Mathematical Foundation of Quantum Computing

Raimondas Čiegis

Department of Mathematical Modelling, email: rc@vgtu.lt

September 1, 2026

1. M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2010. (MMK department has a pdf file of this book)

2. L. Susskind and A. Friedman. *Quantum Mechanics. The Theoretical Minimum*. Basic Books, 2014. (MMK department has a pdf file of this book)

3. R. de Wolf. *Quantum Computing: Lecture Notes*, QuSoft, CWI and University of Amsterdam, 2023.

4. M. Oskin. *Quantum Computing - Lecture Notes.* Department of Computer Science and Engineering University of Washington (pdf file), 2002.

5. https://quantum.cloud.ibm.com/learning/en/courses

Quantum mechanics (QM) is a great mathematical theoretical tool, which is used to create original modern physical models, to formulate hypotheses about physical laws that describe complex real processes.

Quantum mechanics (QM) is a great mathematical theoretical tool, which is used to create original modern physical models, to formulate hypotheses about physical laws that describe complex real processes.

However, the QM tool itself cannot say what laws describe these processes; this requires physical intuition and a long work of testing many and usually false hypotheses.

Conventional computers

Computers operate on the following principles:

- Binary logic: an elementary element can be only in two stable states – 0 and 1.

Computers operate on the following principles:

- Binary logic: an elementary element can be only in two stable states – 0 and 1.
- Such an element (bit) encodes one bit of information.

Conventional computers

Computers operate on the following principles:

- Binary logic: an elementary element can be only in two stable states – 0 and 1.
- Such an element (bit) encodes one bit of information.
- Using two logical operations (gates) NOT and AND we can implement any combinatorial algorithm.

- The state of a bit can be measured without changing it (a soft or arbitrarily gentle measurement).

- The state of a bit can be measured without changing it (a soft or arbitrarily gentle measurement).

- A bit can be copied as many times as needed to execute the algorithm.

- The state of a bit can be measured without changing it (a soft or arbitrarily gentle measurement).
- A bit can be copied as many times as needed to execute the algorithm.
- The total number of degrees of freedom for a system of n individual bits is equal to $2n$.

- The state of a bit can be measured without changing it (a soft or arbitrarily gentle measurement).
- A bit can be copied as many times as needed to execute the algorithm.
- The total number of degrees of freedom for a system of n individual bits is equal to $2n$.
- Parallelism is proportional to the number of processes.

Let's recall the definition of linear vector spaces. We consider spaces of complex numbers.

Let's take n-dimensional column vectors $(z_1, \ldots, z_n)^T$.

Then we define the vector addition operation –
the sum of any two vectors is also a vector:

$$(z_1, \ldots, z_n)^T + (v_1, \ldots, v_n)^T := (z_1 + v_1, \ldots, z_n + v_n)^T.$$

Vector addition is commutative and associative.

Vectors can be multiplied by a constant a

$$a(z_1, \ldots, z_n)^T := (a\, z_1, \ldots, a\, z_n)^T.$$

There is a special zero vector 0:

$$(z_1, \ldots, z_n)^T + 0 := (z_1, \ldots, z_n)^T.$$

Given any vector Z, there is a unique vector (-Z) such that

$$Z + (-Z) = 0.$$

The distributive property holds:

$$z\,(A + B) = z\,A + z\,B,$$
$$(z + w)\,A = z\,A + w\,A.$$

Given any vector Z, there is a unique vector (-Z) such that

$$Z + (-Z) = 0.$$

The distributive property holds:

$$z\,(A + B) = z\,A + z\,B,$$
$$(z + w)\,A = z\,A + w\,A.$$

We will use Hilbert linear vector spaces.

Thus the dot product of two vectors is defined

$$(Z, V) := Z \cdot V.$$

The length of the vector Z is defined by using the norm

$$\|Z\| = (Z \cdot Z)^{1/2}.$$

The elements of a linear vector space do not necessarily have to be classical vectors, it is only important to **define the specified operations** for the selected objects.

- The basic element (vector) is a quantum bit – a (qubit).

- The basic element (vector) is a quantum bit – a (qubit).
- A qubit is an element of a linear vector space over complex numbers $|\psi\rangle \in \mathbb{C}^2$. Due to Dirac they are called *ket*–vectors.

- The basic element (vector) is a quantum bit – a (qubit).
- A qubit is an element of a linear vector space over complex numbers $|\psi\rangle \in \mathbb{C}^2$. Due to Dirac they are called *ket*–vectors.

- The basic element (vector) is a quantum bit – a (qubit).
- A qubit is an element of a linear vector space over complex numbers $|\psi\rangle \in \mathbb{C}^2$. Due to Dirac they are called *ket*–vectors.

