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

Lecture 3: Matrices

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

3.1 Basic Definitions

In this course, we focus our attention on matrices over $\mathbb{C}$. An m by n matrice over $\mathbb{C}$ is give by $n.m$ coefficients in $\mathbb{C}$ ordered in an array:

$$A = \begin{pmatrix} a_{00} & \dots & a_{0n} \\ \vdots & \ddots & \vdots \\ a_{m0} & \dots & a_{mn} \end{pmatrix}.$$

We denote the space of m by n matrices over $\mathbb{C}$ by $\mathbb{C}^{m\times n}$. They form a group for the addition law induced by the addition over $\mathbb{C}$:

$$\begin{pmatrix} a_{00} & \dots & a_{0n} \\ \vdots & \ddots & \vdots \\ a_{m0} & \dots & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{00} & \dots & b_{0n} \\ \vdots & \ddots & \vdots \\ b_{m0} & \dots & b_{mn} \end{pmatrix} = \begin{pmatrix} a_{00}+b_{00} & \dots & a_{0n}+b_{0n} \\ \vdots & \ddots & \vdots \\ a_{m0}+b_{mn} & \dots & a_{mn}+b_{mn} \end{pmatrix}.$$

We can also define the multiplication of two matrices, but unlike the above, this is not a straightforward generalization of the same law on complex numbers applied coefficient-wise. First of all, a multiplication can only occur between a matrix $A \in \mathbb{C}^{m\times n}$ and a matrix $B \in \mathbb{C}^{n\times k}$. Then, the multiplication of two matrices is given by the following formula:

$$\begin{aligned} AB &= \begin{pmatrix} a_{00} & \dots & a_{0n} \\ \vdots & \ddots & \vdots \\ b_{m0} & \dots & b_{mn} \end{pmatrix} \begin{pmatrix} b_{00} & \dots & b_{0k} \\ \vdots & \ddots & \vdots \\ b_{n0} & \dots & b_{nk} \end{pmatrix} \\ &= \begin{pmatrix} a_{00}b_{00}+ ... + a_{0n}b_{n0} & \dots & a_{00}b_{0k}+ ... + a_{0n}b_{nk} \\ \vdots & \ddots & \vdots \\ a_{m0}b_{00}+ ... + a_{mn}b_{n0} & \dots & a_{m0}b_{0k}+ ... + a_{mn}b_{nk} \end{pmatrix} \in \mathbb{C}^{m\times k} \end{aligned}$$

Example 1 *Let us consider the matrices*

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad B = \begin{pmatrix} 1 & 2 \\ 0 & 0 \\ 1 & 0 \end{pmatrix}$$

The multiplication between A and B is given by

$$\begin{aligned} AB &= \begin{pmatrix} 1\times 1 + 1\times 0 + 1\times 1 & 1\times 2 + 1\times 0 + 1\times 0 \\ 0\times 1 + 1\times 0 + 0\times 1 & 0\times 2 + 1\times 0 + 0\times 0 \end{pmatrix} \\ &= \begin{pmatrix} 2 & 2 \\ 0 & 0 \end{pmatrix} \end{aligned}$$

Row vectors (kets) in $\mathbb{C}^n$ can be seen as matrices in $\mathbb{C}^{n\times 1}$ while column vectors can be seen as matrices in $\mathbb{C}^{1\times n}$. Multiplication between vectors and matrices can therefore be performed by simply following the matrix-matrix multiplication rule:

$$A|\mathbf{v}\rangle = \begin{pmatrix} a_{00} & \dots & a_{0n} \\ \vdots & \ddots & \vdots \\ a_{m0} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} v_0 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} a_{00}v_0 & \dots & a_{0n}v_n \\ \vdots & \ddots & \vdots \\ a_{m0}v_0 & \dots & a_{mn}v_n \end{pmatrix}$$

Example 2 *Let us define*

$$|\boldsymbol{v}\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

Then the matrix-vector product is

$$A|\boldsymbol{v}\rangle = \begin{pmatrix} 1\times 0 + 1\times 1 \\ 1\times 0 + 1\times 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

3.2 Outer product

Inner products can be viewed as a matrix mutiplication between a bra and a ket which results in a matrix in $\mathbb{C}^{1\times 1}$, that is: identified by a single coefficient in $\mathbb{C}$. Likewise, the multiplication between a ket and a bra also result in a matrix, which has interesting properties.

