Interaction and Concurrency

Ana Neri

April 30, 2020

University of Minho - LCC

Table of contents

Complex Numbers[1]

Imaginary Numbers

$$x^2 = -1$$

X is $\sqrt{-1}$ this number does not exist in the real numbers.

So we will call it *imaginary* and denote it i.

$i^2 = -1$ or $i = \sqrt{-1}$

Imaginary Numbers - Exercises 1

1. i^{25}

Imaginary Numbers - Exercises 1

1. i^{25}

Solution:

1. There is a pattern in imaginary numbers.
   $i^0 = 1 \quad i^1 = i \quad i^2 = -1 \quad i^3 = -i$
   $i^4 = 1 \quad i^5 = i \quad i^6 = -1 \quad i^7 = -i$
   ...
   Then we apply modular arithmetic: $25 \mod 4 = 1$

$$i^{25} = i^1 = i$$

Complex Numbers - definition

A complex number is an expression:

$$c = a + b \times i = a + bi$$

where a, b are two real numbers. a is the real part of c and b is its imaginary part.

The set of all complex numbers is denoted $\mathbb{C}$.

Complex Conjugates

$$c = a + bi$$

The conjute of c, is denoted $\overline{c}$:

$$\overline{c} = a - bi$$

Modulus squared:

$$c \times \overline{c} = |c|^2$$

Complex Number - polar representation

$$c = a + bi$$

$$\rho = \sqrt{(a^2 + b^2)} \qquad a = \rho \cos(\theta)$$

$$\theta = \tan^{-1}(\frac{b}{a}) \qquad b = \rho \sin(\theta)$$

$$c = \rho(\cos(\theta) + i \sin(\theta)) = \rho e^{i\theta}$$

A complex number c is a magnitude $|c|$ and a phase θ[1].

[1] More information about complex numbers and their properties in [1].

complex Numbers - Exercise 2

Gate S is a phase gate.

$$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

It does nothing to state $|0\rangle$. When the initial state is $|1\rangle$ the gate applies a rotation giving by the complex number i.

What is the phase of gate S?

Gate S is a phase gate.

$$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

It does nothing to state $|0\rangle$. When the initial state is $|1\rangle$ the gate applies a rotation giving by the complex number i.

What is the phase of gate S?

Solution:

$\theta = \tan^{-1}(1/0) = \tan^{-1}(+\infty)$ or ANGLE whose tangent equals infinity.

$\tan(\theta) = \frac{\sin(\theta)}{\cos(\theta)}$, so $\tan(\theta) = +\infty$ implies $\cos(\theta) = 0$.

$\theta = \frac{\pi}{2}$

Complex Vector Spaces[1]

Complex Vector Spaces - definition

Let $V = \begin{bmatrix} a+bi \\ c+di \end{bmatrix}$, $W = \begin{bmatrix} e+fi \\ g+hi \end{bmatrix}$ and $\mathbf{0} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$.

A complex vector space is a nonempty set $\mathbb{V}$, whose elements we shall call vectors, with three operations:

Addition V + W = $\begin{bmatrix} (a+bi)+(e+fi) \\ (c+di)+(g+hi) \end{bmatrix}$

Negation -V = $\begin{bmatrix} -a-bi \\ -c-di \end{bmatrix}$

Scalar Multiplication s $\cdot V = \begin{bmatrix} s(a+bi) \\ s(c+di) \end{bmatrix}$

and a distinguished element called the zero vector $0 \in \mathbb{V}$ in the set.

