Programming a quantum computer – Day 1
Basics of quantum computing

Peter Brown

June 20, 2022

1 Motivation

Quantum technologies aim to leverage the counterintuitive features of quantum systems in order to achieve things not possible otherwise. For instance, the field of quantum computing looks to leverage quantum parallelism, entanglement and interference (amongst other things) in order to speed up computations. Algorithms like Shor's for factoring large primes demonstrate that quantum computers can sometimes achieve exponential speedups over known classical algorithms and challenge our intuition about what problems are "hard" to solve. In particular, this example has interesting impacts on public key cryptography, where Shor's algorithm could render RSA and elliptic curve cryptography insecure.

Thus, in the wake of a large quantum computer[1] most of our current public key cryptosystems will be useless. A field of postquantum cryptography looks to address this issue by designing problems that are hard to solve, even on a quantum computer. In addition, we can also leverage quantum features like entanglement, intrinsic randomness and no-cloning in order to build cryptographic protocols that are information theoretically secure! Such protocols, like QKD, offer a new way to perform cryptography with everlasting security guarantees.

During this PAF we will explore the features of quantum theory that give us a technological advantage. We will discover interesting consequences of entanglement, quantum computational speedups and cryptographic protocols that we can observe (even with the infantile quantum computers of today). Whenever possible, we will look to try to implement these quantum technologies on real quantum devices by interacting with the cloud quantum computing services offered by IBM. We will learn how to program these devices using quantum circuits and the QISKIT python package. Towards the end of the PAF we will also explore the various competing architectures that we are building our quantum computers from.

2 Single quantum systems

In order to understand how to program a quantum computer we must first understand the basics of quantum systems. In particular, quantum bits (qubits) which are the building blocks of such computers and are the quantum analogues of bits in standard computers. To describe a quantum system we must specify three things:

1. States: How do we represent the current state of a quantum system mathematically?
2. Transformations: How does the system evolve? What transformations of the system can we induce?
3. Measurements: How can we probe the system to extract information about its properties?

Remark. We will be restricting to special cases of quantum systems. There are more general definitions of states, transformations and measurements that we will not cover here but you can look forward to them if you plan to study quantum information and quantum computing at the Masters level.

[1] Fortunately for cryptographers this is not likely to happen soon.

2.1 Qubit states

The quantum bit (qubit) is a two-level quantum system.

Postulate (Qubit state)**.** The state of a qubit is described by a vector $\begin{pmatrix}\alpha\\ \beta\end{pmatrix} \in \mathbb{C}^2$ such that $|\alpha|^2 + |\beta|^2 = 1$. (I.e., a vector with Euclidean norm 1).

Remark (Bra-Ket notation)**.** Quantum theorists often use so-called Bra-Ket or Dirac notation. We write a vector as

$$|\psi\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix} \tag{1}$$

with the angle bracket notation (called a *Ket*). You should think of this object like a 2×1 matrix. The *Bra* vector is then

$$\langle\psi| = \begin{pmatrix}\overline{\alpha} & \overline{\beta}\end{pmatrix} \tag{2}$$

i.e., a row vector with the complex conjugates of the entries of $|\psi\rangle$ ($\overline{z}$ denotes the complex conjugate of $z \in \mathbb{C}$). Again you can think of it as a 1×2 matrix. As matrices we have $\langle\psi| = |\psi\rangle^\dagger$ where $X^\dagger$ denotes the *conjugate transpose* (or *Hermitian conjugate* or *adjoint*) of a matrix X.

Thinking of them as matrices we can then multiply them together. For instance the euclidean product of two vectors $|\psi\rangle, |\phi\rangle \in \mathbb{C}^2$ is then simply $\langle\psi|\,|\phi\rangle$ or $\langle\phi|\,|\psi\rangle$ (we often write this as $\langle\psi\,|\,\phi\rangle$ and $\langle\phi\,|\,\psi\rangle$). We call this an *inner product.* For example the norm of $|\psi\rangle$ is

$$\|\,|\psi\rangle\,\| = \sqrt{|\alpha|^2 + |\beta|^2} = \sqrt{\begin{pmatrix}\overline{\alpha} & \overline{\beta}\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}} = \sqrt{\langle\psi\,|\,\psi\rangle}\,. \tag{3}$$

So a qubit is just a vector $|\psi\rangle \in \mathbb{C}^2$ such that $\langle\psi\,|\,\psi\rangle = 1$.

