How the Schrödinger's cat found a needle in a haystack

Riccardo Adami
Dipartimento di Scienze Matematiche
Politecnico di Torino

Torino, March 21 2013

Dirac's notation

$|0\rangle$ means "the photon" passed through the slit $F0$.

$|1\rangle$ means "the photon" passed through the slit $F1$.

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

means "the photon underwent an experiment where both slits were open".

N.B.: A measurement of a photon in the last state, gives as a result a photon in the "state" $|0\rangle$ with probability 0.5 or in the state $|1\rangle$ with probability 0.5.

Partially closing a slit

Putting an absorber (e.g. a polaroid) on the slit 0, the likelihood of finding the photon in the state $|0\rangle$ is lowered and that of finding the photon in the state $|1\rangle$ is enhanced.

Then, the state of a photon that underwent such an experiment can be represented by

$$a|0\rangle + b|1\rangle$$

with a, b chosen in such a way that $a^2 + b^2 = 1, |a| < |b|$, and the probability of finding the photon in $|0\rangle$ equals a^2.

Changing the optical path

Putting a “dephaser” on the slit 0, the probability of passing through either slit is 0.5, but the interference pattern is shifted. Using the complex representation of the electromagnetic field, it turns out that a good representation of the state of the photon is the following

$$\frac{1}{\sqrt{2}}\left(e^{i\varphi}|0\rangle + |1\rangle\right)$$

Changing the optical path

Putting a "dephaser" on the slit 0, the probability of passing through either slit is 0.5, but the interference pattern is shifted. Using the complex representation of the electromagnetic field, it turns out that a good representation of the state of the photon is the following

$$\frac{1}{\sqrt{2}}\left(e^{i\varphi}|0\rangle + |1\rangle\right)$$

In such a way we allowed complex linear combinations of the symbols $|0\rangle$ and $|1\rangle$, that can be then thought of as elements of a linear space.

Changing the optical path

Putting a "dephaser" on the slit 0, the probability of passing through either slit is 0.5, but the interference pattern is shifted. Using the complex representation of the electromagnetic field, it turns out that a good representation of the state of the photon is the following

$$\frac{1}{\sqrt{2}}\left(e^{i\varphi}|0\rangle + |1\rangle\right)$$

In such a way we allowed complex linear combinations of the symbols $|0\rangle$ and $|1\rangle$, that can be then thought of as elements of a linear space.
Furthermore, we can introduce a scalar (hermitian) product s.t.

$$\langle 0|0\rangle = \langle 1|1\rangle = 1, \qquad \langle 0|1\rangle = 0$$

Axioms

Superposition principle: The states of a photon in a two-slit experiment can be represented by the normalized elements of a two-dimensional complex metric linear space, i.e.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

with $\alpha, \beta \in \mathbb{C}$ s.t. $|\alpha|^2 + |\beta|^2 = 1$.

Von Neumann's Measurement Axiom: If one tries to determine from which slit the photon has passed, then one finds the slit 0 with probability

$$|\langle 0|\psi\rangle|^2 \;=\; |\alpha|^2$$

and 1 with probability

$$|\langle 1|\psi\rangle|^2 \;=\; |\beta|^2$$

The Qubit

A quantum system with a two-dimensional "state space" is called a qubit, and can be considered as the quantum version of the classical bit.

Important:

1. A qubit can experience states that are not $|0\rangle$ nor $|1\rangle$, but rather "simultaneously" $|0\rangle$ and $|1\rangle$. They are called superposition states or Schrödinger's cat states.
2. However, a measurement always makes the state collapse on either $|0\rangle$ or $|1\rangle$.

Two qubits

The space of the states of two qubits is the tensor product of two state spaces of the single qubit. Namely,

$$\begin{aligned} & (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha'|0\rangle + \beta'|1\rangle) \\ = \;& \alpha\alpha'|0\rangle|0\rangle + \alpha\beta'|0\rangle|1\rangle + \alpha'\beta|1\rangle|0\rangle + \beta\beta'|1\rangle|1\rangle \\ = \;& \alpha\alpha'|00\rangle + \alpha\beta'|01\rangle + \alpha'\beta|10\rangle + \beta\beta'|11\rangle \end{aligned}$$

But other states are allowed, e.g.

