Quantum Technology, Present Status and Future Possibilities

Lodewijk Arntzen

29 juni 2023


let's change
YOU. US. THE WORLD.

Overview

- Review on Quantum
- Quantum Secure Communication
- Hardware and Software
- Applications

Review on Quantum

- 1925 Quantum: First Understanding Stability of Atoms
- 1935 Einstein, Podolsky, Rosen
- 1935 Verschränkung (Entanglement)
- 1935 Von Neumann: Mathematische Grundlagen der Quantenmechanik
- 1936 The Logic of Quantum Mechanics, Birkhoff, Von Neumann
- 1964 John Bell: Inequalities, Local Realism
- 1982 Feynman: Simulating Physics with Computers
- 2017 Landsman: (New) Mathematical Foundation of Quantum Mechanics
- 2022 Nobel Prize, Aspect, Clauser and Zeilinger

Highlights

- 1947 Creating the Basic Building Blocks of Modern Classical Computers
- 1982 Feynman: Simulating Physics with a Computer
- 2019 Google Claims Quantum Supremacy using Sycamore (53 qubits)
- 2021 IBM claims a Functional 127 quantum bit processor 'IBM Eagle'
- 2023 Quantum Volume of 128 reached

Review on Quantum

- Basics of Quantum Mechanics
- Superposition
- Entanglement
- Collapse of the Wave Function

Review on Quantum

In general, in quantum mechanics, we may have a coherent superposition

$$|\psi\rangle = c_0\,|0\rangle + c_1\,|1\rangle\,. \tag{1}$$

for the complex numbers c_0 and c_1 we require

$$|c_0|^2 + |c_1|^2 = 1. \tag{2}$$

Review on Quantum

A system of two (or more) qubits can be found in an entangled state. This means that the state of one qubit depends on another qubit

$$|\psi(1,2)\rangle = \frac{1}{\sqrt{2}}\left(|0_1, 1_2\rangle + |1_1, 0_2\rangle\right) \tag{3}$$

and this state cannot be written in a separable way

$$|\psi(1,2)\rangle \neq |\psi(1)\rangle\, |\psi(2)\rangle\,. \tag{4}$$

Review on Quantum

The quantum state of two qubits can now be written as

$$\frac{1}{2}\left(c_0\left|0,0\right\rangle + c_1\left|0,1\right\rangle + c_2\left|1,0\right\rangle + c_3\left|1,1\right\rangle\right) \tag{5}$$

which implies that this is a superposition of $2^2 = 4$ states. So a two-qubit quantum computer can already store four complex numbers.

Review on Quantum

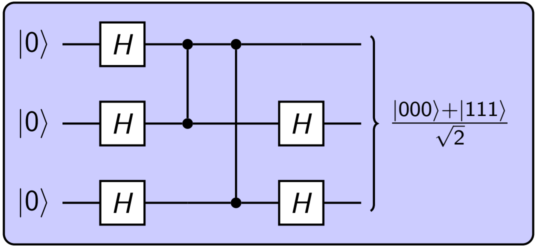
The state of 4 qubits can now be written as

$$\frac{1}{4}\left(c_0 \left|0{,}0{,}0{,}0\right\rangle + c_1 \left|0{,}0{,}0{,}1\right\rangle + c_2 \left|0{,}0{,}1{,}0\right\rangle + c_3 \left|0{,}0{,}1{,}1\right\rangle \ldots c_{15} \left|1{,}1{,}1{,}1\right\rangle\right) \quad (6)$$

which implies that this is a superposition of $2^4 = 16$ states simultaneously.

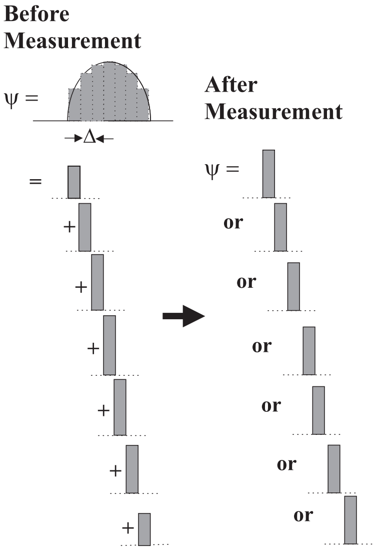
- a four-qubit quantum computer can already store 16 complex numbers.
- Generalizing we conclude that a N-qubit quantum computer can store 2^N numbers.
- How many numbers can a 256 qubit computer store?

