1 Vector spaces

$\mathbb{C}$ is the set of all complex numbers, i.e. numbers of the form $a + ib$, where a and b are real numbers and i is the imaginary unit. Addition and multiplication of complex numbers follow the usual rules of the real numbers, with the additional equality $i^2 = -1$. The complex *conjugate* of a complex number $c = a + ib$ is $\overline{c} = a - ib$. The *norm* or *modulus* of c is $|c| = \sqrt{\overline{c}c} = \sqrt{a^2 + b^2}$. Every complex number c can be written as $|c| \cdot e^{i\theta}$ for some real number θ, due to the fact that $e^{i\theta} = \cos\theta + i\sin\theta$.

We use $V = \mathbb{C}^d$ to denote the d-dimensional complex vector space, which is the set of all *column* vectors of d complex numbers. We use $\underline{0}$ for the zero vector. If $|v\rangle = (\alpha_1, \ldots, \alpha_d)^T \in V$ then $\langle v| = (\overline{\alpha_1}, \ldots, \overline{\alpha_d})$ denotes the corresponding row vector with conjugated entries. The vector $|v\rangle$ is called a "ket", $\langle v|$ is called a "bra". A set of vectors $|v_1\rangle, \ldots, |v_m\rangle$ is called *linearly independent* if the only way to get $\sum_{i=1}^m a_i|v_i\rangle = \underline{0}$ is to set $a_1 = \cdots = a_d = 0$. A *basis* for V is a set of vectors $|v_1\rangle, \ldots, |v_d\rangle$ such that every vector $|v\rangle \in V$ can be written as a linear combination of those basis vectors $|v\rangle = \sum_{i=1}^d a_i|v_i\rangle$. One can show that a basis is linearly independent. The *inner product* or inproduct of vectors $|v\rangle = (\alpha_1, \ldots, \alpha_d)^T$ and $|w\rangle = (\beta_1, \ldots, \beta_d)^T$ is $\langle v|w\rangle = \langle v| \cdot |w\rangle = \sum_{i=1}^d \overline{\alpha_i}\beta_i$. Note that an inproduct is a "bra-ket" product. Such a vector space with inner product is called a *Hilbert space*. Two vectors are *orthogonal* if their inproduct is 0. The *norm* of $|v\rangle$ is $\| \, |v\rangle \, \| = \sqrt{\langle v|v\rangle} = \sqrt{\sum_i |\alpha_i|^2}$. A *unit vector* has norm 1. A set of pairwise orthogonal unit vectors is called *orthonormal*.

2 Properties of matrices

Every linear function $A : V \to V$ corresponds to a $d \times d$ matrix A. The identity function is the identity matrix I. If $A = (a_{ij})$ is a matrix, we use $A^T = (a_{ji})$ for its *transpose*, which is A "swapped" around the diagonal. The *conjugate transpose* or *adjoint* of A, denoted $A^\dagger$ (or A^*), is the matrix obtained by conjugating the entries of A^T. The following are some of the main properties of matrices:

- The *rank* of A is the size of the largest linearly independent set of columns of A. If the rank of A is d, we say A has *full rank*.
- The *inverse* of A is the unique matrix A^{-1} for which $AA^{-1} = A^{-1}A = I$, if such an A^{-1} exists. A has an inverse iff A has full rank.
- The complex number λ is an *eigenvalue* of A if there is a vector $|v\rangle$ (called *eigenvector*) such that $A|v\rangle = \lambda|v\rangle$.
- The *trace* of A is the sum $tr(A) = \sum_{i=1}^d a_{ii}$ of its diagonal entries. It turns out that $tr(A)$ equals the sum of the eigenvalues of A.
- A is *Hermitian* (or *self-adjoint*) if $A = A^\dagger$. The eigenvalues of a Hermitian matrix are real numbers.
- A is *unitary* if $A^{-1} = A^\dagger$. It can be shown that A is unitary iff A preserves the norm of its argument (i.e. $\| A|v\rangle \| = \| \, |v\rangle \, \|$ for all $|v\rangle$). Because of this, the eigenvalues of unitary matrices have norm 1.

3 Quantum states and operations

A classical bit can take on values 0 and 1. We identify these with the vectors $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, which form a basis of the vector space $\mathbb{C}^2$. A quantum bit or *qubit* can be any *unit* vector $\alpha_0|0\rangle + \alpha_1|1\rangle$ in this vector space. Loosely speaking, such a vector has both values of the bit simultaneously. The complex coefficients α_i are called *amplitudes*.

