1 Linear Algebra

We refresh the basic definitions from linear algebra that are needed in the following. In all definitions, we will restrict our attention to the finite dimensional case only.

Definition 1 (Hilbert space) *The n-dimensional* Hilbert space *is $\mathbb{C}^n$, the n-dimensional complex vector space.*[1]*.*

$\mathbb{C}^n$ is endowed with the following inner product*:*

$$\langle \Psi, \Phi \rangle := \sum_{i=1}^{n} \Psi_i^* \Phi_i$$

where x^* is the complex conjugate of x.[2]

The (Euclidean) norm $\|\cdot\|$ *is defined by*

$$\|\Psi\| := \sqrt{\langle \Psi, \Psi \rangle} = \sqrt{\sum_{i=1}^{n} \Psi_i^* \Psi_i} = \sqrt{\sum_{i=1}^{n} |\Psi_i|^2}.$$

We call two vectors Ψ and Φ orthogonal *if $\langle \Psi, \Phi \rangle = 0$. We call Ψ orthogonal to a subspace $V \subseteq \mathbb{C}^n$ if Ψ is orthogonal to all $x \in V$.*

Furthermore, we call a vector *normalised* if $\|\Psi\| = 1$, and we call a *set* of vectors *orthogonal* if they are pairwise orthogonal, and we call a set of vectors *orthonormal* if they are all normalised and pairwise orthogonal.

Definition 2 (Conjugate transpose) *Given a matrix $M \in \mathbb{C}^{n \times n}$, we define $M^\dagger$ as the complex conjugate of the transposition of M, i.e., $(M^\dagger)_{ij} = (M_{ji})^*$. (This is the analogue of transposition.)*

We have $(M^\dagger)^\dagger = M$ and $\langle Mx, y \rangle = \langle x, M^\dagger y \rangle$ (and vice-versa).

Definition 3 (Dirac notation) *In the* Dirac notation*, a vector Ψ in $\mathbb{C}^n$ is written $|\Psi\rangle$. By $\langle \Psi|$ we denote the function mapping $|\Phi\rangle$ to $\langle \Psi, \Phi \rangle$ (or equivalently: $\langle \Psi|$ is the row vector $|\Psi\rangle^\dagger$).*

In particular, we can now write $\langle \Psi | \Phi \rangle$ for the inner product $\langle \Psi, \Phi \rangle$. And for the orthogonal projection P_V onto $V = \operatorname{span} \Psi$ we write $P_V = |\Psi\rangle\langle\Psi|$. (Try it out and evaluate $P_V|\Phi\rangle$!)

Definition 4 (Trace) *The* trace $\operatorname{tr} M$ *of a matrix $M \in \mathbb{C}^{n \times n}$ is $\sum_i M_{ii}$.*

The trace can also be computed as $\sum_i \langle i|M|i\rangle$ for any orthonormal basis $|1\rangle, \ldots, |n\rangle$ of $\mathbb{C}^n$.

Definition 5 (Hermitian matrices) *A matrix $M \in \mathbb{C}^{n \times n}$ is called Hermitian, if $M = M^\dagger$. (This is the analogue of symmetric matrices.)*

A Hermitian matrix M can be diagonalised, i.e., there is an orthonormal basis $|1\rangle, \ldots, |n\rangle$ such that $M = \sum_i \lambda_i |i\rangle\langle i|$ where λ_i are the eigenvalues of M.

[1] Or any complex vector space isomorphic to $\mathbb{C}^n$

[2] I.e., $(a + bi)^* = a - bi$.

Definition 6 (Unitary matrices) *A matrix $M \in \mathbb{C}^{n\times n}$ is unitary if $M^\dagger M = MM^\dagger = I$ where I is the identity matrix. (Unitary matrices are the analogue to rotation matrices.)*

Note: If M is unitary, then $\|Mx\| = \|x\|$ and $\langle Mx, My\rangle = \langle x, y\rangle$.

Definition 7 (Projections) *A matrix $M \in \mathbb{C}^{n\times n}$ is a* projection *if for all x we have $MMx = Mx$ (or equivalently, $MM = M$).*

The orthogonal projection *P_V onto a subspace $V \subseteq \mathbb{C}^n$ is defined by $P_V(u+v) = v$ where $v \in V$ and u is orthogonal to V. (Note that any state $x \in \mathbb{C}^n$ can be represented uniquely as such a sum $x = u + v$.)*

For a one-dimensional subspace $V = \text{span}\{v\}$ with $\|v\| = 1$, we have that $P_V x = v\langle v, x\rangle$.

2 One Qubit

Definition 8 (Qubit) *A single* qubit *is represented by a vector $|\Psi\rangle \in \mathbb{C}^2$ with $\||\Psi\rangle\| = 1$.*

There are two kinds of operations on qubits, unitary transformations and measurements.

Definition 9 (Unitary transformations on qubit) *A* unitary transformation *on a qubit $|\Psi\rangle$ is represented by a unitary matrix $U \in \mathbb{C}^{2\times 2}$. The qubit after the transformation is $U|\Psi\rangle$.*

In the case of polarisation, a typical transformation would be to rotate the polarisation by an angle of α. In this case we have

$$U = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}$$

which can be easily verified to be unitary.

