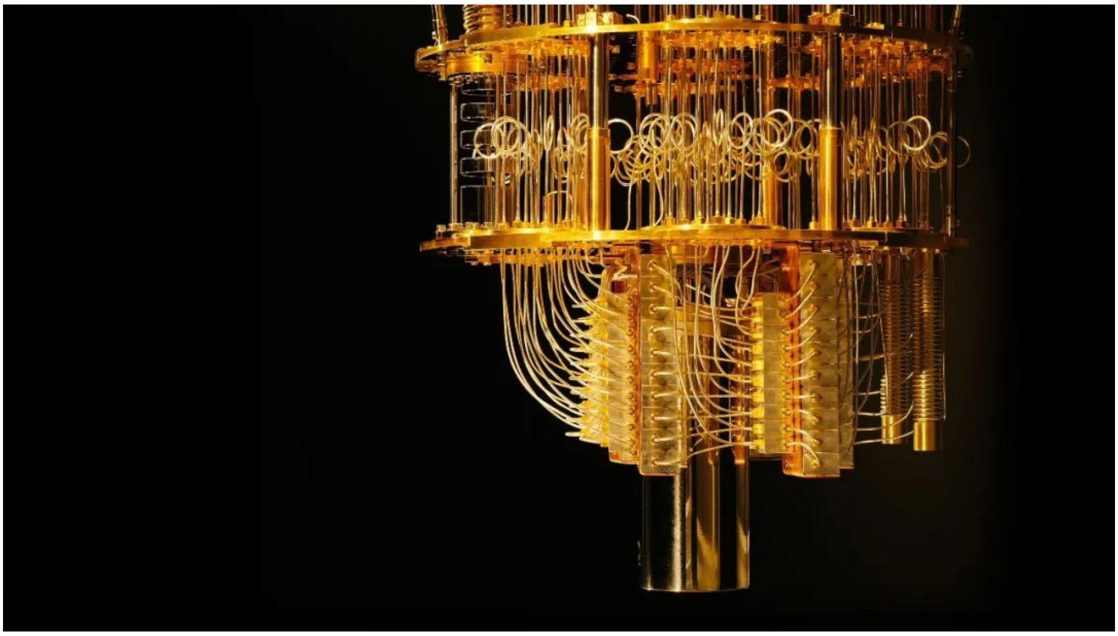
Lecture Notes for Quantum Computing

Chao Liang

cliang@whu.edu.cn

National Engineering Research Centre for Multimedia Software (NERCMS)

School of Computer Science, Wuhan University



Spring, 2024

(Last updated on February 28, 2024)

Contents

1 Introduction and Complex Number

1.1 Introduction to Quantum Computing

1.1.1 A brief history

Quantum Mechanics as a branch of physics began with a set of scientific discoveries in the late 19th Century and has been in active development ever since. Most people will point to the 1980s as the start of physicists actively looking at computing with quantum systems[1]:

- **1982:** History of quantum computing starts with Richard Feynman lectures on the potential advantages of computing with quantum systems.
- **1985:** David Deutsch publishes the idea of a "universal quantum computer".
- **1994:** Peter Shor presents an algorithm that can efficiently find the factors of large numbers, significantly outperforming the best classical algorithm and theoretically putting the underpinning of modern encryption at risk (referred to now as Shors algorithm).
- **1996:** Lov Grover presents an algorithm for quantum computers that would be more efficient for searching databases (referred to now as Groves search algorithm).
- **1996:** Seth Lloyd proposes a quantum algorithm which can simulate quantum-mechanical systems.
- **1999:** D-Wave Systems founded by Geordie Rose.
- **2000:** Eddie Farhi at MIT develops idea for adiabatic quantum computing.
- **2001:** IBM and Stanford University publish the first implementation of Shors algorithm, factoring 15 into its prime factors on a 7-qubit processor.
- **2010:** D-Wave One: first commercial quantum computer released (annealer).
- **2016:** IBM makes quantum computing available on IBM Cloud.
- **2019:** Google claims the achievement of quantum supremacy. Quantum Supremacy was termed by John Preskill in 2012 to describe when quantum systems could perform tasks surpassing those in the classical world.

