Quantum Reading Course

Jake Denton, supervised by Pranav Singh

Autumn Semester 2022

Contents

1 Introduction

2 Background

In this section, the foundations required to begin to tackle the ideas of quantum computing are laid out. A motivating analogy describing the contrast of quantum and classical objects is given, followed by a whistle-stop reminder of the quantum mechanical postulates, with examples focused on qubit systems - these being the fundamental systems in quantum computing.

2.1 Quantum vs Classical objects

Here, an analogy is presented which should motivate the difference between a quantum and classical object. By classical object, we mean an object that obeys the regular rules of probability - that is, put simply, some kind of random object that can be measured many times, giving values (or states) in some space according to some set of probabilities.

An incredibly simple and popular example is the flip of an unbiased coin. In this scenario when we do many flips, we expect that the coin will turn up heads half the time and tails the other half of the time. If we wished, we could represent a single flip by a Bernoulli random variable, which takes value 0 when heads is observed and value 1 when tails is observed, each with probability $\frac{1}{2}$, and a collection of flips by a binomial variable.

Now, let us imagine a **quantum** coin flip. That is, a coin that obeys the postulates of quantum mechanics, and flips heads or tails with equal probability. A representation of the state of the coin is as a superposition of the states $|0\rangle$ meaning heads and $|1\rangle$ meaning tails which ensures each outcome has equal probability is given below. Note that this is only one possible representation as we may have global phase or relative phase factors (more on this later).

$$|coin\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Suppose these two coins lay side by side, but it is not known which is which. How might one distinguish between them? Well the answer is simple, keep flipping them until you observe at least one head and one tail (or vice-versa) from one of the coins. This must be the classical one. This reveals the major difference between quantum and classical objects, it comes from **measurement**.

What is the logic behind this? It is a postulate of quantum mechanics that measurement leads to collapse of the quantum state. That is, as soon as I flip the quantum coin, it is "stuck" at the outcome it lands on, whether that be heads or tails, and so every subsequent flip will give me the same outcome as the first with probability one. On the other hand, with a regular coin, it is known (from experience) that you can continue to get either a heads or tails no matter how many flips you make.

It is this reaction to measurement that makes quantum objects unique, and consequently difficult objects to comprehend and work with.

2.2 Quantum mechanical postulates

As hinted in section 2.1, quantum objects follow a set of rules known as postulates. These are fundamental facts observed in the physical world that motivate the mathematical framework used to explain and model quantum phenomena. In this section, they are discussed as a refresher for the reader. The focus is mainly on the state vector formulation, but it will also be noted that there is an equivalent formulation through the use of density operators at the end.

2.2.1 State space postulate

Postulate 1: Any closed physical system is associated with a Hilbert space known as the state space of the system. The system is completely described by a state vector, which is a unit vector in state space.

Closed means that the physical system has no interaction with other physical systems. Unpacking the mathematics in this postulate, a Hilbert space is simply a complex vector space with an inner product. A unit vector is a vector with unit norm, which one can easily confirm using the inner product from the Hilbert space.

The most basic quantum mechanical system is that of a single **qubit**, which is the quantum version of the bit from classical computing. As such, it is the basic constituent of a quantum computer. A qubit has a 2-dimensional state space. Take an orthonormal basis for this space, with two basis vectors $|0\rangle$ and $|1\rangle$ (this notation is chosen to be analogous to the values of a classical bit, and as such this basis is called the **computational** basis), then an arbitrary state vector can be written as:

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle$$

where a and b are complex numbers. Remember that if $|\psi\rangle$ is to describe a system, it must be a unit vector. This requirement restricts the values of a and b in the following way:

Example 2.1. (Normalisation condition) We find the square of the norm by taking the inner product of $|\psi\rangle$ with itself:

$$\begin{aligned} 1 = \langle\psi|\psi\rangle &= |a|^2\,\langle 0|0\rangle + a^* b\,\langle 0|1\rangle + b^* a\,\langle 1|0\rangle + |b|^2\,\langle 1|1\rangle \\ &= |a|^2 + |b|^2 \end{aligned}$$

Here, unit norm is set on the left side. The right side is an expansion of the inner product followed by substitution of the orthonormality of the basis vectors. The modulus squared of a here is simply the product of a with its complex conjugate.

