Quantum Computation (CO484)
Quantum States and Evolution

Herbert Wiklicky

herbert@doc.ic.ac.uk
Autumn 2017

Quantum Postulates

- The state of an (isolated) quantum system is represented by a (normalised) vector in a complex Hilbert space $\mathcal{H}$.
- An observable is represented by a self-adjoint matrix (operator) $A$ acting on the Hilbert space $\mathcal{H}$.
- The expected result (average) when measuring observable $A$ of a system in state $|x\rangle \in \mathcal{H}$ is given by:
  \[
  \langle A \rangle_x = \langle x | A | x \rangle = \langle x | Ax \rangle
  \]
- The only possible results are eigen-values $\lambda_i$ of $A$.
- The probability of measuring $\lambda_n$ in state $|x\rangle$ is given by:
  \[
  Pr(A = \lambda_n | x) = \langle x | P_n | x \rangle = \langle x | P_n x \rangle
  \]
  with $P_n = |\lambda_n\rangle\langle\lambda_n|$ the orthogonal projection onto the space generated by eigen-vector $|\lambda_n\rangle = |n\rangle$ of $A$. 

Complex Numbers

Quantitative information, e.g. measurement results, is usually represented by real numbers \( \mathbb{R} \). For quantum systems we need to consider also complex numbers \( \mathbb{C} \).

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

\[
z = x + iy
\]

with \( i^2 = -1 \) or \( i = \sqrt{-1} \). The complex conjugate of a complex number \( z = x + iy \in \mathbb{C} \) is:

\[
z^* = \overline{z} = x + iy = x - iy = z^\dagger
\]

Hauptsatz of Algebra

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

Polar Coordinates

One can represent numbers \( z \in \mathbb{C} \) using the complex plane.

Conversion:

\[
x = r \cdot \cos(\phi) \quad y = r \cdot \sin(\phi)
\]

\[
r = \sqrt{x^2 + y^2} \quad \phi = \arctan\left(\frac{y}{x}\right)
\]

Another representation:

\[
(r, \phi) = r \cdot e^{i\phi} \quad e^{i\phi} = \cos(\phi) + i \sin(\phi),
\]
Computational Quantum States
Consider a simple systems with two degrees of freedom.

\[ |0\rangle \quad |1\rangle \]

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

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

where \( \alpha \) and \( \beta \) 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.

\[ \| |\psi\rangle \| = \langle \psi | \psi \rangle = 1. \]

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:

Scalar Product \( \cdot : \mathbb{K} \times \mathcal{V} \mapsto \mathcal{V} \)
Vector Addition \( .+ : \mathcal{V} \times \mathcal{V} \mapsto \mathcal{V} \)

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 $\mathbb{C}^n$).

$\vec{x} = (x_1, x_2, x_3, \ldots, x_n)$ represents $x = \sum_{i=1}^{n} x_i b_i$

$\vec{y} = (y_1, y_2, y_3, \ldots, y_n)$ represents $y = \sum_{i=1}^{n} y_i b_i$

Finite dimensional vectors can be represented as tuples via their coordinates with respect to a base $\{b_i\}_{i=1}^{n}$.

$\alpha \vec{x} = (\alpha x_1, \alpha x_2, \alpha x_3, \ldots, \alpha x_n)$

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

Hilbert Spaces

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. $\langle x + y, z \rangle = \langle x, z \rangle + \langle y, z \rangle$
5. $\langle x, y \rangle = \overline{\langle y, x \rangle}$

The function $\langle ., . \rangle$ is called an inner product on $\mathcal{H}$. 
Caveat: Linear in first or second argument?

