Quantum Systems

(Lecture 3: The principles of quantum computation)

Luís Soares Barbosa

Universidade do Minho

The principles

If quantum computation explores the laws of quantum mechanics as computational resources, principles of the former are directly derived from the postulates of the latter.

- The state space postulate
- The state evolution postulate
- The state composition postulate
- The state measurement postulate

The state space postulate

Postulate 1

The state space of a quantum system is described by a unit vector in a Hilbert space

- In practice, with finite resources, one cannot distinguish between a continuous state space from a discrete one with arbitrarily small minimum spacing between adjacente locations.
- One may, then, restrict to finite-dimensional (complex) Hilbert spaces.

The state space postulate

A qubit is encoded in a 2-dimensional such space as a linear combination (superposition) of basis vectors with complex coefficients:

$$|\phi\rangle \;=\; \alpha|0\rangle + \beta|1\rangle \;=\; \begin{bmatrix}\alpha \\ \beta\end{bmatrix}$$

obeying the normalization constraint

$$\| \alpha \|^2 + \| \beta \|^2 = \; 1$$

which enforces quantum states to be represented by unit vectors (to ensure compatibility with the measurement postulate)

Recall that a complex amplitude α can always be presented as a phase factor $e^{i\theta}$, where θ is know the phase

The state space of a qubit

Representation redundancy:

qubit state space $\neq$ complex vector space used for representation

Global phase

Unit vectors equivalent up to multiplication by a complex number of modulus one, i.e. a phase $e^{i\theta}$, represent the same state.

Let

$$|v\rangle = \alpha|u\rangle + \beta|u'\rangle$$

$$\| e^{i\theta}\alpha \|^2 = (\overline{e^{i\theta}\alpha})(e^{i\theta}\alpha) = (e^{-i\theta}\overline{\alpha})(e^{i\theta}\alpha) = \overline{\alpha}\alpha = \| \alpha \|^2$$

and similarly for β.

As the probabilities $\| \alpha \|^2$ and $\| \beta \|^2$ are the only measurable quantities, the global phase has no physical meaning.

The state space of a qubit

Relative phase

It is a measure of the angle between the two complex numbers.
Thus, it cannot be discarded!

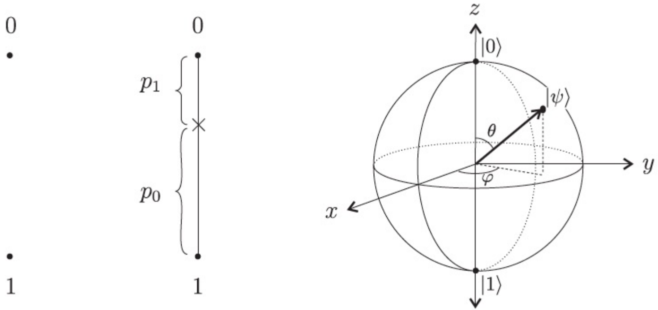
Those are different states

$$\frac{1}{\sqrt{2}}(|u\rangle + |u'\rangle) \quad \frac{1}{\sqrt{2}}(|u\rangle - |u'\rangle) \quad \frac{1}{\sqrt{2}}(e^{i\theta}|u\rangle + |u'\rangle)$$

...

The Bloch sphere

Deterministic, probabilistic and quantum bits



(from [Kaeys *et al*, 2007])

The Bloch sphere

The state of a quantum bit is described by a complex unit vector in a 2-dim Hilbert space, which, up to a physically irrelevant global phase factor, can be written as

$$|\psi\rangle = \underbrace{\cos\frac{\theta}{2}}_{\alpha}|0\rangle + \underbrace{e^{i\varphi}\sin\frac{\theta}{2}}_{\beta}|1\rangle$$

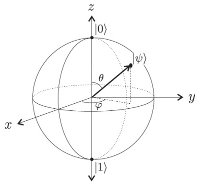
where $0 \leq \theta \leq \pi$, $0 \leq \varphi \leq 2\pi$, and depicted as a point on the surface of a 3-dim Bloch sphere, defined by θ and φ.
The Bloch vector $|\psi\rangle$ has