Complex Vector Spaces - definition

These operations and zero must satisfy the following properties: for all $V, W, X \in \mathbb{V}$ and for all $c, c_1, c_2 \in \mathbb{C}$,

1. Commutative of addition: $V + W = W + V$
2. Associative of addition: $(V + W) + X = V + (W + X)$
3. Zero is an additive identity: $V + \mathbf{0} = V$
4. Every vector has an inverse: $V + (-V) = \mathbf{0} = (-V) + V$
5. Scalar multiplication has a unit: $1 \cdot V = V$
6. Scalar multiplication respects complex multiplication: $c_1 \cdot (c_2 \cdot V) = (c_1 \times c_2) \cdot V$
7. Scalar multiplication distributes over addition: $c \cdot (V + W) = c \cdot V + c \cdot W$
8. Scalar multiplication distributes over complex addition: $(c_1 + c_2) \cdot V = c_1 \cdot V + c_2 \cdot V$

In the previous definitions the examples were given with $V, W \in \mathbb{C}^2$ (a specific type vector).

This properties work with any $V, W \in \mathbb{C}^n$

And in any $M \in \mathbb{C}^{m \times n}$.

$$M = \begin{bmatrix} c_{0,0} & c_{0,1} & \dots & c_{n-1} \\ c_{1,0} & c_{1,1} & \dots & c_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m-1,0} & c_{m-1,1} & \dots & c_{m-1,n-1} \end{bmatrix}$$

Complex Vector Space - $\mathbb{C}^{m \times n}$

$A \in \mathbb{C}^{m \times n}$ is matrix with j rows and k columns denoted by $A[j,k]$ or $c_{j,k}$.

When $n = 1 \rightarrow$ vectors can be special types of matrices.

When $n = m \rightarrow$ This has more operations and more structure than just a complex vector space.

- transpose - $A^T[j,k] = A[k,j]$
- conjugate - $\overline{A}[j,k] = \overline{A[j,k]}$
- adjoint or dagger - $A^{\dagger} = (\overline{A}^T) = \overline{(A^T)}$ or $A \dagger [j,k] = \overline{A[k,j]}$

Complex Vector Space - A^T, $\overline{A}$ and $A^\dagger$

1. Transpose is idempotent $(A^T)^T = A$
2. Transpose respects addition $(A + B)^T = A^T + B^T$
3. Transpose respects scalar multiplication $(c \cdot A)^T = c \cdot A^T$
4. Conjugate is idempotent $\overline{\overline{A}} = A$
5. Conjugate respects addition $\overline{A + B} = \overline{A} + \overline{B}$
6. Conjugate respects scalar multiplication $\overline{c \cdot A} = \overline{c} \cdot \overline{A}$
7. Adjoint is idempotent $(A^\dagger)^\dagger = A$
8. Adjoint respects addition $(A + B)^\dagger = A^\dagger + B^\dagger$
9. Adjoint relates to scalar multiplication $(c \cdot A)^\dagger = \overline{c} \cdot A^\dagger$

Complex Vector Space - Matrix multiplication

Given $A \in \mathbb{C}^{m \times n}$ and $B \in \mathbb{C}^{n \times p}$, $A \cdot B \in \mathbb{C}^{m \times p}$ is defined as :

$$(A \cdot B)[j,k] = \sum_{h=0}^{n-1} (A[j,h] \times B[h,k])$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} (a \times e + b \times g) & (a \times f + b \times h) \\ (c \times e + d \times g) & (c \times f + d \times h) \end{bmatrix}$$

Complex Vector Space - Exercise 3

1. $\begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix} \cdot \begin{bmatrix} 3 & 4 \\ 10 & 5 \end{bmatrix}$

2. $\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \end{bmatrix}^T$

Complex Vector Space - Exercise 3

1. $\begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix} \cdot \begin{bmatrix} 3 & 4 \\ 10 & 5 \end{bmatrix}$

2. $\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \end{bmatrix}^T$

Solution:

1. $\begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix} \cdot \begin{bmatrix} 3 & 4 \\ 10 & 5 \end{bmatrix} = \begin{bmatrix} 0 \times 3 + 1 \times 10 & 0 \times 4 + 1 \times 5 \\ 2 \times 3 + 0 \times 10 & 2 \times 4 + 0 \times 5 \end{bmatrix} = \begin{bmatrix} 0 + 10 & 0 + 5 \\ 6 + 0 & 8 + 0 \end{bmatrix} = \begin{bmatrix} 10 & 5 \\ 6 & 8 \end{bmatrix}$

2. $\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \end{bmatrix}^T = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 + 1 \\ 0 - 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$

Complex Vector Space - Identity matrix

$$Id_n = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

The common notation of the identity matrix : Id, I or $\mathbb{1}$.