The complex numbers a and b are referred to as probability **amplitudes**, so that this state vector provides a probability distribution of measurement outcomes of the system. This is a physical interpretation of the state vector, originating from the famous German physicist Max Born (REFERENCE).

Notice that since the single qubit system has a 2-dimensional state space and as such has an orthonormal basis with two elements defined above, the state vectors can

be expressed more conveniently by applying an isomorphism onto the 2-dimensional complex space, which is equipped with vectors instead of these bras and kets. In other words, the vectors $|0\rangle$ and $|1\rangle$ and the state vector $|\psi\rangle$ can be equivalently written in terms of 2×1 vectors as (and will be throughout this report):

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \ |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \ |\psi\rangle = a\,|0\rangle + b\,|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$$

A note for the reader: the two equivalent forms are swapped and interchanged a lot over the course of this report which may be confusing, refer back to the above if and when you need.

2.2.2 Evolution postulate

Postulate 2: The evolution of a closed quantum system is described by a unitary transformation.

Evolution is how the system changes over time. Unitary transformations basically refers to those that are reversible, norm- and trace-preserving. The important property here is norm-preserving, as from postulate 1, the system is completely described by unit vectors in the state space, so when a transformation is applied this property ensures that the new system can also be completely described using a state vector.

In the case of our single qubit system, what do these unitary transformations, often referred to as gates after their classical counterparts, look like? Taking the equivalent 2×1 vectors, they can be seen as 2×2 matrices that preserve the unit norm of the vector. A few examples are given below:

Example 2.2.

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

It is useful to note that the left-hand side is the notation of an operator (i.e. on the Hilbert space) and the right-hand side is the equivalent matrix representation (coming from the complex space of 2×1 vectors), it is worthwhile identifying these two separate representations in the calculation below. How does this transformation affect the state vector? Well, it takes the ket vector $|0\rangle$ and flips it to $|1\rangle$ and vice-versa. The matrix does of course also perform this transformation:

$$X\,|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

This flipping gifts this operator with the name bit-flip, since it flips the 'classical' states between each other. It is also sometimes called the X- or NOT-gate.

Other gates include:

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$
$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$
$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

The first two gates here can be grouped with the X-gate, and may be recognised as the Pauli spin matrices. The Y-gate performs both a bit flip and also changes the phase by a factor of $\pm i$. On the other hand, the Z-gate simply multiplies the amplitude of state $|1\rangle$ by -1, so it is sometimes called the phase flip. These three matrices represent rotations around some X,Y and Z axes, which is explained shortly.

The third gate here is known as the Hadamard gate. It has the following effect on the computational basis states:

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = |+\rangle$$
$$H|1\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = |-\rangle$$

From the above, these states are sent by the Hadamard gate to states in superposition, which have equal probability of being measured in either of the basis states. These states are often written in literature as the 'plus' $|+\rangle$ and 'minus' $|-\rangle$ states. This gate is incredibly useful as it takes the initial state $|0\rangle$ that a qubit begins as to a superposition. It turns out that this gate is also a (less obvious) rotation, and in fact, any gate is a rotation!

Okay, so it has been stated above that unitary gates are rotations, so there must be a geometric representation of the state of a qubit which can be rotated. This is where the **Bloch sphere** (REFERENCE) comes in.

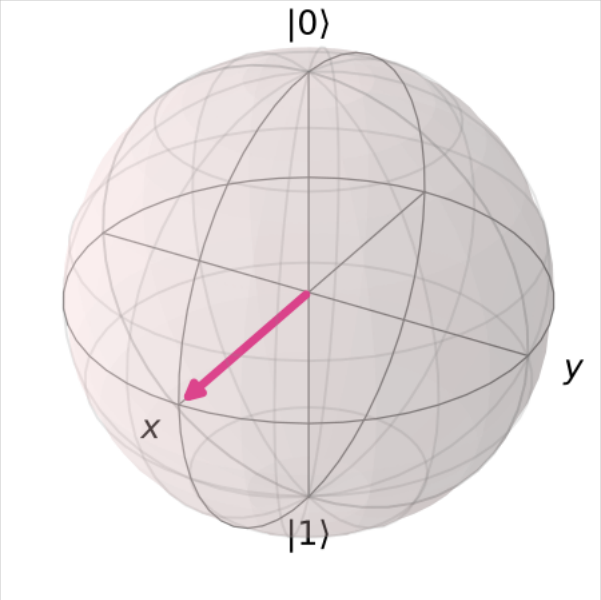

Figure 1: The Bloch sphere. [Source: Qiskit (REFERENCE)]

