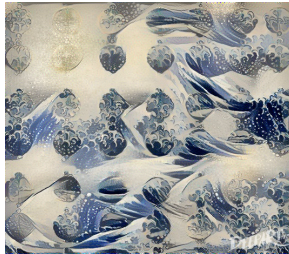


Introduction to Quantum Computing

Ugo Jardonnet



December 2017



Table of Contents

1 A Simple Experiment

2 Mathematical Framework

- Hilbert space and Dirac notation
- Operators in \mathcal{H}

3 Quantum Algorithm

- Shor's algorithm
- Groover's algorithm



Outline

1 A Simple Experiment

2 Mathematical Framework

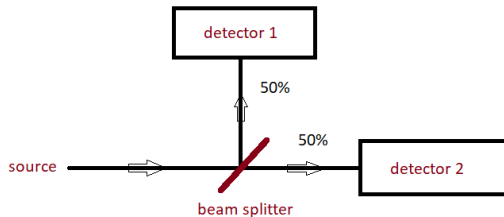
- Hilbert space and Dirac notation
- Operators in \mathcal{H}

3 Quantum Algorithm

- Shor's algorithm
- Groover's algorithm



A Simple Experiment

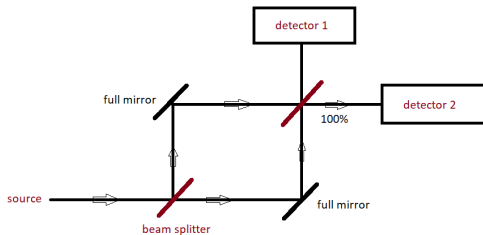


Suppose we have an experimental set-up consisting of a photon source, a beam splitter (half silvered mirror) and a pair of photon detectors. We observe that photons hit each detector 50% of the time.

The simplest explanation here is that the beam splitter has a 50% chance to transmit or reflect each photon.



A Simple Experiment



We modify the experiment by adding a second beam splitter and two fully reflecting mirrors. In this modified set-up the result is non-intuitive. The photons do not hit each detector with a 50% chance.

The photons arrive at the same detector, detector 2, 100% of the time.



A Simple Experiment

The mathematical framework of quantum physics models the experiment in a way that correctly predicts the observed outcomes.

The beam splitter can be model by the following operator: $\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}$

At each step, photons can be in 2 possible paths noted $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

- ① At the beginning of the experiment we know from which side photons are hitting the first beam splitter. Meaning the state of the system is known to be path 1 = $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

- ② After the first beam splitter we get: $\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{i}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

We will see later that this mean a $(\frac{1}{\sqrt{2}})^2 = (\frac{i}{\sqrt{2}})^2 = \frac{1}{2}$ probability for each outgoing path.

- ③ After the second beam splitter we get: $\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, meaning a 100% probability of observing photons in path 2.



A Simple Experiment [1]

- Photons are modeled as taking a superposition of both paths and physical "gates" as operators modifying the probabilities of measuring photons in each of their possible states.
- Quantum physics can model experiment that cannot be described by classical physics.
- The exponential processing power needed to model some complex quantum system led to the idea of quantum computing.



Outline

1 A Simple Experiment

2 Mathematical Framework

- Hilbert space and Dirac notation
- Operators in \mathcal{H}

3 Quantum Algorithm

- Shor's algorithm
- Groover's algorithm



Hilbert space and Dirac Notation

The state of a n -qbit system is described by a 2^n -dimensional vector in a finite dimensional complex vector space, referred as a Hilbert space \mathcal{H} .

Vectors from \mathcal{H} basis are called state vectors. They represent the possible states in which qbits can collapse when measured.

Dirac Notation

- Vectors in \mathcal{H} are written inside a 'ket' as follow $|v\rangle$
- The 2^n basis vectors of \mathcal{H} are labeled by their binary index: $|00\rangle, |01\rangle, \dots$



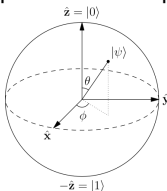
Dirac Notation

Single-qubit System Example

Each possible state of a single-qubit system can be written as a vector $\vec{\phi} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}$, with α_1, α_2 complex.

Following Dirac notation we get: $|\phi\rangle = \alpha_1|0\rangle + \alpha_2|1\rangle$

The pure state space of a qubit can be represented by a bloch sphere.



Dirac Notation

4-qbit System Example - \mathcal{H} of dimension 4

$$\begin{aligned} \begin{vmatrix} 0 \\ 1 \\ 0 \\ 0 \end{vmatrix} &\equiv 2^{nd} \text{ basis vector} \\ &\equiv 0b01^{th} \text{ basis vector, binary 0-indexed} \\ &\equiv |01\rangle \text{ in Dirac notation} \end{aligned}$$

the 4 basis vectors are therefore $B = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Any vectors in \mathcal{H} can then be written as a combination of vectors in B .