Another useful product is the *outer product* which is the matrix product $|\psi\rangle\,\langle\phi|$ which gives a 2×2 matrix. For example

$$|\psi\rangle\langle\psi| = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}\begin{pmatrix}\overline{\alpha} & \overline{\beta}\end{pmatrix} = \begin{pmatrix}|\alpha^2| & \alpha\overline{\beta}\\ \overline{\alpha}\beta & |\beta^2|\end{pmatrix} \tag{4}$$

Example.

- The *computational basis* states are

$$|0\rangle = \begin{pmatrix}1\\ 0\end{pmatrix} \qquad \text{and} \qquad |1\rangle = \begin{pmatrix}0\\ 1\end{pmatrix}\,. \tag{5}$$

  Any qubit can be written as $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ with $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$.

- The *Hadamard basis* states are

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad \text{and} \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{6}$$

You can verify that both sets form orthonormal bases for $\mathbb{C}^2$, i.e., they are normalized and orthogonal $\langle 0\,|\,1\rangle = \langle 1\,|\,0\rangle = 0 = \langle +\,|\,-\rangle = \langle -\,|\,+\rangle$.

Remark (Global phase)**.** If two quantum states $|\psi\rangle$ and $|\phi\rangle$ are such that $|\psi\rangle = e^{i\theta}\,|\phi\rangle$ for some $\theta \in (0, 2\pi]$, i.e., they differ by a global phase. Then we consider them to be 'equal' as there is no physical way to distinguish them. (See exercises).

This means that any single qubit state, up to a global phase can be written as

$$|\psi\rangle = \cos(\theta/2)\,|0\rangle + \sin(\theta/2)e^{i\phi}\,|1\rangle \qquad\qquad \theta \in [0, \pi], \quad \phi \in [0, 2\pi). \tag{7}$$

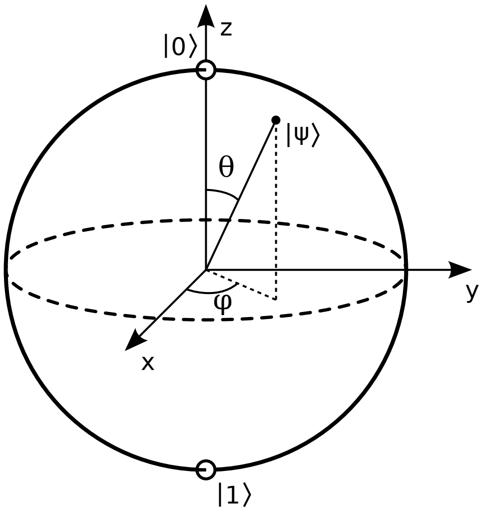


Figure 1: Single qubit states have a useful representation as points on the surface of a sphere. By using the general form of a qubit (see Eq. (7)) we can see each qubit state (up to global phase) as a unique point on the sphere. The antipodal points on the X axis are the states $|+\rangle$ and $|-\rangle$. And the antipodal points for the Y axis are

$$|i\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle \qquad |-i\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{i}{\sqrt{2}}|1\rangle \ .$$

The antipodal points for the 3 axis correspond to the eigenvectors of the 3 Pauli matrices. Credit: Figure by Smite-Meister - Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=5829358.

2.2 Qubit Transformations

Recall that unitary matrices are square matrices U such that

$$U^\dagger U = UU^\dagger = I \, . \tag{8}$$

Postulate (Qubit transformations)**.** The evolution of a single qubit (in isolation) is described by a unitary matrix on $\mathbb{C}^2$.

Example. Single qubit unitaries are also sometimes call *single qubit quantum gates.* Some are used so often that we give them special names.

- *The Pauli gates.* The three unitary matrices

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{9}$$

  are referred to as the Pauli X/Y/Z gates.

- *The Hadamard gate.* The matrix

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{10}$$

  is called the Hadamard gate. It transforms between the computational and Hadamard bases, $H|0\rangle = |+\rangle$ and $H|1\rangle = |-\rangle$ and $H^2 = I$.