Mathematical Convention:

\[ \langle \alpha x, y \rangle = \alpha \langle x, y \rangle \]

Physical Convention:

\[ \langle x \mid \alpha y \rangle = \alpha \langle x \mid y \rangle \]

In mathematics we have:

\[ \langle x, \alpha y \rangle = \overline{\alpha} \overline{\langle y, x \rangle} = \overline{\alpha} \bar{x} = \overline{\alpha} \langle x, y \rangle \]

For physicists it is simply:

\[ \langle x \mid \alpha y \rangle = \alpha \langle x \mid y \rangle \]

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 set of vectors with:

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

Theorem

*For a Hilbert space there exists an orthonormal basis \( \{b\} \). The representation of each vector is unique:*

\[ x = \sum_i x_i b_i = \sum_i \langle x, b_i \rangle b_i \]
**The Finite-Dimensional Hilbert Spaces \( \mathbb{C}^n \)**

We represent vectors and their transpose using coordinates:

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

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

\[
\vec{x}^\dagger = (\bar{x}_1, \ldots, \bar{x}_n)^T = (x_1^*, \ldots, x_n^*)^T
\]

The inner product is then represented by:

\[
\langle \vec{y}, \vec{x} \rangle = \sum_i \bar{y}_i x_i = \sum_i y_i^* x_i
\]

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

**Dual and Adjoint States**

A linear functional on a vector space \( \mathcal{V} \) is a map \( f : \mathcal{V} \to \mathbb{K} \) such that (i) \( f(x + y) = f(x) + f(y) \) and (ii) \( f(\alpha x) = \alpha f(x) \) for all \( x, y \in \mathcal{V}, \alpha \in \mathbb{K} \). The space of all linear functionals on \( \mathcal{V} \) form the dual space \( \mathcal{V}^* \).

**Theorem (Riesz Representation Theorem)**

Every linear functional \( f : \mathcal{H} \to \mathbb{C} \) on a Hilbert space \( \mathcal{H} \) can be represented by a vector \( \vec{y}_f \) in \( \mathcal{H} \), such that

\[
f(x) = \langle \vec{y}_f, x \rangle = f_{\vec{y}}(x)
\]

Dual Hilbert spaces \( \mathcal{H}^* \) are isomorphic to the original Hilbert space \( \mathcal{H}^* \); in particular we have: \( (\mathbb{C}^n)^* = \mathbb{C}^n \).

We represent vectors or ket-vectors as column vectors; and functionals, dual vector or bra-vectors as row vectors.
Dirac Notation and Einstein Convention

We will use throughout P.A.M. Dirac’s bra-(c)-ket notation:

\[ \langle x_i, y_j \rangle = \langle \vec{x}_i, \vec{y}_j \rangle \] denoted as \( \langle x_i | y_j \rangle = \langle i | j \rangle \)

We will enumerate the (eigen-)base vectors (of an operator):

\[ \vec{b}_i = b_i \text{ or } \vec{e}_i = e_i \] are denoted by \( |i\rangle \)

but we may need also to specify the coordinates of a vector:

- Ket-Vectors (column): \( |x\rangle = (x_j)_{j=1}^n \) in \( \mathbb{C}^n \).
- Bra-Vectors (row): \( \langle x| = (x^l)_j^1 \) in \( (\mathbb{C}^n)^* = \mathbb{C}^n \).

A. Einstein: If in an expression there are matching sub- and super-scripts then this implicitly indicates a summation,

\[ \bar{x}_i y^i = \sum_i \bar{x}_i y^i = \langle \vec{x}, \vec{y} \rangle \text{ and } x_i y^i* = \sum_i x_i \bar{y}^i = \langle \vec{x} | \vec{y} \rangle \]

Qubit

The postulates of Quantum Mechanics simply require that a computational quantum state is represented by a normalised vector in \( \mathbb{C}^n \). A qubit is a two-dimensional quantum state in \( \mathbb{C}^2 \)

We represent the coordinates of a qubit (state) or ket-vector as a column vector:

\[ |\psi\rangle = \left( \begin{array}{c} \alpha \\ \beta \end{array} \right) = \alpha \left( \begin{array}{c} 1 \\ 0 \end{array} \right) + \beta \left( \begin{array}{c} 0 \\ 1 \end{array} \right) = \alpha |0\rangle + \beta |1\rangle \]

with respect to the (orthonormal) basis \( \{ |0\rangle, |1\rangle \} \), i.e. the so-called standard base:

\[ |0\rangle = \left( \begin{array}{c} 1 \\ 0 \end{array} \right) \text{ and } |1\rangle = \left( \begin{array}{c} 0 \\ 1 \end{array} \right) \]
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 $\rho$. Set $\theta/2 = \rho$, 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

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

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 [*]

$$\cos(\theta/2) |0\rangle + e^{i\varphi} \sin(\theta/2) |1\rangle$$
Change of Basis
We can represent (the coordinates of) any vector in $\mathbb{C}^n$ with respect to any basis we like.