  We represent a qubit $|\psi\rangle$ as a linear combination (superposition) of two basis states $|0\rangle$ and $|1\rangle$:

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle ,$$

  where $\alpha_j \in \mathbb{C}$ are complex numbers and satisfy the normalization condition:

$$|\alpha_0|^2 + |\alpha_1|^2 = 1.$$

It is often convenient to write these two basis *ket*-vectors $|0\rangle$ and $|1\rangle$ as ordinary column vectors:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

n QUBIT SYSTEM

n qubit system is defined using a tensor product of basis qubits

$$\{\, |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle \,\}, \quad \psi_k \in \{0, 1\}.$$

so the number of degrees of freedom is equal to $N = 2^n$.

n qubit system is defined using a tensor product of basis qubits

$$\{\, |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle \,\}, \quad \psi_k \in \{0, 1\}.$$

so the number of degrees of freedom is equal to $N = 2^n$.

It is convenient to represent a ket $|A\rangle$ by the column of complex numbers

$$|A\rangle := (\alpha_1 \;\; \alpha_2 \;\; \cdots \;\; \alpha_N)^T.$$

Shortly we will see how components α_j can be calculated.

For every *ket* – vector $|A\rangle$, there is a *bra* – vector in the dual space, denoted by $\langle A|$

The corresponding *bra* – vector $\langle A|$ is represented by the row

$$\langle A| := (\alpha_1^* \ \ \alpha_2^* \ \ \cdots \ \ \alpha_N^*).$$

For every *ket* – vector $|A\rangle$, there is a *bra* – vector in the dual space, denoted by $\langle A|$

The corresponding *bra* – vector $\langle A|$ is represented by the row

$$\langle A| := (\alpha_1^* \;\; \alpha_2^* \;\; \cdots \;\; \alpha_N^*).$$

Inner product

The inner product is always the product of a *bra* $\langle B|$ and a *ket* $|A\rangle$ and is denoted this way

$$\langle B|A\rangle \, .$$

For every *ket* – vector $|A\rangle$, there is a *bra* – vector in the dual space, denoted by $\langle A|$

The corresponding *bra* – vector $\langle A|$ is represented by the row

$$\langle A| := (\alpha_1^* \ \ \alpha_2^* \ \ \cdots \ \ \alpha_N^*).$$

Inner product

The inner product is always the product of a *bra* $\langle B|$ and a *ket* $|A\rangle$ and is denoted this way

$$\langle B|A\rangle .$$

In the concrete representation of bras and kets by row and column vectors, the inner product is defined in terms of components

$$\langle B|A\rangle := \beta_1^* \alpha_1 + \beta_2^* \alpha_2 + \ \cdots \ + \beta_N^* \alpha_N.$$

Exercise 1. Using the definition of the inner product, prove

a)

$$(\langle A| + \langle B|)\, |C\rangle = \langle A|C\rangle + \langle B|C\rangle \,.$$

b)
$\langle A|A\rangle$ is a real number.

A vector is said to be normalized if it satisfies

$$\langle A|A\rangle = 1.$$

A vector is said to be normalized if it satisfies

$$\langle A|A\rangle = 1.$$

Two vectors $|A\rangle$ and $|B\rangle$ are said to be orthogonal if

$$\langle A|B\rangle = 0.$$

Orthonormal Bases

It is very useful to construct an orthonomal basis

$$\{ \, |i\rangle : \quad i = 1, 2, \ldots, N \, \},$$
$$\langle i|i\rangle = 1, \quad \langle j|i\rangle = 0, \;\; \forall i \neq j$$

and use it to construct a representation of any vector $|A\rangle$

$$|A\rangle := \alpha_1 \; |1\rangle + \alpha_2 \; |2\rangle + \quad \cdots \quad + \alpha_N \; |N\rangle \, .$$

where α_j are complex numbers. It is easy to see that components α_j can be computed as

$$\alpha_j = \langle j|A\rangle \, .$$

If vector $|A\rangle$ is normalized then

$$|\alpha_1|^2 + |\alpha_2|^2 + \cdots + |\alpha_N|^2 = 1.$$

Let's consider an example of two qubits, the expansion is defined as

$$|\psi\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle ,$$

where

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1.$$

Let's consider an example of two qubits, the expansion is defined as

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle,$$

where

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1.$$

The element simultaneously exists in all basis states $|j\rangle$.

Let's consider an example of two qubits, the expansion is defined as

$$|\psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle\,,$$

where

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1.$$

The element simultaneously exists in all basis states $|j\rangle$.

Measurement

If we perform a measurement, then with probability $|\alpha_k|^2$ we will obtain a value v_k corresponding to the basis vector $|k\rangle$.

After the measurement, the state of the element changes to

$$|\psi\rangle = |k\rangle\,.$$

Let's consider an example of two qubits, the expansion is defined as

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle,$$

where

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1.$$

The element simultaneously exists in all basis states $|j\rangle$.

Measurement

If we perform a measurement, then with probability $|\alpha_k|^2$ we will obtain a value v_k corresponding to the basis vector $|k\rangle$.