Complex Vector Space - Matrix Multiplication Properties

1. Matrix multiplication is associative $(A \cdot B) \cdot C = A \cdot (B \cdot C)$
2. Matrix multiplication has I_n as a unit $I_n \cdot A = A = A \cdot I_n$
3. Matrix multiplication distributes over addition
   $A \cdot (B + C) = (A \cdot B) + (A \cdot C)$
4. Matrix multiplication respects scalar multiplication
   $c \cdot (A \cdot B) = (c \cdot A) \cdot B = A \cdot (c \cdot B)$
5. Matrix multiplication relates to the transpose $(A \cdot B)^T = B^T \cdot A^T$
6. Matrix multiplication respects the conjugate $\overline{A \cdot B} = \overline{A} \cdot \overline{B}$
7. Matrix multiplication relates to the adjoint $(A \cdot B)^\dagger = B^\dagger \cdot A^\dagger$

*commutativity is **not** a basic property of matrix multiplication*

Complex Vector Space - Matrix Multiplication

In **quantum computation**, matrix multiplication corresponds to serially wired gates.

$$-\boxed{X}-\boxed{Z}- = -\boxed{X \cdot Z}-$$

Matrix multiplication can also be used to represent the action of a gate U in an arbitrary quantum state $|\psi_{in}\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$

$$|\psi_{in}\rangle \ -\boxed{U}- \ |\psi_{out}\rangle$$

$$U|\psi_{in}\rangle = U \begin{bmatrix} \alpha & \beta \end{bmatrix}^T = |\psi_{out}\rangle$$

Complex Vector Space - Linear Maps

When a matrix acts on a vector space, it is a linear map.

An operator is a linear map from a complex vector space to itself.

If $F : \mathbb{C}^n \to \mathbb{C}^n$ is an operator on $\mathbb{C}^n$ and A is a matrix $n \times n$ such that for all V we have $F(V) = A \cdot V$, then F is represented by A.

Several different matrices might represent the same operator.

Complex Vector Spaces - Basis

Let $\mathbb{V}$ be a complex vector space. $V \in \mathbb{V}$ is a **linear combination** of the vectors V_0, V_1,..., V_{n-1} in $\mathbb{V}$ if V can be written as

$$V = c_0 \cdot V_0 + c_1 \cdot V_1 + \ldots + c_{n-1} \cdot V_{n-1}$$

for some c_0, c_1, ..., c_{n-1} in $\mathbb{C}$.

A set $\{V_0, V_1, \ldots, V_{n-1}\}$ of vectors in $\mathbb{V}$ is called **linearly independent** if

$$\mathbf{0} = c_0 \cdot V_0 + c_1 \cdot V_1 + \ldots + c_{n-1} \cdot V_{n-1}$$

implies tha $c_0 = c_1 = \ldots = c_{n-1} = 0$.

A set $B = \{V_0, V_1, \ldots, V_{n-1}\} \subseteq \mathbb{V}$ of vectors is called a **basis** of complex vectors $\mathbb{V}$ if every, $V \in \mathbb{V}$ can be written as a linear combination of vectors from B and B is linear independent.

Complex Vector Spaces - Exercise 4

In **quantum computation**, the most used bases are $|0\rangle$ and $|1\rangle$.

Exercise

Write a qubit state as linear combination of these basis.

In **quantum computation**, the most used bases are $|0\rangle$ and $|1\rangle$.

