Quantum Computation

Alessandra Di Pierro

alessandra.dipierro@univr.it

2010

Info + Programme

- Info:
  http://profs.sci.univr.it/~dipierro/InfQuant/InfQuant10.html
- Preliminary Programme:
  - Introduction and Background
    - Complex vector spaces
    - Quantum mechanics
  - Quantum computation:
    - Computational models (Circuits, QTM)
    - Algorithms (QFT, Quantum search)
  - Quantum Cryptography
  - Quantum programming languages

Text Books

- Noson S. Yanofsky, Mirco A. Mannucci: Quantum Computing for Computer Scientists, Cambridge University Press 2008
- Michael A. Nielsen, Issac L. Chuang: Quantum Computation and Quantum Information, Cambridge University Press 2000
- Phillip Kaye, Raymond Laflamme, Michael Mosca: An Introduction to Quantum Computing, Oxford 2007
- Alessandra Di Pierro: Appunti delle lezioni

Electronic Resources

Introductory Texts

- Noson S. Yanofsky: An Introduction to Quantum Computing `http://arxiv.org/abs/0708.0261`

Main Preprint Repository

- arXiv `http://arxiv.org`

Physics Background

- Chris J. Isham: Quantum Theory – Mathematical and Structural Foundations, Imperial College Press 1995
- Richard P. Feynman, Robert B. Leighton, Matthew Sands: The Feynman Lectures on Physics, Addison-Wesley 1965

Basics

Complex Numbers

Quantitative information, e.g. measurement results, is usually represented by real numbers $\mathbb{R}$. In the ‘real world’ we do not experience complex numbers.

“The temperature today is (24 - 13i)C” or “The time a process takes is 14.64i seconds” are not very usual statements in the daily life.

Complex numbers, $\mathbb{C}$, play an essential role in quantum mechanics.

Basic Definitions

A **complex number** $z \in \mathbb{C}$ is a (formal) combinations of two reals $x, y \in \mathbb{R}$:

$$z = x + iy$$

with: $i^2 = -1$.

The **complex conjugate** of a complex number $z \in \mathbb{C}$ is:

$$z^* = \overline{z} = \overline{x + iy} = x - iy$$

Hauptsatz of Algebra
Complex numbers are algebraically closed: Every polynomial of order n over $\mathbb{C}$ has exactly n roots.

Algebraic structure of $\mathbb{C}$

The set of complex number $\mathbb{C}$ is a *field*:

Addition is commutative and associative;

Multiplication is commutative and associative;

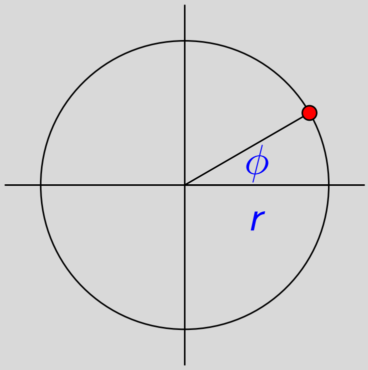
Addition has an identity: $(0, 0)$;

Multiplication has an identity: $(1, 0)$;

Multiplication distributes wrt addition;

Multiplication and addition have inverses.

Polar Coordinates



Conversion

$$x = r \cdot \cos(\phi) \qquad y = r \cdot \sin(\phi)$$

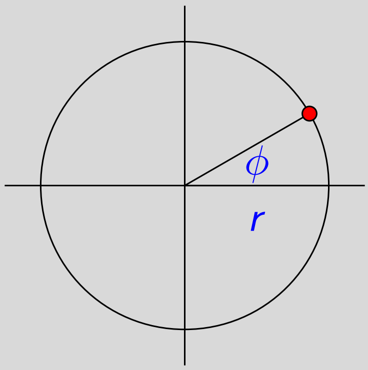
and

$$r = \sqrt{x^2 + y^2} \qquad \phi = \arctan(\frac{y}{x})$$

Another representation:

$$(r, \phi) = r \cdot e^{i\phi} \qquad e^{i\phi} = \cos(\phi) + i \sin(\phi).$$

Phase



If we fix r then we have a different complex number for each $0 \leq \phi \leq 2\pi$.
For $\phi = 0$ we get all positive real numbers.
For $\phi = \pi$ we get all negative real numbers.

