> I think I can safely say that nobody understands quantum mechanics.
>
> Richard Feynman

SCIENCE LECTURE I & II: UNDESTANDING QUANTUM PHYSICS AND INTRODUCTION TO QUANTUM COMPUTERS.

I.- The Key to Understanding Quantum Physics

1.- The Classical Physics Reality

2.- The Quantum Reality

3.- Probabilistic Nature of the Quantum World

4.- Quantum Dynamics: the Schrödinger Equation

5.- A Historical Test: The Structure of the Atom

6.- Critique to the Concept of "Particle."

II.- The Physics of Atom-size Bits: Quantum Computers

1.- The Classical Physics Reality.

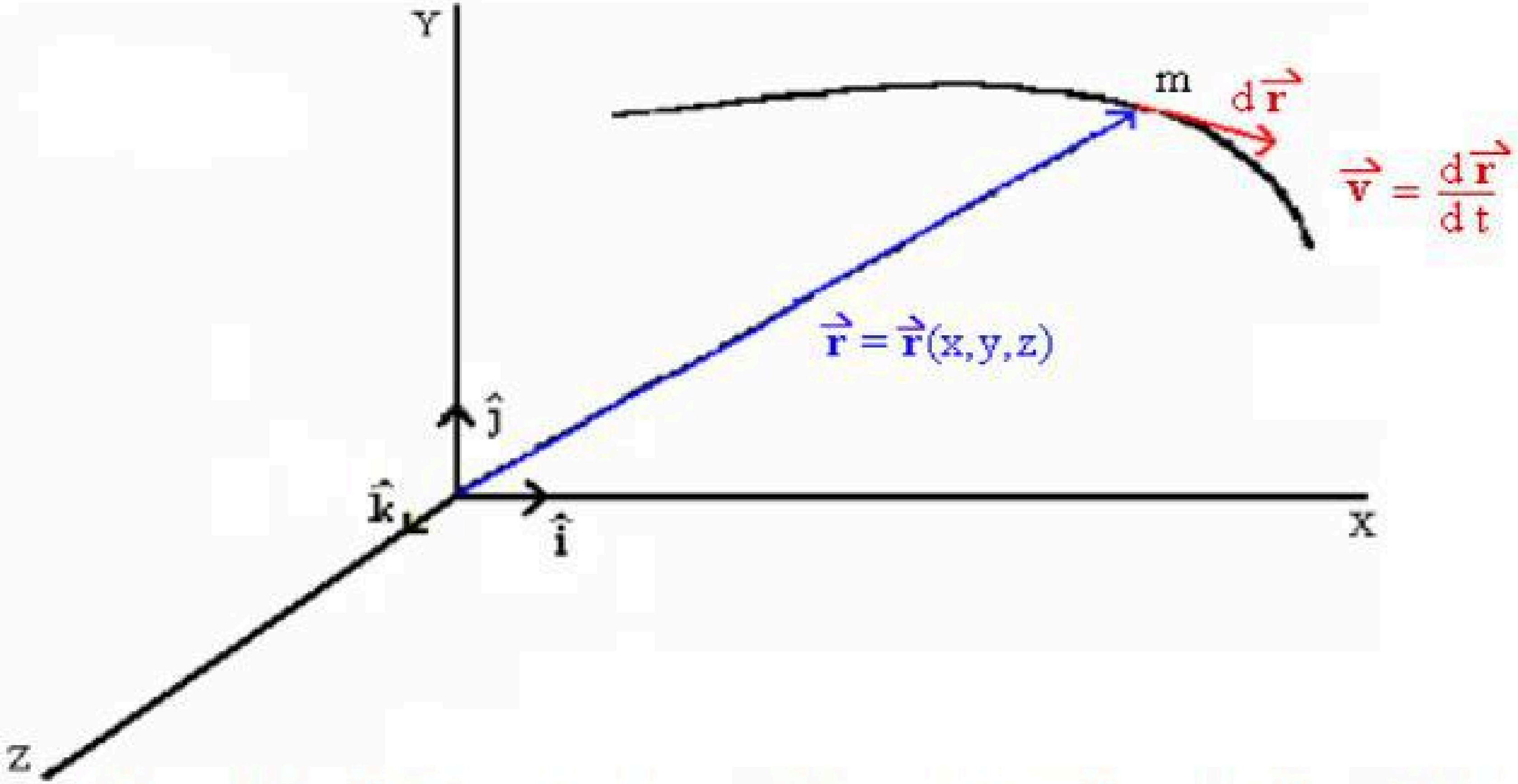
We will start with a quick review of classical physics. An important concept of the classical description of reality is that of a “particle.”