A more complete history comes from the quantumpedia[2], where the development of quantum computing is divided into five distinct periods (Figure 1.1):

[1] https://thequantuminsider.com/2020/05/26/history-of-quantum-computing/

[2] https://quantumpedia.uk/a-brief-history-of-quantum-computing-e0bbd05893d0

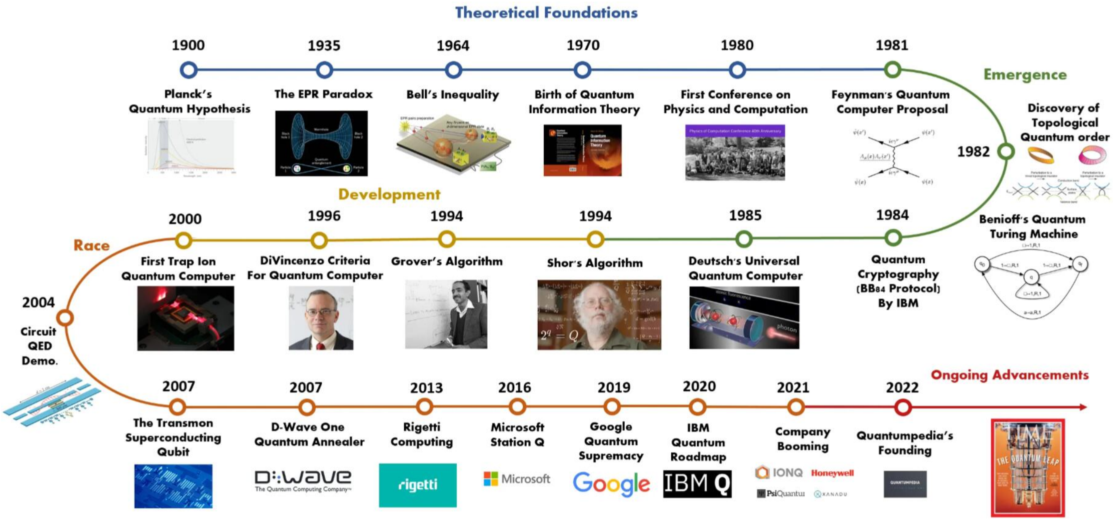

Theoretical Foundations
1900
Planck's Quantum Hypothesis
1935
The EPR Paradox
1964
Bell's Inequality
1970
Birth of Quantum Information Theory
1980
First Conference on Physics and Computation
1981
Feynman's Quantum Computer Proposal
Emergence
1982
Discovery of Topological Quantum order
1984
Benioff's Quantum Turing Machine
1984
Quantum Cryptography (BB84 Protocol) By IBM
1985
Deutsch's Universal Quantum Computer
1994
Shor's Algorithm
Development
1994
Grover's Algorithm
1996
DiVincenzo Criteria For Quantum Computer
2000
First Trap Ion Quantum Computer
Race
2004
Circuit QED Demo.
2007
The Transmon Superconducting Qubit
2007
D-Wave One Quantum Annealer
2013
Rigetti Computing
2016
Microsoft Station Q
2019
Google Quantum Supremacy
2020
IBM Quantum Roadmap
2021
Company Booming
2022
Quantumpedia's Founding
Ongoing Advancements

Figure 1.1: A Brief History of Quantum Computing (Copyright: Quantumpedia)

- **1900–1980:** The Theoretical Foundations of Quantum Computing.
- **1980–1994:** The Emergence of Quantum Computing.
- **1994–2000:** The Development of Quantum Algorithms.
- **2000–2021:** The Race to Build Quantum Computers.
- **2021–present:** Ongoing Advancements.

