Quantum Computing

Teach Me X

Giacomo Fenzi

University of St. Andrews

February 7, 2021

Outline

1. Mathematics
   - Vector Spaces
   - Linear operators
   - Hilbert Spaces
   - Eigenstuff
   - Adjoint and Tensors
2. Physics
   - Postulates
3. Computer Science
   - Reversible circuits
   - Quantum Gates
   - Algorithms
4. Future

Vectors

A vector is an array of n numbers.
Let S be a field. We write S^n as the set of all vectors with n entries in S.

Example

For example, $\mathbb{R}^n$, $\mathbb{C}^n$ are the sets of vectors of n, respectively, real and complex numbers.
Here are a couple of vectors:

$$\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \in \mathbb{R}^3, \begin{pmatrix} 1+i \\ 1-i \end{pmatrix} \in \mathbb{C}^2, \tag{1}$$

Notation

- In school often vectors are denoted as $\boldsymbol{v}$ or $\vec{v}$.
- In Quantum mechanics we use Dirac notation: $|v\rangle$
- This just means the vector named v.

Operation

Vectors are characterized by two operations on their values:

- Addition: given two vectors $|a\rangle, |b\rangle$, then $|a\rangle + |b\rangle$ is also a vector, defined by summing pointwise the components of the two.
- Scalar multiplication: given a vector $|a\rangle$ and a scalar α, then $\alpha |a\rangle$ is a vector, defined by multiplying each component of $|a\rangle$ by α.

Example

Let:

$$|a\rangle = \begin{pmatrix} 1 \\ 2 \end{pmatrix}, |b\rangle = \begin{pmatrix} 3 \\ 4 \end{pmatrix} \tag{2}$$

Then:

$$2|a\rangle + |b\rangle = \begin{pmatrix} 5 \\ 8 \end{pmatrix}, \tag{3}$$

Vector Spaces and Basis

A set like $\mathbb{R}^n, \mathbb{C}^n$ is called[1] a *vector space* In particular, each vector space V contains some set of vectors called a basis for the space, which we denote $|0\rangle, |1\rangle, \ldots, |n-1\rangle$ such that:

- For every $|v\rangle \in V$, there exist α_i such that:

  $$|v\rangle = \sum_i \alpha_i |i\rangle$$

- $$\sum_i \alpha_i |i\rangle = 0$$

  iff $\alpha_i = 0$.

[1] Pedantically, it's the other way around, we first define vectors spaces and prove the two are one

Basis Examples

Example

Consider the vector space $\mathbb{R}^2$. This is the so called standard basis:

$$|0\rangle = \begin{pmatrix}1\end{pmatrix}, |1\rangle = \begin{pmatrix}0\\1\end{pmatrix} \tag{4}$$

Also, the following is an interesting basis we will encounter:

$$|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, |-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} \tag{5}$$

The proof is quite simple, I suggest first showing the standard basis is one, and then note that:

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

Linear Transformation

A linear transformation between two vectors spaces is a function $T : V \to W$ such that, for $|a\rangle, |b\rangle \in V$, and scalar α

- $T(|a\rangle + |b\rangle) = T|a\rangle + T|b\rangle$
- $T(\alpha|a\rangle) = \alpha T|a\rangle$

Since every vector in V can be written as a sum of scaled basis vectors it follows:

$$T|v\rangle = \sum_i \alpha_i T|i\rangle$$

And a linear transformation can be uniquely determined by its action on the bases.
Also, if $V = W$, we call $T : V \to V$ a *linear operator* on V.

Matrix

Encoding this operation, we can write a linear transformation as a matrix (and viceversa).

Example

Consider the following linear operator T on $\mathbb{C}^2$:

$$T|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{6}$$

$$T|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{7}$$

Then the corresponding matrix is the useful *Hadamard Gate*

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix} \tag{8}$$

Pauli Matrices

Example

The following matrices are of particular importance, and X, Y, Z are called the Pauli Matrices.

