \arrow[r, dotted] & Grover's\ algo \\
hashfunctions \arrow[ur] & &
\end{tikzcd}
$$

Large Linear Systems

$$\begin{bmatrix} A_{11} & \dots & A_{1N} \\ \vdots & \ddots & \vdots \\ A_{M1} & \dots & A_{MN} \end{bmatrix} \times \begin{bmatrix} x_1 \\ \vdots \\ x_N \end{bmatrix} = \begin{bmatrix} b_1 \\ \vdots \\ b_N \end{bmatrix}$$

with up to s non-zero A_{ij} per row/column and condition number k

Classical methods solve this in $O(Nsk)$ ... quantum algorithms need $O(log(N)sk)$

How to build a quantum computer

HSBC

Models of Quantum Computing

Gate Model

also Circuit Model. Uses entangled qubits and gates to execute operations

Measurement Based

set up entangled state over all qubits and then measure one by one

Adiabatic

start from flat energy surface and build up slowly, expect the system to stay in the lowest energy state

Annealing

not mathemati-cally equivalent

Physical Realisations of Qubits

Superconducting

typically a tiny line or loop of metal that behaves as one atom

Trapped Ions

ions trapped (with electromagnetic fields) and manipulated using lasers or microwave radiation

Photon Polarization

The polarization of light is the qubit

Spin Qubits

The quantum mechanical spin state of an electron or proton can be used as qubits

Topological

using Majorano Zero-Mode Quasi-particles (sort of non-Abelian anyon)

Energy Levels of Hydrogen Atom

The electron in a hydrogen atom can be in its ground state or in an excited state.

Quantum Supremacy

Definition (quantum supremacy)

Quantum supremacy is the potential ability of quantum computing devices to solve problems that classical computers practically cannot.

Expectation: 50 sufficiently coherent q-bits needed for quantum supremacy.

Definition (quantum advantage)

Quantum advantage is the potential to solve problems faster. In computational complexity-theoretic terms, this generally means providing a superpolynomial speedup over the best known or possible classical algorithm.

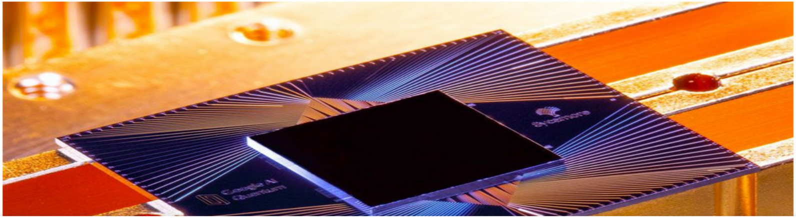
Current State: Quantum Supremacy overconfident claims

NEWS · 23 OCTOBER 2019

Hello quantum world! Google publishes landmark quantum supremacy claim

The company says that its quantum computer is the first to perform a calculation that would be practically impossible for a classical machine.