Review on Quantum

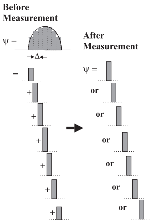


THE HAGUE UNIVERSITY OF APPLIED SCIENCES

Review on Quantum



Review on Quantum

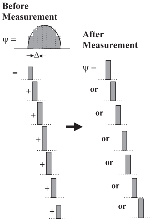


$$\psi = \sum_{n=1}^{n=7} a_n \phi_n \tag{7}$$

The chance of measuring a_n is

$$P(a_n) = |a_n^2| \tag{8}$$

Review on Quantum

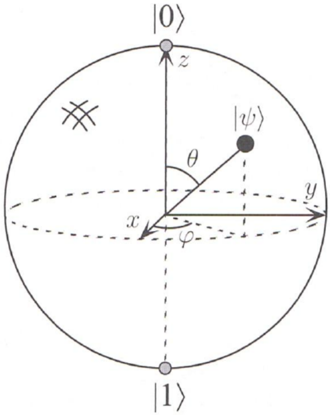


Chance on measuring a_n is

$$P(a_n) = |a_n^2| \tag{9}$$

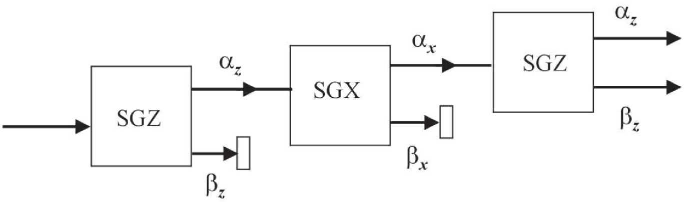
directly after the measurement, the wavefunction is $\psi = \phi_n$ and the system follows the time evolution according to the time-dependent Schrödinger equation again.

Review on Quantum



$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{10}$$

Review on Quantum



Qubit 1: Spin Qubit Spin $\frac{1}{2}$ particle has eigenvalue $\pm\frac{1}{2}\hbar$ with eigenstates α_z en β_z

$$\alpha_x = \frac{1}{\sqrt{2}}(\alpha_z + \beta_z) \tag{11}$$

$$\beta_x = \frac{1}{\sqrt{2}}(\alpha_z - \beta_z) \tag{12}$$

Review on Quantum

Qubit 2: A polarized photon:

- horizontal/vertical α_z en β_z
- ± 45 degrees: α_x en β_x

We write

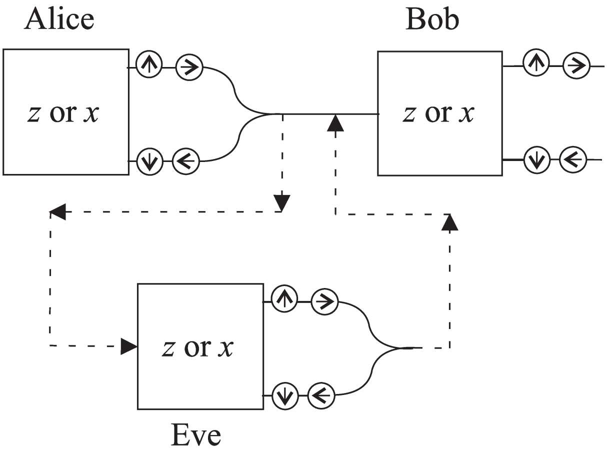
$$\alpha_x = \frac{1}{\sqrt{2}}(\alpha_z + \beta_z) \tag{13}$$

$$\beta_x = \frac{1}{\sqrt{2}}(\alpha_z - \beta_z) \tag{14}$$

Quantum Secure Communication

- Public Key Distribution, RSA (Classical)
- Bennet-Brassard 84 (BB-84)
- Bennet-92 Protocol

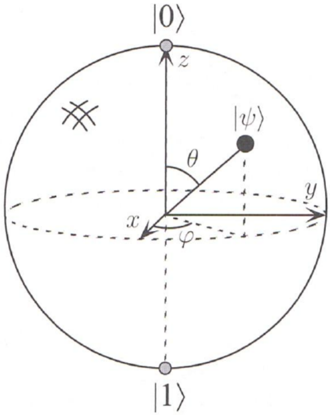
Quantum Secure Communication



Quantum Secure Communication

Alice			Bob Eve inactief				Eve		Bob Eve actief	
O	S	M	O	R	a/r	K	O	R/S	R	K′
		0					x	α	β	
		1					x	β	α	
		0					z	β	β	
z	β	1	x				x	α	α	
x	α	0	x				x	α	α	
x	β	1	z				x	β	β	
z	β	1	x				z	β	β	
x	β	1					z	β	β	
x	α	0					x	α	α	
x	α	0					z	α	α	
z	α	0					x	α	β	
z	β	1					z	β	β	

Hardware and Software



$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{15}$$

Hardware and Software

The DiVincenzo Criteria for Qubits.
Qbits should

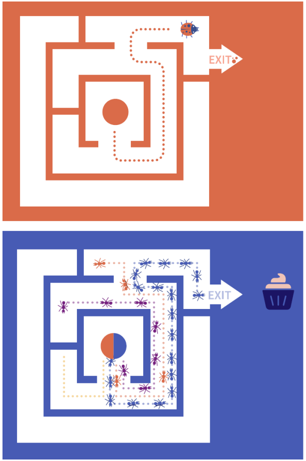
- be well-defined and scalable
- have sufficiently long coherence time
- be reliably initializable
- be connected to a universal gate set
- be measurable at the end of the program (it should be possible to distinguish between 0 and 1)

Hardware and Software

Many different Qubit approaches possible, specialized and suitable depending on the application

- Superconducting Qubits
- Spin Qubits
- Topological Qubits
- Atoms in Optical Tweezer
- Trapped Ions
- Photons (suitable for exchanging quantum information)

Hardware and Software



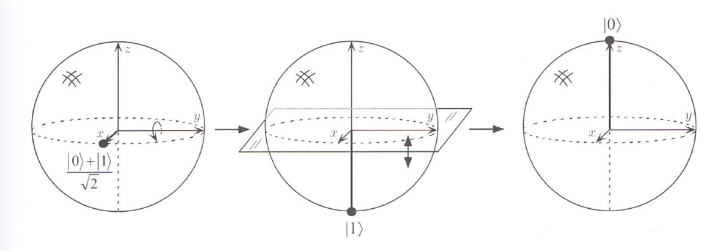
- From: Quantum Computing: From Hardware to Society, TU Delft [1].