Vector Spaces

A **vector space** (over a field $\mathbb{K}$, e.g. $\mathbb{R}$ or $\mathbb{C}$) is a set $\mathcal{V}$ together with two operations:

$$\text{Scalar Product} \quad .\cdot. : \mathbb{K} \times \mathcal{V} \mapsto \mathcal{V}$$
$$\text{Vector Addition} \quad .+. : \mathcal{V} \times \mathcal{V} \mapsto \mathcal{V}$$

such that ($\forall x, y, z \in \mathcal{V}$ and $\alpha, \beta \in \mathbb{K}$):

1. $x + (y + z) = (x + y) + z$
2. $x + y = y + x$
3. $\exists o : x + o = x$
4. $\exists -x : x + (-x) = o$

5. $\alpha(x + y) = \alpha x + \alpha y$
6. $(\alpha + \beta)x = \alpha x + \beta x$
7. $(\alpha\beta)x = \alpha(\beta x)$
8. $1x = x \ (1 \in \mathbb{K})$

Tuple Spaces

Theorem

All finite dimensional vector spaces are isomorphic to the (finite) Cartesian product of the underlying field $\mathbb{K}^n$ (i.e. $\mathbb{R}^n$ or $\mathbb{C}^m$).

$$x = (x_1, x_2, x_3, \ldots, x_n)$$
$$y = (y_1, y_2, y_3, \ldots, y_n)$$

Algebraic Structure

$$\alpha x = (\alpha x_1, \alpha x_2, \alpha x_3, \ldots, \alpha x_n)$$
$$x + y = (x_1 + y_1, x_2 + y_2, x_3 + y_3, \ldots, x_n + y_n)$$

Finite dimensional vectors can be represented via their coordinates with respect to a given base.

Hilbert Spaces I

A complex vector space $\mathcal{H}$ is called an **Inner Product Space** (or **(Pre-)Hilbert Space**) if there is a complex valued function $\langle .,. \rangle$ on $\mathcal{H} \times \mathcal{H}$ that satisfies ($\forall x, y, z \in \mathcal{H}$ and $\forall \alpha \in \mathbb{C}$):

1. $\langle x, x \rangle \geq 0$
2. $\langle x, x \rangle = 0 \iff x = o$
3. $\langle \alpha x, y \rangle = \alpha \langle x, y \rangle$
4. $\langle x, y + z \rangle = \langle x, y \rangle + \langle x, z \rangle$
5. $\langle x, y \rangle = \overline{\langle y, x \rangle}$

The function $\langle .,. \rangle$ is called an **inner product** on $\mathcal{H}$.

Hilbert Spaces II

A complex inner product space $\mathcal{H}$ is called a **Hilbert Space** if for any Cauchy sequence of vectors $x_0, x_1, \ldots,$ there exists a vector $y \in \mathcal{H}$ such that

$$\lim_{n \to \infty} \|x_n - y\| = 0,$$

where $\| \cdot \|$ is the norm defined by

$$\|x\| = \sqrt{\langle x, x \rangle}.$$

Theorem

Every finite-dimensional complex vector space with a inner product is a Hilbert space.

Basis Vectors

A set of vectors x_i is said to be **linearly independent** iff

$$\sum \lambda_i x_i = 0 \quad \text{implies that} \quad \forall\, i : \lambda_i = 0$$

Two vectors in a Hilbert space are **orthogonal** iff

$$\langle x, y \rangle = 0$$

An **orthonormal** system in a Hilbert space is a set of linearly independent vectors of norm 1 such that:

$$\langle b_i, b_j \rangle = \delta_{ij} = \begin{cases} 1 & \text{iff } i = j \\ 0 & \text{iff } i \neq j \end{cases}$$

Theorem

For a Hilbert space there always exists a orthonormal basis $\{b_i\}$ (Gram-Schmidt transformation).

We will always work with vectors represented in a orthonormal basis.

Dirac Notation

P.A.M. Dirac "invented" the Bra-Ket Notation

$$\langle x, y \rangle = \langle x | y \rangle = \langle x | \, | y \rangle$$

In particular, we enumerate the basis vectors:

$$\vec{b}_i \quad \text{is denoted by} \quad |i\rangle$$

- Ket-vectors are vectors in $\mathbb{C}^n$
- Bra-vectors are vectors in $(\mathbb{C}^n)^* = \mathbb{C}^n$.

Conventions

Physical Convention:

$$\langle x|\alpha y\rangle = \alpha \langle x|y\rangle$$

Mathematical Convention:

$$\langle \alpha x, y\rangle = \alpha \langle x, y\rangle$$

Linear in first or second argument.

$$\begin{aligned} \langle \alpha x, y\rangle &= \alpha \langle x, y\rangle \\ \langle x, \alpha y\rangle &= \overline{\langle \alpha y, x\rangle} = \bar{\alpha}\overline{\langle y, x\rangle} = \bar{\alpha} \langle x, y\rangle \end{aligned}$$

Finite-Dimensional Hilbert Spaces – $\mathbb{C}^n$

We represent vectors and their **transpose** by:

$$\vec{x} = |x\rangle = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad \vec{y} = \langle y| = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}^T = (y_1, \ldots, y_n)$$