Elizabeth Gibney



PDF version

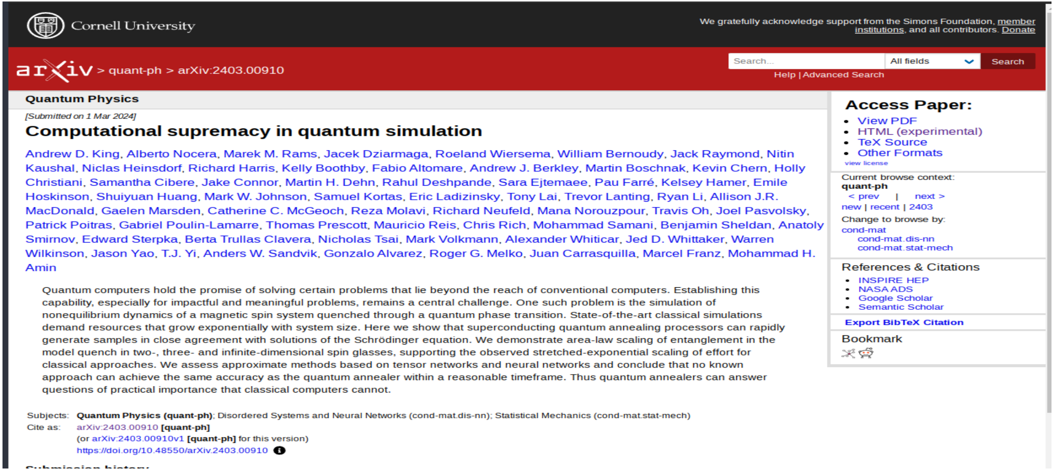
RELATED ARTICLES

Beyond quantum supremacy

Quantum gold rush: the private funding pouring into quantum start-ups

Figure: Submitted, October 1st, 2024 – https://arxiv.org/abs/2403.00910

Current State: Quantum Supremacy with annealers



Cornell University

We gratefully acknowledge support from the Simons Foundation, member institutions, and all contributors. Donate

arXiv > quant-ph > arXiv:2403.00910

Search... All fields Search

Help | Advanced Search

Quantum Physics

[Submitted on 1 Mar 2024]

Computational supremacy in quantum simulation

Andrew D. King, Alberto Nocera, Marek M. Rams, Jacek Dziarmaga, Roeland Wiersema, William Bernoudy, Jack Raymond, Nitin Kaushal, Niclas Heinsdorf, Richard Harris, Kelly Boothby, Fabio Altomare, Andrew J. Berkley, Martin Boschnak, Kevin Chern, Holly Christiani, Samantha Cibere, Jake Connor, Martin H. Dehn, Rahul Deshpande, Sara Ejtemaee, Pau Farré, Kelsey Hamer, Emile Hoskinson, Shuiyuan Huang, Mark W. Johnson, Samuel Kortas, Eric Ladizinsky, Tony Lai, Trevor Lanting, Ryan Li, Allison J.R. MacDonald, Gaelen Marsden, Catherine C. McGeoch, Reza Molavi, Richard Neufeld, Mana Norouzpour, Travis Oh, Joel Pasvolsky, Patrick Poitras, Gabriel Poulin-Lamarre, Thomas Prescott, Mauricio Reis, Chris Rich, Mohammad Samani, Benjamin Sheldan, Anatoly Smirnov, Edward Sterpka, Berta Trullas Clavera, Nicholas Tsai, Mark Volkmann, Alexander Whiticar, Jed D. Whittaker, Warren Wilkinson, Jason Yao, T.J. Yi, Anders W. Sandvik, Gonzalo Alvarez, Roger G. Melko, Juan Carrasquilla, Marcel Franz, Mohammad H. Amin

Quantum computers hold the promise of solving certain problems that lie beyond the reach of conventional computers. Establishing this capability, especially for impactful and meaningful problems, remains a central challenge. One such problem is the simulation of nonequilibrium dynamics of a magnetic spin system quenched through a quantum phase transition. State-of-the-art classical simulations demand resources that grow exponentially with system size. Here we show that superconducting quantum annealing processors can rapidly generate samples in close agreement with solutions of the Schrödinger equation. We demonstrate area-law scaling of entanglement in the model quench in two-, three- and infinite-dimensional spin glasses, supporting the observed stretched-exponential scaling of effort for classical approaches. We assess approximate methods based on tensor networks and neural networks and conclude that no known approach can achieve the same accuracy as the quantum annealer within a reasonable timeframe. Thus quantum annealers can answer questions of practical importance that classical computers cannot.

Subjects: **Quantum Physics (quant-ph)**; Disordered Systems and Neural Networks (cond-mat.dis-nn); Statistical Mechanics (cond-mat.stat-mech)
Cite as: arXiv:2403.00910 **[quant-ph]**
(or arXiv:2403.00910v1 **[quant-ph]** for this version)
https://doi.org/10.48550/arXiv.2403.00910

Access Paper:

- View PDF
- HTML (experimental)
- TeX Source
- Other Formats

view license

Current browse context:
quant-ph
< prev | next >
new | recent | 2403
Change to browse by:
cond-mat
cond-mat.dis-nn
cond-mat.stat-mech

