Quantum Computing @ MEF

Background

Renato Neves

nevrenato@di.uminho.pt

1 Quantum States

Models of computation often put at center stage a notion of state and a corresponding notion of state transition [BM17]. In the quantum world, states usually involve superpositions, angles, and lengths; or in other words, they involve aspects related to geometry. This suggests us to familiarise with both the notion of a *vector space* and (the more refined) notion of an *inner product space*. It also suggests us to delve deep into the inner workings of maps between vector spaces and maps between inner product spaces, both intuitively yielding a notion of a quantum state transition (i.e. a quantum operation).

1.1 Vector spaces

Let $\mathbb{C}$ denote the set of complex numbers.

Definition 1 (Vector Space)**.** A vector space (over the complex numbers) [1] is a set V together with an 'addition' operation $+ : V \times V \to V$, a 'multiplication' operation $\cdot : \mathbb{C} \times V \to V$, a 'zero' element $0 \in V$, and an 'inverse' operation $- : V \to V$ such that the following equations hold for arbitrary $v, u, w \in V$, $s, r \in \mathbb{C}$:

$$\begin{aligned} v + (u + w) &= (v + u) + w & v + u &= u + v \\ v + 0 &= v & v + (-v) &= 0 \\ (sr) \cdot v &= s \cdot (r \cdot v) & 1 \cdot v &= v \\ s \cdot (v + u) &= s \cdot v + s \cdot u & (s + r) \cdot v &= s \cdot v + r \cdot u \end{aligned}$$

To keep notation simple we will often omit the dot of the scalar multiplication, i.e. we will write expressions $s \cdot v$ simply as sv.

Example 1. The complex numbers themselves form a vector space and the set $\mathbb{C}^2$ of pairs of complex numbers also forms a vector space. This last space underlies the mathematical representation of the state of a qubit. Recall that a qubit is the unit in quantum information. Later on we will see that our notion of state corresponds exactly to the state of a sequence of qubits.

[1] In this course we will only consider vector spaces over the complex numbers. Note however that many of the mentioned results hold for a general field.

Exercise 1. Show that for any finite set n we can build a vector space $[n, \mathbb{C}]$ over the complex numbers. Show also that the set $\mathsf{Mat}_{\mathbb{C}}(n, m)$ of matrices with n lines and m columns and whose values are complex numbers also forms a vector space (hint: observe that matrices can be given a functional representation).

Definition 2 (Linear maps a.k.a. linear operators or simply operators)**.** Consider two vector spaces V and W. A linear map $f : V \to W$ is a function that satisfies the equations,

$$f(v_1 + v_2) = f(v_1) + f(v_2) \qquad\qquad f(sv) = sf(v)$$

We call f a *linear isomorphism* or simply isomorphism if it is bijective. When such is the case, we say that V and W are isomorphic to each other (i.e. essentially the same), in symbols $V \simeq W$.

Exercise 2. Show that the identity map $\mathrm{id} : V \to V$ is linear. Additionally show that if $f : V \to W$ and $g : W \to U$ are linear maps then their composition $g \cdot f : V \to U$ is also a linear map.

Exercise 3. Consider a vector space V. Show that linear maps $f : \mathbb{C} \to V$ are in one-to-one correspondence with the elements of V.

A crucial concept for our notion of state and state transition is that of a tensor. In essence, it allows to mathematically represent the state of a *sequence* of qubits (instead of working with just one qubit).

Definition 3 (Tensor)**.** Let V and W be two vector spaces. Their tensor, denoted by $V \otimes W$, is the vector space consisting of all linear combinations $\sum_{i \leq n} s_i (v_i \otimes w_i)$ with $s_i \in \mathbb{C}$, $v_i \in V$, $w_i \in W$, that satisfies the equations,

$$\begin{aligned} v \otimes w + u \otimes w &= (v + u) \otimes w & \qquad v \otimes w + v \otimes u &= v \otimes (w + u) \\ s(v \otimes w) &= (sv) \otimes w & s(v \otimes w) &= v \otimes (sw) \end{aligned}$$

Exercise 4. Show that from linear maps $f : V \to V'$ and $g : W \to W'$ we can define a new linear map $f \otimes g : V \otimes W \to V' \otimes W'$. Show that $(f' \otimes g') \cdot (f \otimes g) = (f' \cdot f) \otimes (g' \cdot g)$. Prove the existence of linear isomorphisms $V \otimes W \simeq W \otimes V$ and $V \otimes \mathbb{C} \simeq V$.

Exercise 5. Show that the map $\Delta : \mathbb{C}^2 \to \mathbb{C}^2 \otimes \mathbb{C}^2$ defined by $\Delta(v) = v \otimes v$ is *non-linear.* What is the relation between this map and the no-cloning theorem?

Another concept that will be imensely useful in the course is that of a basis.

Definition 4 (Basis)**.** A basis for a vector space V is a set $B \subseteq V$ of vectors that respects the following conditions:

- for every $v \in V$, we can find $v_1, \dots, v_n \in B$ and $s_1, \dots, s_n \in \mathbb{C}$ such that $\sum_{i \leq n} s_i v_i = v$
- for every sequence of vectors $v_1, \dots, v_n \in B$ and sequence of complex numbers $s_1, \dots, s_n \in \mathbb{C}$ if $\sum_{i \leq n} s_i v_i = 0$ then $s_i = 0$ for all $i \leq n$.

Example 2. The set $\{1\}$ is a basis for $\mathbb{C}$ and the set $\{(1,0),(0,1)\}$ is a basis for $\mathbb{C}^2$.

Let B be a basis for a vector space V. If B has n elements we say that V is n-dimensional. If B is finite we say that V is *finite-dimensional.*

In this course we are primarily interested in finite-dimensional vector spaces. Intuitively, this is justified by the fact we will only need to work with a finite number of qubits at a time. Thus from now on all vector spaces that we consider are finite-dimensional.

Exercise 6. Let n be a natural number and $\mathbb{C}^n$ be the vector space of n-tuples of complex numbers. Present a basis for $\mathbb{C}^n$ and subsequently indicate its dimension. Next let $\mathsf{Mat}_{\mathbb{C}}(n,m)$ be the vector space of matrices with n lines and m columns and whose values are complex numbers. Present a basis for this space and subsequently indicate its dimension.

Exercise 7. Consider a linear map $f : V \to W$ and let B be a basis for V. Show that this map is *uniquely determined* by the way it maps the elements in B. Moreover, show that a function $B \to W$ mapping elements in the basis of V to W induces a linear map of type $V \to W$.

Exercise 8. Show that any vector space V with dimension n is isomorphic to the vector space $\mathbb{C}^n$.

Matrices provide a very convenient way of representing states and also of representing state transitions. Let us analyse how such a representation works. Let V and W be vector spaces, $\{b_1, \dots, b_n\}$ a basis for V and $\{c_1, \dots, c_m\}$ a basis for W. Consider then a linear map $f : V \to W$ and observe that for every $i \leq n$ we have $f(b_i) = \sum_{j \leq m} s_{ij} c_j$ for some $s_{i1}, \dots, s_{im} \in \mathbb{C}$. We obtain a matrix representation $M \in \mathsf{Mat}_{\mathbb{C}}(m,n)$ of f by setting $M_{ji} = s_{ij}$. Conversely, consider a matrix $M \in \mathsf{Mat}_{\mathbb{C}}(m,n)$. It induces a linear map $f : V \to W$ by setting $f(b_i) = \sum_{j \leq m} M_{ji} c_j$.

Exercise 9. Show that the two operations described above (for switching between linear maps and their matrix representation) are inverse of each other.

Exercise 10. What is the matrix representation of the linear map $f : \mathbb{C}^2 \to \mathbb{C}^2$ defined by $f(1,0) = (0,1)$ and $f(0,1) = (1,0)$? What is the matrix representation of the linear map $f : \mathbb{C}^2 \to \mathbb{C}^2$ defined by $f(1,0) = \frac{1}{\sqrt{2}}(1,0) + \frac{1}{\sqrt{2}}(0,1)$ and $f(0,1) = \frac{1}{\sqrt{2}}(1,0) - \frac{1}{\sqrt{2}}(0,1)$?

Before moving forward in the course, we need to fix extra notation. Specifically, we will use $M : n \to m$ to denote a matrix M with n lines, m columns, and whose values are complex numbers. Also for two matrices $M : n \to m$ and $N : m \to o$, we will use $MN : n \to o$ to denote the matrix multiplication of M with N. Finally, given a linear map $f : V \to W$ such that V and W have dimension n and m, respectively, we will use $M_f : m \to n$ to denote the corresponding matrix.

Exercise 11 (H)**.** Show that elements of V are in one-to-one correspondence with elements of $\mathsf{Mat}_{\mathbb{C}}(n,1)$. For all linear maps $f : V \to W$ and $g : W \to U$ show that $M_g M_f = M_{g \cdot f}$.

Exercise 12 (H)**.** Let $B \subseteq V$, $C \subseteq W$ be bases for vector spaces V and W, respectively. Show that the set $\{b \otimes c \mid b \in B, c \in C\}$ is a basis for $V \otimes W$. Then show that $\mathbb{C}^n \otimes \mathbb{C}^m \simeq \mathbb{C}^{nm}$ (hint: recall Exercise 8).

Consider matrices $M : n \to m$ and $N : o \to p$. Their tensor $M \otimes N : n \cdot o \to m \cdot p$ (also called Kronecker product) is defined by,

$$M \otimes N = \begin{bmatrix} M_{1,1} \cdot N, & \dots, & M_{1,m} \cdot N \\ \vdots & \vdots & \vdots \\ M_{n,1} \cdot N, & \dots, & M_{n,m} \cdot N \end{bmatrix}$$

Exercise 13 (H)**.** For all linear maps $f : V \to V'$ and $g : W \to W'$ show that $M_{f \otimes g} = M_f \otimes M_g$.

Exercise 14. For a given matrix $M : n \to m$, we will use $M^* : n \to m$ to denote the matrix such that $M^*_{ij} = (M_{ij})^*$, $M^T : m \to n$ to denote the transpose of M, and $M^\dagger : m \to n$ to denote the matrix $(M^T)^*$, i.e. the conjugate transpose (a.k.a. adjoint) of M. Show that the following equations hold.

$$(M \otimes N)^* = M^* \otimes N^* \qquad (M \otimes N)^T = M^T \otimes N^T \qquad (M \otimes N)^\dagger = M^\dagger \otimes N^\dagger$$

1.2 Inner product spaces

Recall that for some complex number c the expression c^* denotes the *complex conjugate* of c.

Definition 5 (Inner product space)**.** An inner product space is a vector space V equipped with a function $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{C}$ (the inner product) that satisfies the conditions,

$$\left\langle v, \sum_{i \leq n} s_i v_i \right\rangle = \sum_{i \leq n} s_i \cdot \langle v, v_i \rangle \qquad \langle v, w \rangle = \langle w, v \rangle^*$$

$$\langle v, v \rangle \geq 0 \qquad \langle v, v \rangle = 0 \text{ entails } v = 0$$

for all $v, v_i, w \in V$ and $s_i \in \mathbb{C}$. [2]

Exercise 15. Let n be a natural number. Show that the vector space $\mathbb{C}^n$ becomes an inner product space when equipped with the function $\langle \cdot, \cdot \rangle : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}$ defined by,

$$\langle (a_1, \dots, a_n), (b_1, \dots, b_n) \rangle = \sum_{i \leq n} a_i^* b_i$$

Recall that a norm over a vector space V provides a notion of length to the vector space and is formally defined as a function $\| \cdot \| : V \to [0, \infty)$ such that the following conditions are satisfied,

$$\|v\| = 0 \text{ iff } v = 0 \qquad \|s \cdot v\| = |s| \cdot \|v\| \qquad \|v + w\| \leq \|v\| + \|w\|$$

for all $v, w \in V$, $s \in \mathbb{C}$. Moreover, every inner product space V induces a norm $\| \cdot \| : V \to [0, \infty)$ defined by $\|v\| = \sqrt{\langle v, v \rangle}$.

As we will see, the mathematical representation of the state of n-qubits is a vector $v \in \mathbb{C}^{2^n}$ with norm $\|v\| = 1$.

[2] Since we assume that all vector spaces at hand are finite-dimensional we can see inner product spaces as Hilbert spaces.

Exercise 16 (Vector normalisation)**.** Let $v \in V$ be a vector. Show that,

$$\left\| \frac{v}{\|v\|} \right\| = 1$$

Definition 6 (Orthonormal basis)**.** Two vectors $v, w \in V$ are said to be orthogonal to each other if $\langle v, w\rangle = 0$. A basis B for an inner product space V is called orthonormal if all elements of B have norm 1 and all elements $v \neq w \in B$ are orthogonal to each other.

Exercise 17. Show that the basis $\{(1,0),(0,1)\}$ for $\mathbb{C}^2$ is orthonormal.

Definition 7 (Tensor)**.** Let V and W be two inner spaces. Their tensor, denoted by $V \otimes W$, is the tensor of V and W as vector spaces equipped with the function,

$$\left\langle \sum_{i \leq n} s_i(v_i \otimes w_i), \sum_{j \leq m} r_j(v_j \otimes w_j) \right\rangle = \sum_{i \leq n, j \leq m} s_i^* r_j \cdot \langle v_i, v_j\rangle \cdot \langle w_i, w_j\rangle$$

Exercise 18. Let $B \subseteq V$, $C \subseteq W$ be orthonormal bases for inner product spaces V and W, respectively. Show that the set $\{b \otimes c \mid b \in B, c \in C\}$ is an orthonormal basis for $V \otimes W$.

When working with linear maps $f : V \to W$ between inner product spaces V and W we are often interested in those maps that are isometric.

Definition 8 (Isometry)**.** Consider inner product spaces V and W and a linear map $f : V \to W$ between them. We call f an isometry if the equation,

$$\langle v_1, v_2\rangle = \langle f(v_1), f(v_2)\rangle$$

holds for all $v_1, v_2 \in V$. Equivalently, f is an isometry iff $\|v\| = \|f(v)\|$ for all $v \in V$.

A key property of isometries is they always send unit vectors to unit vectors (because isometries preserve norms). In the particular case of $V = W = \mathbb{C}^{2^n}$, this means that quantum states are always mapped to quantum states (and not to something else).

Additionally, quantum physics postulates that quantum operations on an isolated system must be *reversible.* In other words, maps $f : V \to W$ representing pure quantum operations must have an *inverse* $f^{-1} : W \to V$ which satisfies $f^{-1} \cdot f = f \cdot f^{-1} = \mathrm{id}$. Together with the notion of an isometry, this condition gives rise to the notion of a unitary map.

Definition 9 (Unitary maps)**.** Let V and W be inner product spaces. A linear map $f : V \to W$ is called unitary if f is an isometry and surjective[3].

Postulate 1 (Quantum state and state transition)**.** The state of an *isolated* quantum computer is given by a unit vector in the space $\mathbb{C}^{2^n}$ for some finite number n – the number n corresponds to the number of available qubits. State transitions arise via unitary maps, more concretely the state of an isolated quantum computer changes by an application of a unitary map. [4]

The notion of a unitary map can also be formulated via matrices, and often this alternative formulation is easier to work with: let us consider a linear map $f : V \to V$ and its matrix representation $M_f : n \to n$. Then f is unitary iff $M_f^\dagger M_f = M_f M_f^\dagger = I$.

[3] Both conditions entail that f has an inverse f^{-1}.

[4] See a more general version of this postulate in Section 2.2 of [NC02]

Exercise 19. Show that the following two maps are unitary:

- $f : \mathbb{C}^2 \to \mathbb{C}^2$ defined by $f(1,0) = (0,1)$ and $f(0,1) = (1,0)$.
- $g : \mathbb{C}^2 \to \mathbb{C}^2$ defined by $g(1,0) = \frac{1}{\sqrt{2}}(1,0) + \frac{1}{\sqrt{2}}(0,1)$ and $g(0,1) = \frac{1}{\sqrt{2}}(1,0) - \frac{1}{\sqrt{2}}(1,0)$.

Exercise 20. Prove that if two linear maps are unitary then their tensor is also unitary.

Consider a linear map $f : V \to W$ between inner product spaces V and W. There exists a unique linear map $f^\dagger : W \to V$ such that for all $v \in V$ and $w \in W$ the equation,

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

holds. This map is precisely the functional representation of $M_f^\dagger$.

2 Quantum Measurement

In order to render notation more convenient, we will often omit the parentheses in function application and start to denote linear maps by capital letters. Also, we will now use $|0\rangle$ and $|1\rangle$ to denote the elements $(1,0)$ and $(0,1)$ in $\mathbb{C}^2$, respectively. We extend this notation to any space $\mathbb{C}^{2^n}$ by observing that,

$$\mathbb{C}^{2^n} \simeq \underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n \text{ times}}$$

and representing $|b_1\rangle \otimes \cdots \otimes |b_n\rangle \in \mathbb{C}^{2^n}$ simply as $|b_1, \ldots, b_n\rangle$. Thus, a vector $v \in \mathbb{C}^2$ is a linear combination $\alpha\,|0\rangle + \beta\,|1\rangle$ and $\|v\| = 1$ entails that the equation $|\alpha|^2 + |\beta|^2 = 1$ holds. Later on we will see that $|\alpha|^2$ is the probability of observing $|0\rangle$ when measuring a qubit in state v and analogously for $|\beta|^2$. Similarly, a vector $v \in \mathbb{C}^4$ is a linear combination $\alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle$ and $\|v\| = 1$ entails that the equation $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$ holds. The component $|\alpha|^2$ is the probability of observing $|00\rangle$ when measuring two qubits at state v, and analogously for the three other components.

In this course, we will heavily use two maps M_0 and M_1 of type $\mathbb{C}^2 \to \mathbb{C}^2$ for measuring qubits. The map M_0 is defined by the equations,

$$M_0\,|0\rangle = |0\rangle \qquad\qquad M_0\,|1\rangle = 0$$

and represents the outcome of the qubit measured being at state $|0\rangle$; the map M_1 arises from an analogous reasoning. For the space $\mathbb{C}^{2^n}$ we represent the outcome of the i-th qubit being at state $|k\rangle$ by the map,

$$\underbrace{\mathrm{id} \otimes \cdots \otimes \mathrm{id}}_{i-1 \text{ times}} \otimes\, M_k \otimes \underbrace{\mathrm{id} \otimes \cdots \otimes \mathrm{id}}_{n-i \text{ times}} : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$$

We call ‘measurement maps’ those maps that are built in this way and that arise by composing measurement maps with one another.

Postulate 2 (Quantum measurement)**.** Let $v \in \mathbb{C}^{2^n}$ be a quantum state of n qubits and let us consider a measurement map $M : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$. Then the probability of the outcome represented by M is $\langle M\, v, M\, v \rangle$ and the quantum state of the n qubits after the observed outcome is defined by,

$$\frac{M\, v}{\|M\, v\|}$$

(note that we perform a normalisation, which is necessary because measurement maps are not unitary).

Exercise 21. Let $H : \mathbb{C}^2 \to \mathbb{C}^2$ be the unitary map defined by the matrix,

$$\frac{1}{\sqrt{2}} \cdot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

What is the probability of the outcome $|0\rangle$ when measuring $H\,|0\rangle$?

Exercise 22. Consider the quantum state,

$$\frac{1}{2}\,|00\rangle + \frac{1}{2}\,|01\rangle + \frac{1}{2}\,|10\rangle + \frac{1}{2}\,|11\rangle$$

What is the probability of the outcome $|0\rangle$ when measuring the leftmost qubit? Let us assume that we indeed observed that the leftmost qubit is at state $|0\rangle$. What is the probability of the outcome $|1\rangle$ when measuring the rightmost qubit?

Exercise 23. Consider the quantum state,

$$\frac{1}{\sqrt{2}}\,|00\rangle + \frac{1}{\sqrt{2}}\,|11\rangle$$

What is the probability of the outcome $|0\rangle$ when measuring the leftmost qubit? What is the probability of the outcome $|1\rangle$ when measuring the rightmost qubit? Assume that we indeed observed that the leftmost qubit is at state $|0\rangle$. Then what is the probability of the outcome $|1\rangle$ when measuring the rightmost qubit? [5]

3 Entanglement

Consider two vector spaces V and W. We say that a vector $u \in V \otimes W$ is entangled if it cannot be written as $v \otimes w$ for some $v \in V$ and $w \in W$. In words, the state u (of a composite system) is entangled if it cannot be seen as a mere aggregation v, w of states (of the constituent systems). If the state u is not entangled then we say that is separable.

Exercise 24. Show that the quantum state,

$$\frac{1}{\sqrt{2}}\,|00\rangle + \frac{1}{\sqrt{2}}\,|11\rangle$$

is entangled.

[5] The quantum state briefly studied in this exercise is one of those that gave rise to the famous phrase ‘spooky action at a distance’ by A. Einstein.

The quantum state $\frac{1}{\sqrt{2}}\left|00\right\rangle + \frac{1}{\sqrt{2}}\left|11\right\rangle$ (mentioned in the previous exercise) can be obtained from the unitary map $CX\cdot(H\otimes\mathrm{id})$ and the initial state $\left|0\right\rangle\otimes\left|0\right\rangle$, where $CX : \mathbb{C}^2\otimes\mathbb{C}^2 \to \mathbb{C}^2\otimes\mathbb{C}^2$ reads as "controlled not" and is defined as,

$$CX\left|00\right\rangle = \left|00\right\rangle, \qquad CX\left|01\right\rangle = \left|01\right\rangle, \qquad CX\left|10\right\rangle = \left|11\right\rangle, \qquad CX\left|11\right\rangle = \left|10\right\rangle.$$

In a nutshell CX flips the state of the second qubit depending on the state of the first qubit being $\left|0\right\rangle$ or $\left|1\right\rangle$ – such a behaviour extends to all elements of $\mathbb{C}^2\otimes\mathbb{C}^2$ by linearity. Actually, any initial state $\left|i\right\rangle\otimes\left|j\right\rangle$ in the usual basis of $\mathbb{C}^2\otimes\mathbb{C}^2$ and the operator $CX\cdot(H\otimes\mathrm{id})$ yield an entangled quantum state. The four states obtained in this way are usually called Bell states, and are defined as follows:

$$\frac{1}{\sqrt{2}}\left|00\right\rangle + \frac{1}{\sqrt{2}}\left|11\right\rangle \qquad \frac{1}{\sqrt{2}}\left|00\right\rangle - \frac{1}{\sqrt{2}}\left|11\right\rangle \qquad \frac{1}{\sqrt{2}}\left|01\right\rangle + \frac{1}{\sqrt{2}}\left|10\right\rangle \qquad \frac{1}{\sqrt{2}}\left|01\right\rangle - \frac{1}{\sqrt{2}}\left|10\right\rangle$$

References

[BM17] Roberto Bruni and Ugo Montanari. *Models of computation.* Springer, 2017.

[NC02] Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.