Qubits and Quantum States

Adam Kelly (`ak2316@cam.ac.uk`)

February 1, 2021

A **qubit** is a two-state quantum mechanical system used for representing quantum information. In this article, we will look at how qubits are described mathematically, along with how computation is performed with them.

The approach taken in this article is going to be slightly less abstract than the approach taken in lectures. However, familiarity with Dirac (bra-ket) notation will be assumed. I will also avoid commenting on the general differences between quantum or classical information, except when it suits.

1 Representing Quantum States

In general, the state of an isolated quantum system is described by a vector, the **state vector**, in a complex vector space equipped with an inner product.

1.1 Single Qubit States

One of the simplest possible quantum systems is the *qubit*. The state vector of a single qubit $|\psi\rangle$ is an element of a two-dimensional complex vector space V_2. If this vector space has orthonormal basis vectors $|0\rangle$ and $|1\rangle$, we can write $|\psi\rangle$ in the form

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix},$$

where $\alpha, \beta \in \mathbb{C}$. There is also an additional normalization condition of $|\alpha|^2 + |\beta|^2 = 1$, the reason for which will be described later.

Remark. With the state of a qubit described in this way, we can see that there is states that can correspond with classical bits, $|0\rangle$ and $|1\rangle$, but there is also a whole lot of states in between.

1.2 Multiple Qubit States

We can take two quantum systems and allow them to interact. To describe this combined system, we will need a way to combine their corresponding vector spaces. This is done with the tensor product.

To see how this works, we will consider the case of two qubits A and B, with corresponding two-dimensional vector spaces V_A and V_B. When qubits A and B are combined (and allowed to interact), their combined state is an element of the vector space $V_A \otimes V_B$. The orthonormal basis for this vector space is

$$\{|0\rangle \otimes |0\rangle, \quad |0\rangle \otimes |1\rangle, \quad |1\rangle \otimes |0\rangle, \quad |1\rangle \otimes |1\rangle\}.$$

Remark (Notation). We sometimes use the shorthand notation $|1\rangle \otimes |0\rangle = |1\rangle |0\rangle = |10\rangle$. Also, we may neglect the binary notation and write (for example) $|6\rangle = |110\rangle = |1\rangle |1\rangle |0\rangle = |1\rangle \otimes |1\rangle \otimes |0\rangle$.

The vector space $V_A \otimes V_B$ is the space of all the possible states the qubits can be in together, even after they have interacted with each other. Even though the vector spaces V_A and V_B are isomorphic, it is important to think about them as *completely different* vector spaces. This is because they describe the states of completely different objects (even if they are both just qubits).

Concretely, the vector space $V_A \otimes V_B$ has the orthonormal basis

$$\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\},$$

where each of these vectors is found by calculating the tensor product of the column vectors corresponding to the basis vectors $|0\rangle$ and $|1\rangle$ for V_A and V_B. We can write the state $|\phi\rangle$ of both qubits as

$$|\phi\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle = \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11,} \end{pmatrix}$$

where $\alpha_i \in \mathbb{C}$ and $\sum |\alpha_i|^2 = 1$.

We can generalise this naturally to an n-qubit system. The state of an n-qubit system $|\psi\rangle$ is a vector in a 2^n dimensional complex vector space,

$$|\psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{2^n-1} \end{pmatrix}$$

where $\alpha_i \in \mathbb{C}$ and $\sum |\alpha_i| = 1$.

1.3 Product and Entangled States

We said before that it was possible to bring together two quantum systems to interact. Of course, it is also possible that when we do bring together two quantum systems, they stay independent. We describe this using the notions of *product* and *entangled* states.

Definition. For two quantum systems A and B, we say that their state $|\psi\rangle$ is a **product state** if we can write $|\psi\rangle = |u\rangle_A \otimes |v\rangle_B$, where $|u\rangle_A$ is the state for A and $|v\rangle_B$ is the state for B. Otherwise, we say that they are **entangled**.

It's relatively straightforward to write down an example of an entangled state. Take, for example

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

There is a simple criterion for whether a two qubit state is a product state or not. If we have some state

$$|\psi\rangle = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix},$$

then we can write it as the a product state if and only if $ad - bc = 0$. For larger quantum systems, determining if a given state is a product state or not can be a difficult problem.

