Mathematics of Quantum Computation I

Wim van Dam
Department of Computer Science, University of California at Santa Barbara, Santa Barbara, CA 93106-5110, USA

Notes for the graduate course "Quantum Computation and Quantum Information" (290A), Spring 2005. v1

Complex Values: Let $\alpha \in \mathbb{C}$, then we can write this complex value as $\alpha = x + y\mathrm{i}$ with the real and imaginary components $x, y \in \mathbb{R}$. It is often useful to write the value as $\alpha = r\mathrm{e}^{\mathrm{i}\varphi}$ with the norm $r \in \mathbb{R}_{\geq 0}$ and the phase $\varphi \in [0, 2\pi)$. The "norm squared" of α equals $|\alpha^2| = x^2 + y^2 = r^2$. The complex conjugate of α is defined by $\bar{\alpha} = \alpha^* = x - y\mathrm{i} = r\mathrm{e}^{-\mathrm{i}\varphi}$, which can be used in $|\alpha|^2 = \alpha\alpha^*$. The norm $|\alpha| = \sqrt{x^2+y^2} = r$ obeys the triangle inequality $|\alpha+\beta| \leq |\alpha| + |\beta|$ for all $\alpha, \beta \in \mathbb{C}$.

Finite Dimensional Hilbert Space: Let $\mathcal{A}$ be a finite set of $N = |\mathcal{A}|$ basis states. A quantum state, which is in superposition over all basis states $\mathcal{A}$, is represented by a norm one, complex valued vector $\in \mathbb{C}^N$. In Dirac's braket notation, a column vector is denoted by a $|ket\rangle$ and a row vector by a $\langle bra|$. If $|\psi\rangle = \sum_{x\in\mathcal{A}} \alpha_x |x\rangle$, then $\langle\psi| := \sum_{x\in\mathcal{A}} \alpha_x^* \langle x|$ (note the complex conjugation of α_x). Given column vector $|\psi\rangle$, the row vector $\langle\psi|$ is also denoted by $|\psi\rangle^\dagger$ and is called the *conjugate transpose* of $|\psi\rangle$. If $\mathcal{A} = \{1, \ldots, N\}$, we can write in vector notation:

$$|\psi\rangle^\dagger = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_N \end{pmatrix}^\dagger = \begin{pmatrix} \alpha_1^* & \alpha_2^* & \cdots & \alpha_N^* \end{pmatrix} = \langle\psi|. \quad (1)$$

We equip this space with an *inner product* $\langle\cdot|\cdot\rangle : \mathbb{C}^N \times \mathbb{C}^N \to \mathbb{C}$ such that it becomes a *finite dimensional Hilbert space.* For the vectors

$$|\psi\rangle = \sum_{x\in\mathcal{A}} \alpha_x|x\rangle \text{ and } |\phi\rangle = \sum_{x\in\mathcal{A}} \beta_x|x\rangle \quad (2)$$

the inner product $\langle\psi||\phi\rangle$ is expressed by the *braket*

$$\langle\psi|\phi\rangle = \sum_{x\in\mathcal{A}} \alpha_x^*\beta_x = \langle\phi|\psi\rangle^*, \quad (3)$$

where α^* is the *complex conjugate* of $\alpha \in \mathbb{C}$. The *norm* of a vector in $\mathbb{C}^N$ is defined by $\||\psi\rangle\| := \sqrt{\langle\psi|\psi\rangle}$, which for a valid state representation is always one: $\sum_{x\in\mathcal{A}} \alpha_x\alpha_x^* = 1$ (the normalization restriction). For vectors the triangle inequality holds as well: $\|\alpha|\psi\rangle + \beta|\phi\rangle\| \leq \|\alpha|\psi\rangle\| + \|\beta|\phi\rangle\|$.

The *outer product* $|\cdot\rangle\langle\cdot| : \mathbb{C}^N \times \mathbb{C}^N \to \mathbb{C}^{N\times N}$ maps two N-dimensional vectors to an $N \times N$ matrix:

$$|\psi\rangle\langle\phi| = \sum_{x,y\in\mathcal{A}} \alpha_x\beta_y^*|x\rangle\langle y|, \quad (4)$$

where $|x\rangle\langle y|$ is the all-zero matrix with one 1 value in the x-th row and the y-th column.