After the measurement, the state of the element changes to

$$|\psi\rangle = |k\rangle.$$

If we now perform the measurement again, we will get the same value v_k and the state of the element will not change anymore

$$|\psi\rangle = |k\rangle.$$

It is clear that the state of the element does not depend on the chosen basis, we can also take another basis

$$|\psi\rangle = \sum_{j=1}^{N} \widetilde{\alpha}_j \, |\tilde{j}\rangle\,, \quad \widetilde{\alpha}_j \in \mathbb{C},$$

only the probability of measuring one or another outcome changes.

It is convenient to write the basis vectors in the form of column vectors, e.g.

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

It is convenient to write the basis vectors in the form of column vectors, e.g.

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

If the basis vector system is fixed, then we also can write the state of the system in column vector form

$$|\psi\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{2^n} \end{pmatrix}$$

But we must not forget that it depends on the chosen system of basis vectors.

Linear operators

A linear operator between vector spaces V is defined by the linear function $\mathcal{M} : V \to V$

$$\mathcal{M}\left(\sum_i a_i \left|v_i\right\rangle\right) = \sum_i a_i \mathcal{M}\big(\left|v_i\right\rangle\big).$$

Here $|v_i\rangle$ any vectors from V, a_i are complex numbers.

Linear operators

A linear operator between vector spaces V is defined by the linear function $\mathcal{M} : V \to V$

$$\mathcal{M}\left(\sum_i a_i \left|v_i\right\rangle\right) = \sum_i a_i \mathcal{M}\big(\left|v_i\right\rangle\big).$$

Here $|v_i\rangle$ any vectors from V, a_i are complex numbers.

If we have two linear operators $\mathcal{A} : V \to V$ and $\mathcal{B} : V \to V$, then their composition is defined as follows

$$(\mathcal{B}\mathcal{A})(|v\rangle) = \mathcal{B}\big(\mathcal{A}(|v\rangle)\big), \quad |v\rangle \in V.$$

Matrix form of linear operators

Let's consider a linear operator $\mathcal{M}$ and two vectors $|A\rangle$, $|B\rangle$.

We want to take the equation

$$\mathcal{M}\,|A\rangle = |B\rangle$$

and write it in component form.

Suppose we have fixed the system of basis vectors

$$|j\rangle\,,\ j = 1, \ldots, N.$$

Then we will represent arbitrary *ket* – vectors $|A\rangle$ and $|B\rangle$ as sums over basis vectors

$$|A\rangle = \sum_{j=1}^{N} \alpha_j\ |j\rangle\,, \quad |B\rangle = \sum_{j=1}^{N} \beta_j\ |j\rangle$$

and plug both sums into $\mathcal{M}\,|A\rangle = |B\rangle$:

$$\sum_{j=1}^{N} \alpha_j \mathcal{M}\,|j\rangle = \sum_{j=1}^{N} \beta_j\,|j\rangle\,.$$

Finally we take the inner product of both sides with a particaular basis vector $\langle i|$

$$\sum_{j=1}^{N} \langle i|\,\mathcal{M}\,|j\rangle\,\alpha_j = \sum_{j=1}^{N} \beta_j\,\langle i|j\rangle = \beta_i.$$

The quantities

$$m_{ij} = \langle i|\,\mathcal{M}\,|j\rangle$$

are called the *matrix elements*, we get

$$\sum_{j=1}^{N} m_{ij}\,\alpha_j = \beta_i, \quad i = 1, \ldots, N.$$

We can write this in matrix form (for $N = 4$):

$$M = \begin{pmatrix} m_{11} & m_{12} & m_{13} & m_{14} \\ m_{21} & m_{22} & m_{23} & m_{24} \\ m_{31} & m_{32} & m_{33} & m_{34} \\ m_{41} & m_{42} & m_{43} & m_{44} \end{pmatrix}$$

and the classical matrix multiplication is used

$$\begin{pmatrix} m_{11} & m_{12} & m_{13} & m_{14} \\ m_{21} & m_{22} & m_{23} & m_{24} \\ m_{31} & m_{32} & m_{33} & m_{34} \\ m_{41} & m_{42} & m_{43} & m_{44} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \beta_3 \\ \beta_4 \end{pmatrix}$$

We can write this in matrix form (for $N = 4$):

$$M = \begin{pmatrix} m_{11} & m_{12} & m_{13} & m_{14} \\ m_{21} & m_{22} & m_{23} & m_{24} \\ m_{31} & m_{32} & m_{33} & m_{34} \\ m_{41} & m_{42} & m_{43} & m_{44} \end{pmatrix}$$

and the classical matrix multiplication is used

$$\begin{pmatrix} m_{11} & m_{12} & m_{13} & m_{14} \\ m_{21} & m_{22} & m_{23} & m_{24} \\ m_{31} & m_{32} & m_{33} & m_{34} \\ m_{41} & m_{42} & m_{43} & m_{44} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \beta_3 \\ \beta_4 \end{pmatrix}$$

or

$$M\,|A\rangle = |B\rangle\,.$$

As an example, let's take the popular linear operator

$$H|0\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big),$$
$$H|1\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big).$$

Then we get the following matrix

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