2 Updating Quantum States & Quantum Gates

Once we have described our n-qubit system using some vector $|\psi\rangle$, we want to describe how computation is performed using these qubits. The way we describe this is with *unitary transformations*.

In general, any physical evolution of a quantum system is represented by a unitary linear operation on the system's corresponding vector space. If we have an n-qubit system, then a matrix acting on its vector space will be an $2^n \times 2^n$ matrix U, such that $UU^{-1} = I$ (so that it's unitary).

2.1 Quantum Gates

Transformations that only act on a single qubit in the system are called 'single qubit gates', and correspond to 2×2 unitary matrices. Some common single qubit gates are given below.

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$Y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad P(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}.$$

Gates that act on two (or more) qubits are somewhat more interesting. The most common examples of two qubit gates are the 'controlled' gates. A controlled gate acts on two qubits, the **control** qubit and the **target qubit**. The gate can be thought of as applying a single qubit gate to the target qubit, depending on the value of the control qubit. Two controlled gates are shown below.

$$CX = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

In the gates above, the first qubit is the control qubit and the second qubit is the target qubit (interestingly these are actually symmetrical for the CZ gate).

To see how they work, consider the action of the CX gate on the basis states of a two qubit system.

$$CX\,|00\rangle = |00\rangle$$
$$CX\,|01\rangle = |01\rangle$$
$$CX\,|10\rangle = |11\rangle$$
$$CX\,|11\rangle = |10\rangle$$

2.2   Applying Gates

We can apply a single qubit gate to a single qubit system by multiplying the matrix by the corresponding state vector. For example,

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

Applying a single qubit gate to a qubit in a multiple qubit system is slightly more complicated.

If we had some n-qubit system, and we wanted to apply the gate H to qubit k, then to form full $2^n \times 2^n$ matrix that we can multiply with the state vector, we need to consider the basis vectors of the system's vector space.

If we had some basis vector $|i_1\rangle\,|i_2\rangle \cdots |i_k\rangle \cdots |i_n\rangle$, then the transformed vector would be

$$|i_1\rangle\,|i_2\rangle \cdots (H\,|i_k\rangle) \cdots |i_n\rangle$$

4

We can rewrite this as
$$(I\,|i_1\rangle)(I\,|i_2\rangle)\cdots(H\,|i_k\rangle)\cdots(I\,|i_n\rangle),$$

and using the 'mixed-product' property of the Kronecker product (the tensor product of matrices), this is equal to

$$(\underbrace{I \otimes I \otimes \cdots \otimes I}_{k-1 \text{ times}} \otimes H \otimes \underbrace{I \otimes \cdots \otimes I}_{n-k \text{ times}})[|i_1\rangle\,|i_2\rangle\cdots|i_k\rangle\cdots|i_n\rangle].$$

Thus the full $2^n \times 2^n$ matrix is given by $\underbrace{I \otimes I \otimes \cdots \otimes I}_{k-1 \text{ times}} \otimes H \otimes \underbrace{I \otimes \cdots \otimes I}_{n-k \text{ times}}.$

Remark. If performing this computation by hand (or on a computer), it will be somewhat more efficient if you note that taking $I \otimes I \otimes \cdots \otimes I$ with m identity matrices is just a $2^m \times 2^m$ identity matrix. Also, in some cases the sparsity of the resulting matrix may make it faster to just try and work out the final matrix by hand. This procedure is guaranteed to work, however.

Unlike the in single-qubit gate case, writing down a straightforward formula for expanding a two-qubit gate's 4×4 matrix into a $2^n \times 2^n$ matrix is somewhat harder. Typically the best approach will be to see how the transformation acts on the basis vectors and construct the matrix that way.[1]

---

[1]There is a few tricks that can be used however, and a sufficiently interested reader can send me an email and I will elaborate. Having to actually construct such things is a surprisingly irregular occurrence, however.There are also a number of tricks that can be used to make constructing the matrix redundant. As before, if you want to know more, email me.