There are two things that we can do with a quantum state: observe (measure) it or apply some quantum operation to it. According to quantum mechanics, measuring the qubit will give the bit $|b\rangle$ with probability $|\alpha_b|^2$ and will "collapse" the qubit to the observed basis state $|b\rangle$. For instance, if we observe the qubit

$$|\phi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix},$$

then we will see $|0\rangle$ (with probability $(1/\sqrt{2})^2 = 1/2$) or $|1\rangle$ (also with probability $1/2$), and the state will become the observed classical bit. Note that the probabilities sum to 1, because $|\phi\rangle$ is a unit vector.

Apart from measuring, we can also apply some quantum operation to a quantum state. Quantum mechanics stipulates that such operations are linear. Since they must also map quantum states (unit vectors) to quantum states (unit vectors), these operations must preserve norm. Since a linear operation is norm-preserving iff it is unitary, it follows that the class of operations allowed by quantum mechanics is exactly the set of unitary transformations. Because of this, every quantum operation is reversible. Some simple examples of unitary operations on one qubit:

$$N = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}.$$

The first one is just the classical NOT-operation, which negates the bit: $N|0\rangle = |1\rangle$, $N|1\rangle = |0\rangle$, $N(\alpha_0|0\rangle + \alpha_1|1\rangle) = \alpha_0|1\rangle + \alpha_1|0\rangle$. The second one is the highly important *Hadamard* transform and is more "quantum". It maps $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, and for instance $H|\phi\rangle = |0\rangle$. The third one changes the "direction" of the amplitude of the $|1\rangle$ state: $T(\alpha_0|0\rangle + \alpha_1|1\rangle) = \alpha_0|0\rangle + e^{i\pi/4}\alpha_1|1\rangle$.

Different qubits can be combined using *tensor* products. If $A = (a_{ij})$ is an $m \times n$ matrix and B an $m' \times n'$ matrix, then their *tensor* or *Kronecker* product is the $mm' \times nn'$ matrix

$$A \otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{1n}B \\ a_{21}B & \cdots & a_{2n}B \\ & \cdots & \\ a_{m1}B & \cdots & a_{mn}B \end{pmatrix}.$$

Now consider a space of two qubits. Since each of the two qubits can be in two different basis states, the joint system can be in any of $2 \times 2 = 4$ basis states. For instance $|0\rangle \otimes |1\rangle$ is the basis state where the first qubit has value $|0\rangle$ and the second has value $|1\rangle$. We will usually abbreviate $|0\rangle \otimes |1\rangle$ to $|0\rangle|1\rangle$ or even $|01\rangle$. The four basis states $|00\rangle, |10\rangle, |01\rangle, |11\rangle$ form an orthonormal basis for $\mathbb{C}^4$. The 2-qubit quantum states are exactly the unit vectors in this space. If the first qubit is in state $|\phi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ and the second in state $|\psi\rangle = \beta_0|0\rangle + \beta_1|1\rangle$, then their joint state is

$$|\phi\rangle \otimes |\psi\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \otimes \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} = \begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \end{pmatrix} = \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle.$$

Some 2-qubit states cannot be written in this tensor form $|\phi\rangle \otimes |\psi\rangle$. These states are called *entangled*, for example $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. Here the two qubits do not each have their own 'independent" quantum state, but they are "correlated" in a quantum way. For example, if we measure only the first qubit of the above state, then the whole state will collapse to either $|00\rangle$ or $|11\rangle$, which will also immediately fix the value of the unobserved second qubit to a classical state. Finally, if A is an operation on the first qubit and B an operation on the second qubit, then the operation on the joint qubit state is $A \otimes B$. Note that $(A \otimes B)(|\phi\rangle \otimes |\psi\rangle) = A|\phi\rangle \otimes B|\psi\rangle$. Analogous to 2-qubit states, some 2-qubit operations cannot be written as operations $A \otimes B$ on the qubits individually, for example the operation

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

This operation applies a NOT to the second qubit if the first qubit is 1 and does nothing if the first qubit is 0. It is called the "controlled-NOT" operation and is quite important in quantum computing.

This construction can be iterated to get spaces of more than 2 qubits. In general, an n-qubit state is a unit vector in the space $\mathbb{C}^{2^n}$. The 2^n vectors corresponding to the 2^n classical n-bit strings form an orthonormal basis for $\mathbb{C}^{2^n}$.