MAT 4930: Quantum Algorithms and Complexity **Spring 2021**

Lecture 2: Vectors in the Dirac Notation

Lecturer: Jean-François Biasse *TA: Robert Hart*

2.1 Complex vector spaces

Vectors $\mathbf{x}$ of the vector space $\mathbb{C}^n$ are n-tuple $(x_1, \dots, x_n) \in \mathbb{C}^n$ satisfying the following conditions:

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix} \quad \text{and} \quad \forall c \in \mathbb{C}, c \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} cx_1 \\ \vdots \\ cx_n \end{pmatrix}.$$

Definition 2.1 (Basis of $\mathbb{C}^n$) *A set of vectors $\boldsymbol{v}_1, \cdots, \boldsymbol{v}_n$ of $\mathbb{C}^n$ is a basis if*

$$\forall \boldsymbol{x} \in \mathbb{C}^n \quad \exists!\, (\lambda_1, \dots, \lambda_n), \quad \boldsymbol{x} = \sum_i \lambda_i \boldsymbol{v}_i$$

It can be proved that a basis of $\mathbb{C}^n$ has always n vectors. There are infinitely many ways to create a basis of $\mathbb{C}^n$, and changes of bases will have of particular importance in quantum algorithms. There is however a basis that is especially important to us, namely the *canonical basis*.

Definition 2.2 (Canonical basis) *The canonical basis of $\mathbb{C}^n$ is the set of vectors $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ defined by*

$$\boldsymbol{e}_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \boldsymbol{e}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \end{pmatrix}, \dots, \boldsymbol{e}_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

In the following, we will keep the notation $(\mathbf{e}_i)_{i \leq n}$ to describe the canonical basis of $\mathbb{C}^n$ when there is no ambiguity. Note that we always have $(x_1, \dots, x_n) = \sum_i x_i \mathbf{e}_i$.

2.2 The Dirac notation

Thoughout this course, we will be using the so-called Dirac notation. This notation introduced by Dirac is prominent in quantum science. It is therefore really important to be familiar with it in quantum computing.

Definition 2.3 (Complex conjugate) *Let $c = a + ib \in \mathbb{C}$ for $a, b \in \mathbb{R}$ be a complex number. We denote by c^* its complex conjugate, which is defined as*

$$c^* = a - ib.$$

The Dirac notation is also called the "Bra-ket" notation because is is in fact a notation for two different things: rwo vectors which are *bra* and column vectors that are *kets*.

Definition 2.4 (Bra-ket notation) *Let $\boldsymbol{x} = (x_1, \dots, x_n) \in \mathbb{C}^n$ be an n-tuple of complex numbers. We define the following complex vectors:*

- *The **bra** associated to $\boldsymbol{x}$ is $\langle \boldsymbol{x} | = \begin{pmatrix} x_1^* & \dots & x_n^* \end{pmatrix}$.*
- *The **ket** associated to $\boldsymbol{x}$ is $| \boldsymbol{x} \rangle = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$*

Notice the complex conjugation in the bra. This will be important in the inner product defined in Section 2.3. Before moving on to actual calculations involving vectors in the Dirac notation, we introduce a special notation for the canonical basis which we will re-use extensively in this course.

Definition 2.5 (Canonical basis in Dirac notation) *Let $(\boldsymbol{e}_i)_{i \leq n}$ be the canonical basis of $\mathbb{C}^n$. We define*

$$|i\rangle = \boldsymbol{e}_i.$$

Example 1 *Here are a few examples of canonical basis vectors in the Dirac notation. Note that it is important to specify the ambiant vector space (i.e. which n we are working with).*

- *$|0\rangle \in \mathbb{C}^2$ corresponds to $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$.*
- *$|0\rangle \in \mathbb{C}^4$ corresponds to $\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$.*
- *$|3\rangle \in \mathbb{C}^4$ corresponds to $\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$.*

Notice that counter-intuitively, $|0\rangle$ is not the zero vector!