Definition 3.1 (Outer product) *Let $|\boldsymbol{x}\rangle$ and $|\boldsymbol{y}\rangle$ be two vectors in $\mathbb{C}^n$, the outer product between them is defined by*

$$|x\rangle\langle y| = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \begin{pmatrix} y_1^* & \dots & y_n^* \end{pmatrix} = \begin{pmatrix} x_1y_1^* & \dots & x_1y_n^* \\ \vdots & \ddots & \vdots \\ x_ny_1^* & \dots & x_ny_n^* \end{pmatrix}.$$

Example 3 *Here are a couple of examples of outer products in the Dirac notation:*

$$\begin{aligned} |0\rangle\langle 0| &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 1\times 1 & 0\times 1 \\ 1\times 0 & 0\times 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \end{aligned}$$

$$\begin{aligned} |1\rangle\langle 0| &= \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0\times 1 & 0\times 1 \\ 1\times 1 & 0\times 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \end{aligned}$$

The above example suggests a pattern for the outer multiplication between vectors of the canonical basis.

Proposition 3.2 *Let $n > 1$, for all $0 \leq i, j \leq n-1$, we have*

$$|i\rangle\langle j| = M^{i,j} \in \mathbb{C}^{n\times n}$$

where the coefficients of $M^{i,j}$ are given by

- $M^{i,j}_{k,l} = 1$ *if* $k = i$ *and* $l = j$.
- $M^{i,j}_{k,l} = 0$ *otherwise.*

For example, the matrix with ones on the diagonal and zeros everywhere else (known as the identity matrix) is given by $I_n = \sum_{i<n} |i\rangle\langle i|$.

3.3 Projectors

Let $|\psi_1\rangle, \ldots, |\psi_k\rangle$ be an orthonormal family of vectors of $\mathbb{C}^n$ for $0 < k < n$. Let $V \subseteq \mathbb{C}^n$ be the k-dimensional vectors space spanned by the family $(|\psi_i\rangle)_{i\leq k}$, and let $V^\perp$ its orthogonal complement, i.e.

$$V^\perp := \{|\phi\rangle \in \mathbb{C}^n \text{ such that } \forall i \leq k \text{ we have } \langle\psi_i|\phi\rangle = 0\}$$

Then we can decompose $\mathbb{C}^n$ as the direct sum between V and $V^\perp$, that is:

Proposition 3.3 *For each $|\boldsymbol{x}\rangle \in \mathbb{C}^n$, there exist a unique pair $|\boldsymbol{x}_1\rangle \in V$ and $|\boldsymbol{x}_2\rangle$ such that $|\boldsymbol{x}\rangle = |\boldsymbol{x}_1\rangle + |\boldsymbol{x}_2\rangle$. We denote this property by*

$$\mathbb{C}^n = V \oplus V^\perp.$$

There is a linear operator P_V that returns the summand belonging to V, which we call the projection onto V:

$$P_V : |\mathbf{x}\rangle \in \mathbb{C}^n \longmapsto |\mathbf{x}_1\rangle \in V \text{ where } |\mathbf{x}\rangle = |\mathbf{x}_1\rangle + |\mathbf{x}_2\rangle \text{ with } |\mathbf{x}_2\rangle \in V^\perp$$

As we previously saw with inner products, the decomposition of $|\mathbf{x}_1\rangle$ with respect to the othonormal family of vectors $(|\psi_i\rangle)_{i\leq k}$ is given by the coefficiens $\langle\psi_i|\mathbf{x}_1\rangle$. Since $|\mathbf{x}_2\rangle \in V^\perp$, these coefficients are also equal to $\langle\psi_i|\mathbf{x}_1 + \mathbf{x}_2\rangle = \langle\psi_i|\mathbf{x}\rangle$. Hence, we can give the following expression for the projection onto V:

$$P_V = |\psi_1\rangle\langle\psi_1| + |\psi_2\rangle\langle\psi_2| + \ldots + |\psi_k\rangle\langle\psi_k|.$$