A “particle” is a mathematical abstraction or model that under certain circumstances can be used to represent real physical objects (like planets, bullets, cars, etc,) and their motion.

In the classical description, at all times along its motion, a particle of mass “m” has associated to it a precise position and velocity vectors

$$\mathbf{r} = \mathbf{r}(x,y,z) \qquad \mathbf{v} = \frac{d\,\mathbf{r}}{d\,t}$$

as shown in the diagram on next slide.



We also define some useful magnitudes such as linear momentum $\mathbf{P} = m\,\mathbf{v}$, Kinetic energy $K = \frac{1}{2}\,m\,\mathbf{v}^2$, angular momentum as the cross vector product $\mathbf{L} = \mathbf{r} \times \mathbf{P}$, Total Energy $E = K + U_{\text{potential}}(x,y,z)$, etc.

We also identify the diverse forces $\mathbf{F}_n$ (with n = 0,1…,) that may be acting upon the particle.

The effect of all these forces $\mathbf{F}_n$, is to change the momentum of the particle according to Newton's law:

$$\sum \mathbf{F}_n = \frac{d\,\mathbf{P}}{d\,t}$$

Some of these forces may be described through potential energy functions $U_k(x,y,z)$ as

$$\mathbf{F}_k = -\left(\frac{\partial U_k}{\partial x}\hat{\mathbf{i}} + \frac{\partial U_k}{\partial y}\hat{\mathbf{j}} + \frac{\partial U_k}{\partial z}\hat{\mathbf{k}} \right)$$

.- Some of the assumptions of Classical Physics:

1.- All these magnitudes exist and can be measured simultaneously.

2.- We can achieve any degree of accuracy that any conceivable measuring device can provide.

3.-The measuring process itself does not alter necessarily the magnitudes being measured.

4.- All these magnitudes exist regardless whether they are ever measured or not.

But surprise…!!!...

All these “common sense” assumptions are not valid in the quantum world.

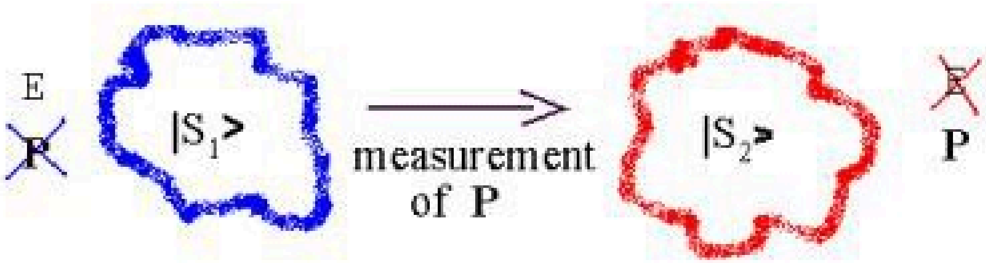
The Quantum Reality

At the atomic level we still describe a quantum physical system using many of the magnitudes used at the classical level: total energy E, linear momentum **P**, angular momentum **L,** etc.

However, there are restriction principles that make impossible the measuring (actually, the very existence!) of all of them at the same time.

For example:

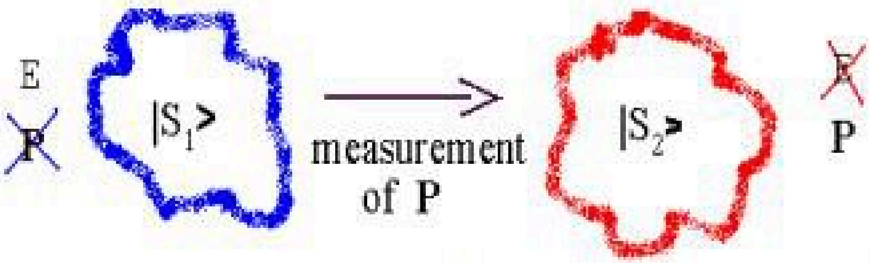
At some moment a quantum object may be in certain state, $|S_1>$. In such state the quantum object may have a definite value of total energy E, but not of momentum **P**.