Notice that the Pauli X gate acts like a NOT on the computational basis

$$X|0\rangle = |1\rangle \qquad X|1\rangle = |0\rangle \, , \tag{11}$$

it is sometimes called a *NOT gate* or a *bit-flip gate.* The Z gate is sometimes referred to as a *phase-flip gate.*

2.3 Qubit measurements

We will restrict to a certain class of measurements known as projective measurements. A matrix P is a projector if it is a square matrix such that $P^\dagger = P$ and $P^2 = P$.

Postulate. A qubit measurement is a collection of projectors $\{P_0, P_1\}$ acting on $\mathbb{C}^2$ such that $P_0 + P_1 = I$. If the qubit state is $|\psi\rangle \in \mathbb{C}^2$ and we perform the measurement defined by $\{P_0, P_1\}$, then we obtain outcome "0" with probability

$$\mathbb{P}(0) = \langle\psi| P_0 |\psi\rangle \tag{12}$$

and we obtain outcome "1" with probability

$$\mathbb{P}(1) = \langle\psi| P_1 |\psi\rangle\ . \tag{13}$$

The qubit is disturbed by the measurement and the state of the qubit after outcome i becomes

$$\frac{P_i |\psi\rangle}{\sqrt{\langle\psi| P_i |\psi\rangle}} \tag{14}$$

Remark.

- Because we need $P_0 + P_1 = I$ we can always write $P_1 = I - P_0$.
- We can measure in an orthonormal basis $\{|v\rangle, |w\rangle\}$ by constructing projectors $P_v = |v\rangle\langle v|$ and $P_w = |w\rangle\langle w|$ and then performing the measurement defined by $\{P_v, P_w\}$.
- Measurement labels are free to choose: "cats" and "dogs". Although in some cases the label is physically meaningful, i.e., corresponds to an energy value.
- Related to this, sometimes people will refer to measuring the "observable" M where M is a Hermitian matrix (i.e., $M = M^\dagger$). Because M is Hermitian it has a set of real eigenvalues $\{\lambda_1, \lambda_2\}$ and corresponding (normalized) eigenvectors $\{|v_1\rangle, |v_2\rangle\}$ which form an orthonormal basis. Measuring the observable M then corresponds performing the measurement in the basis of eigenvectors of M and labeling the measurement by the eigenvalues. The observable M then gives a compact way to compute the expected value of the measurement. Suppose we measure the state $|\psi\rangle$ in the eigenbasis of M, let $\mathbb{E}[M]$ denote the expected value of the measurement then

$$\mathbb{E}[M] = \sum_i \lambda_i \mathbb{P}(\lambda_i) = \sum_i \lambda_i \langle\psi\,|\,v_i\rangle\langle v_i\,|\,\psi\rangle = \langle\psi| \sum_i \lambda_i |v_i\rangle\langle v_i| |\psi\rangle = \langle\psi| M |\psi\rangle\ . \tag{15}$$

  where the final equality follows from the spectral theorem.

Example.

- Suppose we measure $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ in the computational basis. Then we have

$$\begin{aligned} \mathbb{P}(0) &= \langle\psi\,|\,0\rangle\langle 0\,|\,\psi\rangle \\ &= (\overline{\alpha}\langle 0| + \overline{\beta}\langle 1|)\,|0\rangle\langle 0|\,(\alpha|0\rangle + \beta|1\rangle) \\ &= |\alpha|^2 \langle 0\,|\,0\rangle\langle 0\,|\,0\rangle + \overline{\alpha}\beta\langle 0\,|\,0\rangle\langle 0\,|\,1\rangle + \alpha\overline{\beta}\langle 1\,|\,0\rangle\langle 0\,|\,0\rangle + |\beta|^2\langle 1\,|\,0\rangle\langle 0\,|\,1\rangle \\ &= |\alpha|^2\,. \end{aligned} \tag{16}$$

  A similar calculation gives

$$\mathbb{P}(1) = |\beta|^2\,. \tag{17}$$

  In general the coefficients α and β are *probability amplitudes* for measuring the state in the basis in which we write it.

3 Multiple Qubits

A single qubit system is quite limiting. We will find more interesting computations and features if we combine many qubits together. Before we do that we need some understanding of a tensor product.