2.3 Inner product

The inner product in $\mathbb{C}^n$ is the Hermitian form defined by

$$\langle \mathbf{x} | \mathbf{y} \rangle = \begin{pmatrix} x_1^* & \dots & x_n^* \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \sum_{i=1}^{n} x_i^* y_i.$$

Example 2 *Here are a few examples of inner products:*

- $\langle 3,2,1|1,2,3\rangle = 3\times 1 + 2\times 2 + 1\times 3 = 10.$
- $\langle 3,2,1|1,2i,3\rangle = 3\times 1 + 2\times 2i + 1\times 3 = 6+4i.$
- $\langle 3,2i,1|1,2,3\rangle = 3\times 1 - 2i\times 2 + 1\times 3 = 6-4i.$
- *For* $i \in \mathbb{Z}_{\geq 0}$, $\langle i|i\rangle = 1$.
- *For* $i \neq j \in \mathbb{Z}_{\geq 0}$, $\langle i|j\rangle = 0$.

Proposition 2.6 *For all* $|\psi\rangle \in \mathbb{C}^n$, *we have* $\langle\psi|\psi\rangle \geq 0$, *and the function*

$$|\psi\rangle \longmapsto \sqrt{\langle\psi|\psi\rangle} := \|\langle\psi|\|$$

is a norm that generalizes the Euclidean norm in $\mathbb{R}^n$.

Proof: Let $(x_i)_{i\leq n} \in \mathbb{C}^n$. Then we have

$$\langle x_1,\ldots,x_n|x_1,\ldots,x_n\rangle = \sum_i x_i^* x_i = \sum_i |x_i|^2.$$

Necessarily, $\langle x_1,\ldots,x_n|x_1,\ldots,x_n\rangle \geq 0$. Moreover, we have the additional properties that make this function a norm:

- $\sum_i |x_i|^2 = 0 \Leftrightarrow x_i = 0\ \forall i \Leftrightarrow \mathbf{x} = 0.$
- $\forall\lambda \in \mathbb{C}$, $\sqrt{\sum_i |\lambda x_i|^2} = \sqrt{|\lambda|^2}\sqrt{\sum_i |x_i|^2} = |\lambda|\sqrt{\langle\mathbf{x}|\mathbf{x}\rangle}.$

■

2.4 Orthonormal bases

Orthonormal bases play a crucial role in quantum science. As we will see later in this course, they represent *observables*, i.e. values that can be measured. Therefore, we will need to casually perform calculations that use the unique properties of orthonormal bases.

Definition 2.7 (Orthonormal family) *We say that* $|\psi_1\rangle,\ldots,|\psi_k\rangle \in \mathbb{C}^n$ *is an orthonormal family of vectors if:*

- $\forall i \leq k$, $\langle\psi_k|\psi_k\rangle = 1$.
- $\forall i \neq j$, $\langle\psi_i|\psi_j\rangle = 0$.

Example 3 *The canonical basis* $(|i\rangle)_{i\leq n} \in \mathbb{C}^n$ *is an orthonormal family of vectors in* $\mathbb{C}^n$.

We mention a couple of important properties:

Proposition 2.8 *The following properties hold:*

- *An orthonormal family of vectors* $|\psi_1\rangle, \ldots, |\psi_k\rangle \in \mathbb{C}^n$ *is always linearly independant.*
- *If an orthnormal family of* $\mathbb{C}^n$ *has* n *element, then it is a basis which we denote an orthonormal basis.*

Orthonormality is very convenienient when it comes to decompose an input vector in the span of the family (a case of particular interest is when we consider orthonormal bases of course).

Proposition 2.9 *Let* $|\psi_1\rangle, \ldots, |\psi_k\rangle \in \mathbb{C}^n$ *be an orthonormal family. If* $|psi\rangle = \sum_i \lambda_i |\psi_i\rangle$*, then necessarily*

$$\lambda_1 = \langle\psi_1|\psi\rangle, \lambda_2 = \langle\psi_2|\psi\rangle, \ldots, \lambda_n = \langle\psi_n|\psi\rangle.$$

Proof:

$$\forall i \leq k,\ \langle\psi_i|\psi\rangle = \langle\psi_i|\sum_j \lambda_j \psi_j\rangle = \sum_j \lambda_j \underbrace{\langle\psi_i|\psi_j\rangle}_{0 \text{ if } i \neq j} = \lambda_i.$$

■

Example 4 *Let us consider the vectors*

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), \quad |\psi_2\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right).$$

As an exercise, verify that $|\psi_1\rangle, |\psi_2\rangle$ *is an orthonormal basis of* $\mathbb{C}^2$*. Then, we observe that*

- $\langle 1|\psi_1\rangle = \frac{1}{\sqrt{2}}$
- $\langle 1|\psi_2\rangle = \frac{-1}{\sqrt{2}}$

Thus, we conclude that $|1\rangle = \frac{1}{\sqrt{2}}\left(|\psi_1\rangle - |\psi_2\rangle\right)$.