If we want to determine the value of **P** we have to perform a suitable measurement experiment on the object, but… …the same act of measuring and obtaining a value for **P** takes the system to another state $|S_2>$, in which **P** does have a value, but E does not.

The philosophical impact of this subtle idea is tremendous!!!

What we are saying is that while in state $|S_1>$, the quantum object manifests its existence in the universe by its total energy E (and perhaps some other magnitudes that are compatible with E in state $|S_1>$) but it does not have a value for **P** whatsoever.



If the object's state is changed to $|S_2>$, now its presence in the universe manifests by a definite momentum **P**, but in this state the quantum object has no value for energy. It is not that its energy is zero: it just does not posses a value (nor the concept) of energy at all!

The most famous restriction in quantum physics is the Uncertainty Principle of Heisenberg:

"One cannot simultaneously know both the position **r** = (x,y,z) and the momentum **P** = (p_x, p_y, p_z) of a given object to arbitrary precision."

In this context, the word "uncertainty" must be understood as meaning "unknowability" or "nonexistence."

In more mathematical terms, using the symbol Δ to denote "unknowability", Heinsenberg's principle is stated as:

$$\Delta p_x \Delta x > 2 \pi \hbar \qquad \Delta p_y \Delta y > 2 \pi \hbar$$

$$\Delta p_z \Delta z > 2 \pi \hbar \qquad \Delta E \Delta t > 2 \pi \hbar$$

where ħ, the Planck constant, is a very small number:

$$\hbar = 1.0545 \times 10^{-34} \text{ Joules secs.}$$

Example:

Let's examine Heisenberg's principle more carefully using a concrete example: let's consider a single electron in space.

In one state, let's call it |**r**>, the electron has a definite position **r** $(\Delta x, \Delta y, \Delta z \sim 0,)$ but in such state, according to Heisenberg, it does not have a value for momentum because $(\Delta p_x, \Delta p_y, \Delta p_z \sim \infty.)$

If we measure its momentum, we are forcing the electron to change to another state, let's say |**P**>, in which it has a definite value for **P** $(\Delta p_x, \Delta p_y, \Delta p_z \sim 0,)$ but now it does not have a definite position **r** $(\Delta x, \Delta y, \Delta z \sim \infty.)$

In other words, while in $|\mathbf{P}\rangle$ the electron does exist as a momentum in the universe, but it has no position.

This is, it is nowhere!*

The intellectual acceptance of this fact, that an object can exist without been anywhere, constitutes the golden key to the full understanding of quantum mechanics and explain all its apparent paradoxes.

*See appendix A for further elaboration on this.

.- Probabilistic nature of the quantum world.

This conception of the electron being “nowhere” leads logically to the conclusion of the probabilistic nature of the quantum world, as follows.

By forcing the electron to go from one state to another, we are actually forcing the electron to adopt a value for a magnitude that did not exist before… consequently…

… the only way that such value can be adopted, that is consistent with the fact that such magnitude indeed did not exist before, is by adopting its value in a probabilistic way.

In other words, while in state |**P**> the electron does not have position, but it does present a probability distribution function $\mathit{Probability}(x,y,z,t)$ which in general will make some positions more probable to be adopted than others (if a measurement of it is performed.) (More on this in appendix B.)

This $\mathit{Probability}(x,y,z,t)$ function is very closely related to the most central element of the quantum theory, the so-called State Function, usually denoted as $\Psi(x,y,z,t)$:

$$\mathit{Probability}(x,y,z,t) = \Psi^*(x,y,z,t)\,\Psi(x,y,z,t)$$

The state function $\Psi(x,y,z,t)$ is a complex function, and it contains every thing that can be known of a quantum object.

.- Quantum dynamics: the Schrödinger equation.