- Spherical coordinates:
  $x = \rho \sin\theta \cos\varphi \quad y = \rho \sin\theta \sin\varphi \quad = \quad z = \rho\cos\theta$
- Measurement probabilities:

$$\|\alpha\|^2 = \left(\cos\frac{\theta}{2}\right) \quad = \quad \frac{1}{2} + \frac{1}{2}\cos\theta$$

$$\|\beta\|^2 = \left(\sin\frac{\theta}{2}\right) \quad = \quad \frac{1}{2} - \frac{1}{2}\cos\theta$$

The Bloch sphere



- The poles represent the classical bits. In general, orthogonal states correspond to antipodal points and every diameter to a basis for the single-qubit state space.
- Once measured a qubit collapses to one of the two poles. Which pole depends exactly on the arrow direction: The angle θ measures that probability: If the arrow points at the equator, there is 50-50 chance to collapse to any of the two poles.
- Rotating a vector wrt the z-axis results into a phase change (φ), and does not affect which state the arrow will collapse to, when measured.

The Bloch sphere

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

Express $|\psi\rangle$ in polar form

$$|\psi\rangle = \rho_1 e^{i\varphi_1}|0\rangle + \rho_2 e^{i\varphi_2}|1\rangle$$

and eliminate one of the four real parameters multiplying by $e^{-i\varphi_1}$

$$|\psi\rangle = \rho_1|0\rangle + \rho_2 e^{i(\varphi_2 - \varphi_1)}|1\rangle = \rho_1|0\rangle + \rho_2 e^{i\varphi}|1\rangle$$

making $\varphi = \varphi_2 - \varphi_1$.

Switch back the coefficient of $|1\rangle$ to Cartesian coordinates and compute the normalization constraint

$$\| \rho_1 \|^2 + \| a + ib \|^2 = \| \rho_1 \|^2 + (a - ib)(a + ib) \; = \| \rho_1 \|^2 + a^2 + b^2 \; = \; 1$$

which is the equation of a unit sphere in Real 3-dim space with Cartesian coordinates: (a, b, ρ_1).

The Bloch sphere

Back to polar,

$$
\begin{aligned}
x =& \rho \sin\theta \cos\varphi \\
y =& \rho \sin\theta \sin\varphi \\
z =& \rho \cos\theta
\end{aligned}
$$

So, recalling that $\rho = 1$,

$$
\begin{aligned}
|\psi\rangle &= z|0\rangle + (a + ib)|1\rangle \\
&= \cos\theta|0\rangle + \sin\theta(\cos\varphi - i\sin\varphi)|1\rangle \\
&= \cos\theta|0\rangle + e^{i\varphi}\sin\theta|1\rangle
\end{aligned}
$$

which, with two parameters, defines a point in the sphere's surface.

The Bloch sphere

Actually, one may just focus on the upper hemisphere ($0 \leq \theta' \leq \frac{\pi}{2}$) as opposite points in the lower one differ only by a phase factor of -1:

Let $|\psi'\rangle$ be the opposite point on the sphere with polar coordinates $(1, \pi - \theta', \varphi + \pi)$

$$\begin{aligned}
|\psi'\rangle &= \cos(\pi - \theta')|0\rangle + e^{i(\varphi+\pi)} \sin(\pi - \theta')|1\rangle \\
&= -\cos\theta'|0\rangle + e^{i\varphi} e^{i\pi} \sin\theta'|1\rangle \\
&= -\cos\theta'|0\rangle + e^{i\varphi} \sin\theta'|1\rangle \\
&= -|\psi\rangle
\end{aligned}$$

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi} \sin\frac{\theta}{2}|1\rangle$$

where $0 \leq \theta \leq \pi$, $0 \leq \varphi \leq 2\pi$

$\mathcal{C}$ compactification

The Bloch sphere is a bijective correspondence between qubits and point in the space; formally, a latitude (ϕ) and longitude (θ) based representation of the state space of a qubit in the complex projective space of dimension 1.