The **adjoint** of $\vec{x} = (x_1, \ldots, x_n)$ is given by

$$\vec{x}^\dagger = (x_1^*, \ldots, x_n^*)^T$$

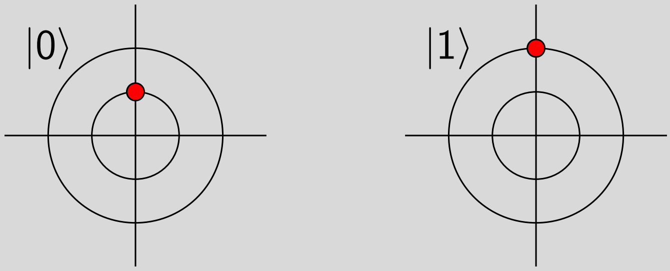
The **inner product** can be represented by:

$$\langle \vec{y}, \vec{x}\rangle = \sum_i y_i^* x_i = \vec{y}^\dagger \vec{x}$$

We can also define a **norm** (length) $\|\vec{x}\| = \sqrt{\langle \vec{x}, \vec{x}\rangle}$.

Qubits

Consider a simple systems with two **degrees of freedom**.



Definition

A **qubit** (quantum bit) is a quantum state of the form

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

where α and β are complex numbers with $|\alpha|^2 + |\beta|^2 = 1$.

Qubits live in a two-dimensional complex vector, more precisely, Hilbert space $\mathbb{C}^2$ and are **normalised**, i.e. $\| \, |\psi\rangle \, \| = \langle \psi, \psi \rangle = 1$.

Quantum States

The postulates of **Quantum Mechanics** require that a computational quantum **state** is given by a normalised vector in $\mathbb{C}^n$. A qubit is a two-dimensional quantum state, i.e. in $\mathbb{C}^2$

Mathematical Notation: x or $\vec{x}_i$

Physical Notation: $|x\rangle$ or $|i\rangle$

We represent the **coordinates** of a state or ket-vector as a column vector, in particular a **qubit**:

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \quad \text{or} \quad \vec{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

with respect to the (orthonormal) **basis** $\{\vec{b}_0, \vec{b}_1\}$ or $\{|0\rangle, |1\rangle\}$.

Change of Basis

We can represent a quantum state $|\psi\rangle$ with respect to any basis. For example, we can consider in $\mathbb{C}^2$, i.e. for qubits, the (alternative) orthonormal basis:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

and thus, vice versa:

$$|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) \qquad |1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$$

A qubit is therefore represented in the two bases as:

$$\begin{aligned} \alpha|0\rangle + \beta|1\rangle &= \frac{\alpha}{\sqrt{2}}(|+\rangle + |-\rangle)\frac{\beta}{\sqrt{2}}(|+\rangle - |-\rangle) \\ &= \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle \end{aligned}$$

Representing a Qubit

A qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$ can be represented:

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\varphi}\sin(\theta/2)|1\rangle,$$

where $\theta \in [0, \pi]$ and $\varphi \in [0, 2\pi]$. Using polar coordinates we have:

$$|\psi\rangle = r_0 e^{i\phi_0}|0\rangle + r_1 e^{i\phi_1}|1\rangle,$$

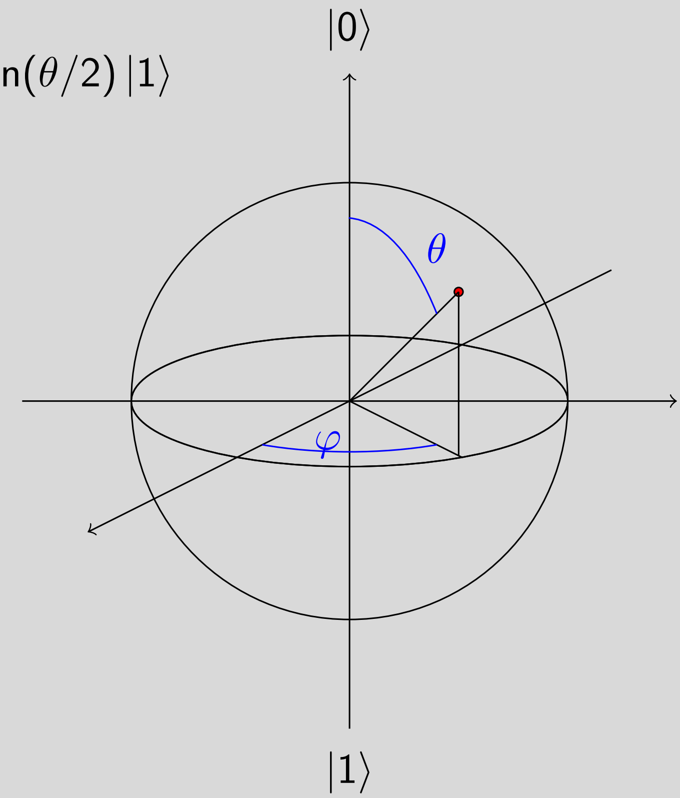
with $r_0^2 + r_1^2 = 1$. Take $r_0 = \cos(\rho)$ and $r_1 = \sin(\rho)$ for some ρ. Set $\theta = \rho/2$, then $|\psi\rangle = \cos(\theta/2)e^{i\phi_0}|0\rangle + \sin(\theta/2)e^{i\phi_1}|1\rangle$, with $0 \leq \theta \leq \pi$, or equivalently