References & Citations

- INSPIRE HEP
- NASA ADS
- Google Scholar
- Semantic Scholar

Export BibTeX Citation

Bookmark

Figure: Submitted, March 1st, 2024 – https://arxiv.org/abs/2403.00910

D-Wave

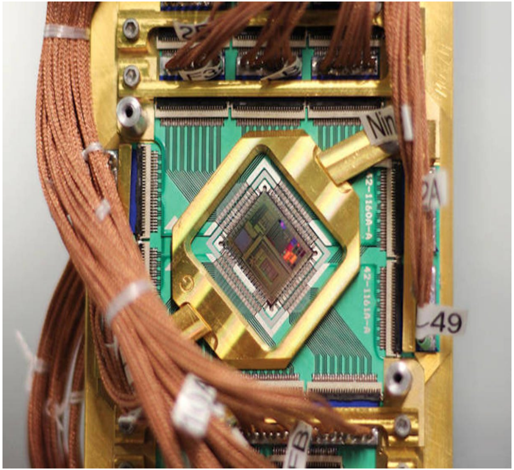
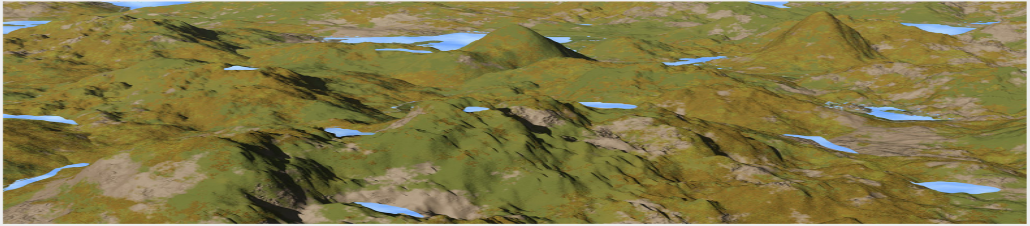


Figure: The quantum computer of D-Wave (pictures: D-Wave) – since 2007

Adiabatic Algorithm

How D-Wave Systems Work

In nature, physical systems tend to evolve toward their lowest energy state: objects slide down hills, hot things cool down, and so on. This behavior also applies to quantum systems. To imagine this, think of a traveler looking for the best solution by finding the lowest valley in the energy landscape that represents the problem.

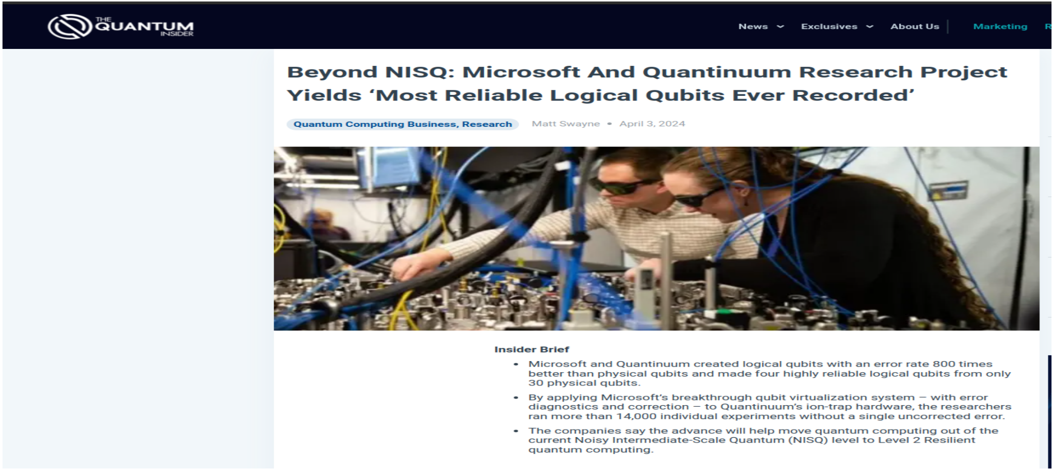


Classical algorithms seek the lowest valley by placing the traveler at some point in the landscape and allowing that traveler to move based on local variations. While it is generally most efficient to move downhill and avoid climbing hills that are too high, such classical algorithms are prone to leading the traveler into nearby valleys that may not be the global minimum. Numerous trials are typically required, with many travelers beginning their journeys from different points.