As was noted earlier, the arbitrary state vector for a single qubit is a superposition of the computational basis states, with amplitudes a and b which satisfy the normalisation condition (thanks to the first postulate) $|a|^2 + |b|^2 = 1$. This condition can be rewritten using the trigonometric identity so that an equivalent form of the state vector is:

$$|\psi\rangle = cos\frac{\theta}{2}|0\rangle + e^{i\phi}sin\frac{\theta}{2}|1\rangle$$

Here, the term $e^{i\phi}$ is the relative phase. The state vector again very clearly has unit norm (since the relative phase cancels out with its conjugate). Then, each state vector can be represented geometrically as the point on a sphere with coordinates given by the Bloch vector:

$$(x, y, z) = (sin\theta cos\phi, sin\theta sin\phi, cos\theta)$$

The north and south poles of this sphere represent the computational basis states $|0\rangle$ and $|1\rangle$ respectively. Fixing $\phi = 0$ for now, when θ increases, the state vector moves away from $|0\rangle$ towards $|1\rangle$, passing the point (1,0,0) on the x-axis when $\theta = \frac{\pi}{2}$. In other words, θ is responsible for the vertical movement around the Bloch sphere, representing a rotation around the x-axis. On the other hand, ψ is responsible for lateral movement. This can be seen by fixing $\theta = \frac{\pi}{2}$. Then starting from (1,0,0) (i.e. $\psi = 0$), as ψ increases the vector moves around the Bloch sphere towards (0,1,0) (i.e. $\psi = \frac{\pi}{2}$), which is anti-clockwise considering figure 1 above. The action of unitary gates rotates the state vector around this sphere. This is a useful visualisation of what each gate does and clearly since rotations are reversible, gate operations should be too. It is worth noting

that if multiple qubits are present in a system, a Bloch vector (or equivalently, a point on the Bloch sphere) can be assigned to each, this will be a useful visualisation tool when multiple qubit gates are introduced later.

2.2.3 Measurement postulate

Postulate 3: The measurement of a quantum state is achieved through a collection of measurement operators $\{M_m\}$, which act on the state space.

The index m refers to the measurement outcomes possible when the measurement operator is applied. The probability $p(m)$ of measuring the outcome m from the state vector $|\psi\rangle$ is given by:

$$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle .$$

Since this is a set of probabilities, their sum over m must be 1. This gives us:

$$\sum_m p(m) = \sum_m \langle\psi| M_m^\dagger M_m |\psi\rangle = \langle\psi| \sum_m M_m^\dagger M_m |\psi\rangle = 1,$$

where here the definition of $p(m)$ has been substituted and the sum is set to 1. Since the state $|\psi\rangle$ is normalised (from postulate 1), the above implies that the measurement operators satisfy the **completeness relation**.

Definition 2.1. (Completeness relation) $\sum_m M_m^\dagger M_m = \mathbb{I}$

Further to this, the post-measurement state of the system is given by:

$$\frac{M_m |\psi\rangle}{\sqrt{\langle\psi| M_m^\dagger M_m |\psi\rangle}}.$$

An important thing to note from the above is that upon measuring the state through a measurement operator, the state vector collapses onto the eigenstate associated with the measurement m. This postulate is responsible for the strange, seemingly unnatural behaviour of quantum systems, and leads to interesting phenomena such as entanglement.