$$|\psi\rangle = e^{i\gamma}(\cos(\theta/2)|0\rangle + e^{i\varphi}\sin(\theta/2)|1\rangle),$$

with$\varphi = \phi_1 - \phi_0$ and $\gamma = \phi_0$, with $0 \leq \varphi \leq 2\pi$. The global **phase shift** $e^{i\gamma}$ is physically irrelevant (unobservable).

Bloch Sphere

$\cos(\theta/2)\,|0\rangle + e^{i\varphi}\sin(\theta/2)\,|1\rangle$



Linear Operators

A map $\mathbf{L} : \mathcal{V} \to \mathcal{W}$ between two vector spaces $\mathcal{V}$ and $\mathcal{W}$ is called a **linear** map if

1. $\mathbf{L}(x + y) = \mathbf{L}(x) + \mathbf{L}(y)$ and
2. $\mathbf{L}(\alpha x) = \alpha \mathbf{L}(x)$

for all $x, y \in \mathcal{V}$ and all $\alpha \in \mathbb{K}$ (e.g. $\mathbb{K} = \mathbb{C}$ or $\mathbb{R}$).

For $\mathcal{V} = \mathcal{W}$ we talk about a linear **operator** on $\mathcal{V}$.

Images of the Basis

Like vectors, we can represent a linear operator $\mathbf{L}$ via its "coordinates" as a **matrix**. Again these depend on the **particular basis** we use.

Specifying the image of the base vectors determines – by **linearity** – the operator (or in general a linear map) uniquely.

Suppose we know the images of the basis vectors $|0\rangle$ and $|1\rangle$

$$\begin{aligned} \mathbf{L}(|0\rangle) &= \alpha_{00}|0\rangle + \alpha_{01}|1\rangle \\ \mathbf{L}(|1\rangle) &= \alpha_{10}|0\rangle + \alpha_{11}|1\rangle \end{aligned}$$

then this is enough to know the α_{ij}'s to know what $\mathbf{L}$ is doing to all vectors (as they are representable as linear combinations of the basis vectors).

Matrices

Using a "mathematical" indexing (starting from 1 rather than 0) and using the first index to indicate a **row** position and the second for a **column** position we can identify the operator/map with a matrix:

$$\mathbf{L} = \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix}$$

The **application** of $\mathbf{L}$ to a general vector (qubit) then becomes a simple matrix multiplication:

$$\mathbf{L}(\begin{pmatrix} \alpha \\ \beta \end{pmatrix}) = \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha_{11}\alpha + \alpha_{12}\beta \\ \alpha_{21}\alpha + \alpha_{22}\beta \end{pmatrix}$$

Multiplications: $(\mathbf{L}_{ij})(x_i) = \sum_i \mathbf{L}_{ij} x_i$ and $(\mathbf{L}_{ij})(\mathbf{K}_{ki}) = \sum_i \mathbf{L}_{ij} \mathbf{K}_{ki}$

Transformations

We can define a linear map $\mathbf{B}$ which implements the base change $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$:

$$\mathbf{B} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Transforming the coordinates (x_i) in $\{|0\rangle, |1\rangle\}$ into coordinates (y_i) using $\{|+\rangle, |-\rangle\}$ can be obtained by matrix multiplication:

$$\mathbf{B}(x_i) = (y_i) \text{ and } \mathbf{B}^{-1}(y_i) = (x_i)$$

The matrix representation $\mathbf{L}$ of an operator using $\{|0\rangle, |1\rangle\}$ can be transformed into the representation $\mathbf{K}$ in $\{|+\rangle, |-\rangle\}$ via:

$$\mathbf{K} = \mathbf{B}\mathbf{L}\mathbf{B}^{-1}$$

Outer Product

Useful means for representing linear maps.
In the bra-ket notation the **outer product** is expressed by $|x\rangle\langle y|$.
Every orthonormal basis $\{|i\rangle\}$ satisfies the completeness relation $\sum_i |i\rangle\langle i| = \mathbf{I}$.
For the canonical basis of $\mathbb{C}^2$ we have $\mathbf{I} = |0\rangle\langle 0| + |1\rangle\langle 1|$; in fact,