3.1 A brief aside on $\otimes$

Given two Hilbert spaces V and W over $\mathbb{C}$ we can form a new Hilbert space $V \otimes W$ in the following way. Take a basis $\{|v_i\rangle\}_i$ for V and a basis $\{|w_i\rangle\}_i$ for W. Then

$$V \otimes W = \operatorname{span}\{|v_i\rangle \otimes |w_j\rangle\}_{i,j} \tag{18}$$

where $\otimes : V \times W \to V \otimes W$ is a *bi-linear* map (linear in both arguments), i.e.,

$$\left(\sum_i \alpha_i |v_i\rangle\right) \otimes \left(\sum_j \beta_j |w_j\rangle\right) = \sum_{ij} \alpha_i \beta_j |v_i\rangle \otimes |w_j\rangle \ . \tag{19}$$

The inner product on $V \otimes W$ is then defined via

$$\left(\langle v_i| \otimes \langle w_j|\right)\left(|v_k\rangle \otimes |w_l\rangle\right) = \langle v_i \,|\, v_k\rangle\langle w_j \,|\, w_l\rangle \ . \tag{20}$$

When working with explicit vectors and matrices we can use the Kronecker product to compute vector and matrix representations of the tensor product. Let

$$|v\rangle = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} \in \mathbb{C}^n \qquad \text{and} \qquad |w\rangle = \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_m \end{pmatrix} \in \mathbb{C}^m \tag{21}$$

then

$$|v\rangle \otimes |w\rangle = \begin{pmatrix} v_1 |w\rangle \\ v_2 |w\rangle \\ \vdots \\ v_n |w\rangle \end{pmatrix} = \begin{pmatrix} v_1 w_1 \\ v_1 w_2 \\ \vdots \\ v_1 w_m \\ v_2 w_1 \\ v_2 w_2 \\ \vdots \\ v_n w_m \end{pmatrix} \tag{22}$$

the result of combining a length m vector with a length n vector is a length nm vector.

We can also take the tensor product of matrices. Let

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} b_{11} & \dots & b_{1q} \\ \vdots & \ddots & \vdots \\ b_{p1} & \dots & b_{pq} \end{pmatrix} \tag{23}$$

i.e., A is an $m \times n$ matrix and B is a $p \times q$ matrix. Then $A \otimes B$ is a $mp \times nq$ matrix given by

$$A \otimes B = \begin{pmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \dots & a_{mn}B \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & \dots & a_{11}b_{1q} & & & a_{1n}b_{11} & \dots & a_{1n}b_{1q} \\ \vdots & \ddots & \vdots & \cdots & \cdots & \vdots & \ddots & \vdots \\ a_{11}b_{p1} & \dots & a_{11}b_{pq} & & & a_{1n}b_{p1} & \dots & a_{1n}b_{pq} \\ & \vdots & & \ddots & & & \vdots & \\ & \vdots & & & \ddots & & \vdots & \\ a_{m1}b_{11} & \dots & a_{m1}b_{1q} & & & a_{mn}b_{11} & \dots & a_{mn}b_{1q} \\ \vdots & \ddots & \vdots & \cdots & \cdots & \vdots & \ddots & \vdots \\ a_{m1}b_{p1} & \dots & a_{m1}b_{pq} & & & a_{mn}b_{p1} & \dots & a_{mn}b_{pq} \end{pmatrix} \tag{24}$$

Remark (Properties)**.** There are a few useful properties for the tensor product.

- **Bilinearity** (see above)
- **Products** $(A \otimes B)(C \otimes D) = AC \otimes BD$
- **Adjoints** $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$
- **Associativity** $(A \otimes B) \otimes C = A \otimes (B \otimes C)$.

3.2 Combining quantum systems

Again, we are only considering a special case of quantum states, transformations and measurements.

Postulate (N-qubit systems)**.**

- The *states* of an n-qubit system is a unit vector in $(\mathbb{C}^2)^{\otimes n}$.
- The *transformations* on an n-qubit system are unitary matrices on $(\mathbb{C}^2)^{\otimes n}$.
- The *measurements* on an n-qubit system are defined by a collection of projectors $\{P_i\}_i$ acting on $(\mathbb{C}^2)^{\otimes n}$ such that $\sum_i P_i = I$. If we have a system in the $|\psi\rangle$ then we obtain the i-th outcome with probability
$$\mathbb{P}(i) = \langle\psi| P_i |\psi\rangle \tag{25}$$
and the state after measurement becomes
$$\frac{P_i |\psi\rangle}{\sqrt{\langle\psi| P_i |\psi\rangle}} \tag{26}$$