To make this concrete, consider measuring the single qubit system in the computational basis. From earlier discussion, this system has two possible measurement outcomes, $|0\rangle$ or $|1\rangle$. Then the two measurement operators are given by $M_0 = |0\rangle\langle 0|$ and $M_1 = |1\rangle\langle 1|$. These are just outer products, so the matrix forms of these operators are:

$$M_0 = |0\rangle\langle 0| = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

$$M_1 = |1\rangle\langle 1| = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

For an arbitrary state vector $|\psi\rangle = a|0\rangle + b|1\rangle$, using the above, the probability of measuring state 1 is:

$$M_1|\psi\rangle = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 0 \\ b \end{bmatrix} \Rightarrow \quad p(1) = \langle\psi| M_1^\dagger M_1 |\psi\rangle = \begin{bmatrix} 0 & b^* \end{bmatrix}\begin{bmatrix} 0 \\ b \end{bmatrix} = b^* b = |b|^2$$

The post-measurement state is then given by:

$$\frac{b|1\rangle}{|b|}.$$

This is a normalised state, and the probability of measuring state 1 is clearly 1, so any subsequent measurements will only result in this outcome. This explains the behaviour of the quantum coin from the example given at the start of this section.

2.2.4 Composite system postulate

Postulate 4: The state space of a composite physical system is the tensor product of individual state spaces that compose the system.

What does this postulate tell us? Well, suppose the composite system is made up of two subsystems A and B in respective states $|A\rangle$ and $|B\rangle$ from two Hilbert spaces. Then this postulate states that there is a larger Hilbert space that describes the state space of the joint system. The tensor product appears as it is a way of stitching the two component state spaces together into a larger space.

This postulate along with the previous allows us to discuss entangled states. An example with two single-qubit systems in the computational basis are the bell states, one of which is defined here:

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

What makes this state interesting? Well, it cannot be split into the tensor product of two single qubit states. From this, it can be seen that if one of the two qubit states is observed to be in state $|0\rangle$ or $|1\rangle$, then the state not measured also collapses to the same state, very strange indeed!

2.2.5 Summary of state vector postulates

A short summary of these postulates is as follows. Postulate 1 sets a foundation in that any quantum system has associated with it a complex vector space (Hilbert space), and can be fully described by a state vector with unit norm. Postulate 2 describes the operations which can be applied to a system and some restrictions on these operations (unitary) so that they conform with the ideas of postulate 1. The third postulate provides a description of how to extract information from a system, and also the effect this has on the system. Finally, the fourth postulate informs us how to factor and combine systems.

2.2.6 The density operator formulation

The above discussion was based upon the idea of a state vector - that is, a superposition of quantum states that fully describes a closed system. There is an alternative, similarly complete way to describe a quantum system, and this is through the **density operator**.

Definition 2.2. (Density operator) Suppose that a quantum system is in one of a number of pure states (pure meaning the possible state is known) $|\psi_i\rangle$ with probability p_i, which can be considered as a classical probability. Then the density operator is defined as:

$$\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i| .$$

This is a sum of outer products, and so can be represented as a matrix (in the isomorphic complex vector space).

This idea of pure versus mixed state can be quite confusing, it is worth considering an example demonstrating the difference between the two.

Take a single qubit system, where first it is assumed to be known that the system is in the pure state $|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Under this assumption, the probability of finding the system in this state is 1, and so the associated density operator is given by:

$$\rho = |\psi_1\rangle \langle\psi_1| = \frac{1}{2}(|0\rangle + |1\rangle)(\langle 0| + \langle 1|) = \frac{1}{2}(|0\rangle \langle 0| + |0\rangle \langle 1| + |1\rangle \langle 0| + |1\rangle \langle 1|) = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

Now, for the same single qubit system, assume that it is known that the system is either in the pure state $|\psi_1\rangle$ with probability $p = \frac{2}{3}$ or in the pure state $|\psi_2\rangle = \frac{1}{\sqrt{3}}(|0\rangle + \sqrt{2}|1\rangle)$ with probability $p = \frac{1}{3}$. Since the system is in one of these two pure states with classical probabilities, the overall system can be described as a mixed state. This mixed state has the following density matrix:

$$\rho = \frac{2}{3}|\psi_1\rangle \langle\psi_1| + \frac{1}{3}|\psi_2\rangle \langle\psi_2| = \frac{2}{3} * \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} + \frac{1}{3} * \begin{bmatrix} \frac{1}{3} & \frac{\sqrt{2}}{3} \\ \frac{\sqrt{2}}{3} & \frac{2}{3} \end{bmatrix} = \begin{bmatrix} \frac{4}{9} & \frac{3+\sqrt{2}}{9} \\ \frac{3+\sqrt{2}}{9} & \frac{5}{9} \end{bmatrix}$$