Dirac Notation

The following Dirac notation and column vector are equivalent:

$$\sqrt{\frac{2}{3}}|001\rangle + \frac{i}{\sqrt{(3)}}|111\rangle \iff \begin{pmatrix} 0 \\ \sqrt{\frac{2}{3}} \\ 0 \\ \vdots \\ 0 \\ \frac{i}{\sqrt{(3)}} \end{pmatrix} \quad (1)$$

As you can see, this notation saves space when the dimension is high and the vectors are sparse.



Dual vector and inner product

Dual vector

$\langle x|$ - x written inside a 'bracket'

A dual vector is obtained by taking the corresponding row matrix of x and then the complex conjugate of every element (Hermitean conjugate).

This allows writing the **inner product** as $\langle x|y\rangle$:

$$\langle x||y\rangle \equiv \langle x|y\rangle = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = (x_1^* x_2^*) \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \sum_i^2 x_i^* y_i$$

where $c^* = a - bi$ for $c = a + bi$



Tensor product

Tensor product

$|x\rangle \otimes |y\rangle$ also written $|x\rangle|y\rangle$ or $|xy\rangle$

Stitch result matrices of multiplying each element x_i in x by y :

$$|xy\rangle = |x\rangle \otimes |y\rangle = \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \otimes \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} = \begin{pmatrix} x_0 y_0 \\ x_0 y_1 \\ x_1 y_0 \\ x_1 y_1 \end{pmatrix}$$

Example:

$$\sqrt{\frac{2}{3}}|01\rangle + \frac{i}{\sqrt{(3)}}|11\rangle \iff \sqrt{\frac{2}{3}}|0\rangle \otimes |1\rangle + \frac{i}{\sqrt{(3)}}|1\rangle \otimes |1\rangle$$



Outer product and Quantum entanglement

Outer product:

$$|x\rangle\langle y|$$

.

Produces an operator that acts as

$$(|x\rangle\langle y|)|z\rangle = |x\rangle(\langle y|z\rangle) = (\langle y|z\rangle)|x\rangle$$

A key point of quantum computing is that n -qbits systems can be described by the tensor product of n vector spaces \mathcal{V} (\mathcal{H} of dimension 1) i.e. $\mathcal{H}^n = \{v_1 \otimes \dots \otimes v_n, \forall v_i \in \mathcal{V}, \forall i \in n\}$

quantum Entanglement

The quantum state of each particle cannot be described independently of the others.



Measurement

Measurement Principle

A measurement results in the system being in the eigenstate corresponding to the eigenvalue result of the measurement

The measurement principle is an axiom of quantum physics, you cannot prove it is true. It just seems to match what is happening. $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. The measurement process alters the state of the qubit: the effect of the measurement is that the new state is exactly the outcome of the measurement.



Outline

1 A Simple Experiment

2 Mathematical Framework

- Hilbert space and Dirac notation
- Operators in \mathcal{H}

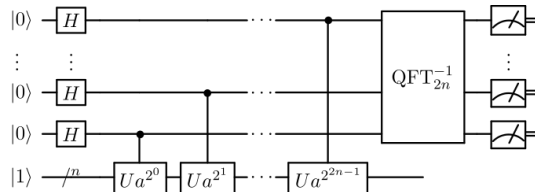
3 Quantum Algorithm

- Shor's algorithm
- Groover's algorithm



Shor's Algorithm

Quantum algorithm for integer factorization formulated by Peter Shor in 1994.

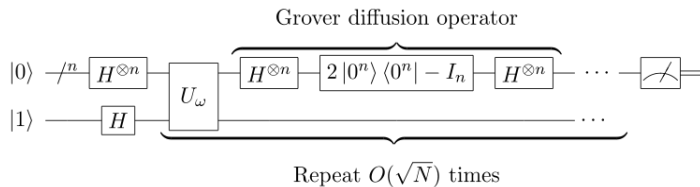


The first part of the algorithm turns the factoring problem into the problem of finding the period of a function, and may be implemented classically. The second part finds the period using the quantum Fourier transform, and is responsible for the quantum speedup.



Groover's Algorithm

Search algorithm in sub-linear time.



Bibliography I



KP Zetie, SF Adams, and RM Tocknell. *How does a Mach-Zehnder interferometer work?*

https://www.cs.princeton.edu/courses/archive/fall06/cos576/papers/zetie_et_al_mach_zehnder00.pdf. Jan. 2000.