$$\begin{aligned} (|0\rangle\langle 0| + |1\rangle\langle 1|)\,|\psi\rangle &= (|0\rangle\langle 0| + |1\rangle\langle 1|)(\alpha\,|0\rangle + \beta\,|1\rangle) \\ &= \alpha\,|0\rangle\langle 0||0\rangle + \alpha\,|1\rangle\langle 1||0\rangle + \\ &\quad\ \beta\,|0\rangle\langle 0||1\rangle + \beta\,|1\rangle\langle 1||1\rangle \\ &= \alpha\,|0\rangle + \beta\,|1\rangle \end{aligned}$$

Using coordinates, we have with $|x\rangle = (x_i)^T$ and $\langle y| = (y_j)$:

$$(|x\rangle\langle y|)_{ij} = x_i y_j \text{ e.g. } |0\rangle\langle 1| = \begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

Adjoint Operator

For a matrix $\mathbf{L} = (\mathbf{L}_{ij})$ its **transpose** matrix $\mathbf{L}^T$ is defined as

$$(\mathbf{L}^T_{ij}) = (\mathbf{L}_{ji})$$

the **conjugate** matrix $\mathbf{L}^*$ is defined by

$$(\mathbf{L}^*_{ij}) = (\mathbf{L}_{ij})^*$$

and the **adjoint** matrix $\mathbf{L}^\dagger$ is given via

$$(\mathbf{L}^\dagger_{ij}) = (\mathbf{L}^*_{ji}) \quad \text{or} \quad \mathbf{L}^\dagger = (\mathbf{L}^*)^T$$

Notation: In **mathematics** the adjoint operator is usually denoted by $\mathbf{L}^*$ and defined implicitly via:

$$\langle \mathbf{L}(x), y \rangle = \langle x, \mathbf{L}^*(y) \rangle \quad \text{or} \quad \left\langle \mathbf{L}^\dagger x | y \right\rangle = \langle x, \mathbf{L} y \rangle$$

Unitary Operators

A square matrix/operator $\mathbf{U}$ is called **unitary** if

$$\mathbf{U}^\dagger \mathbf{U} = \mathbf{I} = \mathbf{U}\mathbf{U}^\dagger$$

That means $\mathbf{U}$'s inverse is $\mathbf{U}^\dagger = \mathbf{U}^{-1}$. It also implies that $\mathbf{U}$ is **invertible** and the inverse is easy to compute.

The postulates of **Quantum Mechanics** require that the **time evolution** to a quantum state, e.g. a qubit, are implemented via a unitary operator (as long as there is no measurement).

The unitary evolution of an (isolated) quantum state/system is a mathematical consequence of being a solution of the Schrödinger equation for some Hamiltonian operator $\mathbf{H}$.

Unitary Operators

It is easy to check that a matrix $\mathbf{U}$ unitary iff its columns (or rows) form a orthonormal basis.

Theorem

A linear operator maps a qubit to a qubit (i.e. preserves normalized vectors) iff it is unitary.

Theorem

A matrix M is unitary iff it preserves all inner products:

$$\langle Mx, My \rangle = \langle x, y \rangle .$$

Quantum Gates

Basic 1-Qubit Operators

Pauli X-Gate $\quad \mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Pauli Y-Gate $\quad \mathbf{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$

Pauli Z-Gate $\quad \mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

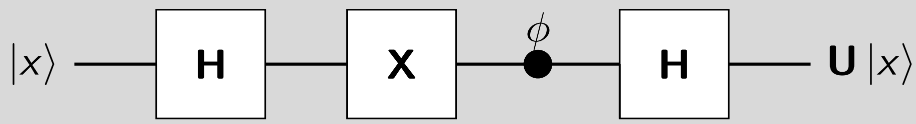
Hadamard Gate $\quad \mathbf{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

Phase Gate $\quad \mathbf{\Phi} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$

The Pauli-X gate is also often referred to as NOT gate.

Graphical "Notation"

The product (combination) of unitary operators results in a unitary operator, i.e. with $\mathbf{U}_1, \ldots, \mathbf{U}_n$ unitary, the product $\mathbf{U} = \mathbf{U}_n \ldots \mathbf{U}_1$ is also unitary (Note: $(\mathbf{LK})^\dagger = \mathbf{K}^\dagger \mathbf{L}^\dagger$).



Any unitary 2×2 matrix $\mathbf{U}$ can be expressed as

$$\mathbf{U} = \begin{pmatrix} e^{i(\alpha-\beta/2-\delta/2)} \cos\gamma/2 & e^{i(\alpha+\beta/2-\delta/2)} \sin\gamma/2 \\ -e^{i(\alpha-\beta/2+\delta/2)} \sin\gamma/2 & e^{i(\alpha+\beta/2+\delta/2)} \cos\gamma/2 \end{pmatrix}$$

where α, β, δ and γ are real numbers (angles).