Notice that the trace of these example density operators is 1. This is one of two conditions the operator must satisfy in order to be characterised as a density operator. The other condition, known as the positivity condition, states that the operator must be a positive operator. It also turns out that there is a way to identify the density operator of a pure state.

Lemma 2.1. Let ρ be a density operator. Then $tr(\rho^2) \leq 1$ with equality if and only if ρ is a pure state.

Indeed, for the two examples above, $tr(\rho^2) = 1$ for the pure state and for the mixed state $tr(\rho^2) = \frac{63+12\sqrt{2}}{81} \approx 0.987 < 1$, as expected from this lemma.

Using the definition of the density operator, the postulates can be reformulated as follows:

1. **Postulate 1:** A quantum system is completely described by its density operator which is positive with unit trace.

2. **Postulate 2:** The density operator evolves according to $\rho^{'} = U\rho U^{\dagger}$ where U is a unitary operator.

3. **Postulate 3:** Measurement is achieved through a collection of measurement operators $\{M_m\}$ which have the following effect on the density operator:

   The probability of measuring outcome m is: $p(m) = tr(M_m^{\dagger} M_m \rho)$

   The post-measurement density operator is: $\dfrac{M_m \rho M_m^{\dagger}}{tr(M_m^{\dagger} M_m \rho)}$

   where the measurement operators satisfy the completeness relation as before.

4. **Postulate 4:** Given n systems labelled $1, 2, ..., n$, with system i prepared with density operator ρ_i, then the joint system has density operator $\rho_1 \otimes \rho_2 \otimes ... \otimes \rho_n$.

Now that the postulates have been discussed in both pictures of quantum mechanics, we can move on to discussing the topic of quantum computing.

3 Quantum computation

3.1 Single qubit operations

3.2 Multiple qubit operations

3.3 Drawing quantum circuits

3.4 Quantum computing in practice

4 Essential subroutines

4.1 Quantum fourier transform

4.2 Quantum phase estimation

5 HHL Algorithm

6 Miscellaneous

6.0.1 Wavefunction and Dirac notation

This section aims to inform the reader of the basic ideas and notation of quantum mechanics. REFERENCES.

The state of a quantum system is given by a **wave-function**. For example, $\psi(x,t) \in \mathbb{C}$, which depends on both space and time. The physical interpretation of this wave-function (Max Born (REFERENCE)) is that it represents a probability distribution of measurement outcomes of the system, so with the example here the probability density of finding the system at position x is given by the squared amplitude $|\psi(x,t)|^2 = \psi(x,t)\psi^*(x,t)$ where the asterisk represents the complex conjugate.

Note that here, the wave-function is written in terms of the position x, therefore we call this the **position representation** of the system. This can make things complicated, as we can represent the same system in lots of different representations, for example momentum representation. Using a different representation is the equivalent of characterising the wave-function with respect to alternative basis vectors, and since there are an infinite number of different bases we could use, it would be far more useful to represent the state through a coordinate-free representation. This is what Dirac introduced (REFERENCE).

This coordinate-free representation of the state is denoted by $|\psi\rangle$. This is called a ket vector, and its conjugate, denoted by $\langle\psi|$, is the bra vector associated with ψ. Ket vectors belong to a complex vector space known as a Hilbert space (denoted $\mathbb{H}$), and it turns out that if the Hilbert space is finite-dimensional then it is isomorphic to a complex space $\mathbb{C}^N$ (REFERENCE). And so, without loss of generality we can write a quantum state in terms of components:

$$|\psi\rangle = \begin{bmatrix} \psi_0 \\ \psi_1 \\ . \\ . \\ . \\ \psi_{N-1} \end{bmatrix}$$