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

or

$$\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

These states cannot be factorized.

n qubits

The space of the states of two qubits is the n.th tensor power of two state spaces of the single qubit. Namely,

$$\bigotimes_{j=1}^{n}(\alpha_j|0\rangle_j+\beta_j|1\rangle_j)=\alpha_1\ldots\alpha_n|0\rangle_1\ldots|0\rangle_n+\ldots$$
$$+\alpha_1\ldots\beta_{n-1}\alpha_n|0\rangle_1\ldots|0\rangle_{n-1}|1\rangle_n+\cdots+\beta_1\ldots\beta_n|1\rangle_1\ldots|1\rangle_n$$

$$\begin{aligned} = \quad & \alpha_1\ldots\alpha_n|0\ldots0\rangle+\alpha_1\ldots\beta_{n-1}\alpha_n|0\ldots01\rangle+\ldots \\ & +\beta_1\ldots\beta_n|1\ldots1\rangle \end{aligned}$$

$$\begin{aligned} = \quad & \alpha_1\ldots\alpha_n|0\rangle+\alpha_1\ldots\beta_{n-1}\alpha_n|1\rangle+\ldots \\ & ++\beta_1\ldots\beta_n|2^n-1\rangle \end{aligned}$$

$$\frac{1}{\sqrt{2}}(|0\ldots0\rangle+|1\ldots1\rangle)$$

cannot be factorized.

A needle in a haystack

We are given an unsorted list of items. We need one of them, but we don't have any reasonable method to sort it out from the bad ones, but to *try* all of them, until we don't get it.

Examples:
- A *name* in the telephone book.
- A forgotten password.
- A divisor of a given number...

The best classical algorithm known is to try all items. The mean value of attempts we have to perform is $N/2$.
A quantum computer can find the desired item in $\mathcal{O}(\sqrt{N})$ attempts.

Testing (oracles)

All the problems in the examples share a feature: it is *difficult* to *find* the solution, but it is *easy* to verify whether a given candidate is the solution or not.
Mathematically, one
-first labels any item in the list by a natural number in $\{0, \ldots N-1\}$. Call ω the label of the solution.
- then evaluates the function

$$\begin{aligned} f_\omega : \{0, \ldots N-1\} &\rightarrow \{0,1\} \\ f_\omega(x) = 1 & \quad \text{if} \ \ x = \omega \\ f_\omega(x) = 0 & \quad \text{otherwise} \end{aligned}$$

The problem is solved when the output in one. The length of the precedure is the number of times you evaluate f_ω.

Schrödinger's cats run faster

Classically, the average number of tests ($=$ evaluations of f) required to find the solution is $N/2$.

Using qubit in Schrödinger's cat-like states, the number of tests required is $\mathcal{O}(\sqrt{N})$.

(Quantum speed-up algrithms, Deutsch 85, Shor 93, Grover 96)

Step 1

Suppose the list is made of $N = 2^n$ items.

Measure a huge number of qubits. Sometimes you will obtain 0, sometimes 1. Keep n qubits in the state $|0\rangle$. You are then left with

$$|000\ldots0000\rangle \;=:\; |\mathbf{0}\rangle$$

Now one has to process the n-qubit system. It is useful to introduce a third axiom:
Any unitary transformation can be performed on the system.