Measurement Principle

The values α and β describing a qubit are called **probability amplitudes**. If we measure a qubit

$$|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

in the **computational basis** $\{|0\rangle, |1\rangle\}$ then we observe state $|0\rangle$ with probability $|\alpha|^2$ and $|1\rangle$ with probability $|\beta|^2$.

Furthermore, the state $|\phi\rangle$ changes: it **collapses** into state $|0\rangle$ with probability $|\alpha|^2$ or $|1\rangle$ with probability $|\beta|^2$, respectively.

Self Adjoint Operators

An operator $\mathbf{A}$ is called **self-adjoint** or **hermitean** iff

$$\mathbf{A} = \mathbf{A}^\dagger$$

The postulates of **Quantum Mechanics** require that a quantum **observable** A is represented by a self-adjoint operator $\mathbf{A}$.

Possible measurement results are **eigenvalues** λ_i of $\mathbf{A}$ defined as

$$\mathbf{A} |i\rangle = \lambda_i |i\rangle \quad \text{or} \quad \mathbf{A}\vec{a}_i = \lambda_i \vec{a}_i$$

Probability to observe λ_k in state $|x\rangle = \sum_i \alpha_i |i\rangle$ is

$$Pr(A = \lambda_k, |x\rangle) = |\alpha_k|^2$$

Spectrum

The set of eigen-values $\{\lambda_1, \lambda_2, \ldots\}$ of an operator $\mathbf{L}$ is called its **spectrum** $\sigma(\mathbf{L})$.

$$\sigma(\mathbf{L}) = \{\lambda \mid \lambda\mathbf{I} - \mathbf{L} \text{ is not invertible}\}$$

It is possible that for an eigen-value λ_i in the equation

$$\mathbf{L} |i\rangle = \lambda_i |i\rangle$$

we may have more than one eigen-vector $|i\rangle$, i.e. the dimension of the eigen-space $d(n) > 1$. We will not consider these **degenerate** cases here.

Terminology: "eigen" means "self" or "own" in German (cf Italian "auto-valore").

Projections

Projections
An operator $\mathbf{P}$ on $\mathbb{C}^n$ is called **projection** (or **idempotent**) iff

$$\mathbf{P}^2 = \mathbf{PP} = \mathbf{P}$$

Orthogonal Projection
An operator $\mathbf{P}$ on $\mathbb{C}^n$ is called **(orthogonal) projection** iff

$$\mathbf{P}^2 = \mathbf{P} = \mathbf{P}^\dagger$$

We say that an (orthogonal) projection $\mathbf{P}$ projects **onto** its image space $\mathbf{P}(\mathbb{C}^n)$, which is always a linear sub-spaces of $\mathbb{C}^n$.

Spectral Theorem

In the bra-ket notation we can represent a projection onto the sub-space generated by $|x\rangle$ by the outer product $\mathbf{P}_x = |x\rangle\langle x|$.

Theorem

A self-adjoint operator $\mathbf{A}$ (on a finite dimensional Hilbert space, e.g. $\mathbb{C}^n$) can be represented uniquely as a linear combination

$$\mathbf{A} = \sum_i \lambda_i \mathbf{P}_i$$

with $\lambda_i \in \mathbb{R}$ and $\mathbf{P}_i$ the (orthogonal) projection onto the eigen-space generated by the eigen-vector $|i\rangle$:

$$\mathbf{P}_i = |i\rangle\langle i|$$

In the degenerate case we had to consider: $P_i = \sum_{j=1}^{d(n)} |i_j\rangle\langle i_j|$.

Measurement Process

If we perform a measurement of the observable represented by:

$$\mathbf{A} = \sum_i \lambda_i |i\rangle\langle i|$$

with eigen-values λ_i and eigen-vectors $|i\rangle$ in a state $|x\rangle$ we have to decompose the state according to the observable, i.e.

