Chapter 1: Fundamental Properties of Cbits and Qbits

Warren Alphonso

March 27, 2019

For a computer to be a quantum computer, it must have no physical interactions that are not completely under the control of the program. Any such interaction would cause quantum decoherence. To avoid decoherence, individual qbits cannot be encoded in macroscopic physical systems because these systems cannot be isolated from their own irrelevant internal degrees of freedom. Two things keep this from being hopeless:

1. Separation between discrete energy levels on the atomic scale can be much larger than separations between levels of a large system. This means we can achieve dynamical isolation.
2. Error correction can be used as long as errors occur at a sufficiently low rate.

Immense knowledge of quantum mechanics is not necessary to contribute to the theory of quantum computation:

1. An abstract quantum computer is an extremely simple example of a physical system. It is discrete, made up of finite number of units, and easily analyzed. Much of the complexity of learning quantum mechanics is connected to mastering the description of continuous systems.
2. Developing intuition about how abstract formalism of quantum mechanics can be applied to actual phenomena is incredibly difficult to build. Quantum computation, however, is entirely concerned with the abstract model. To build a quantum computer will require mastery of quantum mechanics but to understand the capabilities of the device does not require full understanding of the subject.

1 Cbits and their states

A classical computer operates on strings of 0's and 1's. Each position in such strings is called a *bit*, and it contains either a 0 or a 1. We use the term *Cbit* to describe the two-state classical physical system and *Qbit* to describe its quantum generalization.

We will represent the state of each Cbit as a kind of box, depicted by the symbol $|\ \rangle$, in which we place the value, 0 or 1. Thus, the two distinguishable *states* of a Cbit are represented as $|0\rangle$ and $|1\rangle$. Similarly, we can characterize the states of 5 Cbits represnting 11001 with the symbol $|1\rangle|1\rangle|0\rangle|0\rangle|1\rangle$ and refer to this symbol as the state of all five Cbits.It is easier to read if we enclose the whole string in a single box like $|11001\rangle$.
Dirac introduced the $|\ \rangle$ notation as a useful way to write *vectors*. In Dirac notation, we can put into the box anything that serves to specify what the vector is.
Now imagine the two states $|0\rangle$ and $|1\rangle$ to be represented by two *orthogonal unit vectors in a 2-dimensional space*. This representation is necessary and fundamental when attempting to grasp Qbits.

$$|0\rangle \longleftrightarrow \begin{pmatrix}1\\0\end{pmatrix}, |1\rangle \longleftrightarrow \begin{pmatrix}0\\1\end{pmatrix}$$

In the case of **two** Cbits, the vector space is *4-dimensional*, with an orthonormal basis

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

An alternative notation for this is

$$|0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|0\rangle, |1\rangle|1\rangle$$

This notation suggests multiplication and is in fact a short-hand notation for the *tensor products* of the two single-Cbit 2-vectors written as

$$|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle$$

Once we see the two 1-Cbit states as orthogonal unit vectors, the tensor product is the natural way to represent multi-Cbit states.

$$|5\rangle_3 = |101\rangle = |1\rangle|0\rangle|1\rangle \longleftrightarrow \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\0\\0\\1\\0\\0\end{pmatrix}$$

Note that the single non-zero component of $|5\rangle_3$ is the 1 in position 5, specified by the number 5 in binary.

2 Reversible Operations on Cbits

Quantum computers do many *reversible* operations, which transform the initial state of the Qbits into its final form using only processes that can be inverted. There is only one *irreversible* part of the operation of a quantum computer. It is called *measurement* and is the only way to extract useful information from the Qbits. Measurement is a crucial part of the quantum computational process, but in classical computers it is so trivial that it is rarely considered a part of the computational process.
In a reversible operation, every final state arises from a *unique* initial state. The only non-trivial reversible operation we can apply to a single Cbit is the NOT (*flip*) operation, denoted by the symbol $\mathbf{X}$ which interchanges the two states $|0\rangle$ and $|1\rangle$.

$$\mathbf{X} \longleftrightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

We introduce a *number operator* $\mathbf{n}$ for a single Cbit:

$$\mathbf{n}|x\rangle = x|x\rangle, x = 0 \text{ or } 1$$

In other words, $|0\rangle$ and $|1\rangle$ are eigenvectors of $\mathbf{n}$ with eigenvalues 0 and 1. Recall that $|0\rangle$ represents the vector $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle$ represents the vector $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$.
We also define the complementary operator,

$$\overline{n} = 1 - \mathbf{n}$$

so now the eigenvalues and eigenvectors are flipped. These operators have the matrix representations

$$\mathbf{n} \longleftrightarrow \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \overline{n} \longleftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