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{9}$$

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{10}$$

Inner Product

The inner product is a generalization of the dot product to complex vectors in $\mathbb{C}^n$. We write $\langle v|w\rangle$ for the inner product of $|v\rangle, |w\rangle$. It has the properties that:

- $(\langle v|w\rangle)^* = \langle w|v\rangle$, where $\cdot^*$ is the complex conjugate.
- $\langle v|v\rangle \geq 0$. We define also $||\,|v\rangle\,|| \equiv \sqrt{\langle v|v\rangle}$
- If $|w\rangle = \sum_i \alpha_i |w_i\rangle$, then $\langle v|w\rangle = \sum_i \alpha_i \langle v|w_i\rangle$

We define an Hilbert space to be a vector space with such inner product. In $\mathbb{C}^n$ we define that if:

$$|v\rangle = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}, |w\rangle = \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} \implies \langle v|w\rangle = \sum_i v_i^* w_n = (v_1^* \dots v_n^*) \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} \tag{11}$$

Also, if $||\,|\psi\rangle\,|| = 1$, we say that $|\psi\rangle$ is a unit vector.

Inner Products

Example

Consider the following (all in $\mathbb{C}^2$):

$$|a\rangle = \begin{pmatrix} 1+i \\ 2 \end{pmatrix}, |b\rangle = \begin{pmatrix} 2 \\ 3 \end{pmatrix} \tag{12}$$

And $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ as defined before. Then:

$$\langle 0|1\rangle = \langle +|-\rangle = 0 \tag{13}$$

$$\langle 0|0\rangle = \langle 1|1\rangle = \langle +|+\rangle = \langle -|-\rangle = 1 \tag{14}$$

$$\langle a|b\rangle = 6-2i, \langle b|b\rangle = 13, \langle a|0\rangle = 1-i \tag{15}$$

Orthonormality

You might have noticed before that our standard basis (and in fact also $|+\rangle, |-\rangle$) of $\mathbb{C}^2$ satisfies the following property:

$$\langle i|j\rangle = \delta_{ij} \tag{16}$$

Where δ_{ij} is the Kronecker delta, defined as:

$$\delta_{ij} = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{if } i \neq j. \end{cases} \tag{17}$$

Any basis, satisfying this condition is called *orthonormal*. A result in linear algebra is that any basis can be converted to an orthonormal one thanks to the Gram Schmidt process, which simplifies a lot of proofs.

Eigenvalues

In the whole of linear algebra one equation is of particular interest:

$$A\left|v\right\rangle = \lambda\left|v\right\rangle \tag{18}$$

If the above hold, then λ is called an *eigenvalue* of A, with $\left|v\right\rangle$ its corresponding *eigenvector*. We are particularly interested in *spectral decompositions*, i.e. operators for which:

$$A = \sum_{\lambda} \lambda \left|\lambda\right\rangle \left\langle\lambda\right| . \tag{19}$$

Where λ is the eigenvalue with eigenvector $\left|\lambda\right\rangle$, and $\left|v\right\rangle\left\langle w\right|$ is defined to be the linear operator such that $\left|v\right\rangle\left\langle w\right|\left(\left|z\right\rangle\right) \equiv \left|v\right\rangle\left\langle w|z\right\rangle$

Eigenvalues

Example

Consider H as in 8. Then H has eigenvalues ±1, with (non normalized) eigenvectors $(1 \pm \sqrt{2})\left|0\right\rangle + \left|1\right\rangle$. The Pauli Matrices defined in 9 also have eigenvalues ±1. The eigenvectors are:

$$\left|\lambda_{x+}\right\rangle = \left|+\right\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \left|\lambda_{x-}\right\rangle = \left|-\right\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} \tag{20}$$

$$\left|\lambda_{y+}\right\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}, \left|\lambda_{y-}\right\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}i\\1\end{pmatrix} \tag{21}$$

$$\left|\lambda_{z+}\right\rangle = \left|0\right\rangle = \begin{pmatrix}1\end{pmatrix}, \left|\lambda_{z-}\right\rangle = \left|1\right\rangle = \begin{pmatrix}0\\1\end{pmatrix} \tag{22}$$

Adjoint

For a linear operator A, we define $A^\dagger \equiv (A^T)^*$, where $\cdot^T$ is the transpose operation. It has the defining property that $\langle v|A|w\rangle = \langle v'|w\rangle$ where $|v'\rangle = A^\dagger |v\rangle$. Some matrices behave particularly well with respect with their adjoint, and so we denote then appropriately:

- $H = H^\dagger$, then H is Hermitian
- $UU^\dagger = I$, then U is Unitary
- $NN^\dagger = N^\dagger N$, then N is Normal

It is quite easy to show that an Hermitian or Unitary operator is automatically normal, and the spectral theorem shows that any Normal operator has a spectral decompositions, which comes in quite handy.