Step 2

On a single qubit it possible to apply the Hadamard transformation

$$\begin{aligned} H|0\rangle &= 1/\sqrt{2}(|0\rangle + |1\rangle) \\ H|1\rangle &= 1/\sqrt{2}(|0\rangle - |1\rangle) \end{aligned}$$

so that

$$H|0\rangle H|0\rangle \ldots H|0\rangle = \frac{1}{\sqrt{N}} \sum_{j_i=0}^{1} |j_1\rangle \ldots |j_n\rangle$$

Or, in shorthand notation

$$H^{\otimes n}|0\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |j\rangle$$

I will denote this state by

$$|s\rangle$$

Steps 3 - $\mathcal{O}(\sqrt{N})$: Grover's operator

Define the operator (on the n-qubit space)

$$G := H^{\otimes n} R H^{\otimes n} O$$

where $H^{\otimes n}$ is the Hadamard operator acting on n qubits, and

$$R = 2P_0 - \mathbb{I} = 2|0\rangle\langle 0| - \mathbb{I}$$

So

$$\begin{aligned}
H^{\otimes n} R H^{\otimes n} &= H^{\otimes n}\left(2|0\rangle\langle 0| - \mathbb{I}\right) H^{\otimes n} \\
&= 2H^{\otimes n}|0\rangle\langle 0|H^{\otimes n} - H^{\otimes n}H^{\otimes n} \\
&= 2|s\rangle\langle s| - (H^2)^{\otimes n} \\
&= 2|s\rangle\langle s| - \mathbb{I}
\end{aligned}$$

The operator O: testing

Add a $n+1^{\text{st}}$ qubit, $|q\rangle$ and implement the following unitary operator that acts on $n+1$ qubits as follows:

$$|x\rangle|q\rangle \to |x\rangle|q + f_\omega(x) \ mod \ 2\rangle$$

If the additional qubit is prepared in the state

$$|q\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle),$$

then

$$\begin{aligned} |q + f_\omega(x)\rangle &= |q\rangle \qquad \text{if } f_\omega(x) = 0 \\ |q + f_\omega(x)\rangle &= -|q\rangle \qquad \text{if } f_\omega(x) = 1 \end{aligned}$$

so

$$|x\rangle|q\rangle \to (-1)^{f_\omega(x)}|x\rangle|q\rangle$$

Now forget about the additional qubit
Called $|\omega\rangle$ the state to be found, with the aid of the additional qubit we implement the following operator O:

$$\begin{aligned} O|j\rangle &= |j\rangle, \qquad j \neq \omega \\ O|\omega\rangle &= -|\omega\rangle \end{aligned}$$

Therefore

$$O|s\rangle = \frac{1}{\sqrt{N}} \sum_{j\neq\omega, j=0}^{N-1} (|j\rangle - |\omega\rangle) = |s\rangle - \frac{2}{\sqrt{N}}|\omega\rangle$$

As an operator,

$$O = \mathbb{I} - 2P_\omega = \mathbb{I} - 2|\omega\rangle\langle\omega|$$

N.B.: whenever we apply the operator O we are testing the function f.

$$
\begin{aligned}
G &= (2|s\rangle\langle s| - \mathbb{I})\,(\mathbb{I} - 2|\omega\rangle\langle\omega|) \\
&= 2|s\rangle\langle s| - 4|s\rangle\langle s|\omega\rangle\langle\omega| + 2|\omega\rangle\langle\omega| - \mathbb{I} \\
&= 2|s\rangle\langle s| - \frac{4}{\sqrt{N}}|s\rangle\langle\omega| + 2|\omega\rangle\langle\omega| - \mathbb{I}
\end{aligned}
$$

Let us define

$$|s'\rangle := |s\rangle - \frac{1}{\sqrt{N}}|\omega\rangle$$

so that

$$\langle\omega|s'\rangle = \langle\omega|s\rangle - \frac{1}{\sqrt{N}} = 0$$

Then, rewriting the operator G by using $|s'\rangle$ instead of $|s\rangle$

$$G = 2|s'\rangle\langle s'| + \left(2 - \frac{2}{N}\right)|\omega\rangle\langle\omega| - \frac{2}{\sqrt{N}}|s'\rangle\langle\omega| + \frac{2}{\sqrt{N}}|\omega\rangle\langle s'| - \mathbb{I}$$