Example. It's perhaps easiest to grasp with some examples

1. $$|0\rangle \otimes |+\rangle = |0\rangle \otimes \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) = \frac{1}{\sqrt{2}}|0\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}}|0\rangle \otimes |1\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ 0 \\ 0 \end{pmatrix} \tag{27}$$

2. Take $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, then
$$Z \otimes X = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{pmatrix} \tag{28}$$

3. We often use the shorthand
$$\begin{aligned} |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle &= |x_1\rangle |x_2\rangle \ldots |x_n\rangle \\ &= |x_1 x_2 \ldots x_n\rangle \\ &= |\mathbf{x}\rangle \end{aligned} \tag{29}$$
where on the last line we have just identified $\mathbf{x} = x_1 \ldots x_n$. And the notation $X^{\otimes n}$ corresponds to X tensored with itself n times, i.e., $X \otimes X \otimes \cdots \otimes X$. One example of this you will see a lot in quantum algorithms is
$$H^{\otimes n}(|0\rangle^{\otimes n}) = (H|0\rangle)^{\otimes n} = |+\rangle^{\otimes n} = 2^{-n/2} \sum_{\mathbf{x} \in \{0,1\}^n} |\mathbf{x}\rangle \tag{30}$$
the latter is a uniform superposition over all n-bit strings.

4. Suppose we have a two-qubit state $|\psi\rangle$ and we want to measure the first qubit in the computational basis and the second qubit in the Hadamard basis. We can define 4 projectors

$$\begin{aligned} P_{0+} &= |0\rangle\langle 0| \otimes |+\rangle\langle +| \\ P_{0-} &= |0\rangle\langle 0| \otimes |-\rangle\langle -| \\ P_{1+} &= |1\rangle\langle 1| \otimes |+\rangle\langle +| \\ P_{1-} &= |1\rangle\langle 1| \otimes |-\rangle\langle -| \end{aligned} \tag{31}$$

   one can check that these sum to I. If $|\psi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$, then we have for instance that

$$\begin{aligned} \mathbb{P}(0,+) &= \langle\psi|\,(|0\rangle\langle 0| \otimes |+\rangle\,|\psi\rangle \\ &= \begin{pmatrix} 1/\sqrt{2} & 0 & 0 & 1/\sqrt{2} \end{pmatrix} \begin{pmatrix} 1/2 & 1/2 & 0 & 0 \\ 1/2 & 1/2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1/\sqrt{2} \\ 0 \\ 0 \\ 1/\sqrt{2} \end{pmatrix} \\ &= \begin{pmatrix} 1/\sqrt{2} & 0 & 0 & 1/\sqrt{2} \end{pmatrix} \begin{pmatrix} 1/(2\sqrt{2}) \\ 1/(2\sqrt{2}) \\ 0 \\ 0 \end{pmatrix} \\ &= 1/4\,. \end{aligned} \tag{32}$$

   If we instead only want to measure the first system in the computational basis we can construct the projectors $P_0 = |0\rangle\langle 0| \otimes I$ and $P_1 = |1\rangle\langle 1| \otimes I$, where the I operator is on the qubit that we are not measuring. Note again they sum to I and so form a valid measurement. Then

$$\begin{aligned} \mathbb{P}(0) &= \langle\psi|\,(|0\rangle\langle 0| \otimes I)\,|\psi\rangle \\ &= \begin{pmatrix} 1/\sqrt{2} & 0 & 0 & 1/\sqrt{2} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1/\sqrt{2} \\ 0 \\ 0 \\ 1/\sqrt{2} \end{pmatrix} \\ &= \begin{pmatrix} 1/\sqrt{2} & 0 & 0 & 1/\sqrt{2} \end{pmatrix} \begin{pmatrix} 1/\sqrt{2} \\ 0 \\ 0 \\ 0 \end{pmatrix} \\ &= 1/2 \end{aligned} \tag{33}$$

   Notice the state after measurement when we obtain the outcome 0 is $|00\rangle$. If we then measure the second qubit in the Hadamard basis we will get outcome + with $\mathbb{P}(+|0) = 1/2$. This agrees with the joint probability that we observed when measuring together. $\mathbb{P}(0,+) = \mathbb{P}(+|0)\mathbb{P}(0)$.

Remark (Independent systems, entanglement and local interactions)**.** For simplicity I'll describe the two-qubit case but it extends naturally to n-qubits. We'll call the first qubit A and the second qubit B.