Hardware and Software

- From: Quantum Computing: From Hardware to Society, TU Delft

Hardware and Software

Hadamard gate



Hardware and Software

Example 1: Shell game: Quantum Searching Tool

Hardware and Software

Imagine a shell game using four cups and one pea.

- Question: Is it possible to find the pea in one try, with certainty every time?

Hardware and Software

Imagine a shell game using four cups and one pea. We represent our database as follows

$$|S\rangle = \frac{1}{2}\left[|0_1,0_2\rangle + |0_1,1_2\rangle + |1_1,0_2\rangle + |1_1,1_2\rangle\right]. \tag{16}$$

Each term represents a shell, and all amplitudes are equal to $\frac{1}{2}$. Suppose someone (without us knowing) changes the state into

$$|F\rangle = \frac{1}{2}\left[|0_1,0_2\rangle + |0_1,1_2\rangle - |1_1,0_2\rangle + |1_1,1_2\rangle\right]. \tag{17}$$

- Is it possible to find the position of the sign-change with just one measurement? The answer is Yes - this is possible.
- Inversion about the mean value of the amplitude (which due the flip has become $\frac{1}{4}$) brings the amplitude of all the states to zero, except for the flipped state: This amplitude becomes one.

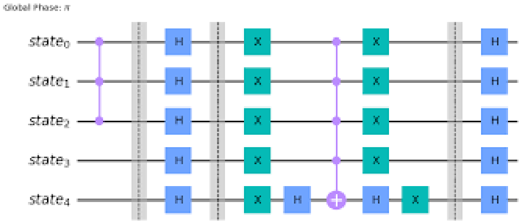
IARIA

THE HAGUE UNIVERSITY OF APPLIED SCIENCES

Hardware and Software

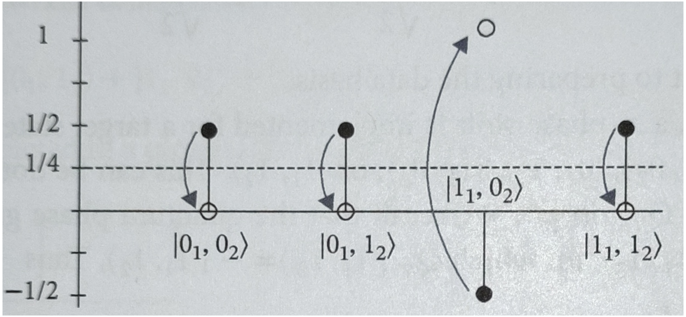
Example 1: Grover's algorithm: Powerful Searching Tool The following sequence of operations does exactly this

$$N = H_1 H_2 Q_\pi H_1 H_2 X_1 X_2. \tag{18}$$

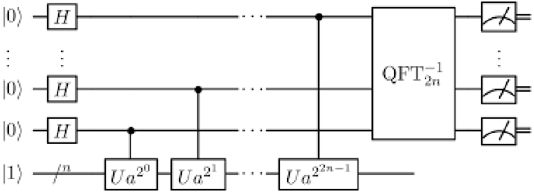


Hardware and Software

Example 1: Grover's algorithm: Powerful Searching Tool (Image from M. Suhail Zubairy, Quantum Mechanics for Beginners [2]))



Example 2: Shor's algorithm: Factorization and Encryption



THE HAGUE UNIVERSITY OF APPLIED SCIENCES

Future of Quantum

- Simulations (Analog, Hybrid)
- Optimization
- Searching
- Factorization
- Encrypting
- Forecasting
- AI

Future of Quantum

- Prototype Logical Qubit
- Real Logical Qubit
- Specialised Computers
- Improving Fault Tolerance
- Combining Qubits
- Distributed Computing
- Quantum Internet

References

1. Vermaas, Pieter, Wimmer, Michael, Lomas, Derek, Almudever, Carmen G., Scappucci, Giordano (2022) Quantum Computing: From Hardware to Society. TU Delft. https://doi.org/10.4233/uuid:144218f9-7b7a-4208-8242-dc19fb14164b.
2. M. Suhail Zubairy, Quantum Mechanics for Beginners, Oxford University Press, ISBN 978-0-19-885422-7.
3. M.A. Nielsen, I.L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, ISBN 978-1-107-00217-3
4. K. Landsman, Foundations of Quantum Theory, From Classical Concepts to Operater Algebras, Springer Open, ISBN978-3-319-51777-3