In contrast, quantum annealing begins with the traveler simultaneously occupying many coordinates thanks to the quantum phenomenon of superposition. The probability of being at any given coordinate smoothly evolves as annealing progresses, with the probability increasing around the coordinates of deep valleys. Quantum tunneling allows the traveller to pass through hills—rather than be forced to climb them—reducing the chance of becoming trapped in valleys that are not the global minimum. Quantum entanglement further improves the outcome by allowing the traveler to discover correlations between the coordinates that lead to deep valleys.

Figure: https://www.dwavesys.com/quantum-computing

Logical Quibits: recent progress: 2024-03-04



THE QUANTUM INSIDER

News | Exclusives | About Us | Marketing

Beyond NISQ: Microsoft And Quantinuum Research Project Yields 'Most Reliable Logical Qubits Ever Recorded'

Quantum Computing Business, Research — Matt Swayne • April 3, 2024

Insider Brief

- Microsoft and Quantinuum created logical qubits with an error rate 800 times better than physical qubits and made four highly reliable logical qubits from only 30 physical qubits.
- By applying Microsoft's breakthrough qubit virtualization system – with error diagnostics and correction – to Quantinuum's ion-trap hardware, the researchers ran more than 14,000 individual experiments without a single uncorrected error.
- The companies say the advance will help move quantum computing out of the current Noisy Intermediate-Scale Quantum (NISQ) level to Level 2 Resilient quantum computing.

Figure: https://thequantuminsider.com 2024-04-03 – also on https://blogs.microsoft.com and https://www.quantinuum.com.

Challenges in Quantum Computing

HSBC

Decoherence

Coherence and Decoherence

Systems interacting with the environment in which they reside generally become entangled with that environment, a phenomenon known as quantum decoherence. This can explain why, in practice, quantum effects are difficult to observe in systems larger than microscopic.

Decoherence

Coherence and Decoherence

Systems interacting with the environment in which they reside generally become entangled with that environment, a phenomenon known as quantum decoherence. This can explain why, in practice, quantum effects are difficult to observe in systems larger than microscopic.

Note: temperature

$$v_{rms} = \sqrt{\frac{3kT}{m}}$$

with:

- v_{rms} the average speed of a molecule in a gas in $\frac{m}{s}$
- $k = 1.38x10^{-23} \frac{J}{K}$
- T the temperature in Kelvin
- m the molecular mass in Kg

Scalability

Each qubit needs a connection . . .

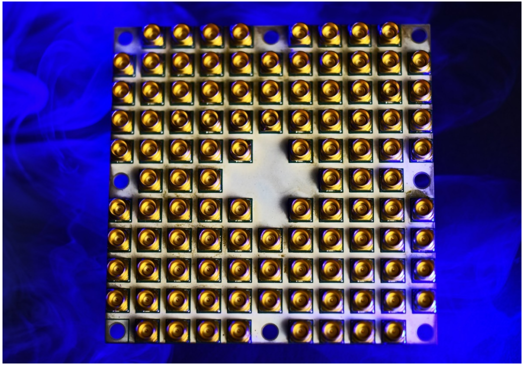


Figure: Intel Corporation's 49-qubit quantum computing test chip, "Tangle Lake," – 2018.
Credit: Intel Corporation