The natural law that governs the evolution in time of the state function $\Psi(x,y,z,t)$ of a single quantum object of mass "m" (disregarding its inner structure, if any,) is described by the Schrödinger equation, which involves state function $\Psi(x,y,z,t)$:

$$i\,\hbar\frac{\partial\Psi(x,y,z,t)}{\partial t} = -\frac{\hbar^2}{2m}\nabla^2\,\Psi(x,y,z,t) + U(x,y,z,t)\Psi(x,y,z,t)$$

where $i = \sqrt{-1}$ and the symbol ∇^2 stands for the second partial derivative operator:

$$\nabla^2 \equiv \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2}$$

An important quality of this intimidating equation is that it is a wave equation. In other words, at the microscopy level, physical systems exhibit wave-like behaviors.

This equation does not describe abrupt changes, like the ones that occur in most measurements: these are completely probabilistic unpredictable irreversible processes. Schrödinger's equation only describes smooth changes of the state function.

Since it is certain that the quantum object described by $\Psi(x,y,z,t)$ must be found "somewhere" if we measured its position, then at all times we must have that

$$\int_{\substack{\text{all}\\\text{space}}} \mathit{Probability}(x,y,z,t)\ dx\,dy\,dz = 1$$

because total probability = 1 means "certainty." This also means

$$\int_{\substack{\text{all}\\\text{space}}} \Psi^*(x,y,z,t)\,\Psi(x,y,z,t)\ dx\,dy\,dz = 1$$

This is, $\Psi(x,y,z,t)$ is normalized at all times.

.- A historical test: The structure of the atom.

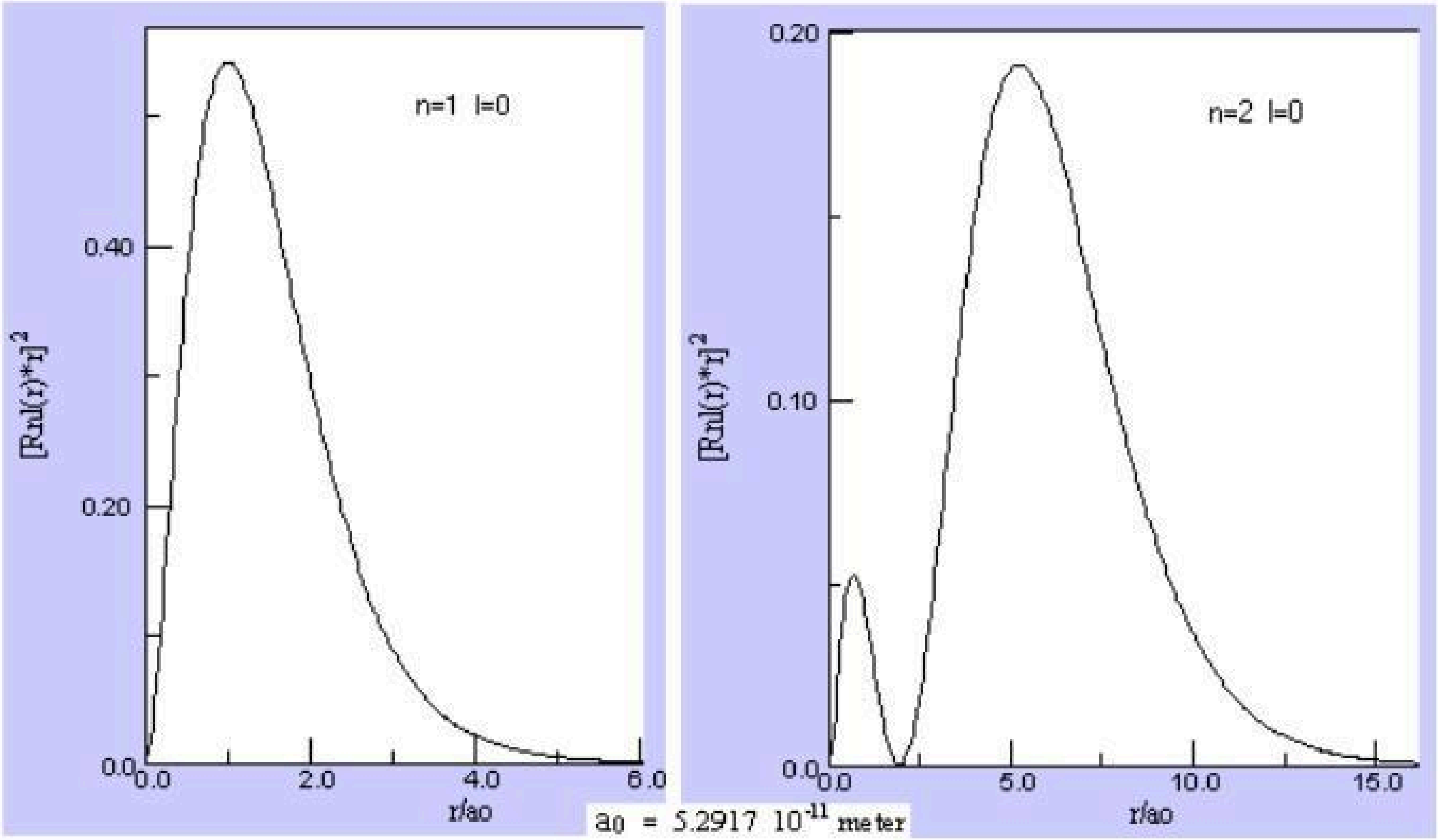
Among its many achievements, the Schrödinger equation has been a resounding success in explaining the structure of the atom.