1.1.2 Prof. Andrew Chi-Chih Yao's Talk in Micius Salon

Prof. Yao gave a talk entitled "The Advent of Quantum Computing" in Micius Salon in 2018[3]. Here are some key points:

- Two key topics: (1) what is the nature of quantum computer?; and (2) where does quantum computer gets its power from?
- The particle-wave duality plays the starting role in making it possible for us to do quantum computing faster than classic computing under certain circumstances
- Richard Feynman's question: can quantum physics be simulated efficiently? Answer: unlikely by a classic computer, but hopefully by a quantum computer.
- The comparison of classic computer and quantum computers (Figure 1.2). Classic computers manipulate classic bits $0110\cdots$ with Boolean operations in $\{0,1\}^n$, while quantum computers manipulate quantum bits $|0101\cdots\rangle$ with "rotations" in $\mathbb{C}^{2^n}$

[3] https://www.bilibili.com/video/BV1Ct411Z7BQ/?spm_id_from=333.337.search-card.all.click&vd_source=322773747f9aa504da745054e83290e9

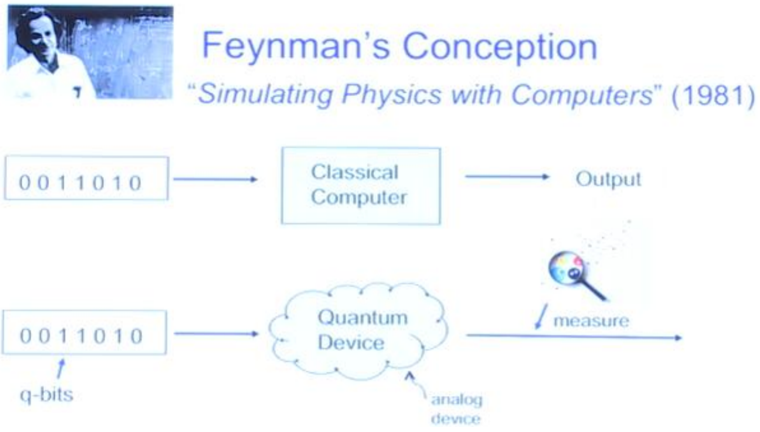


Figure 1.2: The comparison of classic and quantum computers.

- The parallel superposition is brought by the fact that each quantum bit represents not a single state, but a “probabilistic distribution” of state. Parallelism could speed up computational tasks.
- quantum parallelism is only a metaphor, subtle and restricted, not equivalent to a parallel computer with many processors.

1.2 Complex Numbers

The original motivation for the introduction of complex numbers was seeking solutions of polynomial equations. Here is the simplest example:

$$x^2 + 1 = 0 \tag{1.1}$$

Obviously, we cannot find its solution in the set of real numbers. To solve this problem, Mathematics introduces following definitions.

1.2.1 Definitions

Definition 1.1 (Imaginary Number). *An imaginary number is a real number multiplied by the imaginary unit i, which is defined by its property $i^2 = 1$ or $i = \sqrt{-1}$.*

Definition 1.2 (Complex Number). *A complex number is a hybrid entity which adds a real number with an imaginary number, for instance,*

$$c = a + b \times i = a + bi \tag{1.2}$$

where a, b are two real numbers, a is called the real part of c, whereas b is its imaginary part. The set of all complex numbers will be denoted as $\mathbb{C}$. When the × is understood, we shall omit it.

Proposition 1 (Fundamental Theorem of Algebra). *Every polynomial equation of one variable with complex coefficients has a complex solution.*

1.2.2 The Algebra of Complex Numbers

Definition 1.3 (Ordered Pair Representation). *Ordered pair representation defines a complex number as an ordered pair of reals:*

$$c = a + b \mapsto (a, b) \tag{1.3}$$

Hence, ordinary real numbers can be identified with pairs $(a, 0)$

$$a \mapsto (a, b) \tag{1.4}$$

whereas imaginary numbers can be identified with pairs $(0, b)$. In particular,

$$i \mapsto (0, 1) \tag{1.5}$$

The four **arithmetic operations** between two complex numbers can be expressed as:

- Addition:
$$c_1 + c_2 = (a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2) \tag{1.6}$$
- Subtraction:
$$c_1 - c_2 = (a_1, b_1) - (a_2, b_2) = (a_1 - a_2, b_1 - b_2) \tag{1.7}$$
- Multiplication:
$$c_1 \times c_2 = (a_1, b_1) \times (a_2, b_2) = (a_1a_2 - b_1b_2, a_1b_2 + a_2b_1) \tag{1.8}$$
- Subdivision:
$$\frac{c_1}{c_2} = \frac{(a_1, b_1)}{(a_2, b_2)} = \left(\frac{a_1a_2 + b_1b_2}{a_2^2 + b_2^2}, \frac{a_2b_1 - a_1b_2}{a_2^2 + b_2^2}\right) \tag{1.9}$$

With the addition and multiplication operations, we can re-write a complex number as

$$c = a + bi = (a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0) \times (0, 1) \tag{1.10}$$

and from the denominator in the quotient formula in Eq.(1.9), we can define the **modulus** of a complex number as:

$$|c| = |a + bi| = +\sqrt{a^2 + b^2} \tag{1.11}$$

which has two useful properties:

- Property 1: $\forall c_1, c_2 \in \mathbb{C}, |c_1||c_2| = |c_1c_2|$.
- Property 2: $\forall c_1, c_2 \in \mathbb{C}, |c_1 + c_2| \leq |c_1| + |c_2|$.

where the second property is also called triangular inequality of modulus operation.

Based on the above basic operations, it is easy to verify that complex numbers have the following **algebraic properties**:

- Addition has an identity called **additive identity**: $(0, 0)$, such that

$$\forall c \in \mathbb{C}, c + (0, 0) = c \tag{1.12}$$

- Multiplication has an identity called **multiplicative identity**: $(1, 0)$, such that

$$\forall c \in \mathbb{C}, c \times (1, 0) = (1, 0) \times c = c \tag{1.13}$$

- Both addition and multiplication are commutative:

$$\begin{cases} c_1 + c_2 = c_2 + c_1 \\ c_1 \times c_2 = c_2 \times c_1 \end{cases} \tag{1.14}$$

- Both addition and multiplication are associative:

$$\begin{cases} (c_1 + c_2) + c_3 = c_1 + (c_2 + c_3) \\ (c_1 \times c_2) \times c_3 = c_1 \times (c_2 \times c_3) \end{cases} \tag{1.15}$$

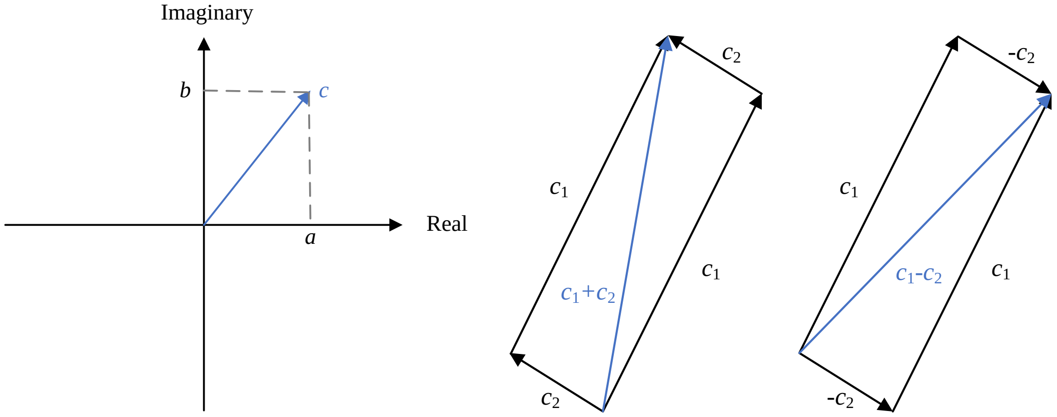
- Multiplication distributes with respect to addition:

$$c_1 \times (c_2 + c_3) = c_1 \times c_2 + c_1 \times c_3 \tag{1.16}$$

- Subtraction is defined everywhere.
- Division is defined everywhere except when the divisor is zero.