Notice that $|s'\rangle$ is not normalized. Indeed

$$|s'\rangle = |s\rangle - \frac{1}{\sqrt{N}}|\omega\rangle = \frac{1}{\sqrt{N}}\sum_{j=0,j\neq\omega}^{N-1}|j\rangle$$

so

$$\langle s'|s'\rangle = \frac{N-1}{N}$$

thus we define the normalized vector

$$|s''\rangle = \sqrt{\frac{N-1}{N}}|s'\rangle$$

G in the orthonormal basis $|s''\rangle, |\omega\rangle$

$$
\begin{aligned}
G \;=\;& \left(1-\frac{2}{N}\right)|s''\rangle\langle s''| + \left(1-\frac{2}{N}\right)|\omega\rangle\langle\omega| + \frac{2}{N}\sqrt{N-1}|\omega\rangle\langle s''| \\
& -\frac{2}{N}\sqrt{N-1}|s''\rangle\langle\omega| - P_\perp
\end{aligned}
$$

where $P_\perp$ is the orthogonal projection on

$$
Span\left(|s''\rangle, |\omega\rangle\right)
$$

Notice that the interesting dynamics of G is in the two-dimensional space spanned by $|s''\rangle$ and $|\omega\rangle$.

Geometrical interpretation of G

Restrict to $\mathrm{Span}(|s''\rangle, |\omega\rangle)$. In the given basis, the operator G is represented by the matrix

$$G \mapsto \begin{pmatrix} 1-\frac{2}{N} & \frac{2}{N}\sqrt{N-1} \\ -\frac{2}{N}\sqrt{N-1} & 1-\frac{2}{N} \end{pmatrix}$$

Since

$$\left(1-\frac{2}{N}\right)^2 + \frac{4}{N^2}N - 1 = 1 - \frac{4}{N} + \frac{4}{N^2} + \frac{4}{N} - \frac{4}{N}^2 = 1$$

one can define $\theta \in [0, 2\pi)$ s.t.

$$\cos\theta = 1 - \frac{2}{N}, \qquad \sin\theta = \frac{2}{N}\sqrt{N-1}$$

so that

$$G \mapsto \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$$

is a rotation in the plane.

The end

At each iteration of G the vector state is rotated by

$$\theta = \arcsin\left(\frac{2}{N}\sqrt{N-1}\right) \sim \frac{2}{\sqrt{N}}$$

The angle to be covered is

$$\Theta = \arccos\frac{1}{\sqrt{N}} \sim \frac{\pi}{2} - \frac{1}{\sqrt{N}} \sim \frac{\pi}{2}$$

After

$$\frac{\pi}{4}\sqrt{N}$$

iteration, a measurement gives $|\omega\rangle$ with probability

$$\geq 1 - \frac{4}{N}$$

In the case $n = 2, N = 4$ one has $\theta = \arcsin \frac{\sqrt{3}}{2} = \frac{\pi}{3}$, while the angle between $|s''\rangle$ and $s\rangle$ equals $\frac{\pi}{6}$.

In order to get $|\omega\rangle$ one must evaluate f just once.

References

On Grover's algorithm and quantum information:

1. L. Grover, "Quantum Mechanics Helps in Searching for a Needle in a Haystack", Phys. Rev. Lett. 79, 325–328 (1997)
2. J. Preskill's on-line course on Qunatum Information http://www.theory.caltech.edu/people/preskill/ph229/
3. M. Nielsen, I. Chuang, "Quantum Computation and Qunatum Information", Cambirdge University Press, 2000.
4. Wikipedia page on Grover's algorithm

On the basics of quantum mechanics:

1. L. Picasso, "Lezioni di Meccanica Quantistica", ETS Pisa, 2000.
2. R. Feynman, "Lectures on Physics" vol. 3 (available in Italian too, ed. Zanichelli).

Videos

1. The celebrated lecture by R. Feynman on the two-slit experiment: http://www.youtube.com/watch?v=hUJfjRoxCbk (with the famous statement "Nobody understands quantum mechanics" (8'04)).
2. A nice animation on two-slit experiment http://www.youtube.com/watch?v=DfPeprQ7oGc
3. A still nicer one: video "Double Slit Experiment - The Strangeness Of Quantum Mechanics" on YouTube.