Quantum Computation (CO484)

Quantum Measurement and Registers

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) $\mathbf{A}$ acting on the Hilbert space $\mathcal{H}$.
- The expected result (average) when measuring observable $\mathbf{A}$ of a system in state $|x\rangle \in \mathcal{H}$ is given by:

$$\langle A \rangle_x = \langle x| \mathbf{A} |x\rangle = \langle x| |\mathbf{A}x\rangle$$

- The only possible results are eigen-values λ_i of $\mathbf{A}$.
- The probability of measuring λ_n in state $|x\rangle$ is given by:

$$Pr(A = \lambda_n | x) = \langle x| \mathbf{P}_n |x\rangle = \langle x| |\mathbf{P}_n x\rangle$$

with $\mathbf{P}_n = |\lambda_n\rangle\langle\lambda_n|$ the orthogonal projection onto the space generated by eigen-vector $|\lambda_n\rangle = |n\rangle$ of $\mathbf{A}$.

Basic Measurement Principle

The values α and β describing a qubit are often 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 **A** is called self-adjoint or hermitian iff

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

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

Possible measurement results are eigenvalues λ_i of **A** (always real for self-adjoint operators) defined as

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

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

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

Physicist refer to α_k as probability amplitude.

Spectrum

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

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

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

$$\mathbf{T}\,|i\rangle = \lambda_i\,|i\rangle$$

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

Terminology: "eigen" means "self" or "own" in German (cf also Italian "auto-valore"), it **characterises** a matrix/operator.

Projections

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

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

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

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

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

Birkhoff-von Neumann: Projections on Hilbert space form an (ortho-)lattice which gives rise to non-classical "quantum logic".

Outer Product

The outer product $|x\rangle\langle y|$ for vectors $|x\rangle = (x_1, \ldots, x_n)^T$ and $\langle y| = (y_1, \ldots, y_n)$ is an operator/matrix (actually: $|x\rangle \otimes \langle y|$):

$$(|x\rangle\langle y|)_{ij} = x_i y_j$$

$$\text{e.g.} \quad |0\rangle\langle 1| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

It could be treated just as a formal combination, e.g. we can express the identity as $\mathbf{I} = |0\rangle\langle 0| + |1\rangle\langle 1|$ because

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

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* $|i\rangle$*, i.e.*

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

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.

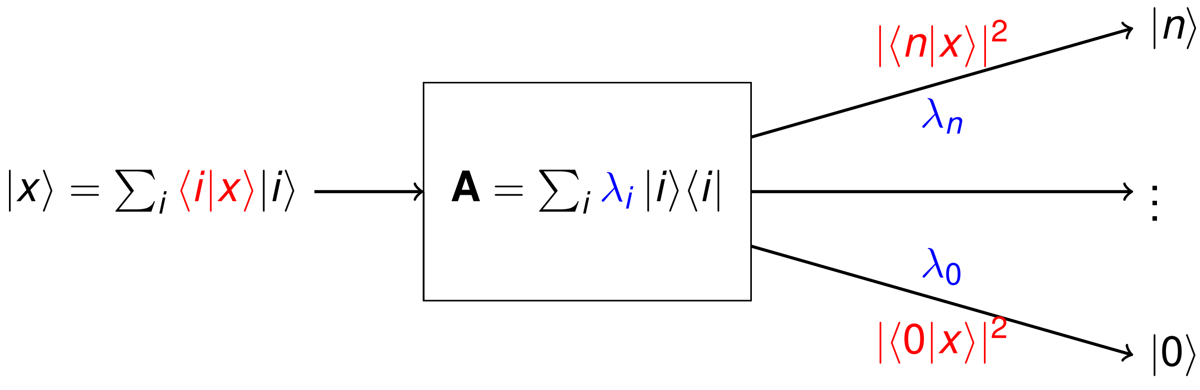
$$|x\rangle = \sum_i \mathbf{P}_i |x\rangle = \sum_i |i\rangle\langle i|x\rangle = \sum_i \langle i|x\rangle |i\rangle = \sum_i \alpha_i |i\rangle$$

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 in quantum measurement (typically):

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

i.e. the quantum measurement is not **reversible**. However

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

i.e. the quantum measurement is **idempotent**.

Beyond Qubits – Quantum Registers

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. There could be two options:

- 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 build quantum devices based on not just binary basic states, even then it will be necessary to combine these larger "Qubits".

Free Vector Spaces

In the theory of formal languages we have the construction of words out of some (finite) set of letters, i.e. alphabet Σ or S.

For vector spaces there is similar construction: Take any (finite) set of objects B and "declare" it a base. The free vector space is the set of all linear combinations of elements in $B = \{\mathbf{b}_1, \mathbf{b}_2, \ldots\}$, i.e.

$$\mathcal{V}(B) = \left\{ \sum_i \lambda_i \mathbf{b}_i \mid \lambda_i \in \mathbb{C} \text{ and } \mathbf{b}_i \in B \right\}$$

or

$$\mathcal{V}(B) = \left\{ \sum_i \lambda_i |i\rangle \mid \lambda_i \in \mathbb{C} \text{ and } |i\rangle \in B \right\}$$

with the obvious algebraic operations (incl. inner product).

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):

$$B_2 = \{(0,0), (1,0), (0,1), (1,1)\}$$

or we use a "short-hand" notation $B_2 = \{00, 01, 10, 11\}$

Issue: What about $\mathcal{V}(B \times B \times B)$? What is its dimension, or how many base vectores are there in B_3?

Tensor Product

Given a $n \times m$ **matrix A** and a $k \times l$ matrix **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 fulfils a number of nice algebraic properties, such as

1. The **bilinearity** property:

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

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

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

$$\langle \mathbf{v} \otimes \mathbf{w}, \mathbf{v}' \otimes \mathbf{w}' \rangle = \langle \mathbf{v}, \mathbf{v}' \rangle \langle \mathbf{w}, \mathbf{w}' \rangle$$

3. We denote by $\mathbf{b}_i^m \in B_m \subseteq \mathbb{C}^m$ the i'th basis vector in $\mathbb{C}^m$ then

$$\mathbf{b}_i^k \otimes \mathbf{b}_j^l = \mathbf{b}_{(i-1)l+j}^{kl}$$

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 $\mathbf{v} \in \mathbb{C}^m$ and $\mathbf{w} \in \mathbb{C}^n$:

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

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

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

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

$$\mathcal{H}_1 \otimes \mathcal{H}_2 = \mathcal{V}(\{\mathbf{b}_i \otimes \mathbf{b}_j \mid \mathbf{b}_i \in B_1, \mathbf{b}_j \in B_2\})$$

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:

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

Often one also represents them using a "decimal" notation, i.e. $|00\rangle \equiv |0\rangle$, $|01\rangle \equiv |1\rangle$, $|10\rangle \equiv |2\rangle$, 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 be represented as a linear combination of the base vectors $|0\ldots 00\rangle, |0\ldots 10\rangle, \ldots, |1\ldots 11\rangle$ 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.

Entanglement and Classical Probabilities

In quantum physics the state is given by a vector in a complex Hilbert space. Instead of probability amplitudes in $\mathbb{C}^n$ let us consider probability distributions in a real vector space, i.e. $\mathbb{R}^d$.

All the normalised (using the 1-norm, i.e. $\|(p_i)_i\|_1 = \sum_i |p_i|$) elements ρ in $\mathbb{R}^d$ represent probability distributions on a d element probability space $\Omega_d = \{\omega_1, \omega_2, \ldots, \omega_d\}$ i.e. $\rho = (\rho_i) \in \mathcal{D}(\Omega_d)$ with $\rho_i = P(\omega_i) \in [0,1]$.

The normalised elements in $\mathbb{R}^{d_1} \otimes \mathbb{R}^{d_2}$ correspond to the joint probability distributions on $\Omega_{d_1} \times \Omega_{d_1}$, with $\rho_{ij} = P(\omega_i \wedge \omega_j)$, i.e.

$$\mathcal{D}(\Omega_{d_1} \times \Omega_{d_1}) = \mathcal{D}(\Omega_{d_1}) \otimes \mathcal{D}(\Omega_{d_1})$$

Classical Correlations

If the events in Ω_{d_1} and Ω_{d_2} are independent ("uncorrelated") then their joint distribution is given as a product of distributions on Ω_{d_1} and Ω_{d_1}, i.e. $\rho = \rho_1 \otimes \rho_2$ or $P(\omega_i \wedge \omega_j) = P(\omega_i) \cdot P(\omega_j)$.

If there is a "correlation" or "dependency" then it is impossible to express a certain joint distribution as a simple (tensor product) but only as a sum of (tensor) products.

Consider, for example, two coins which "miraculously" always fall on the same side, i.e. a joint distribution:

ρ_{ij}	H	T
H	$\frac{1}{2}$	0
T	0	$\frac{1}{2}$

$$\rho = \frac{1}{2}(1,0) \otimes (1,0)^T + \frac{1}{2}(0,1) \otimes (0,1)^T \neq \rho_1 \otimes \rho_2$$

Relational Program Analysis [*]

$$\begin{array}{rcl} 1! & = & 1 \\ n! & = & n \cdot (n-1)! \end{array} \qquad \text{parity}(m) = \begin{cases} \textbf{even} & \text{if } m = 2k \\ \textbf{odd} & \text{otherwise.} \end{cases}$$

Consider random input $n \in \{1,2,3\}$ to the factorial, i.e. $P(n=1) = P(n=2) = P(n=3) = \frac{1}{3}$. Determine the probability that $n!$ is **even** or **odd**.

$$P(\text{parity}(n!) = \textbf{even}) = \frac{2}{3} \text{ and } P(\text{parity}(n!) = \textbf{odd}) = \frac{1}{3}.$$

However – the probabilities are not independent – we have, e.g.

$$0 = P(\textbf{even}(n!) \ \wedge \ n = 1) \neq P(\textbf{even}(n!)) \cdot P(n=1) = \frac{2}{9}$$

Entanglement represents correlation (non-independence):

$$P(\text{parity(n!)} \mid n) \neq P(\text{parity}(n!)) \otimes P(n).$$