Finally, we mention that any linearly independant family of vectors can be turned into an orthonormal family via the Gram-Schmidt orthogonalization process.

Definition 2.10 (Gram-Schmidt process) *Let* $|\psi_1\rangle, \ldots, |\psi_k\rangle \in \mathbb{C}^n$ *be linearly independent vectors. The Gram-Schmidt process consists in the following steps:*

$$\begin{aligned}
&|\boldsymbol{u}_1\rangle = |\psi_1\rangle, \quad |\boldsymbol{v}_1\rangle = \frac{|\boldsymbol{u}_1\rangle}{\langle\boldsymbol{u}_1|\boldsymbol{u}_1\rangle} \\
&|\boldsymbol{u}_2\rangle = |\psi_2\rangle - \langle\boldsymbol{v}_1|\psi_2\rangle|\boldsymbol{v}_1\rangle, \quad |\boldsymbol{v}_2\rangle = \frac{|\boldsymbol{u}_2\rangle}{\langle\boldsymbol{u}_2|\boldsymbol{u}_2\rangle} \\
&|\boldsymbol{u}_3\rangle = |\psi_3\rangle - \langle\boldsymbol{v}_1|\psi_3\rangle|\boldsymbol{v}_1\rangle - \langle\boldsymbol{v}_2|\psi_3\rangle|\boldsymbol{v}_2\rangle, \quad |\boldsymbol{v}_3\rangle = \frac{|\boldsymbol{u}_3\rangle}{\langle\boldsymbol{u}_3|\boldsymbol{u}_3\rangle} \\
&\quad\vdots \\
&|\boldsymbol{u}_k\rangle = |\psi_k\rangle - \sum_{i<k}\langle\boldsymbol{v}_i|\psi_k\rangle|\boldsymbol{v}_i\rangle, \quad |\boldsymbol{v}_k\rangle = \frac{|\boldsymbol{u}_k\rangle}{\langle\boldsymbol{u}_k|\boldsymbol{u}_k\rangle}
\end{aligned}$$

Proposition 2.11 *The family created during the Gram-Schmidt process is orthonormal and is a basis of the span of* $|\psi_1\rangle, \ldots, |\psi_k\rangle$*.*

Proof: By induction, it is clear that each $|\mathbf{v}_i\rangle$ is in the span of $|\psi_1\rangle, \ldots, |\psi_k\rangle$. Likewise, it is clear that they all have norm 1. If we can prove that $\langle \mathbf{v}_i|\mathbf{v}_j\rangle = 0$ for $i \neq j$, then this would imply that they are an orthonormal family, thus linearly independant, which mean they are a basis of the span of $|\psi_1\rangle, \ldots, |\psi_k\rangle$.

To prove that $\langle \mathbf{v}_i|\mathbf{v}_j\rangle = 0$ for $i \neq j$, we fist notice that

$$\forall 1 < j \leq k,\ |\mathbf{u}_j\rangle = |\psi_j\rangle - \sum_{l<j} \langle \mathbf{v}_l|\psi_j\rangle |\mathbf{v}_l\rangle.$$

Then we prove by induction on $j \leq k$ that the $(|\mathbf{v}_i\rangle)_{i \leq j}$ are an orthonormal family. By linearity of the inner product, we have

$$\forall i < j, \quad \langle \mathbf{v}_i|\mathbf{u}_j\rangle = \langle \mathbf{v}_i|\psi_j\rangle - \sum_{l<j} \langle \mathbf{v}_l|\psi_j\rangle \underbrace{\langle \mathbf{v}_i|\mathbf{v}_l\rangle}_{0 \text{ if } l \neq i \text{ by induction}} = \langle \mathbf{v}_i|\psi_j\rangle - \langle \mathbf{v}_i|\psi_j\rangle = 0.$$

■