Under the attractive potential of the atomic nucleus this equation predicts that electrons will reach stable states at definite values of total energy E_{n}, for n = 1, 2, 3…

$$E_{\mathrm{n}} = -\frac{\mathrm{m}\, \mathrm{e}^4}{2\, \hbar^2} \frac{1}{\mathrm{n}^2}$$

In such states, electrons also have precise absolute values for angular momentum but do not have values of linear momentum **P** nor position **r**(x,y,z) (again, they are nowhere.)

The probability distribution $\Psi^*(x,y,z,t)\Psi(x,y,z,t)$ along the atomic radius “r” is shown in the figure on the next slide for the two lowest levels of energy (n = 1 and n = 2.) and zero angular momentum (l = 0.)



The reader may notice that, in principle, these probability functions spread all the way to infinite.

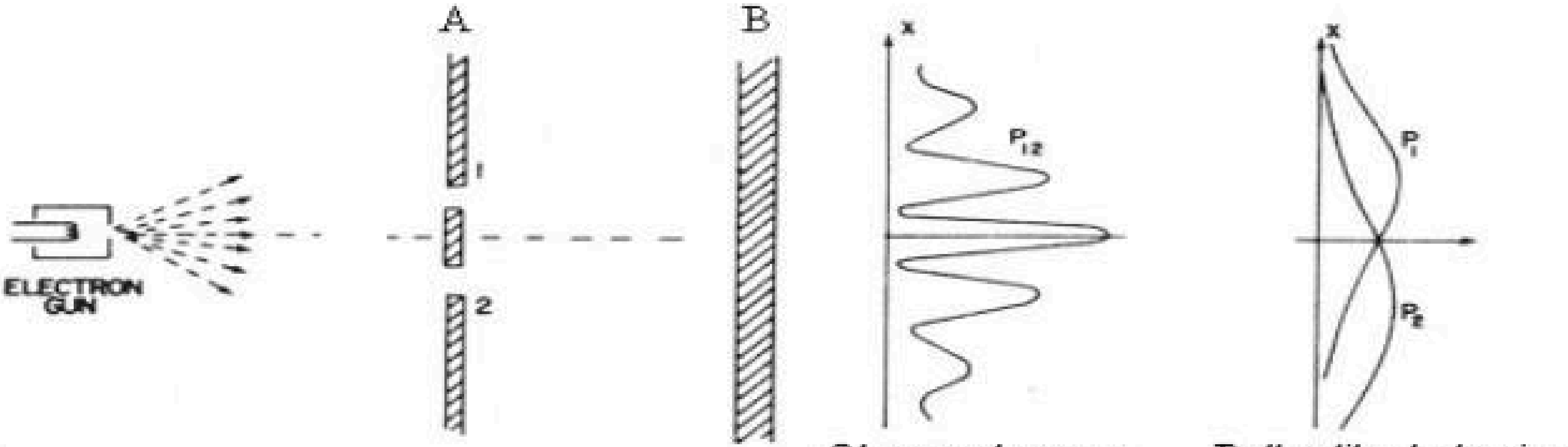
.- Critique to the Concept of "particle."