Tensor Product

Finally, we want a way to put together Hilbert spaces. For Hilbert spaces V, W we define the tensor product $V \otimes W$. If $|v_i\rangle, |w_i\rangle$ is a basis for respectively V, W, then $|v_i\rangle \otimes |w_i\rangle$ is a basis for the product. Also the following hold:

- $\alpha(|v\rangle \otimes |w\rangle) = (\alpha |v\rangle) \otimes |w\rangle = |v\rangle \otimes (\alpha |w\rangle)$
- $(|v\rangle + |v'\rangle) \otimes |w\rangle = |v\rangle \otimes |w\rangle + |v'\rangle \otimes |w\rangle$
- $|v\rangle \otimes (|w\rangle + |w'\rangle) = |v\rangle \otimes |w\rangle + |v\rangle \otimes |w'\rangle$

Also, for linear operators $A : V \to V$, $B : W \to W$ we define $(A \otimes B)(|v\rangle \otimes |w\rangle) \equiv A |v\rangle \otimes B |w\rangle$ Finally, the inner product of $|a\rangle = \sum_i \alpha_i |v_i\rangle \otimes |w_i\rangle$ and $|b\rangle = \sum_j \beta_j |v_j'\rangle \otimes |w_j'\rangle$ is quite[2] naturally:

$$\langle a|b\rangle \equiv \sum_{ij} \alpha_i^* \beta_j \langle v_i|v_j'\rangle \langle w_i|w_j'\rangle \tag{23}$$

Or, more simply: $(\langle v| \otimes \langle w|)(|v'\rangle \otimes |w'\rangle) = \langle v|v'\rangle \langle w|w'\rangle$

[2] lol

Notes on notation

It is common to abbreviate $|v\rangle \otimes |w\rangle$ as $|v\rangle|w\rangle$ or $|v, w\rangle$ or even, sometimes (especially in qubit systems) as $|v_L w_R\rangle$ or $|vw\rangle$.
Also we have the operation $\cdot^{\otimes n}$ is the operation of tensoring the object with itself n times.

Example

Consider $\mathbb{C}^2 \otimes \mathbb{C}^2 = (\mathbb{C}^2)^{\otimes 2}$. This vector space has then basis $|0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|0\rangle, |1\rangle|1\rangle$. Then $|0\rangle^{\otimes 2} = |0\rangle \otimes |0\rangle = |00\rangle$ Note that here I am switching notation just for explanation, I'll try to be consistent afterwards.

Kronecker product

In order to make this more concrete, we define the Kronecker product for tensoring two matrices (vec) together. Let A be a $m \times n$ matrix, and B be a $p \times q$ matrix. Then

$$A \otimes B = \begin{pmatrix} A_{11}B \dots A_{1n}B \\ \vdots \ddots \vdots \\ A_{m1}B \dots A_{mn}B \end{pmatrix} \tag{24}$$

is a $mp \times nq$ matrix, and is called the Kronecker product of A, B.

Tensor Product

Example

Consider now the the tensor product $T = (\mathbb{C}^2)^{\otimes 2}$. The vector $(|0\rangle + 2\,|1\rangle) \otimes (2\,|0\rangle + 3\,|1\rangle)$ in T is equal to $2\,|00\rangle + 3\,|01\rangle + 4\,|10\rangle + 6\,|11\rangle$ This is also apparent from the Kronecker representation:

$$\begin{pmatrix} 1 \\ 2 \end{pmatrix} \otimes \begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 \times 2 \\ 1 \times 3 \\ 2 \times 2 \\ 2 \times 3 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \\ 4 \\ 6 \end{pmatrix} \tag{25}$$

You can also check that the product of Pauli matrices X, Y is:

$$X \otimes Y = \begin{pmatrix} 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \\ 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \end{pmatrix} \tag{26}$$

State space

Quantum Mechanics is a framework for understanding quantum systems. It has some fundamental postulates that it uses as axioms and are experimentally validated.

Definition

Postulate 1: Every closed quantum system has an associated Hilbert space. This space is known as the *state space* of the system. The system is completely described by its *state vector*, which is simply a unit vector in the state space.

