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

$$|\psi\rangle = c_0 |0\rangle + c_1 |1\rangle.$$ \hspace{1cm} (1)

for the complex numbers $c_0$ and $c_1$ we require

$$|c_0|^2 + |c_1|^2 = 1.$$ \hspace{1cm} (2)
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

\[ |\psi(1,2)\rangle = \frac{1}{\sqrt{2}} (|0_1,1_2\rangle + |1_1,0_2\rangle) \]  

(3)

and this state cannot be written in a separable way

\[ |\psi(1,2)\rangle \neq |\psi(1)\rangle \langle \psi(2)| \]  

(4)
The quantum state of two qubits can now be written as

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

which implies that this is a superposition of $2^2 = 4$ states. So a two-qubit quantum computer can already store four complex numbers.
The state of 4 qubits can now be written as

\[ \frac{1}{4} (c_0 |0,0,0,0\rangle + c_1 |0,0,0,1\rangle + c_2 |0,0,1,0\rangle + c_3 |0,0,1,1\rangle + \ldots c_{15} |1,1,1,1\rangle) \]  

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

\[ |0\rangle H |000\rangle + \frac{1}{\sqrt{2}} |0\rangle H |111\rangle \]
Review on Quantum

Before Measurement

\[ \psi = \]

After Measurement

\[ \psi = \]

or

or

or

or

or

or

or
The chance of measuring $a_n$ is

$$P(a_n) = |a_n^2|$$
Review on Quantum

Chance on measuring $a_n$ is

$$P(a_n) = |a_n^2|$$

(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.
|ψ⟩ = α |0⟩ + β |1⟩
Qubit 1: Spin Qubit Spin $\frac{1}{2}$ particle has eigenvalue $\pm \frac{1}{2} \hbar$ with eigenstates $\alpha_z$ and $\beta_z$

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

$$\beta_x = \frac{1}{\sqrt{2}} (\alpha_z - \beta_z)$$  \hspace{1cm} (12)
Review on Quantum

Qubit 2: A polarized photon:

- horizontal/vertical $\alpha_z$ en $\beta_z$
- $\pm45$ degrees: $\alpha_x$ en $\beta_x$

We write

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

$$\beta_x = \frac{1}{\sqrt{2}} (\alpha_z - \beta_z)$$ \hspace{1cm} (14)$$
Quantum Secure Communication

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

Alice

Bob

Eve

$z$ or $x$

$z$ or $x$

$z$ or $x$
# Quantum Secure Communication

<table>
<thead>
<tr>
<th>Alice</th>
<th>Bob Eve inactief</th>
<th>Eve</th>
<th>Bob Eve actief</th>
</tr>
</thead>
<tbody>
<tr>
<td>O</td>
<td>O</td>
<td>O/R</td>
<td>R/K</td>
</tr>
<tr>
<td>S</td>
<td>R</td>
<td>a/r</td>
<td>K</td>
</tr>
<tr>
<td>M</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>1</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>0</td>
<td>z</td>
<td>z</td>
<td>z</td>
</tr>
<tr>
<td>z</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>β</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>1</td>
<td>z</td>
<td>z</td>
<td>z</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>β</td>
<td>z</td>
<td>z</td>
<td>z</td>
</tr>
<tr>
<td>1</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>z</td>
<td>z</td>
<td>z</td>
</tr>
<tr>
<td>α</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>0</td>
<td>z</td>
<td>z</td>
<td>z</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>α</td>
<td>z</td>
<td>z</td>
<td>z</td>
</tr>
<tr>
<td>0</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>z</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>α</td>
<td>z</td>
<td>z</td>
<td>z</td>
</tr>
<tr>
<td>0</td>
<td>z</td>
<td>z</td>
<td>z</td>
</tr>
<tr>
<td>z</td>
<td>β</td>
<td>β</td>
<td>β</td>
</tr>
<tr>
<td>β</td>
<td>β</td>
<td>β</td>
<td>β</td>
</tr>
</tbody>
</table>
Hardware and Software

\[ |\psi\rangle = \alpha |0\rangle + \beta |1\rangle \]
Hardware and Software

The DiVincenzo Criteria for Qubits.
Qubits 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

\[ |0\rangle + i|1\rangle \quad \sqrt{2} \]
Hardware and Software

Example 1: Shell game: Quantum Searching Tool
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

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

(16)

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

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

(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.
Example 1: Grover’s algorithm: Powerful Searching Tool

The following sequence of operations does exactly this

\[ N = H_1 H_2 Q_\pi H_1 H_2 X_1 X_2. \]  

(18)
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
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