The concept of particle, as an abstract mathematical model, has been very successful in classical physics, where we can define a point, the Center of Mass, to represent the whole body in its translation.

Even in electrostatics, the related concept of "point charge" has been quite useful.

The inertia of this success has tricked physicists into carrying the concept of "particle" into the microscopic world, where it has become a monumental obstacle to the intuitive understanding of quantum physics, since the word "particle" suggests having a position, being somewhere, all the time.

Even the quintessential mystery of quantum mechanics, the double slit electron interference experiment:



Observed wave-like behavior.

Bullet-like behavior (not observed.)

presents little problem if we keep in mind that until the electron is detected on screen B, it never was in a definite position state (it never was "somewhere.") Therefore, questions such as "what slit the electron did go through?" make no sense, since the electron was nowhere to pass through any slit.

Notice that the double slit wall A does not constitute a position measurement operation on the electron.

Due to its importance let's examine the dynamics of this case more carefully:

When released from the gun, the electron is in a "particle" state, meaning it is localized at some small volume in space. Since the "particle" state is unstable, as $\Delta E \, \Delta t > 2\pi\hbar$, shortly after leaving the gun the electron is firmly in a definite energy state ($\Delta E \rightarrow 0$ as $\Delta t \rightarrow \infty$) A definite energy implies a definite frequency associated to the wave function.

It is in such flat wave state that the electron meets screen A. Such collision changes the electron state again, but not to a definite position state because A has two slits (a screen with only one slit would constitute a sort of definite position operator which would change the electron state to one of definite position, within the width of the slit.) That's not the case when we have two slits.

Shortly after leaving screen A towards screen B the electron is back to a definite energy state (evolved from the initial state at leaving screen A as specified by the Schrödinger equation.) Such definite energy state in this case can be written as the superposition of two flat waves with the same frequency of the wave incoming to screen A from the electron gun.

But back to the concept of “particle” in the quantum world, and to refer to another example, we saw in the previous section that an electron is not “somewhere” (at a definite position) even when it is bound to an atomic nucleus in a state of definite energy.

The closest thing to a “particle” that we have in quantum physics is a definite position state, where $\Delta x, \Delta y, \Delta z = 0$ or, using Dirac’s δ functional, $\Psi(x,y,z,t_o) = \delta(x,y,z)$.

However, such state function would rapidly spread over space, and such spreading leads to a state of definite energy, following Heisenberg’s principle with ΔE tending to zero as $\Delta E \sim 1/\Delta t$ (if such process occurs under a time independent potential $U(x,y,z)$)

The reader may have noticed that in our exposition of the quantum reality we never used the concept of “particle.”

.-Closing Comments:

The quantum theory is still a controversial subject, full of philosophical implications. It has many interpretations, some of them very disparate:

.- From one that postulates the existence of countless parallel universes (H. Everett, 1957.)

.- To another that claims that "consciousness" is one of the elements that must be taken into account to explain quantum processes (J. von Neumann, 1955.)

We reject these as invalid implications of the Quantum Theory. It is clear to us that the realization that a quantum entity can exist without been anywhere is all that is needed to intuitively understand all quantum phenomena and resolve all paradoxes.

Therefore our much simpler conclusion is that the reality we perceive (including our own bodies) is just the macroscopic manifestation of a thermal chaos of quantum collisions and interactions which are continuously taking quantum entities into and out of their localized "particle" states and, likewise, putting all other kind of observable magnitudes into and out of existence. In some sense they are continuously creating and destroying the world… same as the deity Shiva does, according to the Hindu tradition.

It is only because of the huge number of quantum entities involved that this continuous creation and destruction of the world is always bound to yield the same most probable result at the macroscopic level.

And in this process of continuous creation and destruction of the world, the natural tendency $\Delta E \sim 1/\Delta t$ to delocalize quantum entities into states of definite energy, plays a relevant role.

II.- The physics of atom-size bits: Quantum Computing.

.- Why atom-size bits?

In 1965, Gordon Moore predicted that the computing speed of a single chip would double every 18 months. This would be a consequence mainly of the increasing miniaturization of components.