A general state vector is of the form:

$$|\psi\rangle = \sum_i \alpha_i |\psi_i\rangle \tag{27}$$

We say that $|\psi\rangle$ is in a superposition of states, with state $|\psi_i\rangle$ having amplitude α_i.

State space

Example

Let us consider the simplest quantum system: a *qubit*. This is simply a quantum system with an associated two dimensional state space. Letting $|0\rangle, |1\rangle$ be a orthonormal basis for the state space, a general state vector is described as:

$$|\psi\rangle = a|0\rangle + b|1\rangle \tag{28}$$

And, since $|\psi\rangle$ is a unit, $\langle\psi|\psi\rangle = |a|^2 + |b|^2 = 1$ For example, the following is a valid state for a qubit:

$$\frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{29}$$

Where state $|0\rangle$ has amplitude $\frac{1}{\sqrt{2}}$ and state $|1\rangle$ has amplitude $\frac{-1}{\sqrt{2}}$

System Evolution

Definition

Postulate 2: The evolution of a closed Quantum System is described by a Unitary transformation. So if the state vector at time t_1 is $|\psi\rangle$, and at time t_2 it becomes $|\psi'\rangle$, then there exist a Unitary operator U, which depends only on t_1, t_2 such that:

$$|\psi'\rangle = U\,|\psi\rangle \tag{30}$$

Some unitary transformation we might consider are the Pauli matrices that we introduced before. For example X acts as a gate that flips the single qubit $a\,|0\rangle + b\,|1\rangle \xrightarrow{X} b\,|0\rangle + a\,|1\rangle$

System Evolution

Postulate 2 before deals only with a discrete step in time. It turns out we can refine this to deal with continuos time evolution, and doing so results in the famous Schrödinger equation.

Definition

Postulate 2': The evolution of a closed Quantum System is described by *Schrödinger equation*:

$$i\hbar \frac{\mathrm{d}\,|\psi\rangle}{\mathrm{d}t} = H\,|\psi\rangle \tag{31}$$

Where $\hbar$ is the reduced Planck Constant, and H is an Hermitian operator which needs to be figured out for the system in question.

Sometime it is useful that, if H is independent from time, and we know the state $|\psi_0\rangle$ at $t = 0$

$$|\psi(t)\rangle = \exp\left(\frac{-itH}{\hbar}\right)|\psi_0\rangle \tag{32}$$

Energy states

In particular, since H is Hermitian in 31, it has spectral decomposition:

$$H = \sum_{E} E \left| E \right\rangle \left\langle E \right| \tag{33}$$

where all the eigenvalues E are real[3]. The states $|E\rangle$ are known as the *energy eigenstates* (or sometimes stationary), and the E is the corresponding energy of the eigenstate. The lowest energy and the corresponding eigenstate are known as the *ground state energy* and the *ground state*.

[3] This is a property of Hermitian operator

System Evolution

Example

Consider $H = \hbar\omega Z$, for some $\omega > 0$. Then, using 20, $H = \hbar\omega(|+\rangle\langle+| - |-\rangle\langle-|)$ and as such the energy eigenstate are $|+\rangle, |-\rangle$, with energies respectively $\hbar\omega, -\hbar\omega$. So the ground state is $|-\rangle$, with energy $-\hbar\omega$. Also, if $|\psi_0\rangle = |0\rangle$, then using the solution before we have:

$$\begin{aligned} |\psi(t)\rangle &= \exp(-i\omega t Z)|0\rangle && (34)\\ &= (e^{-i\omega t}|+\rangle\langle+| + e^{i\omega t}|-\rangle\langle-|)|0\rangle && (35)\\ &= \frac{1}{\sqrt{2}}\left(e^{-i\omega t}|+\rangle + e^{i\omega t}|-\rangle\right) && (36)\end{aligned}$$

Measurement

Now, we aim to find a way to measure the state of a system.

