Quantum Computing @ MEF

Background

Ana Neri

ana.i.neri@inesctec.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 $+ : V + V \to V$, 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 $v, u, w \in V$, $s, r \in \mathbb{C}$:

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

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.

1. Show that for any finite set n we can build a vector space $\mathbb{C}^n$ over the complex numbers.
2. 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).

Exercise 2.

Consider the following matrices:

$Id = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$; $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$; $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$; $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$; $S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$;

Determine each of the following:

1. $Z \cdot S$
2. $S \cdot S$
3. $H \cdot H$
4. $H \cdot X \cdot H$

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 3.

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.

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,

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

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 $v_1, \ldots, v_n \in B$ 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 $\mathbb{C}^2$.

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 4.

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.

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, $\{b_1, \ldots, b_n\}$ 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 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 5.

1. 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 $f(0,1) = (1,0)$?
2. 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 6.

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 $V \otimes W$.

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,

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

Exercise 7.

Consider the matrices in exercise 2. Determine each of the following:

1. $H \otimes Id$
2. $Id \otimes X$
3. $Id \otimes (H \cdot Z \cdot H)$

Definition 5 (Tranpose)**.** Let A be a matrix. $A[j,k]$ represents the j-th row , k-th column element of A. The transpose of A is

$$A^T[j,k] = A[k,j] \tag{1}$$

Definition 6 (Conjugate)**.**

$$\overline{A}[j,k] = \overline{A[j,k]} \tag{2}$$

Definition 7 (Adjoint)**.**

$$A^\dagger = (\overline{A}^T) = (\overline{A^T}) \tag{3}$$

or

$$A^\dagger[j,k] = \overline{A[k,j]} \tag{4}$$

1.2 Inner product spaces

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

Definition 8 (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]

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 8 (Vector normalisation).

Let $v \in V$ be a vector. Show that,

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

Definition 9 (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 9.

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

Definition 10 (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,

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

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 11 (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 12 (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 10.

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 $g(0, 1) = \frac{1}{\sqrt{2}}(1, 0) - \frac{1}{\sqrt{2}}(0, 1)$.

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 $M_f^\dagger$.

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.