The bra-vector for the above is given by:

$$\langle\psi| = \begin{bmatrix} \overline{\psi_0} & \overline{\psi_1} & ... & \overline{\psi_{N-1}} \end{bmatrix}$$

where the overline represents the complex conjugate. The inner product in this vector space is given by:

$$\langle\phi|\psi\rangle = \sum_{i=0}^{N-1} \overline{\phi_i}\psi_i$$

If $\{|i\rangle\}$ is the standard basis of $\mathbb{C}^n$, that is for example:

$$|i\rangle = \begin{bmatrix} 0 \\ 0 \\ ... \\ 0 \\ i \\ 0 \\ ... \\ 0 \end{bmatrix}$$

then it is clear that the inner product between the state and the i basis vector will return the i^{th} element, that is $\langle i|\psi\rangle = \psi_i$. The outer product on the other hand, is a matrix (as you might expect from the dimensions of kets and bras), which has elements given by $\langle i|\,(|\psi\rangle\langle\phi|)\,|j\rangle = \psi_i\overline{\phi_j}$. We will always assume that ket vectors are normalised (i.e. $\langle\psi|\psi\rangle = 1$), otherwise we will denote them ψ.

This notation should allow us to consider single qubit systems and gates, which we motivate and discuss in the next two parts.

6.0.2 Classical bits

Within your classical desktop, as you flick through your favourite websites, all the information you see is expressed in bits. A bit is like the atom of information, the smallest unit you can have, and in a classical computer takes a value of either 0 or 1, and whichever value the bit takes is also called its **state**.

Of course, since this is true, all the letters and numbers and pixels that you can see whilst reading this can be expressed as strings of these bits. How does a computer do that?

Well, let's take the simplest example, a number. Since a bit only gives us values of 0 or 1 to work with, using the base 2 representation of a number is the obvious way to go about representing this.

Example 6.1. (Binary representation) Suppose we want the binary representation of 1812. In terms of a sum of the powers of 2, we can write this as:

$$\begin{aligned} 1812 &= 1 * 2^{10} + 1 * 2^9 + 1 * 2^8 + 1 * 2^4 + 2^2 \\ &= 11100010100 \text{ in base 2.} \end{aligned}$$

Therefore, your classical computer stores the number 1812 using 11 of these classical bits. So, how many numbers can n bits represent? This is easy! Each bit can be in one of two states 0 or 1, so if we have n of them, than we can represent 2^n states. However, we are after distinct numbers, so if the leading bit (the one representing the largest power of 2) is equal to 0 we get the same number as if we used one fewer bits! Therefore, if we fix this to be 1, the n bits represent 2^{n-1} distinct numbers.

We have learnt about the classical bit and the values it can take, and also how the everyday computer stores numbers using a string of these bits. Furthermore, we mentioned that everything on a computer can be, and is, stored as a string of bits.

So what about quantum computers? It turns out that these have their own versions of a bit, namely qubits. The difference between the two is that whilst classical bits are restricted to values of either 0 or 1 throughout an algorithm, qubits only take one of two values (often 0 or 1, a standard basis) when we measure them to extract an output. Until this point, they behave in a more complex way, dictated by the rules of quantum mechanics.

6.0.3 Single qubit system

To represent a single quantum bit, let us take the single spin system, which has basis states of the form (where y^T denotes the transpose of y):

$$|0\rangle = (1,0)^T \text{ and } |1\rangle = (0,1)^T$$

A general state vector in this system has $|\psi\rangle = a|0\rangle + b|1\rangle$, where we have a normalisation condition $|a|^2 + |b|^2 = 1$.

6.0.4 Single qubit gates

The evolution of a quantum state on an n-qubit system is through a unitary operator, denoted $U \in \mathbb{C}^{n\times n}$. Unitary operators are referred to as gates in quantum computing, thanks to their classical counterparts. We have:

$$|\psi'\rangle = U|\psi\rangle \text{ where } U^\dagger U = I,$$

I representing the $n \times n$ identity matrix.

Returning to the single qubit system, let us look at some gates that can act on this system.

Example 6.2. (Pauli-gates)