Exercise

Write a qubit state as linear combination of these basis.

Solution:

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

Complex Vector Spaces - Inner Product

An inner product on a complex vector space $\mathbb{V}$ is a function

$$\langle -, - \rangle : \mathbb{V} \times \mathbb{V} \to \mathbb{C}$$

that satisfies the following conditions for all V, V_1, V_2, and V_3 in $\mathbb{V}$ and for a $c \in \mathbb{C}$:

1. Nondegenerate (exception $V = 0$, $\langle V, V \rangle = 0$): $\langle V, V \rangle \geqslant 0$
2. Respects addition: $\langle V_1 + V_2, V_3 \rangle = \langle V_1, V_3 \rangle + \langle V_2, V_3 \rangle$; $\langle V_1, V_2 + V_3 \rangle = \langle V_1, V_2 \rangle + \langle V_1, V_3 \rangle$
3. Respects scalar multiplication: $\langle c \cdot V_1, V_2 \rangle = c \times \langle V_1, V_2 \rangle$; $V_1, c \cdot V_2 = \overline{c} \times \langle V_1, V_2 \rangle$
4. Skew symmetric: $\langle V_1, V_2 \rangle = \overline{\langle V_2, V_1 \rangle}$

Complex Vector Space - Inner Product

In $\mathbb{C}^n$ the inner product is : $\langle V_1, V_2 \rangle = V_1^\dagger \cdot V_2$

In $\mathbb{C}^{n \times m}$ the inner product of matrices is: $\langle A, B \rangle = Trace(A^\dagger \cdot B)$

Complex Vector Space - Orthogonal

Two vectors V_1 and V_2 in an inner product space $\mathbb{V}$ are orthogonal if $\langle V_1, V_2 \rangle = 0$

Complex Vector Space - Norm and normalization

Norm:

$$||V\rangle| = \sqrt{\langle V|V\rangle}$$

Nomalization:

$$\frac{|V\rangle}{||V\rangle|}$$

Complex Vector Space - Kronecker delta function

A basis $B = V_0, V_1, ..., V_{n-1}$ for an inner product space V is called an orthogonal basis if the vectors are pairwise orthogonal to each other, i.e., $j \neq k$ implies $\langle V_j, V_k \rangle = 0$.

An orthogonal basis is called an orthonormal basis if every vector in the basis is of norm 1, i.e.,

$$\langle V_j | V_k \rangle = \delta_{j,k} = \begin{cases} 1, \text{if} j = k \\ 0, \text{if} i \neq k \end{cases}$$

$\delta_{j,k}$ is called the Kronecker delta function

Complex Vector Space - Hilbert Space

Hilbert Space is a complex inner product space that is complete.

A **finite-dimensional complex vector space with an inner product** is an Hilbert Space.

Complex Vector Space - Exercise 5

1. Proof that the quantum state $|0\rangle$ is orthogonal to $|1\rangle$.
2. Proof that the quantum state $|+\rangle$ is orthogonal to $|-\rangle$.

Complex Vector Space - Exercise 5

1. Proof that the quantum state $|0\rangle$ is orthogonal to $|1\rangle$.
2. Proof that the quantum state $|+\rangle$ is orthogonal to $|-\rangle$.

Solution:

1. $\langle 0|1\rangle$ needs to be 0.
   Recall $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$
   $\langle 0|1\rangle = \begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} =$
   $(1 \times 0) + (0 \times 1) = 0$

2. $\langle +|-\rangle$ needs to be 0.
   Recall $|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$
   and $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$
   $\langle +|-\rangle =$
   $(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \end{bmatrix}) \cdot (\frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}) =$
   $\frac{1}{2}((1 \times 1) + (1 \times (-1))) = 0$