Braket Calculus: The difference between the inner and the outer product shows that 'multiplying' bras and kets does not commute: $\langle\psi||\phi\rangle \neq |\phi\rangle\langle\psi|$. However, this multiplication *is* associative and distributive. Hence, for example, $|\psi\rangle(\langle\phi| + \langle\phi'|) = |\psi\rangle\langle\phi| + |\psi\rangle\langle\phi'|$ and $(|\psi\rangle\langle\phi|)(|\psi\rangle\langle\phi|) = |\psi\rangle(\langle\phi|\phi\rangle)\langle\psi| = |\psi\rangle\langle\psi|$ (because $\langle\phi|\phi\rangle = 1$).

Measurement Projection: According to quantum mechanics, the 'inner product squared' $|\langle\psi|\phi\rangle|^2 = \langle\psi|\phi\rangle\langle\phi|\psi\rangle$ between two states $|\psi\rangle$ and $|\phi\rangle$ gives the probability that one observes the outcome "$|\psi\rangle$" when one observes the state "$|\phi\rangle$". It is straightforward to verify that $0 \leq |\langle\psi|\phi\rangle|^2 \leq 1$. If $\langle\psi|\phi\rangle = 0$, the two states are *orthogonal.* If $|\langle\psi|\phi\rangle| = 1$, then the two states are identical *up to a general phase factor* (because we can still have $\langle\psi|\phi\rangle = \mathrm{e}^{\mathrm{i}\gamma}$). Although mathematically present, such a general phase difference can never be observed in reality, hence it has no physical relevance.

Tensor Product Construction: We can combine the spaces $\mathbb{C}^N$ and $\mathbb{C}^M$ to a joint space $\mathbb{C}^{NM} := \mathbb{C}^N \otimes \mathbb{C}^M$. If $\mathcal{A}$ and $\mathcal{B}$ are the respective basis sets of these two spaces, then the joint basis of $\mathbb{C}^N \otimes \mathbb{C}^M$ is given by the Cartesian product $\mathcal{A} \times \mathcal{B}$. As a result, using the *tensor product* $\otimes : \mathbb{C}^N \times \mathbb{C}^M \to \mathbb{C}^{NM}$, we can combine the states

$$|\psi\rangle = \sum_{x\in\mathcal{A}} \alpha_x|x\rangle \in \mathbb{C}^N \text{ and } |\phi\rangle = \sum_{y\in\mathcal{B}} \beta_y|y\rangle \in \mathbb{C}^M \quad (5)$$

to the tensor product state

$$|\psi\rangle \otimes |\phi\rangle = |\psi,\phi\rangle = \sum_{x\in\mathcal{A},y\in\mathcal{B}} \alpha_x\beta_y|x,y\rangle \in \mathbb{C}^{NM}. \quad (6)$$

For the conjugate transpose of a tensor product it holds that $(|\psi\rangle \otimes |\phi\rangle)^\dagger = \langle\psi| \otimes \langle\phi|$.

If we assume $\mathcal{A} = \{1, \ldots, N\}$ and $\mathcal{B} = \{1, \ldots, M\}$, then this tensor product equation is described in vector notation by

$$\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_N \end{pmatrix} \otimes \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_M \end{pmatrix} = \begin{pmatrix} \alpha_1\beta_1 \\ \alpha_1\beta_2 \\ \vdots \\ \alpha_1\beta_M \\ \alpha_2\beta_1 \\ \vdots \\ \vdots \\ \alpha_N\beta_M \end{pmatrix}. \quad (7)$$

If $|\psi\rangle$ and $|\phi\rangle$ are norm one vectors, then so is $|\psi\rangle \otimes |\phi\rangle$. Note that the tensor product does not commute: $|\psi\rangle \otimes |\phi\rangle \neq |\phi\rangle \otimes |\psi\rangle$, but that it is associative and distributive. For example, $|\psi\rangle \otimes (|\phi\rangle \otimes |\phi'\rangle) = (|\psi\rangle \otimes |\phi\rangle) \otimes |\phi'\rangle$, and $|\psi\rangle \otimes (\alpha|\phi\rangle + \beta|\phi'\rangle) = |\psi\rangle \otimes \alpha|\phi\rangle + |\psi\rangle \otimes \beta|\psi'\rangle = \alpha|\psi,\phi\rangle + \beta|\psi,\phi'\rangle$.