However, due to physical limits this trend cannot continue forever. At the current rate, by the year 2020 a bit of data would require only one atom to represent it.

Reaching these physical limits will have profound consequences, because the behavior of computer components will then become dominated by the laws of quantum physics.

As we saw these laws are unimaginably different from those ruling our familiar macroscopic classical world, which includes present-day computers.

Current research also seems to indicate that computers that would function under quantum laws might be more powerful than any classical computer can be, and ahead we going to take a glimpse at some of these powers.

.- The nature of quantum bits (or qubits).

Same as classical bits, qubits can be in a quantum magnetic state associated to binary value 1 (let's call it |1>,) or in another, associated to binary value 0 (state |0>.)

However, unlike its classical counter part, a qubit can also be in many alternative states $|\Psi_b>$ which do not have any definite "bit" value.

While in any of these states, we can certainly measure the qubit's bit value, but that will abruptly change its current state $|\Psi_b>$ into either |0> (with probability p_0) or into |1>, (with probability p_1.)

Effect of measuring the bit value of a qubit while in state $|\Psi_b>$

$$\begin{tikzcd}
 & \mathbf{|0>} \\
|\Psi_b> \arrow[ur, "p_0"'] \arrow[dr, "p_1"'] & \\
 & \mathbf{|1>}
\end{tikzcd}$$

$$p_0 + p_1 = 1$$

.- Quantum registers.

A quantum register is a set of "n" qubits. Classically, a register of "n" bits has 2^n possible states. For example:

2 classical bits

$$\left.\begin{array}{cc} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{array}\right\} \begin{array}{l} 2^2 = 4 \\ \text{states} \end{array}$$

3 classical bits

$$\left.\begin{array}{ccc} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{array}\right\} \begin{array}{l} 2^3 = 8 \\ \text{states} \end{array}$$

Question:

How many general states are available to a quantum register of "n" qubits? 2^n states? Less than 2^n? More than 2^n?

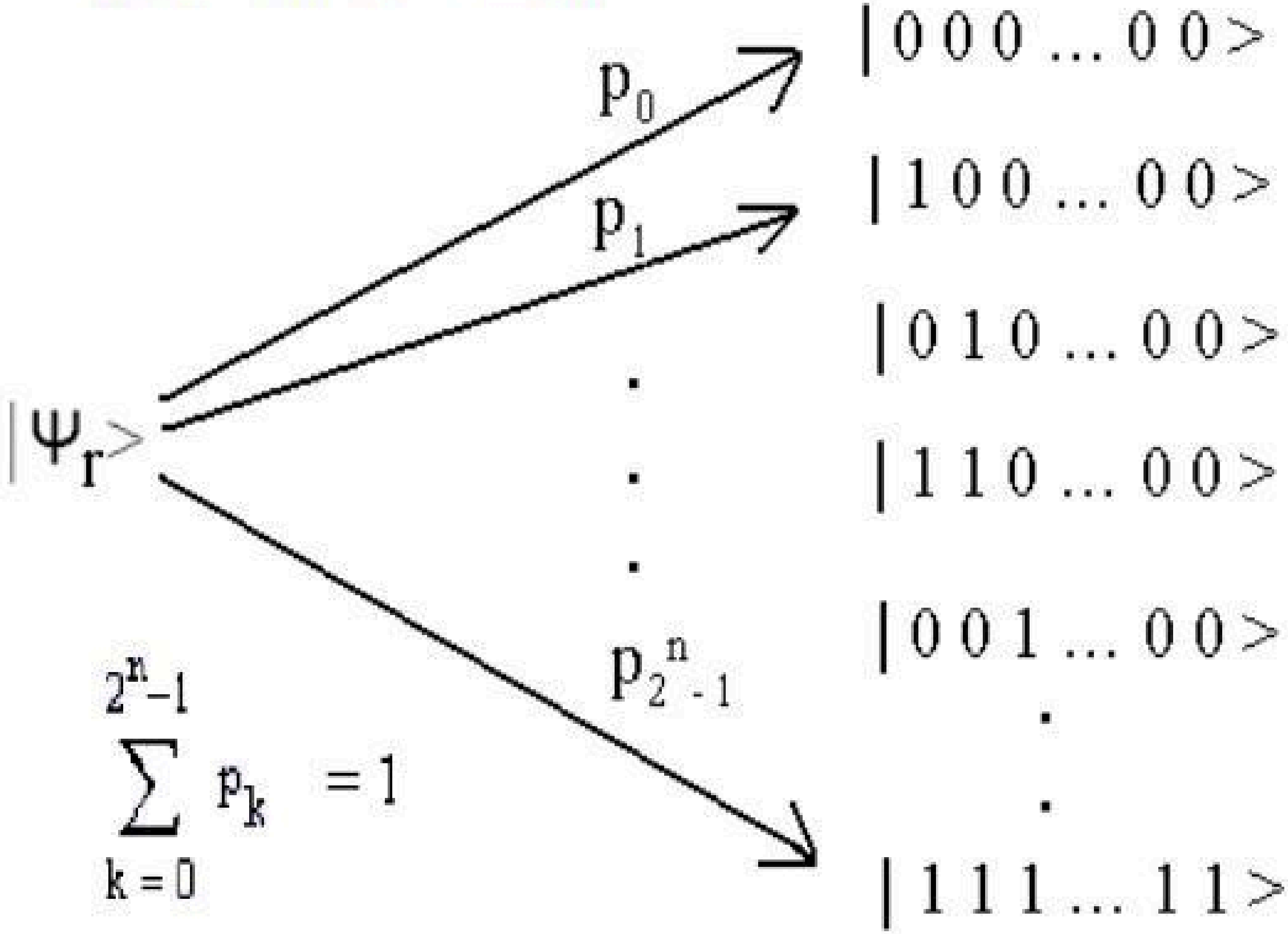
A quantum register can also be in many others alternative states $|\Psi_r>$ which do not have definite bit values.