Besides basic arithmetic operations and modulus operation, complex numbers have a unique operation called **conjugation**. If $c = a + bi$ is an arbitrary complex number, then the conjugate of c is $\overline{c} = a - bi$. Two numbers related by conjugation are said to be **complex conjugates** of each other. The conjugation operation has several basic properties:

- Property 1: Conjugate respects addition $\overline{c_1 + c_2} = \overline{c_1} + \overline{c_2}$.
- Property 2: Conjugate respects multiplication $\overline{c_1 \times c_2} = \overline{c_1} \times \overline{c_2}$.
- Property 3: Conjugate $c \mapsto \overline{c}$ is bijective.
- Property 4: The modulus squared of a complex number is obtained by multiplying the number with its conjugate $c \times \overline{c} = |c|^2$.



(a) Complex plane

(b) Addition

(c) Subtraction

Figure 1.3: The complex plane (a) and parallelogram rule for (b) addition and (c) subtraction.

1.2.3 The Geometry of Complex Numbers

Definition 1.4 (**Complex Plane** or **Argand Plane**). *The complex plane is the plane formed by the complex numbers, with a Cartesian coordinate system such that the horizontal x-axis, called the real axis, is formed by the real numbers, and the vertical y-axis, called the imaginary axis, is formed by the imaginary numbers.*

In the complex plane (Figure 1.3a), we can easily find that the modulus is nothing more than the length of the vector. Indeed, the length of a vector, via Pythagoras theorem, is the square root of the sum of the squares of its edges, which is precisely the modulus, as defined in the previous section.

Next comes addition: vectors can be added using the so-called **parallelogram rule** illustrated by Figure 1.3b. In words, draw the parallelogram whose parallel edges are the two vectors to be added; their sum is the diagonal.

Subtraction too has a clear geometric meaning: subtracting c_2 from c_1 is the same as adding the negation of c_2, i.e., $-c_2$, to c_1 (Figure 1.3c).

To give a simple geometrical meaning to multiplication, we need to develop yet another characterization of complex numbers.

Definition 1.5 (**Polar Coordinate System**). *The polar coordinate system is a two-dimensional coordinate system in which each point on a plane is determined by a distance ρ from a reference point and an angle θ from a reference direction.*

Similar to the previous **Cartesian representation** (a, b), the **polar representation** (ρ, θ) is capable to uniquely determine a complex number because these two representations can be mutually converted:

$$(a, b) \mapsto (\rho, \theta) \tag{1.17}$$

where ρ is the modulus

$$\rho = \sqrt{a^2 + b^2} \tag{1.18}$$

and θ is also easy, via trigonometry

$$\theta = \tan^{-1}\left(\frac{b}{a}\right) \tag{1.19}$$

$$(\rho, \theta) \mapsto (a, b) \tag{1.20}$$

where a is the real part

$$a = \rho\cos(\theta) \tag{1.21}$$

and b is the imaginary part

$$b = \rho\sin(\theta) \tag{1.22}$$

In physics and engineering, angle θ is also known as **phase** and distance ρ is also known as **magnitude**. Hence, we have another definition of a complex number

Definition 1.6 (Complex Number)**.** *A complex number is a magnitude and a phase.*

We are now ready for multiplication: given two complex numbers in polar coordinates, $c_1 = (\rho_1, \theta_1)$ and $c_2 = (\rho_2, \theta_2)$, their product can be obtained by simply multiplying their magnitude and adding their phase:

$$c_1 \times c_2 = (\rho_1, \theta_1) \times (\rho_2, \theta_2) = (\rho_1\rho_2, \theta_1 + \theta_2) \tag{1.23}$$

Now that we are armed with a geometric way of looking at multiplication, we can tackle division as well. After all, division is nothing more than the inverse operation of multiplication:

$$\frac{c_1}{c_2} = \left(\frac{\rho_1}{\rho_2}, \theta_1 - \theta_2\right) \tag{1.24}$$

On this basis, we can further derive fast n-order power and root calculations about a complex number $c = (\rho, \theta)$

$$c^n = (\rho^n, n\theta) \tag{1.25}$$

and

$$c^{\frac{1}{n}} = \left(\rho^{\frac{1}{n}}, \frac{1}{n}(n + k2\pi)\right), \text{ where } k = 0, 1, \cdots, n-1 \tag{1.26}$$