Definition 10 (Projective measurements) *An* projective measurement *on a qubit is defined by two orthonormal vectors $|yes\rangle$ and $|no\rangle$. The outcomes of the measurement can be yes or no.*[3]

When applying the measurement to a qubit $|\Psi\rangle$, the probability for the yes outcome is $|\langle yes|\Psi\rangle|^2$, and the probability for the no outcome is $|\langle no|\Psi\rangle|^2$.

In case of a yes outcome, the resulting state is $|yes\rangle$, and in case of a no outcome, the resulting state is $|no\rangle$.[4]

An example for a measurement is a polarising filter. If the filter lets only vertically polarised light through, it corresponds to a measurement with $|\text{yes}\rangle = |\updownarrow\rangle$ and $|\text{no}\rangle = |\leftrightarrow\rangle$, and a yes-outcome corresponds to the fact that the photon passes the filter. In this case, the resulting photon will be vertically polarised (i.e., in the $|\updownarrow\rangle$ state). (In the no-outcome, the photon is destroyed, so talking about the resulting photon does not make sense in that case.)

[3] Of course, the labelling yes/no is arbitrary. Any other two labels are possible.

[4] Up to a scalar factor of absolute value 1. To be completely exact, the state after measuring yes is $\frac{\langle \text{yes}|\Psi\rangle}{|\langle \text{yes}|\Psi\rangle|} \cdot |\text{yes}\rangle$ (and analogous for no), but this should not worry us now. Furthermore, scalar factors (called a *global phase*) do not have physical meaning anyway.

3 Larger quantum systems

Definition 11 (Quantum states) *An n-dimensional* quantum state *is represented by a vector $|\Psi\rangle \in \mathbb{C}^n$ with $\||\Psi\rangle\| = 1$ (here $\mathbb{C}^n$ is a Hilbert space).*

In most cases, we assume some canonical orthonormal basis of $\mathbb{C}^n$ (representing the classical possibilities of the system) which we call the *computational basis*. We then use the following convention: If $|b_1\rangle, \ldots, |b_n\rangle$ are the basis vectors, and $b_1, \ldots, b_n$ are some labels we assign to these vectors sorted according to some natural ordering (e.g., for an m-qubit system (i.e., $n = 2^m$) b_i is the bitstring $b_i \in \{0,1\}^m$ which is the binary representation of $i-1$), then $|b_i\rangle = (0, \ldots, 0, 1, 0, \ldots, 0)^t$ where the 1 is at the i-th position.

There are two kinds of operations on quantum states, unitary transformations and measurements.

Definition 12 (Unitary transformation) *A* unitary transformation *on a quantum state $|\Psi\rangle \in \mathbb{C}^n$ is represented by a unitary matrix $U \in \mathbb{C}^{n\times n}$. The state after the transformation is $U|\Psi\rangle$.*

Definition 13 (Measurement) *A* (projective) measurement *on a Hilbert space $\mathcal{H}$ is specified by a family $\{P_i\}_{i\in I}$ of orthogonal projections on $\mathcal{H}$ labelled with the possible measurement outcomes $i \in I$. The projections have to be pairwise orthogonal, i.e., $P_iP_j = 0$ for $i \neq j$. And the projections sum to 1, i.e., $\sum_i P_i = 1_{\mathcal{H}}$ where $1_{\mathcal{H}}$ is the identity on $\mathcal{H}$.*

When measuring a state $|\Psi\rangle \in \mathcal{H}$, the outcome i occurs with probability

$$\|P_i|\Psi\rangle\|^2.$$

If the outcome i occurs, the state after the measurement (post-measurement state) is

$$\frac{P_i|\Psi\rangle}{\|P_i|\Psi\rangle\|}.$$

A special case of a measurement is the complete measurement in which every projection is the projection onto a one-dimensional subspace.

Note that we can also represent a measurement by giving the images V_i of the projectors P_i instead of the projectors themselves. This is equivalent, as the P_i can be recovered from V_i and vice versa.

Definition 14 (Complete measurement) *A* complete measurement *on $\mathcal{H}$ is specified by an orthonormal basis $B = \{|i\rangle\}_{i\in I}$ of $\mathcal{H}$ labelled with the possible measurement outcomes $i \in I$.*

When measuring a state $|\Psi\rangle \in \mathcal{H}$, the outcome i occurs with probability

$$|\langle i|\Psi\rangle|^2.$$

and the corresponding post-measurement state is

$$\frac{\langle i|\Psi\rangle}{|\langle i|\Psi\rangle|} \cdot |i\rangle$$

(which is $|i\rangle$ up to a (physically irrelevant) scalar factor $\frac{\langle i|\Psi\rangle}{|\langle i|\Psi\rangle|}$ of absolute value 1, the global phase*).*

Note that the complete measurement with basis $\{|i\rangle\}_{i\in I}$ has the same effect as the measurement with projectors $\{P_i\}_{i\in I}$ where $P_i := |i\rangle\langle i|$. Thus complete measurements are a special case of measurements as in Definition 13.