Future of Quantum Computing

HSBC

IBM’s Road-map

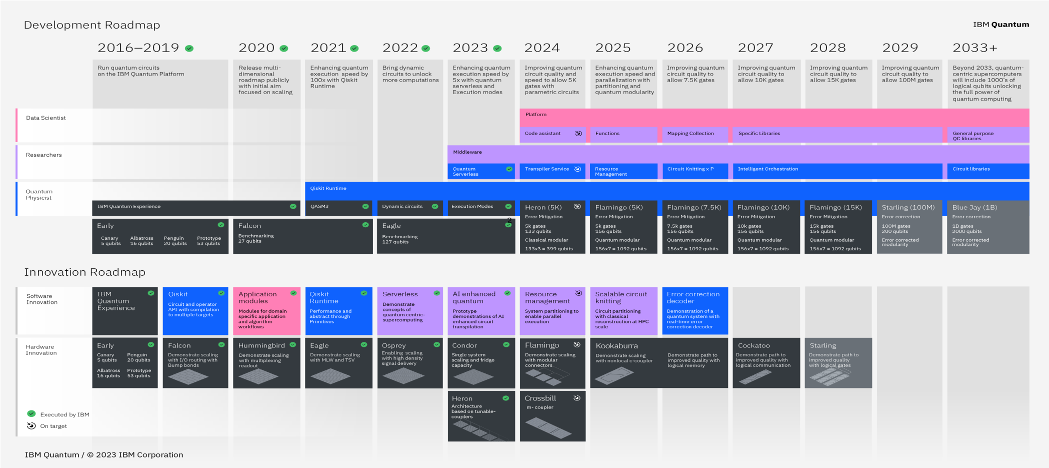


Figure: IBM’s Quantum Roadmap (newsroom.ibm.com)

Applications for quantum computers

- **Modeling of the quantum world**
- **Biochemical modeling**
- **Climate modeling**
- **Material Science** (eg. semiconductor, semiconductors)
- **Cryptography**
- **Optimizations**: financial markets, traffic optimization, resource planning, etc.

Applications for quantum computers

- **Modeling of the quantum world**
- **Biochemical modeling**
- **Climate modeling**
- **Material Science** (eg. semiconductor, semiconductors)
- **Cryptography**
- **Optimizations**: financial markets, traffic optimization, resource planning, etc.

Figure: McKinsey Quantum Technology Monitor (April 2023) predicts USD 1.3 trillion in value by 2035 – source: https://www.mckinsey.com

Use cases in banking

- **Optimization**:
  1. portfolio optimization
  2. collateral optimization
  3. stress testing
  4. transaction settlement
  5. asset pricing
  6. ATM replenishment
- Machine Learning
  - fraud detection
  - credit scoring
  - synthetic data and data augmentation

Use cases in banking

- **Optimization**:
  1. portfolio optimization
  2. collateral optimization
  3. stress testing
  4. transaction settlement
  5. asset pricing
  6. ATM replenishment
- Machine Learning
  - fraud detection
  - credit scoring
  - synthetic data and data augmentation

- **Simulations**:
  - random number generator
  - Monte Carlo, LPDE simulations, etc.
  - asset valuation
  - ES and VaR calculations
- **Encryption**:
  - quantum key encryption
  - quantum currency
  - quantum blockchain

Resulting Advantages

quadratic to exponential speedup

- better risk management

Boston Consulting Group estimates a value of $42B to $67B for financial institutions

Resulting Advantages

quadratic to exponential speedup

- better risk management
- lower costs

Boston Consulting Group estimates a value of $42B to $67B for financial institutions

Resulting Advantages

quadratic to exponential speedup

- better risk management
- lower costs
- greener computing

Boston Consulting Group estimates a value of $42B to $67B for financial institutions

Resulting Advantages

quadratic to exponential speedup

- better risk management
- lower costs
- greener computing
- better forecasting

Boston Consulting Group estimates a value of \$42B to \$67B for financial institutions

Resulting Advantages

quadratic to exponential speedup

- better risk management
- lower costs
- greener computing
- better forecasting
- more suitable investment

Boston Consulting Group estimates a value of $42B to $67B for financial institutions

Resulting Advantages

quadratic to exponential speedup

- better risk management
- lower costs
- greener computing
- better forecasting
- more suitable investment
- etc.

Boston Consulting Group estimates a value of $42B to $67B for financial institutions

Why is HSBC interested

- Quantum computing could revolutionise financial services in areas like portfolio optimisation, fraud detection and cybersecurity.
- Quantum computers promise to deliver a step-change in computational power, with the potential to tackle highly complex tasks far beyond the capabilities of today's machines
- The quantum sector is estimated USD1.3 trillion in value by 2035

source: HSBC and quantum

HSBC’s strategy

1. Working with a range of **organisations like IBM, Fujitsu and Quantinuum, leading academic institutions, and governmental organisations**, to put us at the forefront of the financial services industry in exploring how to integrate quantum computing into our products and services
2. Building a **dedicated quantum research team** and in-house team of PhD scientists at HSBC to formalise our use cases into deep research projects and develop patents and quantum products
3. **Bank-wide strategy**: Collaborating across business lines and functions to develop real world use cases to improve our processes and prepare for a quantum-secure economy

source: HSBC and quantum

Proofs of Concept in HSBC

Pricing Optimisation

HSBC facilitates US$760B of trade annually. We aim to develop a POC which can provide real-time, flexible pricing options.