It follows that

$$\mathbf{n}^2 = \mathbf{n}, \overline{n}^2 = \overline{n}, \mathbf{n}\overline{n} = \overline{n}\mathbf{n} = 0, \mathbf{n} + \overline{n} = 1$$

Since flipping the state of a Cbit and then acting on it with $\mathbf{n}$ is the same as acting on the state with $\overline{n}$ and then flipping it, we have

$$\mathbf{n}\mathbf{X} = \mathbf{X}\overline{n}$$

Also note that

$$\mathbf{X}^2 = 1$$

which means the NOT operator is its own inverse.

Swap operator:

$$S = n \otimes n + \overline{n} \otimes \overline{n} + (X \otimes X)(n \otimes \overline{n}) + (X \otimes X)(\overline{n} \otimes n)$$

If both Cbits are in state $|1\rangle$, only the first term in the sum acts and the same pattern continues for the 3 other configurations.
We can use subscripts instead of long tensor products to indicate which bit an operation is acting on:

$$1 \otimes 1 \otimes a \otimes 1 \otimes b \otimes 1 = a_3 b_1 = b_1 a_3$$

Figure 1: a has subscript 3 because it is acting on the bit corresponding to 2^3 and b has subscript 1 because it is acting on the bit corresponding to 2^1.
We use this notation to illustrate the *controlled-not* or cNOT operation, C_{ij}. If the value represented by the i-th Cbit (the *control bit*) is 0, C_{ij} leaves the value represented by the j-th Cbit (the *target bit*) unchanged, but if the control bit is 1, C_{ij} flips the target bit. In both cases, the control bit is left unchanged.

$$C_{10}|x\rangle|y\rangle = |x\rangle|y \bigoplus x\rangle$$

Figure 2: where $\bigoplus$ denotes addition modulo 2 (ie the "exclusive OR")

$$y \bigoplus 0 = y, y \bigoplus 1 = \overline{y} = 1 - y$$

We can build a swap out of three cNOT operations:

$$S_{ij} = C_{ij} C_{ji} C_{ij}$$

A symmetry of the cNOT operator is revealed if we define the operator

$$Z = \overline{n} - n \longleftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

This is a weird operator because if applied to $|1\rangle$, it produces $-|1\rangle$ which isn't defined in classical computing. We will see this becomes the NOT operator X in quantum computing but for now we will only use it combined with other operators in classical computing.
We notice that the NOT operator X anticommutes with Z:

$$ZX = -XZ$$

Since $\overline{n} + n = 1$, we can express $\overline{n}$ and n in terms of 1 and Z:

$$n = \frac{1}{2}(1 - Z), \overline{n} = \frac{1}{2}(1 + Z)$$

We can actually rewrite the cNOT operator in terms of X and Z operators:

$$C_{ij} = \frac{1}{2}(1 + Z_i) + \frac{1}{2} X_j (1 - Z_i) = \frac{1}{2}(1 + X_j) + \frac{1}{2} Z_i (1 - X_j)$$

In fact, we can switch which bit is the control and which is the target. An operator that produces this effect is the *Hadamard transformation*:

$$H = \frac{1}{\sqrt{2}}(X + Z) \longleftrightarrow \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Since we know $X^2 = Z^2 = 1$ and $XZ = -ZX$, we can show that

$$H^2 = 1$$

and that

$$HXH = Z, HZH = X$$

This shows how H can be used to interchange the X and Z operators. It follows that

$$C_{ji} = (H_i H_j) C_{ij} (H_i H_j)$$

The action of H on a Cbit is:

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),\ H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

which makes no sense at all in classical computing.
A reversible operation on two Cbits is any permutation of their 4 possible states. There are $4! = 24$ such operations. Generally, there are $(2^n)!$ distinct reversible operations on n Cbits.