Example 4 *Let $|\psi_1\rangle = |0\rangle \in \mathbb{C}^2$ and $V = \mathrm{Span}(|\psi_1\rangle)$. Then $P_V = |0\rangle\langle 0|$, and for all $|\boldsymbol{x}\rangle = x_0|0\rangle + x_1|1\rangle$ we have*

$$P_V|\boldsymbol{x}\rangle = |0\rangle\langle 0|(x_0|0\rangle + x_1|1\rangle) = x_0|0\rangle\langle 0|0\rangle + x_1|0\rangle\langle 0|1\rangle = x_0|0\rangle.$$

Example 5 *Let*

- $|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \in \mathbb{C}^4$,
- $|\psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \in \mathbb{C}^4$,
- *and* $V = \mathrm{Span}(|\psi_1\rangle, |\psi_2\rangle)$.

Then $P_V = |\psi_1\rangle\langle\psi_1| + |\psi_2\rangle\langle\psi_2|$ and for all $|\boldsymbol{x}\rangle = x_0|0\rangle + x_1|1\rangle + x_2|2\rangle + x_3|3\rangle$ we have

$$\begin{aligned}
P_V|\boldsymbol{x}\rangle &= |\psi_1\rangle\langle\psi_1|(x_0|0\rangle + x_1|1\rangle + x_2|2\rangle + x_3|3\rangle) + |\psi_2\rangle\langle\psi_2|(x_0|0\rangle + x_1|1\rangle + x_2|2\rangle + x_3|3\rangle) \\
&= \left(\frac{x_1}{\sqrt{2}} + \frac{x_2}{\sqrt{2}}\right)|\psi_1\rangle + \left(\frac{x_1}{\sqrt{2}} - \frac{x_2}{\sqrt{2}}\right)|\psi_2\rangle \\
&= x_0|0\rangle + x_1|1\rangle
\end{aligned}$$

3.4 Unitary matrices

We say that a matrix $A \in \mathbb{C}^{n\times n}$ is invertible if there exists a matrix $A^{-1}\mathbb{C}^{n\times n}$ such that

$$AA^{-1} = A^{-1}A = I_n = |0\rangle\langle 0| + |1\rangle\langle 1| + \ldots + |n-1\rangle\langle n-1|.$$

The matrix $I_n = \sum_i |i\rangle\langle i| \in \mathbb{C}^{n\times n}$ is called the identity matrix as it is an identity for the multiplication law.

Proposition 3.4 *A matrix $A \in \mathbb{C}^{n\times n}$ is inversible if and only if* $\det(A) \neq 0$.

A linear operator A has a unique adjoint, or Hermitian conjugate that satisfies the following property:

$$\forall |\mathbf{x}_1\rangle, |\mathbf{x}_2\rangle \in \mathbb{C}^n,\ \langle \mathbf{x}_1|(A|\mathbf{x}_2\rangle) = \langle \mathbf{y}_1|\mathbf{x}_2\rangle \text{ for } |\mathbf{y}_1\rangle = A^\dagger|\mathbf{x}_1\rangle$$

Proposition 3.5 *The matrix corresponding to the adjoint of the linear operator represented by A is the conjugate of the transpose of A, that is $A^\dagger = \left(A^T\right)^*$.*

Definition 3.6 (Unitary matrix) *A matrix $U \in \mathbb{C}^{n\times n}$ is said to be unitary if it has the property that*

$$UU^\dagger = U^\dagger U = I_n.$$

Unitary matrices play an important role in quantum computing as they represent the evolution of a closed quantum system.

Example 6 *A typical example of unitary matrices is the Pauli Matrices which are defined by*

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},\ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$