Complex Vector Spaces - Unitary Matrix

A matrix U is unitary if

$$U \cdot U^\dagger = U^\dagger \cdot U = Id$$

Complex Vector Spaces - Tensor Product

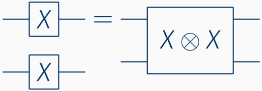
$$A = \begin{bmatrix} a_{0,0} & a_{0,1} \\ a_{1,0} & a_{1,1} \end{bmatrix} \text{ and } B = \begin{bmatrix} b_{0,0} & b_{0,1} \\ b_{1,0} & b_{1,1} \end{bmatrix}$$

$$A \otimes B = \begin{bmatrix} a_{0,0} \begin{bmatrix} b_{0,0} & b_{0,1} \\ b_{1,0} & b_{1,1} \end{bmatrix} & a_{0,1} \begin{bmatrix} b_{0,0} & b_{0,1} \\ b_{1,0} & b_{1,1} \end{bmatrix} \\ a_{1,0} \begin{bmatrix} b_{0,0} & b_{0,1} \\ b_{1,0} & b_{1,1} \end{bmatrix} & a_{1,1} \begin{bmatrix} b_{0,0} & b_{0,1} \\ b_{1,0} & b_{1,1} \end{bmatrix} \end{bmatrix} =$$

$$\begin{bmatrix} a_{0,0} \times b_{0,0} & a_{0,0} \times b_{0,1} & a_{0,1} \times b_{0,0} & a_{0,1} \times b_{0,1} \\ a_{0,0} \times b_{1,0} & a_{0,0} \times b_{1,1} & a_{0,1} \times b_{1,0} & a_{0,1} \times b_{1,1} \\ a_{1,0} \times b_{0,0} & a_{1,0} \times b_{0,1} & a_{1,1} \times b_{1,0} & a_{1,1} \times b_{0,1} \\ a_{1,0} \times b_{1,0} & a_{1,0} \times b_{1,1} & a_{1,1} \times b_{1,0} & a_{1,1} \times b_{1,1} \end{bmatrix}$$

Complex Vector Spaces - Tensor Product

In **quantum computation**, the tensor product corresponds to parallel gates:



Two vectors that can be written as a tensor are **separable**:

$$|0\rangle \otimes |0\rangle = |00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Quantum Computation Basics

Quantum Computing Basics

A quantum arbitrary state:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

A system of n-qubits:

$$\sum_{q_1,\ldots,q_n \in \{0,1\}^n} c_{q_1 \ldots q_n} |q_1 \ldots q_n\rangle = \sum_{i=0}^{2^n-1} c_i|i\rangle$$

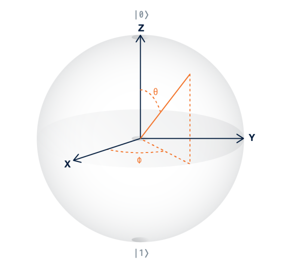


Figure 1: Bloch Sphere

Quantum computing Basics

Hadamard	H	$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$
Pauli-X	X	$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$
Pauli-Y	Y	$\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}$
Pauli-Z	Z	$\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$
Phase	S	$\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}$
$\frac{\pi}{8}$	T	$\begin{bmatrix}1 & 0\\ 0 & e^{i\frac{\pi}{4}}\end{bmatrix}$

Table 1: single qubit gates

Quantum gates are reversible gates responsible for change in the qubit state.
Are described by a unitary matrix U:

$$U^\dagger U = 1, U^\dagger \text{ is the adjoint of } U$$

CNOT

$$\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$$

Table 2: multiqubit gate

Important notes on Quantum

- Besides the classics (0 and 1) states, the qubits can also be in any superposition state.
- In quantum computation, entanglement is created with multiqubit gates (like the CNOT).
- The measurement collapses the quantum state.
- A qubit' state cannot be copied!

References

[1] Noson S. Yanofsky and Mirco A. Mannucci. *Quantum computing for computer scientists*, volume 9780521879. 2008. ISBN 9780511813887. doi: 10.1017/CBO9780511813887.