Definition

Postulate 3: Quantum measurement is defined by a collection of operators M_m called *measurement operators*. In particular, given that the system is in state $|\psi\rangle$, the probability of obtaining result m is:

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle \tag{37}$$

And the state after that measurement m changes to:

$$|\psi'\rangle = \frac{M_m\,|\psi\rangle}{\sqrt{p(m)}} \tag{38}$$

It is important to also have that $\sum_m p(m) = 1$ for every $|\psi\rangle$. Equivalently, the operators need to satisfy $\sum_m M_m^\dagger M_m = I$

Measurement

Example

Let us consider the usual qubit system, and measurement operators:

$$M_0 = |0\rangle \langle 0| \tag{39}$$

$$M_1 = |1\rangle \langle 1| \tag{40}$$

It is easy to verify completeness is satisfied. Now, consider the general state $|\psi\rangle = a|0\rangle + b|1\rangle$. Then

$$p(0) = |a|^2 \text{ and } |\psi\rangle \to \frac{a}{|a|} |0\rangle \tag{41}$$

$$p(1) = |b|^2 \text{ and } |\psi\rangle \to \frac{b}{|b|} |1\rangle \tag{42}$$

Taking a concrete example: the state $|+\rangle$ when measured collapses to $|0\rangle$ precisely half of the times. Also note that measuring it with operators $M_\pm = |\pm\rangle \langle \pm|$ yields the result $|+\rangle$ with probability 1.

Measurement

An alternative way to describe measurement operators, is by using projective measurements. The operators are described by a single Hermitian operator, called an *observable*:

$$M = \sum_m mP_m \tag{43}$$

where P_m is the projector[4] onto the eigenspace of M with eigenvalue m. Using those, we have that, if we are on state $|\psi\rangle$:

$$p(m) = \langle\psi|P_m|\psi\rangle \tag{44}$$

$$|\psi'\rangle = \frac{P_m|\psi\rangle}{\sqrt{p(m)}} \tag{45}$$

These are especially useful since $\mathbb{E}(M) = \langle\psi|M|\psi\rangle$. We also write $\langle M\rangle \equiv \mathbb{E}(M)$, and $(\Delta(M))^2 = \mathrm{Var}(M) = \langle M^2\rangle - \langle M\rangle^2$

[4] An operator such that $P^2 = P$

Measurement

Example

Consider for example the observable Z as defined in 9. Then we know from 20 that:

$$Z = |0\rangle \langle 0| - |1\rangle \langle 1| \tag{46}$$

So measuring our usual single qubit state $|+\rangle$ yields $+1$ or -1 with probability $\frac{1}{2}$. In particular, the expected value and standard deviation of the observable are

$$\langle Z \rangle = \langle + | Z | + \rangle = \langle + | - \rangle = 0 \tag{47}$$

$$\Delta(Z) = \sqrt{\langle Z^2 \rangle - \langle Z \rangle} = \sqrt{\langle + | + \rangle} = 1 \tag{48}$$

Heisenberg uncertainty principle can be written in this language as:

$$\Delta(A)\Delta(B) \geq \frac{| \langle \psi | [A, B] | \psi \rangle |}{2} \tag{49}$$

Notes on Phase

Often you will hear the term of phase, and of two states being not distinguishable up to a global phase. What this means is that state $|\psi'\rangle = e^{i\theta}|\psi\rangle$ for some real θ. These are called undistinguishable as, for any measurement operator M_m we have that:

$$\begin{aligned} p_{\psi'}(m) &= \langle\psi'|M_m^\dagger M_m|\psi'\rangle && (50)\\ &= \langle\psi|e^{-i\theta}M_m^\dagger M_m e^{i\theta}|\psi\rangle && (51)\\ &= \langle\psi|M_m^\dagger M_m|\psi\rangle = p_\psi(m) && (52) \end{aligned}$$

Composition

Our final postulate, involves putting together Quantum Systems. It should come as no surprise that it involves the Tensor Product:

Definition

Postulate 4: The state space of a composite physical system is the tensor product of the state spaces of the individual systems. Furthermore, if there are n systems, and system i is in state $|\psi_i\rangle$, then the state of the composite system is:

$$\bigotimes_{i=1}^{n} |\psi_i\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle \tag{53}$$

Composition

Example

Consider two single qubit system, in states $|\psi_1\rangle = |+\rangle$, and $|\psi_2\rangle = |-\rangle$. Recall that each of the systems should have a probability $\frac{1}{2}$ to be measured as $0, 1$. So we expect that the tensor product of the two should obey the probability composition.

$$\begin{aligned} |\psi_1\rangle \otimes |\psi_2\rangle &= |+\rangle |-\rangle && (54) \\ &= \frac{1}{2} \left(|00\rangle + |01\rangle - |10\rangle - |11\rangle \right) && (55) \end{aligned}$$

Using the idea that measurement probability is the square of the amplitude [a] we see that each of the states can be measured with probability $\frac{1}{4}$ as expected.