Alternative: $\mathcal{C}$ compactification

Represents a qubit by a complex number in $\mathcal{C} \cup \{\perp\}$ through a correspondence ξ:

$$\xi = \alpha|0\rangle + \beta|1\rangle \mapsto b/a \quad \text{and} \quad |1\rangle \mapsto \perp$$

$$\xi^{-1} = \gamma \mapsto \frac{1}{\sqrt{1+\|\gamma\|^2}}|0\rangle + \frac{\gamma}{\sqrt{1+\|\gamma\|^2}}|1\rangle \quad \text{and} \quad \perp \mapsto |1\rangle$$

The state evolution postulate

Postulate 2

The evolution over time of the state of a closed quantum system is described by a unitary operator.

The evolution is linear

$$U\left(\sum_j \alpha_j |v_j\rangle\right) = \sum_j \alpha_j U(|v_j\rangle)$$

and preserves the normalization constraint

$$\text{If } \sum_j \alpha_j U(|v_j\rangle) = \sum_j \alpha'_j |v_j\rangle \text{ then } \sum_j \| \alpha'_j \|^2 = 1$$

Unitarity

Unitary

This entails a condition on valid quantum operators: they must preserve the inner product, i.e.

$$(U|v\rangle, U|w\rangle) = \langle v|U^\dagger U|w\rangle = \langle v|w\rangle$$

which is the case iff U is unitary

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

- Preserving the inner product means that a unitary operator maps orthonormal bases to orthonormal bases.
- Conversely, any operator with this property is unitary.
- If given in matrix form, being unitary means that the set of columns of its matrix representation are orthonormal (because the jth column is the image of $U|j\rangle$). Equivalently, rows are orthonormal (why?)

Unitarity

Unitarity is the only constraint on quantum operators: Any unitary matrix specifies a valid quantum operator.

This means that there are many non-trivial operators on a single qubit (in contrast with the classical case where the only non-trivial operation on a bit is complement.

Finally, because the inverse of a unitary matrix is also a unitary matrix, a quantum operator can always be inverted by another quantum operator

$\boxed{\text{Unitary transformations are reversible}}$

The state evolution postulate

Examples: The Pauli operators

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

- Operators X, Y and Z correspond to rotations in the Bloch sphere along the x, y and z axis, respectively.
- Any 1-qubit unitary operator can be expressed as a linear combination of Pauli operators.

The no-cloning theorem

Linearity implies that quantum states cannot be cloned

Let $U(|a\rangle|0\rangle) = |a\rangle|a\rangle$ be a 2-qubit operator and $|c\rangle = \frac{1}{\sqrt{2}}(|a\rangle + |b\rangle)$ for $|a\rangle$, $|b\rangle$ orthogonal. Then,

$$
\begin{aligned}
U(|c\rangle|0\rangle) &= \frac{1}{\sqrt{2}}(U(|a\rangle|0\rangle) + U(|b\rangle|0\rangle)) \\
&= \frac{1}{\sqrt{2}}(|a\rangle|a\rangle + |b\rangle|b\rangle) \\
&\neq \frac{1}{\sqrt{2}}(|a\rangle|a\rangle + |a\rangle|b\rangle + |b\rangle|a\rangle + |b\rangle|b\rangle) \\
&= |c\rangle|c\rangle \\
&= U(|c\rangle|0\rangle)
\end{aligned}
$$

This, however, does not preclude the construction of a known quantum state from a known quantum state.

Building larger states from smaller

Operator U in the no-cloning theorem acts on a 2-dimensional state, i.e. over the composition of two qubits.

$\boxed{\text{What does composition mean?}}$

Postulate 3

The state space of a combined quantum system is the tensor product $V \otimes W$ of the state spaces V and W of its components.

Composing classical states

State spaces in a classical system combine through direct sum: $\oplus$

$$\boxed{n\ m\text{-dimensional vectors} \rightsquigarrow \text{a vector in } mn\text{-dimensional space}}$$

Example

$$\begin{bmatrix} a \\ b \\ c \end{bmatrix} \oplus \begin{bmatrix} d \\ e \\ f \end{bmatrix} = \begin{bmatrix} a \\ b \\ c \\ d \\ e \\ f \end{bmatrix}$$

Composing classical states

Direct sum $V \oplus W$

- $B_{V \oplus W} = B_V \cup B_W$ and $\dim(\mathrm{V} \oplus \mathrm{W}) = \dim(\mathrm{V}) + \dim(\mathrm{W})$
- Vector addition and scalar multiplication are performed in each component and the results added
- $\langle (|u_2\rangle \oplus |z_2\rangle) | (|u_1\rangle \oplus |z_1\rangle) \rangle \; = \; \langle u_2 | u_1 \rangle + \langle z_2 | z_1 \rangle$
- V and W embed canonically in $V \oplus W$ and the images are orthogonal under the standard inner product

Composing quantum states

State spaces in a quantum system combine through tensor: $\otimes$

$$\boxed{n\ m\text{-dimensional vectors} \quad \rightsquigarrow \quad \text{a vector in } m^n\text{-dimensional space}}$$

i.e. the state space of a quantum system grows exponentially with the number of particles: cf, Feyman's original motivation

Example

$$\begin{bmatrix} a \\ b \\ c \end{bmatrix} \otimes \begin{bmatrix} d \\ e \\ f \end{bmatrix} = \begin{bmatrix} a \begin{bmatrix} d \\ e \\ f \end{bmatrix} \\ b \begin{bmatrix} d \\ e \\ f \end{bmatrix} \\ c \begin{bmatrix} d \\ e \\ f \end{bmatrix} \end{bmatrix} = \begin{bmatrix} ad \\ ae \\ af \\ bd \\ be \\ bf \\ cd \\ ce \\ cf \end{bmatrix}$$

Composing quantum states

Tensor $V \otimes W$

- $B_{V\otimes W}$ is a set of elements of the form $|v_i\rangle \otimes |w_j\rangle$, for each $|v_i\rangle \in B_V$, $|w_i\rangle \in B_W$ and $\dim(\mathrm{V} \otimes \mathrm{W}) = \dim(\mathrm{V}) \times \dim(\mathrm{W})$
- $(|u_1\rangle + |u_2\rangle) \otimes |z\rangle \;=\; |u_1\rangle \otimes |z\rangle + |u_2\rangle \otimes |z\rangle$
- $|z\rangle \otimes (|u_1\rangle + |u_2\rangle) \;=\; |z\rangle \otimes |u_1\rangle + |z\rangle \otimes |u_2\rangle$
- $(\alpha|u\rangle) \otimes |z\rangle \;=\; |u\rangle \otimes (\alpha|z\rangle) \;=\; \alpha(|u\rangle \otimes |z\rangle)$
- $\langle(|u_2\rangle \otimes |z_2\rangle)|(|u_1\rangle \otimes |z_1\rangle)\rangle \;=\; \langle u_2|u_1\rangle\langle z_2|z_1\rangle$

Composing quantum states

Clearly, every element of $V \otimes W$ can be written as

$$\alpha_1(|v_1\rangle \otimes |w_1\rangle) + \alpha_2(|v_2\rangle \otimes |w_1\rangle) + \cdots + \alpha_{nm}(|v_n\rangle \otimes |w_m\rangle)$$

Example

The basis of $V \otimes W$, for V, W qubits with the computational basis is

$$\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\}$$

Thus, the tensor of $\alpha_1|0\rangle + \alpha_2|1\rangle$ and $\beta_1|0\rangle + \beta_2|1\rangle$ is

$$\alpha_1\beta_1|0\rangle \otimes |0\rangle \; + \; \alpha_1\beta_2|0\rangle \otimes |1\rangle \; + \; \alpha_2\beta_1|1\rangle \otimes |0\rangle \; + \; \alpha_2\beta_2|1\rangle \otimes |1\rangle$$

i.e., in a simplified notation,

$$\alpha_1\beta_1|00\rangle \; + \; \alpha_1\beta_2|01\rangle \; + \; \alpha_2\beta_1|10\rangle \; + \; \alpha_2\beta_2|11\rangle$$