3 Qbits and their states

While Cbits can only be one of two orthonormal vectors, Qbits can be any unit vector in the two-dimensional space spanned by $|0\rangle$ and $|1\rangle$. The scalars in the two-dimensional vector space containing the states of a Qbit are complex numbers. The general state of a Qbit is:

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle \longleftrightarrow \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$$

where α_0 and α_1 are complex numbers constrained by the requirement that $|\psi\rangle$ must be a unit vector:

$$|\alpha_0|^2 + |\alpha_1|^2 = 1$$

We say that $|\psi\rangle$ is a *superposition* of the states $|0\rangle$ and $|1\rangle$ with *amplitudes* α_0 and α_1. Qbits, in contrast to Cbits, cannot be said to "have values." They ***are described by*** states. Just like the general state of a single Qbit, the general state of two Qbits is an arbitrary normalized superposition of the four orthogonal classical states.

$$|\Psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

with the complex amplitudes being constrained only by the normalization condition

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

In quantum computation, the 2^n possible classical state products is called the *computational basis*. If we have two Qbits, one in the state $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ and the other in the state $|\phi\rangle = \beta_0|0\rangle + \beta_1|1\rangle$, then the state of the pair is the tensor product of the individual states:

$$|\Psi\rangle = |\psi\rangle \otimes |\phi\rangle = \begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \end{pmatrix}$$

Unlike Cbits, whose general state can only be one of the 2^n products of the orthonormal vectors, a general state of n Qbits is a superposition of these 2^n product states which will not, in general, be any product of any set of 1-Qbit states. These nonproduct states of two or more Qbits are called *entangled* states. Section A3 of Appendix.

4 Reversible Operations on Qbits

Recall that the only nontrivial reversible operation a classical computer can perform on a single Cbit is the NOT operation X. A quantum computer can perform any linear transformation u that takes in a unit vector and returns a unit vector on a single Qbit. These transformations u are called *unitary* and satisfy:

$$uu^\dagger = u^\dagger u = 1$$

where $\dagger$ represents the adjoint of matrix u which is the transposed complex conjugate.
These transformations are called n-Qbit gates.
Any operation P that acts on n Cbits can be associated with a corresponding unitary operation U on n Qbits. Since U works on the classical basis, we can extend that to Qbits which are just on the span of that basis. Since the action of U on classical-basis states merely permutes them, its effect on any superposition of states is to permute the amplitudes. Since it is norm-preserving and linear, it is unitary.
In the design of quantum algorithms, we typically only use unitary transformations that act on one or two Qbits at a time because the technical problems of making higher order quantum gates are incredibly formidable. Luckily, we can approximate a many-degree gate with just gates of 1 or 2 Qbits.

5 The Measurement of Qbits

To specify the state of a single Cbit, we only need one bit of information: whether the state is 0 or 1. For a Qbit, we need a high degree of precision

to specify the two complex numbers α and β. However, there is a huge catch: making a measurement on a Qbit binds its outcomes to either 0 or 1, with the squared magnitude of the amplitudes being the probability of each outcome.
This rule was discovered by Max Born and is known as the *Born rule*: the squared magnitudes of the amplitudes give the probabilities of outcomes of measurements.
The process of measurement is carried out by hardware known as an *n-Qbit measurement gate*. In contrast to unitary gates, this act of measurement cannot be undone. In quantum computation, "measurement" means nothing more than applying and reading the display of an appropriate measurement gate to each of the n Qbits. After measurement, the amplitudes disappear. This is referred to as a *reduction* or *collapse* of the state.
The Born rule does not mean that prior to measurement, the Qbit is in state 0 or 1 with some probability, rather that only after subjecting the Qbit to a measurement does it output 0 or 1.
Quantum computing is really just the artistry of applying cunningly constructed unitary transformations to get a superposition in which most amplitudes are zero while all significant amplitudes carry useful information.
The *generalized Born rule* plays a very important role in quantum computing. It states that when one measures only one out of n Qbits, the register can be represented as

$$|\Psi\rangle = a_0 |0\rangle |\Psi_0\rangle + a_1 |1\rangle |\Psi_1\rangle, |a_0|^2 + |a_1|^2 = 1$$

where $|\Psi_0\rangle$ and $|\Psi_1\rangle$ are normalized states of $n-1$ unmeasured Qbits.
Another way to see this is to generalize even further. Given some register with $m+n$ Qbits, measuring a single gate m times gives us:

$$|\Psi\rangle_{m+n} = \sum_x a_x |x\rangle_m |\Psi_x\rangle_n$$

where $\sum_x |a_x|^2 = 1$