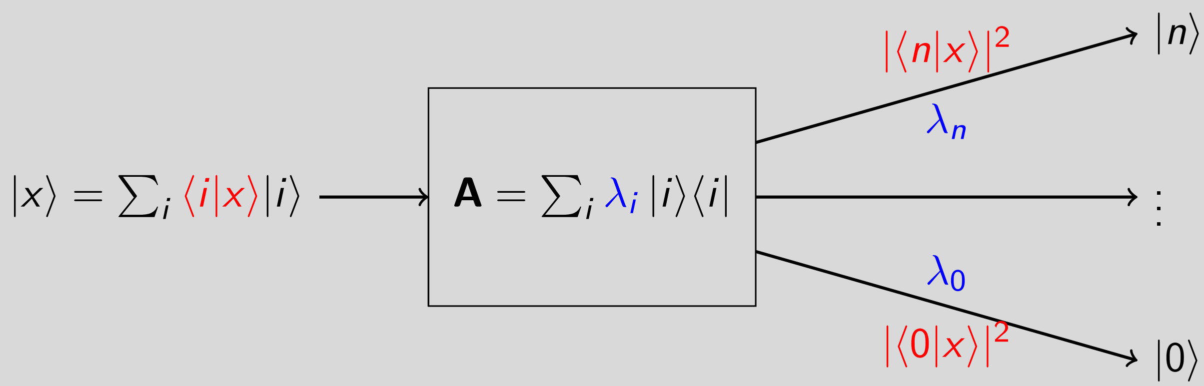
$$|x\rangle = \sum_i \mathbf{P}_i |x\rangle = \sum_i |i\rangle\langle i|x\rangle = \sum_i \langle i|x\rangle |i\rangle = \sum_i \alpha_i |i\rangle$$

With probability $|\alpha_i|^2 = |\langle i|x\rangle|^2$ two things happen

- The measurement instrument will the **display** λ_i.
- The state $|x\rangle$ **collapses** to $|i\rangle$.

Do-It-Yourself Observable

We can take any (orthonormal) basis $\{|i\rangle\}_0^n$ of $\mathbb{C}^{n+1}$ to act as **computational basis**. We are free to choose (different) measurement results λ_i to indicate different states in $\{|i\rangle\}$.



The "display" values λ_i are **essential** for physicists, in a quantum computing context they are just **side-effects**.

Reversibility

Quantum Dynamics
For unitary transformations describing qubit dynamics:

$$\mathbf{U}^\dagger = \mathbf{U}^{-1}$$

The quantum dynamics is **invertible** or **reversible**

Quantum Measurement
For projection operators involved in quantum measurement:

$$\mathbf{P}^\dagger \neq \mathbf{P}^{-1}$$

The quantum measurement is not **reversible**. However

$$\mathbf{P}^2 = \mathbf{P}$$

The quantum measurement is **idempotent**.

Beyond Qubits

Operations on a single Qubit are nice and interesting but don't give us much computational power.

We need to consider "larger" computational states which contain more information.

- Quantum Systems with a larger number of freedoms.
- Quantum Registers as a combination of several Qubits.

Though it might one day be physically more realistic/cheaper to built quantum devices based on not just binary basic states, even then it will be necessary to combine these larger "Qubits".

Multi Qubit State

We encountered already the state space of a single qubit with $B = \{0, 1\}$ but also with $B = \{+, -\}$.

The state space of a **two qubit** system is given by

$$\mathcal{V}(\{0,1\} \times \{0,1\}) \text{ or } \mathcal{V}(\{+,-\} \times \{+,-\})$$

i.e. the base vectors are (in the standard base):

$$B = \{(0,0),(1,0),(0,1),(1,1)\}$$

or we use a "short-hand" notation $B = \{00, 01, 10, 11\}$

In order to understand the relation between $\mathcal{V}(B)$ and $\mathcal{V}(B \times B)$ and in general $\mathcal{V}(B^n)$ we need to consider the **tensor product**.

Tensor Product

Given a $n \times m$ **matrix** $\mathbf{A}$ and a $k \times l$ matrix $\mathbf{B}$:

$$\mathbf{A} = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nm} \end{pmatrix} \quad \mathbf{B} = \begin{pmatrix} b_{11} & \dots & b_{1l} \\ \vdots & \ddots & \vdots \\ b_{k1} & \dots & b_{kl} \end{pmatrix}$$

The **tensor** or **Kronecker product** $\mathbf{A} \otimes \mathbf{B}$ is a $nk \times ml$ matrix:

$$\mathbf{A} \otimes \mathbf{B} = \begin{pmatrix} a_{11}\mathbf{B} & \dots & a_{1m}\mathbf{B} \\ \vdots & \ddots & \vdots \\ a_{n1}\mathbf{B} & \dots & a_{nm}\mathbf{B} \end{pmatrix}$$

Special cases are **square matrices** ($n = m$ and $k = l$) and **vectors** (row $n = k = 1$, column $m = l = 1$).

Tensor Product of Vectors

The tensor product of (ket) vectors fulfills a number of nice algebraic properties, such as

1. The **bilinearity** property:

$$(\alpha v + \alpha' v') \otimes (\beta w + \beta' w') = \\ = \alpha\beta(v \otimes w) + \alpha\beta'(v \otimes w') + \alpha'\beta(v' \otimes w) + \alpha'\beta'(v' \otimes w')$$

   with $\alpha, \alpha', \beta, \beta' \in \mathbb{C}$, and $v, v' \in \mathbb{C}^k$, $w, w' \in \mathbb{C}^l$.