For example, we can consider for qubits in $\mathbb{C}^2$ the (alternative) orthonormal basis:

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

and thus, vice versa:

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

A qubit is therefore represented in the two bases as:

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

Linear Operators

Arguably, the best understood and controlled type of functions or maps between two vector spaces $\mathcal{V}$ and $\mathcal{W}$ are those preserving their basic algebraic structure.

Definition
A map $T : \mathcal{V} \rightarrow \mathcal{W}$ between two vector spaces $\mathcal{V}$ and $\mathcal{W}$ is called a linear map if

1. $T(x + y) = T(x) + T(y)$ and
2. $T(\alpha x) = \alpha T(x)$

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 $T$ 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 $|1\rangle$

\[
T(|0\rangle) = T_{00}|0\rangle + T_{01}|1\rangle \\
T(|1\rangle) = T_{10}|0\rangle + T_{11}|1\rangle
\]

then this is enough to know the $T_{ij}$’s to know what $T$ 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 ten 0), using the first index to indicate a row position and second for a column position, we can identify $T$ with a matrix:

\[
T = \begin{pmatrix}
T_{11} & T_{12} \\
T_{21} & T_{22}
\end{pmatrix} = (T_{ij})_{i,j=1}^{n} = (T_{ij})
\]

The application of $T$ to a general vector (qubit) then becomes a simple matrix (pre-)multiplication:

\[
T \left( \begin{pmatrix}
\alpha \\
\beta
\end{pmatrix} \right) = \begin{pmatrix}
T_{11} & T_{12} \\
T_{21} & T_{22}
\end{pmatrix} \begin{pmatrix}
\alpha \\
\beta
\end{pmatrix} = \begin{pmatrix}
T_{11}\alpha + T_{12}\beta \\
T_{21}\alpha + T_{22}\beta
\end{pmatrix}
\]

One can also express this, for $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ also as:

$T(|\psi\rangle) = T(\alpha|0\rangle + \beta|1\rangle) = \alpha T(|0\rangle) + \beta T(|1\rangle) = T |\psi\rangle$
Matrix Multiplications

The application of a linear operator $T$ (represented by a matrix) to a vector $x$ (represented via its coordinates) becomes:

$$T(x) = Tx = (T_{ij})(x_i) = \sum_i T_{ij}x_i$$

The standard convention is pre-multiplication so as the sequence is the same as with application.

The composition of linear operators $T$ and $S$ becomes also a matrix/matrix pre-multiplications:

$$T \circ S = TS = (T_{ij})(S_{ki}) = \sum_i T_{ij}S_{ki}$$

Some authors use the more “computational” pre-multiplication.

Finite-dimensional linear operators (matrices) form a vector space and with the multiplication a (linear) algebra. Adding the adjoint operation (see below) turns this into a $C^*$-algebra.

Transformations

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

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

Transforming the coordinates $(x_i)$ with respect to $\{|0\rangle, |1\rangle\}$ into coordinates $(y_i)$ using $\{|+, |\rangle\}$ can be obtained by:

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

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

$$S = BTB^{-1}$$

Problem: It is not easy to compute inverse $B^{-1}$, defined on implicitly by $BB^{-1} = B^{-1}B = I$ the identity (existence?!).
Adjoint Operator
For a matrix \( \mathbf{T} = (T_{ij}) \) its transpose matrix \( \mathbf{T}^T \) is defined as
\[
\mathbf{T}^T = (T_{ij}) = (T_{ji})
\]
the conjugate matrix \( \mathbf{T}^* \) is defined by
\[
\mathbf{T}^* = (T_{ij}^*) = (T_{ji})^* = \overline{(T_{ji})}
\]
and the adjoint matrix \( \mathbf{T}^\dagger \) is given via
\[
\mathbf{T}^\dagger = (T_{ij}^\dagger) = (T_{ji}^*) \quad \text{or} \quad \mathbf{T}^\dagger = (\mathbf{T}^*)^T = (\mathbf{T}^T)^*
\]
Note that \( (\mathbf{T}\mathbf{S})^T = \mathbf{S}^T\mathbf{T}^T \) and thus \( (\mathbf{T}\mathbf{S})^\dagger = \mathbf{S}^\dagger\mathbf{T}^\dagger \).

In mathematics the adjoint operator is usually denoted by \( \mathbf{T}^* \) (cf. conjugate in physics) and defined implicitly via:
\[
\langle \mathbf{T}(\mathbf{x}), \mathbf{y} \rangle = \langle \mathbf{x}, \mathbf{T}^*(\mathbf{y}) \rangle \quad \text{or} \quad \langle \mathbf{T}^\dagger \mathbf{x} | \mathbf{y} \rangle = \langle \mathbf{x} | \mathbf{T} \mathbf{y} \rangle
\]

Adjoint Vectors
Bra and ket vectors are also related using the adjoint:
\[
|\mathbf{x}\rangle^\dagger = \langle \mathbf{x} |
\]
or using their coordinates:
\[
(x_i)^\dagger = \left( \begin{array}{c} x_1 \\ \vdots \\ x_n \end{array} \right)^\dagger = \left( \begin{array}{c} \bar{x}_1 \\ \cdots \\ \bar{x}_n \end{array} \right) = (\bar{x}^\dagger)
\]
The adjoint operator specifies the effect on dual vectors:
\[
(\mathbf{T} |\mathbf{x}\rangle)^\dagger = |\mathbf{x}\rangle^\dagger \mathbf{T}^\dagger = \langle \mathbf{x} | \mathbf{T}^\dagger
\]
Unitary Operators

A square matrix/operator $U$ is called unitary if

$$U^\dagger U = I = UU^\dagger$$

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

Quantum Mechanics requires that the dynamics or time evolution of a quantum state, e.g. qubit, is 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 $H$.

Properties of Unitary Operators

Unitary operators generalise in some sense permutations (in fact every permutation of base vectors gives rise to a simple unitary map). They can also be seen as generalised rotations.

Unitary operators also preserve the “geometry” of a Hilbert space, i.e. they preserve the inner product:

$$\langle x | U^\dagger U | y \rangle = \langle x | y \rangle .$$

Any single qubit operation, i.e. unitary $2 \times 2$ matrix $U$ can be expressed as via 4 (real) parameters:

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

where $\alpha$, $\beta$, $\delta$ and $\gamma$ are real numbers.
Basic 1-Qubit Operators

Pauli X-Gate
\[ X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \]

Pauli Y-Gate
\[ Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \]

Pauli Z-Gate
\[ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \]

Hadamard Gate
\[ H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \]

Phase Gate
\[ \Phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix} \]

The Pauli-X gate is often referred to as NOT gate. Note that the notation for Hamiltonian and Hadamard gate are both \( H \).

Graphical “Notation”

The product (combination) of unitary operators results in a unitary operator, i.e. with \( U_1, \ldots, U_n \) unitary, the product \( U = U_n \ldots U_1 \) is also unitary (Note: \((TS)^\dagger = S^\dagger T^\dagger\)).

A simple example: \(|y\rangle = HH|x\rangle\) or \(|x\rangle; \quad H; \quad H = |y\rangle\):

\[ |x\rangle \quad H \quad H \quad |y\rangle \equiv |x\rangle \quad I \quad |y\rangle = |x\rangle \]

because \( H^2 = I \), i.e.
\[ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \]