Quantum Computing @ MEF

Background

Renato Neves

nevrenato@di.uminho.pt

1 Quantum States

Models of computation traditionally 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 get familiar with both vector spaces and the more refined notion of an inner product space. We will also need to delve deep into the inner workings of maps between vector spaces and maps between inner product spaces, both intuitively giving rise to the notion of a quantum state transition.

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:

$$v + (u + w) = (v + u) + w \qquad v + u = u + v$$
$$v + 0 = v \qquad v + (-v) = 0$$
$$(sr) \cdot v = s \cdot (r \cdot v) \qquad 1 \cdot v = v$$
$$s \cdot (v + u) = s \cdot v + s \cdot u \qquad (s + r) \cdot v = s \cdot v + r \cdot u$$

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. Note that the complex numbers themselves form a vector space, and that the set $\mathbb{C}^2$ of pairs of complex numbers also forms a vector space. Recall that this last set underlies the mathematical representation of a qubit – i.e. the unit in quantum information (later on we will see that our notion of quantum state is based on sequences of qubits).

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

[1] In this course we will only consider vector spaces over the complex numbers.

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.

Another important concept for the notion of quantum state and quantum state transition is that of tensoring. In essence, it allow us to mathematically represent multiple qubits (instead of working with just one) and thus to increase the computational power at hand[2].

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 $v_i \in V$, $w_i \in W$, that satisfies the equations,

$$(v \otimes w) + (u \otimes w) = (v + u) \otimes w \qquad (w \otimes v) + (w \otimes u) = w \otimes (v + u)$$
$$s(v \otimes w) = (sv) \otimes w \qquad s(v \otimes w) = v \otimes (sw)$$

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 that there exist linear isomorphisms $V \otimes W \simeq W \otimes V$ and $V \otimes \mathbb{C} \simeq V$.

Exercise 5. Show that the map $\Delta : V \to V \otimes V$ defined by $\Delta(v) = v \otimes v$ is *non-linear*. How is this related to the no-cloning theorem?

Another concept that we will use extensively 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 $v_1, \ldots, v_n \in B$ and $s_1, \ldots, s_n \in \mathbb{C}$ such that $\sum_{i \leq n} s_i v_i = v$
- for every sequence of vectors $v_1, \ldots, v_n \in B$ and sequence of complex numbers $s_1, \ldots, s_n \in \mathbb{C}$ 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 $\mathbb{C}^2$.

[2]This is actually critical for taking full advantage of quantum computing.

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 finite numbers of qubits at a time. 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 the basis of V. 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 are often a convenient way of expressing states and computing state transitions. In our case we are fortunate enough that states $\mathbb{C} \to V$ and linear maps $V \to W$ can be equivalently represented as matrices (whose dimensions depend on those of V and W). We briefly describe how this works next. Let V and W be vector spaces, $\{b_1, \ldots, b_n\}$ a basis for V and $\{c_1, \ldots, c_m\}$ 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 $s_{i1}, \ldots, s_{im} \in \mathbb{C}$. We obtain a matrix $M \in \mathsf{Mat}_{\mathbb{C}}(m, n)$ by setting $M_{ji} = s_{ij}$. Conversely, consider a matrix $M \in \mathsf{Mat}_{\mathbb{C}}(m, n)$. We obtain 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 corresponding to 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 corresponding to 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 $f(0, 1) = \frac{1}{\sqrt{2}}(1, 0) - \frac{1}{\sqrt{2}}(1, 0)$?

In the sequel, let $M : n \to m$ denote a matrix with n lines, m columns, and whose values are complex numbers. Also for two matrices $M : n \to m$ and $N : m \to o$, let $MN : n \to o$ 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, let $M_f : m \to n$ denote the corresponding matrix.

Exercise 11. Show that elements of $v \in V$ are in one-to-one correspondence with elements M_v of $\mathsf{Mat}_{\mathbb{C}}(n, 1)$. Then show that $M_f M_g = M_{g \cdot f}$.

Exercise 12. 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 $\mathbb{C}^n \otimes \mathbb{C}^m \simeq \mathbb{C}^{nm}$.

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,

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

Note that $M_{f \otimes g} = M_f \otimes M_g$.

Exercise 13. For a given matrix $M : n \to m$, let us 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 $(M^T)^*$, i.e. the conjugate transpose 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,

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

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

Exercise 14. 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,

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

Every inner product space V induces a norm $\| \cdot \| : V \to [0, \infty)$ defined by $\|v\| = \sqrt{\langle v, v \rangle}$. The mathematical representation of the state of n-qubits is a vector $v \in \mathbb{C}^{2^n}$ with norm $\|v\| = 1$.

Exercise 15 (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 are orthogonal to each other.

Exercise 16. 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,

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

Exercise 17. 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 $V \otimes W$.

The notion of reversible computation in quantum computing is related to the following fact. 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 often called the Hermitian conjugate (or adjoint) of f – its matrix representation is precisely the conjugate transpose of the matrix M_f. A particularly important family of operations that builds on this notion is that of unitary maps.

Definition 8 (Unitary maps)**.** Let V be an inner product space. A linear map $f : V \to V$ is called unitary if f^{-1} exists and $f^{-1} = f^\dagger$. An equivalent (and insightful) characterisation of unitary maps tells that they are precisely those that satisfy the equation,

$$\|v\| = \|f(v)\|$$

which in the particular case of $V = \mathbb{C}^{2^n}$ means that quantum states are always mapped to quantum states (and not something else).

Exercise 18. 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 19. Prove that if two linear maps are unitary then their tensor is also unitary.

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. [3]

2 Quantum Measurement

In order to render notation more convenient, 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 $|b_1, \ldots, b_n\rangle$.

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,

$$m_0(|0\rangle) = |0\rangle \qquad\qquad m_0(|1\rangle) = 0$$

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

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,

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

We call maps built in this way and by composing them with one another 'measurement maps'.

Postulate 2 (Quantum measurement)**.** Let $v \in \mathbb{C}^{2^n}$ be a quantum state 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 after the observed outcome is defined by,

$$\frac{m(v)}{\|m(v)\|}$$

Exercise 20. 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 21. 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 22. 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?

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.