2. For $v, v' \in \mathbb{C}^k$ and $w, w' \in \mathbb{C}^l$ we have:

$$\left\langle v \otimes w | v' \otimes w' \right\rangle = \left\langle v | v' \right\rangle \left\langle w | w' \right\rangle$$

3. We denote by $b_i^m \in B_n \subseteq \mathbb{C}^m$ the i'th basis vector in $\mathbb{C}^m$ then

$$b_i^k \otimes b_j^l = b_{(i-1)l+j}^{kl}$$

Tensor Product of Matrices

For the tensor product of square matrices we also have:

1. The **bilinearity** property:

$$(\alpha \mathbf{M} + \alpha' \mathbf{M}') \otimes (\beta \mathbf{N} + \beta' \mathbf{N}') = \\ = \alpha\beta(\mathbf{M} \otimes \mathbf{N}) + \alpha\beta'(\mathbf{M} \otimes \mathbf{N}') + \alpha'\beta(\mathbf{M}' \otimes \mathbf{N}) + \alpha'\beta'(\mathbf{M}' \otimes \mathbf{N}')$$

   $\alpha, \alpha', \beta, \beta' \in \mathbb{C}$, $\mathbf{M}, \mathbf{M}'$ $m \times m$ matrices $\mathbf{N}, \mathbf{N}'$ $n \times n$ matrices.

2. We have, with $v \in \mathbb{C}^m$ and $w \in \mathbb{C}^n$:

$$(\mathbf{M} \otimes \mathbf{N})(v \otimes w) = (\mathbf{M}v) \otimes (\mathbf{N}w) \\ (\mathbf{M} \otimes \mathbf{N})(\mathbf{M}' \otimes \mathbf{N}') = (\mathbf{M}\mathbf{M}') \otimes (\mathbf{N}\mathbf{N}')$$

3. If $\mathbf{M}$ and $\mathbf{N}$ are unitary (or invertible) so is $\mathbf{M} \otimes \mathbf{N}$, and:

$$(\mathbf{M} \otimes \mathbf{N})^T = \mathbf{M}^T \otimes \mathbf{N}^T \quad \text{and} \quad (\mathbf{M} \otimes \mathbf{N})^\dagger = \mathbf{M}^\dagger \otimes \mathbf{N}^\dagger$$

The Two Qubit States

Given two Hilbert spaces $\mathcal{H}_1$ with basis B_1 and $\mathcal{H}_2$ with basis B_2 we can define the tensor product of **spaces** as

$$\mathcal{H}_1 \otimes \mathcal{H}_2 = \mathcal{V}(\{b_i \otimes b_j \mid b_i \in B_1, b_j \in B_2\})$$

Using the notation $|i\rangle \otimes |j\rangle = |i\rangle |j\rangle = |ij\rangle$ the standard base of the state space of a two qubit system $\mathbb{C}^4 = \mathbb{C}^2 \otimes \mathbb{C}^2$ are:

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

Use lexigographical order for enumeration of the base in the n-qubit state space $\mathbb{C}^{2^n}$ and represent them also using a decimal notation, e.g. $|00\rangle \equiv |0\rangle$, $|01\rangle \equiv |1\rangle$, $|10\rangle \equiv |2\rangle$, and $|11\rangle \equiv |3\rangle$.

Entanglement

The important relation between $\mathcal{V}(B)$, e.g. $\mathcal{V}(\{0,1\})$, and $\mathcal{V}(B^n)$, e.g. $\mathcal{V}(\{0,1\}^n)$ is given by $\mathcal{V}(B^n) = (\mathcal{V}(B))^{\otimes n}$, i.e.:

$$\mathcal{V}(B \times B \times \ldots \times B) = \mathcal{V}(B) \otimes \mathcal{V}(B) \otimes \ldots \otimes \mathcal{V}(B)$$

Every n qubit state in $\mathbb{C}^{2^n}$ can represented as a linear combination of the base vectors $|0\ldots00\rangle, |0\ldots01\rangle, |0\ldots10\rangle, \ldots, |1\ldots11\rangle$ or decimal $|0\rangle, |1\rangle, |2\rangle, \ldots, \ldots, |2^n - 1\rangle$.

A two-qubit quantum state $|\psi\rangle \in \mathbb{C}^{2^2}$ is said to be **separable** iff there exist two single-qubit states $|\psi_1\rangle$ and $|\psi_2\rangle$ in $\mathbb{C}^2$ such that

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$$

If $|\psi\rangle$ is not separable then we say that $|\psi\rangle$ is **entangled**.