Collateral Optimisation

Develop a hybrid quantum-classical POC to optimise allocation of collateral in the most cost effective way.

QRNG for Monte Carlo

Use quantum random number generation (QRNG) to improve Monte Carlo Simulations in stochastic modelling.

Quantum Machine Learning

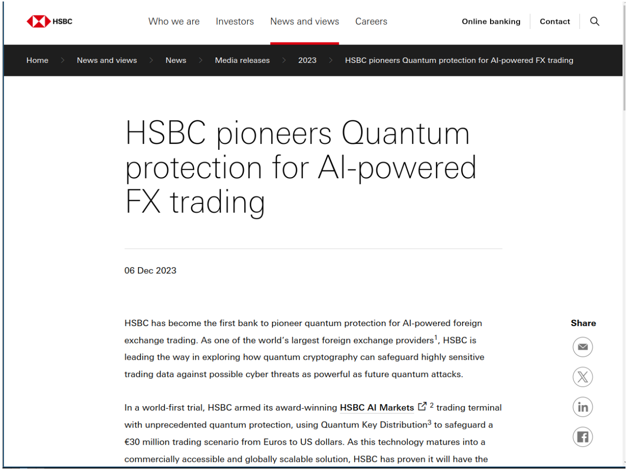
Use Quantum Machine Learning algorithms to improve fraud detection rate.

Quantum Key Distribution

A method of key exchange which is secure against quantum attack. Aim to set up QKD based protocols between two locations.

Figure: Proofs of concept in HSBC. source: HSBC and quantum

Quantum Key Distribution in HSBC


HSBC

Who we are | Investors | News and views | Careers | Online banking | Contact

Home > News and views > News > Media releases > 2023 > HSBC pioneers Quantum protection for AI-powered FX trading

HSBC pioneers Quantum protection for AI-powered FX trading

06 Dec 2023

HSBC has become the first bank to pioneer quantum protection for AI-powered foreign exchange trading. As one of the world's largest foreign exchange providers[1], HSBC is leading the way in exploring how quantum cryptography can safeguard highly sensitive trading data against possible cyber threats as powerful as future quantum attacks.

In a world-first trial, HSBC armed its award-winning **HSBC AI Markets** [2] trading terminal with unprecedented quantum protection, using Quantum Key Distribution[3] to safeguard a €30 million trading scenario from Euros to US dollars. As this technology matures into a commercially accessible and globally scalable solution, HSBC has proven it will have the

Share

Figure: Proofs of concept in HSBC: quantum key distribution. source: HSBC and quantum