[a] You can prove using measurement operator $M_\alpha = |\alpha\rangle \langle\alpha|$ for $\alpha \in \{0, 1\}^2$

Entanglement

One of the most important yet obscure term in quantum mechanics is the term entanglement. Consider two quantum systems, with states spaces V, W. Then the composite space is the space: $V \otimes W$. We say that the system is in an entangled state $|\beta\rangle$ if there are no $|\psi\rangle \in V$, $|\psi'\rangle \in W$ such that $|\beta\rangle = |\psi\rangle \otimes |\psi'\rangle$. Actually, it turns out most of the computational power in Quantum computing comes from entangled states. To see this, note that for a n Qubit system, non entangled states can be written as:

$$\bigotimes_{i=1}^{n}(a_i|0\rangle + b_i|1\rangle) = (a_1|0\rangle + b_1|1\rangle) \otimes \cdots \otimes (a_n|0\rangle + b_n|1\rangle) \tag{56}$$

And so they are described by n independent amplitudes. Instead a general state of the systems is of the form:

$$\sum_{\alpha \in \{0,1\}^n} a_\alpha |\alpha\rangle = a_1|00\ldots0\rangle + a_2|00\ldots1\rangle + \cdots + a_n|11\ldots1\rangle \tag{57}$$

Which has 2^n independent amplitudes.

Entanglement

Example

Consider a two qubit system. Then some simple algebra shows that the following are entangled.

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{58}$$

$$|\beta_{01}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \tag{59}$$

$$|\beta_{10}\rangle = \frac{|10\rangle + |01\rangle}{\sqrt{2}} \tag{60}$$

$$|\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{61}$$

In particular, these are called the Bell States, and form a basis for the two qubit space. Note how for $|\beta_{00}\rangle$ a 0-measurement in the first basis i.e. $|0\rangle\langle 0| \otimes I$ modifies the composite state to $|00\rangle$.

Model of Computation

In order to leverage Quantum for our computation, we aim to define a model of computation that can be used consistently with our postulates. In classical computing some common models are:

- Turing Machine
- Circuits
- Minsky Register
- Petri Nets

Definition

Complexity-Theoretic Church-Turing Thesis A probabilistic Turing machine can efficiently simulate any realistic model of computation.

Definition

Quantum Complexity-Theoretic Church-Turing Thesis A quantum Turing machine can efficiently simulate any realistic model of computation.

Reversible Quantum Circuit

The most common model for quantum computation is that of reversible circuits. It is motivated by the fact that the laws of Physics are time reversible, and that erasing information costs energy.

Definition

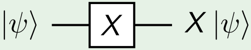
Landauer's Principle: Suppose a computer erases a single bit of information. The amount of energy dissipated in the environment is at least $k_B T \ln 2$ where T is the temperature of the environment, and k_B is Boltzmann's constant

Reversible Circuits

Reversible circuits are also a classical computation device. Each reversible gate is characterized by the fact that each input configuration uniquely corresponds to an output. For example, `NOT` is reversible as $0 \to 1$ and $1 \to 0$. Instead `AND` is not reversible, as 0 is the output of $00, 01, 10$. We will denote the `NOT` gate as X, as in 9.

Example

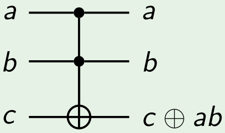
Here is an example of how the X gate operates. Since we are operating classically so far $|\psi\rangle$ are simply either of $|0\rangle, |1\rangle$, but we will see that for arbitrary $|\psi\rangle = a|0\rangle + b|1\rangle$ the quantum X applies the unitary matrix X as expected, resulting in $X|\psi\rangle = b|0\rangle + a|1\rangle$.



Friedkin Gate

Example

Here is an example of reversible gate, the Toffoli gate.

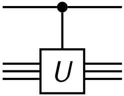


It is important as it is universal, as in every classical circuit can be simulated using this circuit [a]. In a nutshell, it use a, b as control bits, and if both are set then it flips the target bit c. It is also easy to see that the 8×8 matrix corresponding to the Toffoli is Unitary.