- Suppose the qubits are *independent* (haven't interacted), then the state of the two-qubit system is of the form

$$|\psi\rangle_{AB} = |\psi_0\rangle_A \otimes |\psi_1\rangle_B\ . \tag{34}$$

  We call such a state a *product* state. However, there are more two-qubit states than just product states, for example

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}\,|00\rangle + \frac{1}{\sqrt{2}}\,|11\rangle \tag{35}$$

  such a state cannot be written in the form (34) (see exercises). We call such a state *entangled*, these are exactly states that have interacted in the past and become correlated.

- Suppose we have a two-qubit state $|\psi\rangle_{AB}$. If we want to apply the single-qubit unitary U to system A then we model this by the two-qubit unitary $U \otimes I$ where I is the identity matrix, so

$$|\psi\rangle_{AB} \mapsto (U \otimes I) |\psi\rangle_{AB} . \tag{36}$$

  Similarly if we wanted to apply U to system B then we'd model this by the two-qubit unitary $I \otimes U$.

  In a similar fashion to entanglement, there are more two-qubit unitaries than just those of the form $U \otimes V$, for example the controlled-not unitary CNOT

$$\mathrm{CNOT} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} . \tag{37}$$

  This is a two-qubit gate which when the first qubit is in the $|0\rangle$ state it does nothing and when the first qubit is in state $|1\rangle$ it performs a bit-flip on the second qubit.

- We can also measure the two-qubit state but measuring the two-qubits individually. If you have an orthonormal basis $\{|v_i\rangle\}_i$ for system A and an orthonormal basis $\{|w_j\rangle\}_j$ for system B then $\{|v_i\rangle \otimes |w_j\rangle\}_{i,j}$ is an orthonormal basis for a two-qubit system. Measuring in this basis is equivalent to measuring each qubit in their respective bases, i.e.,

$$\mathbb{P}(A = i, B = j) = \langle\psi| (|v_i\rangle\langle v_i| \otimes |w_j\rangle\langle w_j|) |\psi\rangle \tag{38}$$

  circuit

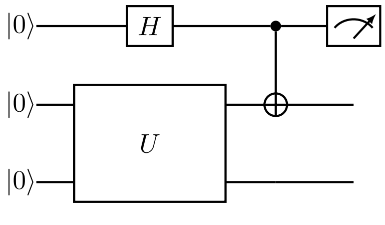
  You can also choose to measure only one of the qubits. If you only want to measure qubit A for example you replace the basis for the qubit you don't want to measure by an identity operator, so

$$\mathbb{P}(A = i) = \langle\psi| (|v_i\rangle\langle v_i| \otimes I) |\psi\rangle \tag{39}$$

  this is consistent with the standard rules of probability theory $\sum_j \mathbb{P}(A = i, B = j) = \mathbb{P}(A = i)$, can you see why?

4 Quantum circuits

Quantum circuits are a useful method of depicting what we want to do on the quantum computer. In essence, we are just combining states evolutions and measurements. Here is an example of a quantum circuit



(40)

This circuit describes the following

1. We initialize 3 qubits in the state 0, call the qubits A, B and C.
2. We then apply a Hadamard gate to qubit A and apply two-qubit unitary U to qubits B and C.
3. Then apply a CNOT gate acting on qubit B and controlled on qubit A.
4. Finally measure qubit A in the computational basis.

The state before measurement is

$$|\psi\rangle = (\mathrm{CNOT}_{AB} \otimes I_C)(H_A \otimes U_{BC}) |000\rangle_{ABC} . \tag{41}$$

Suppose U is the CNOT gate acting on C and controlled on B, then the state becomes

$$\begin{aligned}
|\psi\rangle &= (\mathrm{CNOT}_{AB} \otimes I_C)(H_A \otimes \mathrm{CNOT}_{BC}) |000\rangle_{ABC} \\
&= (\mathrm{CNOT}_{AB} \otimes I_C) |{+00}\rangle_{ABC} \\
&= (\mathrm{CNOT}_{AB} \otimes I_C)(\frac{1}{\sqrt{2}} |000\rangle + \frac{1}{\sqrt{2}} |100\rangle) \\
&= \frac{1}{\sqrt{2}} |000\rangle + \frac{1}{\sqrt{2}} |110\rangle
\end{aligned} \tag{42}$$

If we measure the first qubit in the computational basis we get