Bases

The computational basis for a vector space

$$\underbrace{V \otimes V \otimes \cdots \otimes V}_{n}$$

corresponding to the composition of n qubits (each living in V) is the set

$$\{\underbrace{|0\rangle \cdots |0\rangle|0\rangle}_{n}, \underbrace{|0\rangle \cdots |0\rangle|1\rangle}_{n}, \underbrace{|0\rangle \cdots |1\rangle|0\rangle}_{n}, \cdots \underbrace{|1\rangle \cdots |1\rangle|1\rangle}_{n}\}$$

$$\stackrel{\text{abv}}{=}$$

$$\{\underbrace{|0 \cdots 00\rangle}_{n}, \underbrace{|0 \cdots 01\rangle}_{n}, \underbrace{|0 \cdots 10\rangle}_{n}, \cdots \underbrace{|1 \cdots 11\rangle}_{n}\}$$

which may be written in a compressed (decimal) way as

$$\{|0\rangle, |1\rangle, |2\rangle, |3\rangle, \cdots |2^n - 1\rangle\}$$

Bases

The computational basis for a two qubit system would be

$$\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$$

with

$$|0\rangle = |00\rangle = \begin{bmatrix}1\\0\\0\\0\end{bmatrix} \quad |1\rangle = |01\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix} \quad |2\rangle = |10\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix} \quad |3\rangle = |11\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

Bases

There are of course other bases
... besides the standard one, e.g.

The Bell basis

$$
\begin{aligned}
|\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
|\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\
|\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\
|\Psi^-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)
\end{aligned}
$$

Compare with the Hadamard basis for the single qubit systems

Representing multi-qubit states

Any unit vector in a 2^n Hilbert space represents a possible n-qubit state, but for

... a certain level of redundancy

- As before, vectors that differ only in a global phase represent the same quantum state
- but also the same phase factor in different qubits of a tensor product represent the same state:

$$|u\rangle \otimes (e^{i\Phi}|z\rangle) \;=\; e^{i\Phi}(|u\rangle \otimes |z\rangle) \;=\; (e^{i\Phi}|u\rangle) \otimes |z\rangle$$

Actually, phase factors in qubits of a single term of a superposition can always be factored out into a coefficient for that term, i.e. phase factors distribute over tensors

Representing multi-qubit states

Representation

- Relative phases still matter (of course!)

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad \text{differs from} \quad \frac{1}{\sqrt{2}}(e^{i\Phi}|00\rangle + |11\rangle)$$

even if

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(e^{i\Phi}|00\rangle + e^{i\Phi}|11\rangle) = \frac{e^{i\Phi}}{\sqrt{2}}(|00\rangle + |11\rangle)$$

- The complex projective space of dimension 1 (depicted in the Block sphere) generalises to higher dimensions, although in practice linearity makes Hilbert spaces easier to use.

Entanglement

Most states in $V \otimes W$ cannot be written as $|u\rangle \otimes |z\rangle$

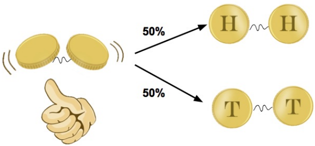
- By $\mathbb{C}$ compactification a single-qubit state can be specified by a single complex number so any tensor product of n qubit states can be specified by n complex numbers. But it takes $2^n - 1$ complex numbers to describe states of an n qubit system.
- Since $2^n \gg n$, the vast majority of n-qubit states cannot be described in terms of the state of n separate qubits.
- Such states, that cannot be written as the tensor product of n single-qubit states, are entangled states.

Entanglement

For example, the Bell state

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \;=\; \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

is entangled



Entanglement

Actually, to make $|\Phi^+\rangle$ equal to

$$(\alpha_1|0\rangle+\beta_1|1\rangle)\otimes(\alpha_2|0\rangle+\beta_2|1\rangle) \;=\; \alpha_1\alpha_2|00\rangle+\alpha_1\beta_2|01\rangle+\beta_1\alpha_2|10\rangle+\beta_1\beta_2|11\rangle$$

would require that $\alpha_1\beta_2 = \beta_1\alpha_2 = 0$ which implies that either

$$\alpha_1\alpha_2 = 0 \;\text{ or }\; \beta_1\beta_2 = 0$$

Note
Entanglement can also be observed in simpler structures, e.g. relations:

$$\{(a, a), (b, b)\} \subseteq A \times A$$

cannot be separated, i.e. written as a Cartesian product of subsets of A.