[a] Set $c = 1$, then the output of the gate is $\neg(ab)$. Since NAND is universal, the result follows

Controlled Operations

A really interesting kind of operation are the controlled operation. These are operations on multiple bit such that the first bit is used as a control. If it is not set nothing happens. Else some operation is applied. For any Unitary U we define the controlled-U operation as:



In matrix form, this corresponds to:

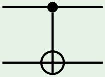
$$\begin{pmatrix} 1 & \dots & 0 \\ \vdots & \ddots & 0 \\ 0 & \dots & U \end{pmatrix} \tag{62}$$

So the matrix with 1's on half of the diagonal, zeros every else and U in the bottom quarter.

CNOT

Example

The CNOT gate is just a controlled-X operation, yet it is so important that we have an alternative notation for it.



In matrix form, it is represented by:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{63}$$

Note how Toffoli is just a CNOT with two control bits, and as such it is sometimes called CCNOT.

Quantum Gates

For now we have just used gates that are classical, in the sense that they transform "bits" $|0\rangle, |1\rangle$ into other bits of the same kind. Our aim would be to simulate arbitrary Unitary transformations. Turns out that CNOT, and single qubit Unitary operations are all we need to compute arbitrary Unitary operations. Furthermore, we can use the Hadamard, the phase, the $\pi/8$ [5] and the CNOT gates to compute any Unitary operation to an arbitrary accuracy.

[5] Next slide

Quantum Gates

Hadamard	$-\boxed{H}-$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$
Pauli-X	$-\boxed{X}-$	$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$
Pauli-Y	$-\boxed{Y}-$	$\begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}$
Pauli-Z	$-\boxed{Z}-$	$\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$
Phase	$-\boxed{S}-$	$\begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}$
$\pi/8$	$-\boxed{T}-$	$\begin{pmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{pmatrix}$

Quantum Speedups

We are interested in finding ways to solve some problems more easily then with classical methods. As we know, here we have some problems that we think are solvable more efficiently on quantum computers (with caveats).

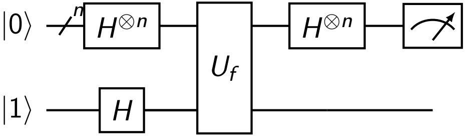
- Deutsch–Jozsa algorithm 2^{n-1} calls to 1
- Quantum Fourier Transform $O(n2^n) \to O(n^2)$
- Shor's algorithm $O(\exp(1.9(\log N)^{1/3})(\log \log N)^{2/3}) \to O((\log N)^3)$
- Grover's quantum search, $O(n) \to O(\sqrt{n})$
- Superdense coding, send 2 classical bits using only a single qubit
- Hidden subgroup problems

We show quantum circuits for the first two. Also, we stress that we have no efficient Quantum algorithm for $\mathcal{NP}$-complete problems. As such, we believe (no proof) that $\mathcal{P} \subseteq \mathcal{BPP} \subseteq \mathcal{BQP} \subseteq \mathcal{NP}$ [6]

[6] Actually, a recent paper (https://www.quantum-bits.org/?p=2309) seem to suggest that $\mathcal{BQP}/\mathcal{NP} \neq \emptyset$

Deutsch-Jozsa

Consider a function $f : \{0,1\}^n \to \{0,1\}$ that is either constant or balanced. By balanced we mean that $\sum_s f(s) = 2^{n-1}$. With how many calls can we determine which kind of function is f? The classical approach takes at most $2^{n-1}+1$ applications. In the quantum world, we show an algorithm that, given a black box U_f that can compute the Unitary $(x,y) \to (x, y \oplus f(x))$, can determine the kind of the function with a single call.



Deutsch-Jozsa

The original input state is $|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle$. This gets transformed to:

$$|\psi_1\rangle = \sum_{x\in\{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \tag{64}$$

And applying $U_f : |x, y\rangle \to |x, y \oplus f(x)\rangle$ gets us:

$$|\psi_2\rangle = \sum_x \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \tag{65}$$

Finally, evaluating the last Hadamard gates yields:

$$|\psi_3\rangle = \sum_z \sum_x \frac{(-1)^{x\cdot z + f(x)}|z\rangle}{2^n} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \tag{66}$$

Now, the amplitude of $|0\rangle^{\otimes n}$ is $\sum_x (-1)^{f(x)}/2^n$. So if f is constant it is ± 1. Otherwise it will be balanced and so equal 0.