HSBC's Philip Intallura

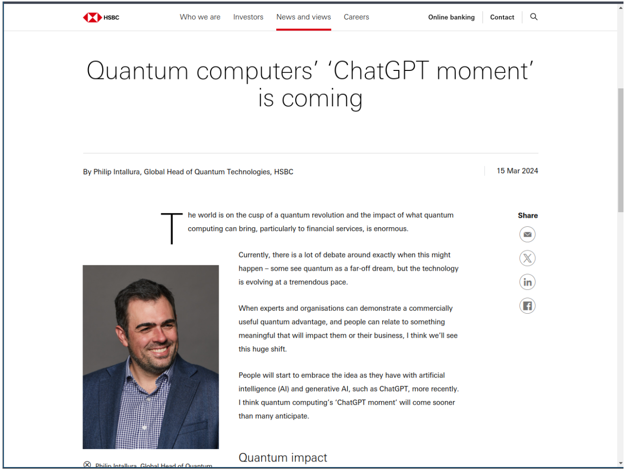


Figure: Proofs of concept in HSBC: quantum key distribution. source: HSBC news

Limits of Quantum Computers

Limits of Quantum Computers: Complexity Theory

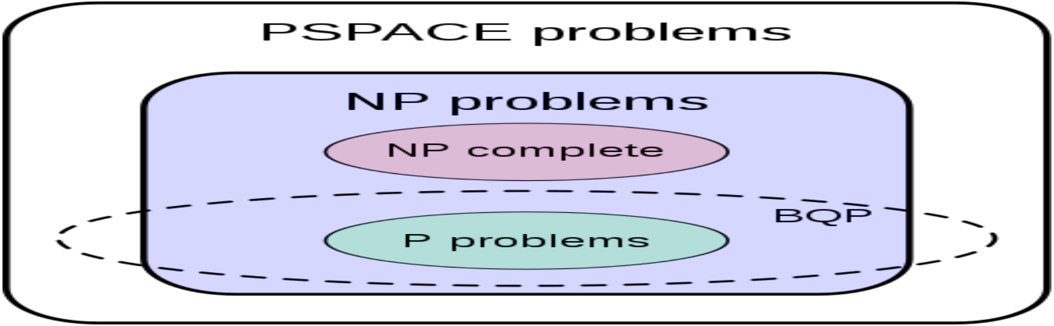


Figure: BQP –bounded-error quantum polynomial time– is the quantum equivalent of BPP –bounded-error probabilistic polynomial time

Turing Machines are Turing Complete

Turing Complete

A system is Turing complete if it can simulate any Turing machine, meaning it can compute any Turing-computable function. Essentially, it can perform any calculation that a computer with unlimited resources could. Most modern programming languages are Turing complete.
In practical terms, a Turing Complete system means a system in which a program can be written that will find an answer, although with no guarantees regarding runtime or memory use.

Quantum Computers are impractical for many applications

While a (theoretical) Quantum Turing Machine is Turing Complete, there are much practical barriers.

Conclusions

Conclusions: Q-Day is near

I predict that in 1 to 10 years quantum computers will bring us

- insight in quantum physics

Conclusions: Q-Day is near

I predict that in 1 to 10 years quantum computers will bring us

- insight in quantum physics
- new medications, better batteries, better materials, etc.

Conclusions: Q-Day is near

I predict that in 1 to 10 years quantum computers will bring us

- insight in quantum physics
- new medications, better batteries, better materials, etc.
- other encryption

Conclusions: Q-Day is near

I predict that in 1 to 10 years quantum computers will bring us

- insight in quantum physics
- new medications, better batteries, better materials, etc.
- other encryption
- the ability to to gather more data and use it

Conclusions: Q-Day is near

I predict that in 1 to 10 years quantum computers will bring us

- insight in quantum physics
- new medications, better batteries, better materials, etc.
- other encryption
- the ability to to gather more data and use it
- all kinds of optimizations, such as better optimized investment portfolios

Conclusions: Q-Day is near

I predict that in 1 to 10 years quantum computers will bring us

- insight in quantum physics
- new medications, better batteries, better materials, etc.
- other encryption
- the ability to to gather more data and use it
- all kinds of optimizations, such as better optimized investment portfolios
- Artificial General Intelligence

Conclusions: Q-Day is near

I predict that in 1 to 10 years quantum computers will bring us

- insight in quantum physics
- new medications, better batteries, better materials, etc.
- other encryption
- the ability to to gather more data and use it
- all kinds of optimizations, such as better optimized investment portfolios
- Artificial General Intelligence
- greener computing (e.g. bitcoin alone is responsible for 1.5% of the world's CO_2 production)

Conclusions: Q-Day is near

I predict that in 1 to 10 years quantum computers will bring us

- insight in quantum physics
- new medications, better batteries, better materials, etc.
- other encryption
- the ability to to gather more data and use it
- all kinds of optimizations, such as better optimized investment portfolios
- Artificial General Intelligence
- greener computing (e.g. bitcoin alone is responsible for 1.5% of the world's CO_2 production)
- but most exciting: . . . answers to questions that we don't know yet.

Further Reading

- Michio Kaku, Quantum Supremacy: How the Quantum Computer Revolution Will Change Everything – order on Amazon.com
- McKinsey, McKinsey Quantum Technology Monitor, April 2023 – download
- McKinsey, 2020, “How quantum computing could change financial services” – download
- IBM, “The Quantum Decade” (e-book) – download
- E. Rieffel and W Polak, MIT Press, “Quantum Computing, a Gentle Introduction” – download
- Quantum Computing for the Quantum Curious, C. Hughes et al., Springer – download
- a list of books: download

Thank you for your attention!

handouts of this presentation

Philippe’s business card