The measurement postulate

Postulate 4

For a given orthonormal basis $B = \{|v_1\rangle, |v_2\rangle, \cdots\}$, a measurement of a state space $|v\rangle = \sum_i \alpha_i |v_i\rangle$ wrt B, outputs the label i with probability $\| \alpha_i \|^2$ and leaves the system in state $|v_i\rangle$.

- Measurements are made through projectors which identify the ‘data’ (i.e. the subspace of the relevant Hilbert space where the quntum system lives) one wants to measure.
- Let us start with a couple of examples ... but for the general notion let us recall the notion of adjoint operator.

Adjoints

Given an operator U, its adjoint is the unique operator satisfying

$$(|w\rangle, U|v\rangle) \;=\; (U^{\dagger}|w\rangle, |v\rangle)$$

where $(|x\rangle, |y\rangle)$ is the 'verbose' representation for the inner product $\langle x, y\rangle$. Thus, in Dirac notation the equality above becomes

$$\langle w|Uv\rangle = (U^{\dagger}|w\rangle)^{\dagger}|v\rangle \;=\; \langle wU|v\rangle$$

or simply

$$\langle w|U|v\rangle$$

The matrix representation of $U^{\dagger}$ is the conjugate transpose of that of U

Exercise: Prove that $\overline{\langle w|U|v\rangle} \;=\; \langle v|U^{\dagger}|w\rangle$

Projectors

Any projector P identifies in the state space V a subspace V_P of all vectors $|\phi\rangle$ that are left unchanged by P, i.e. such that

$$P|\phi\rangle = |\phi\rangle$$

Examples

- The identity I projects onto the whole space V.
- The zero operator projects onto the space $\{0\}$ consisting only of the zero vector.
- $|u\rangle\langle u|$ is the projector onto the subspace spanned by $|u\rangle$.

Projectors

Examples

- Projector $|0\rangle\langle 0|$ projects onto the subspace generated by $|0\rangle$, i.e.

$$|0\rangle\langle 0|\,(\alpha|0\rangle + \beta|1\rangle) \;=\; \alpha|0\rangle\langle 0|(|0\rangle) + \beta|0\rangle\langle 0|(|1\rangle) \;=\; \alpha|0\rangle$$

- Similarly, $|10\rangle\langle 10|$ acts on a two-qubit state

$$v \;=\; \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

yielding

$$|10\rangle\langle 10|\,(|v\rangle) \;=\; \alpha_{10}|10\rangle$$

and

$$|00\rangle\langle 00| + |10\rangle\langle 10|(|v\rangle) \;=\; \alpha_{00}|00\rangle + \alpha_{10}|10\rangle$$

Projectors

A projector $P : V \to V_P$ is an operator such that

$$P^2 = P$$

Additionally, we require P to be Hermitian, i.e.

$$P = P^\dagger$$

Note that the combination of both properties yields

$$\| P|v\rangle \|^2 = (\langle v|P^\dagger)(\mathrm{P}|v\rangle) = \langle v|P|v\rangle$$

Example

The probability of getting state $|0\rangle$ when measuring $\alpha|0\rangle + \beta|1\rangle$ with $P = |0\rangle\langle 0|$ is computed as

$$\| P|v\rangle \|^2 = \langle v|P|v\rangle = \langle v||0\rangle\langle 0||v\rangle = \langle v|0\rangle \langle 0|v\rangle = \overline{\alpha}\alpha = \| \alpha \|^2$$

Projectors

Two projectors P, Q are orthogonal if $PQ = 0$.

The sum of any collection of orthogonal projectors $\{P_1, P_2, \cdots\}$ is still a projector (verify!).

A projector P has a decomposition if it can be written as a sum of orthogonal projectors:

$$P = \sum_i P_i$$

Such projectors yield measurements wrt to the corresponding decomposition.