Quantum Fourier Transform

The Discrete Fourier Transform is an operation that has many applications in a variety of problems. Classically[7], it transforms a set of numbers $x_0, \ldots, x_{N-1}$ into:

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi ijk/N} x_j \tag{67}$$

The Quantum Fourier Transform is a linear transformation that, for orthonormal basis $|0\rangle, \ldots, |N-1\rangle$, computes:

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N} |k\rangle \tag{68}$$

The connection with the classical is that:

$$\sum_{k=0}^{N-1} x_k |k\rangle \rightarrow \sum_{k=0}^{N-1} y_k |k\rangle \tag{69}$$

[7] Good visual intro https://www.youtube.com/watch?v=spUNpyF58BY

Quantum Fourier Transform

Let us set $N \equiv 2^n$. Then, the best classical algorithm to perform the Discrete Fourier Transform uses $\Theta(n2^n) = \Theta(N \log N)$ operations. In constrast, we can show a quantum algorithm that uses only $\Theta(n^2)$ gates to compute the Quantum Fourier Transform transformation. The algorithm uses the fact[8] that the transformation can be written as:

$$|j_1, \ldots, j_n\rangle \to \frac{(|0\rangle + e^{2\pi i 0.j_n}|1\rangle)\ldots(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle)}{2^{n/2}} \qquad (70)$$

Where $0.j_l \ldots j_m \equiv \sum_{i=l}^{m} \frac{j_i}{2^i}$.
A note is in order: while we have a fast algorithm for the Quantum Fourier Transform, this does not give us a fast algorithm for the Discrete version. In order to achieve this speedup we need to incorporate the QFT as a routine, which is what Shor's algorithm does in its order finding routine.

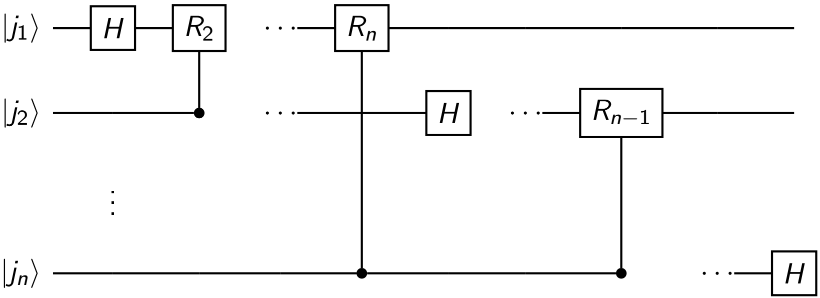
[8] Which is supposed to be elementary smh

Quantum Fourier Transform

Let

$$R_k \equiv \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix} \tag{71}$$

The following circuit computes QFT.



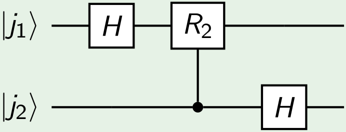
QFT

Example

In the case $N = 4 = 2^2$, we get that $F\,|j\rangle = \frac{1}{2}\sum_{i=0}^{3} e^{\pi ijk/2}\,|k\rangle$
Alternatively:

$$|j_1, j_2\rangle \to \frac{(|0\rangle + e^{\pi i j_2}\,|1\rangle)(|0\rangle + e^{\pi i(j_1 + j_2/2)}\,|1\rangle)}{2} \tag{72}$$

The corresponding circuit is:



$\frac{1}{\sqrt{2}}(|0\rangle + e^{\pi i(j_1 + j_2/2)}\,|1\rangle)$

$\frac{1}{\sqrt{2}}(|0\rangle + e^{\pi i j_2}\,|1\rangle)$

And swapping the last two completes the operation.

What's next

We don't really know!

- Physical realization
- Noise
- Quantum information
- Quantum cryptography
- Graph isomorphism?[9]

[9] Might be solved, paper is 2019 but not published yet afaik https://arxiv.org/abs/1901.06530

Learning

- Linear Algebra:
  - 3Blue1Brown, Essence of Linear Algebra
  - Linear Algebra Done Right. Sheldon Axler
  - Linear Algebra and Its Applications, David C. Lay
- Physics:
  - The Feynman Lectures on Physics
  - Minute Physics I guess?
- Quantum Computing:
  - Quantum Computation and Quantum Information, Isaac Chuang and Michael Nielsen
  - Brilliant
  - Q# Quantum Programming Language