Unitary Operations: The group of norm preserving, linear operations on $\mathbb{C}^N$ is the group $\mathsf{U}(N)$ of unitary, complex valued $N\times N$ matrices $U\in\mathbb{C}^{N\times N}$ that obey the equality $U\cdot U^\dagger = I$. Here $U^\dagger$ is the *Hermitian conjugate* (or the *conjugate transpose*) of U defined by $U^\dagger_{ij} := U^*_{ji}$ for all $1\le i,j\le N$, and I is the N-dimensional identity matrix. As these operations are linear, we have

$$U|\psi\rangle = \sum_{x\in A}\alpha_x U|x\rangle \tag{8}$$

for all $|\psi\rangle\in\mathbb{C}^N$. *Hence, if we know the values of U on the basis states $|x\in\mathcal{A}\rangle$, we know the values of U on all quantum states in $\mathbb{C}^N$.* We can describe $U\in\mathsf{U}(N)$ as a summation of outer products by

$$U := \sum_{x,y\in A} U_{xy}|x\rangle\langle y|, \tag{9}$$

or equivalently $U_{xy} := \langle x|U|y\rangle$, such that by linearity we see that

$$U|\psi\rangle = \sum_{x,y\in A} U_{xy}|x\rangle\langle y|\sum_{z\in A}\alpha_z|z\rangle = \sum_{x,z\in A}\alpha_z U_{xz}|x\rangle. \tag{10}$$

Unitary matrices are inner product preserving (and hence also norm preserving) as is shown by $\langle\phi|\psi\rangle = \langle\phi|I|\psi\rangle = \langle\phi|U^\dagger U|\psi\rangle = \langle\phi'|\psi'\rangle$, where $|\phi'\rangle := U|\phi\rangle$ and $|\psi'\rangle := U|\psi\rangle$. This shows that U is unitary if and only if the row vectors of U form a orthonormal basis of $\mathbb{C}^N$ (similarly for the columns of U).

Just as with vectors, we can define the tensor product between two matrices. Specifically, if $U\in\mathsf{U}(N)$ and $W\in\mathsf{U}(M)$ are unitary matrices defined by

$$U := \sum_{x,y\in\mathcal{A}} U_{xy}|x\rangle\langle y| \text{ and } W := \sum_{p,q\in\mathcal{B}} W_{pq}|p\rangle\langle q|, \tag{11}$$

then for the tensor product $\otimes : \mathbb{C}^{N\times N}\times\mathbb{C}^{M\times M}\to\mathbb{C}^{NM\times NM}$ we have

$$U\otimes W = \sum_{x,y\in\mathcal{A}}\sum_{p,q\in\mathcal{B}} U_{xy}W_{pq}|x,p\rangle\langle y,q| \in \mathbb{C}^{NM\times NM}. \tag{12}$$

This matrix acts on the space $\mathbb{C}^{NM} = \mathbb{C}^N\otimes\mathbb{C}^M$ spanned by the set of basis states $\mathcal{A}\times\mathcal{B}$. For the states $|\psi\rangle\in\mathbb{C}^N$ and $|\phi\rangle\in\mathbb{C}^M$ we have $(U\otimes W)(|\psi\rangle\otimes|\phi\rangle) = U|\psi\rangle\otimes W|\phi\rangle\in\mathbb{C}^{NM}$. Again assuming $\mathcal{A}=\{1,\ldots,N\}$ and $\mathcal{B}=\{1,\ldots,M\}$, the tensor product of two matrices is described in matrix notation by