Examples

- Complete measurement in the computational basis wrt to decomposition

$$I = \sum_{i \in 2^n} |i\rangle\langle i|$$

in a state with n qubits.

- Incomplete measurement: e.g.

$$\sum_{\{i \in 2^n \mid i \text{ even}\}} |i\rangle\langle i|$$

Projectors

Example: measuring up to (bit equality)

$$V = S_e \oplus S_n$$

with S_e the subspace generated by $\{|00\rangle, |11\rangle\}$ in which the two bits are equal, and S_n its complement. P_e and P_n, are the corresponding projectors.

When measuring

$$v \;=\; \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

with this device, yields a state in which the two bit values are equal with probability

$$\langle v|P_e|v\rangle \;=\; (\sqrt{\| \alpha_{00} \|^2 + \| \alpha_{11} \|^2}) \;= \| \alpha_{00} \|^2 + \| \alpha_{11} \|^2$$

Of course, the measurement does not determine the value of the two bits, only whether the two bits are equal

Projectors

Any orthonormal collection of vectors $B = \{|v_1\rangle, |v_2\rangle, \cdots\}$ defines a projector

$$P = \sum_i |v_i\rangle\langle v_i|$$

If B spans the entire Hilbert space V, it forms a basis for V and $P = I$, i.e. B provides a decompostion for the identity.

Is there a standard way to provide a decomposition for P?

Yes, if P is a Hermitian operator, because of the

Spectral theorem
Any Hermitian operator on a finite Hilbert space V provides a basis for V consisting of its eigenvectors.

Projectors are Hermitian

Hermitian operators

- define a unique orthogonal subspace decomposition, their eigenspace decomposition, and
- for every such decomposition, there exists a corresponding Hermitian operator whose eigenspace decomposition coincides with it

Properties

Every eigenvalue λ with eigenvector $|r\rangle$ is real, because

$$\lambda\langle r|r\rangle \;=\; \langle r|\lambda|r\rangle \;=\; \langle r|\left(P|r\rangle\right) \;=\; \left(\langle r|P^\dagger\right)|r\rangle \;=\; \bar{\lambda}\langle r|r\rangle$$

Projectors are Hermitian

Properties

For any P Hermitian, two distinct eigenvalues have disjoint eigenspaces, because, for any unit vector $|v\rangle$,

$$P|v\rangle = \lambda|v\rangle \text{ and } P|v\rangle = \lambda'|v\rangle \text{ and } (\lambda - \lambda')|v\rangle = 0$$

and thus $\lambda = \lambda'$.

Moreover, the eigenvectors for distinct eigenvalues must be orthogonal, because

$$\lambda\langle v|w\rangle \;=\; (\langle v|P^\dagger)\,|w\rangle \;=\; \langle v|\,(P|w\rangle) \;=\; \mu\langle v|w\rangle$$

for any pairs $(\lambda, |v\rangle), (\mu, |w\rangle)$ with $\lambda \neq \mu$.
Thus, $\langle v|w\rangle = 0$, because $\lambda \neq \mu$, and the corresponding subspaces are orthogonal.

Projectors are Hermitian

Eigenspace decomposition of V for P

Any Hermitian P determines a unique decomposition for V

$$V = \oplus_{\lambda_i} S_{\lambda_i}$$

and any decomposition $V = \oplus_{i=1}^{k} S_i$ can be realized as the eigenspace decomposition of a Hermitian operator

$$P = \sum_i \lambda_i \mathrm{P}_i$$

where each P_i is the projector onto S_{λ_i}

Projectors are Hermitian

A decomposition can be specified by a Hermitian operator

- Any measurement is specified by a Hermitian operator P
- The possible outcomes of measuring a state $|v\rangle$ with P are labeled by the eigenvalues of P
- The probability of obtaining the outcome labelled by λ_i is

$$\| P_i|v\rangle \|^2$$

- The state after measurement is the normalized projection

$$\frac{P_i|v\rangle}{\| \mathrm{P}_i|v\rangle \|}$$

  onto the λ_i-eigenspace S_i. Thus, the state after measurement is a unit length eigenvector of P with eigenvalue λ_i