$$U\otimes W = \begin{pmatrix} U_{11}W & U_{12}W & \cdots & U_{1N}W \\ U_{21}W & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ U_{N1}W & \cdots & \cdots & U_{NN}W \end{pmatrix} \tag{13}$$

$$= \begin{pmatrix} U_{11}W_{11} & U_{11}W_{12} & \cdots & U_{1N}W_{1M} \\ U_{11}W_{21} & \ddots & & U_{1N}W_{2M} \\ \vdots & & \ddots & \vdots \\ U_{N1}W_{M1} & \cdots & \cdots & U_{NN}W_{MM} \end{pmatrix} \in \mathbb{C}^{NM\times NM}.$$

As was the case with vectors, the tensor product of matrices is not commutative, but it is distributive and associative. Also, if $U,U'\in\mathsf{U}(N)$ and $W,W'\in\mathsf{U}(M)$, then $(U\otimes W)(U'\otimes W') = UU'\otimes WW'$; if U,W are unitary, then so is $U\otimes W$ and $(U\otimes W)^\dagger = U^\dagger\otimes W^\dagger$.

Eigenvector / Eigenvalue Decomposition: We can decompose a unitary matrix $U\in\mathsf{U}(N)$ into its eigenvectors $|\psi_1\rangle,\ldots,|\psi_N\rangle$ and its corresponding eigenvalues $\lambda_1,\ldots,\lambda_N\in\mathbb{C}$. With these values we can express the operator as

$$U = \sum_{i=1}^{N}\lambda_i|\psi_i\rangle\langle\psi_i|. \tag{14}$$

The unitarity of U corresponds with the requirement that all eigenvalues λ_i have norm one, and that the eigenvectors form a orthonormal basis of $\mathbb{C}^N$. The identity matrix I has for all eigenvalues $\lambda_i = 1$. The conjugate transpose of this U is given by

$$U^\dagger = \sum_{i=1}^{N}\lambda_i^*|\psi_i\rangle\langle\psi_i|. \tag{15}$$

When U is as above and $W\in\mathsf{U}(M)$ has eigenvector decomposition $W = \sum_{j=1}^{M}\mu_j|\phi_j\rangle\langle\phi_j|$ then for the tensor product we have

$$V\otimes W = \sum_{i=1}^{N}\sum_{j=1}^{M}\lambda_i\mu_j|\psi_i,\phi_j\rangle\langle\psi_i,\phi_j|. \tag{16}$$

Quantum Computing: The typical setting for a quantum circuit is quantum mechanical system that is described by an n-fold tensor product of two dimensional Hilbert spaces: $\mathbb{C}^2\otimes\mathbb{C}^2\otimes\cdots\otimes\mathbb{C}^2 = \mathbb{C}^{2^n}$ (where each $\mathbb{C}^2$ corresponds to a single qubit). The elementary quantum gates that we can apply to an initial state $|0,\ldots,0\rangle$ are unitary operators that act only a small number of qubits. For example, if we apply the NOT gate $X = \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$ to the second qubit, then the overall unitary operator is described by $I\otimes X\otimes I\otimes\cdots\otimes I\in\mathsf{U}(2^n)$, where the I are the identity operators on the qubits $1,3,\ldots,n$. For operators that act on two non-adjacent qubits, the notation becomes a bit tricky. Consider for example a CNOT gate that acts on the first and the last qubit. To avoid these problems one can introduce the notation where the identity operators are omitted, and a subscript is used to indicate on which qubit the gates act. Hence the previous NOT circuit has the much shorter description $X_2\in\mathsf{U}(2^n)$, and the CNOT example becomes $\mathrm{CNOT}_{1,n}\in\mathsf{U}(2^n)$. Regardless, it is often advisable to draw a quantum circuit diagram to explain the operation.

Further Reading: For more information see Sections 1.2, 1.3 and especially Sections 2–2.1.7 in

- *Quantum Computation and Quantum Information,* M.A. Nielsen and I.L. Chuang, Cambridge University Press (2000).