If we performed a measurement to find the bit configuration when in any of these states $|\Psi_r>$, then this operation would *collapse* (this is, abruptly change) this state into any of these 2^n bit configuration states, each one with its own probability $p_0, p_1 \cdots p_k \cdots p_{2^n - 1}$.

Now, since it is certain that one of these bit configurations is going to be found, then these p_k's must meet the condition:

$$\sum_{k=0}^{2^n-1} p_k = 1$$

Effect of measuring the bit value of a qu-register of "n" qubits



$|\Psi_r>$

p_0

p_1

.

.

.

p_{2^n-1}

$|0 0 0 \ldots 0 0>$

$|1 0 0 \ldots 0 0>$

$|0 1 0 \ldots 0 0>$

$|1 1 0 \ldots 0 0>$

$|0 0 1 \ldots 0 0>$

.

.

$|1 1 1 \ldots 1 1>$

$$\sum_{k=0}^{2^n-1} p_k = 1$$

.- The state function of a qu-register.

If the qubits are free of mutual interaction, then the state function of a qu-register can be expressed as the product of the individual state functions of each independent qubit:

$$|\Psi_{r}> = |\Psi_{b\_0}> |\Psi_{b\_1}> |\Psi_{b\_2}> \dots |\Psi_{b\_(n-1)}>$$

or using a more concise notation:

$$|\Psi_{r}> = |\Psi_{b\_0} \Psi_{b\_1} \Psi_{b\_2} \dots \Psi_{b\_(n-1)}>$$

In the particular case when the qu-register is in a state with a definite bit-configuration, all the individual elements $|\Psi_{b\_k}>$ are either equal to $|0>$ or $|1>$.

.- A vector space for the state function?

Now, let's call $|\hat{e}_k>$ these different bit configuration states and list them below:

Basis state $|\hat{e}_0>$: $|0\,0\,0 \ldots 0\,0>$ ← Bit configuration where all qubits are "0".

" $|\hat{e}_1>$: $|1\,0\,0 \ldots 0\,0>$

" $|\hat{e}_2>$: $|0\,1\,0 \ldots 0\,0>$

" $|\hat{e}_3>$: $|1\,1\,0 \ldots 0\,0>$

" $|\hat{e}_4>$: $|0\,0\,1 \ldots 0\,0>$

.

.

" $|\hat{e}_{2^p-1}>$: $|1\,1\,1 \ldots 1\,0 \ldots 0\,0>$ ← Bit configuration where the first p qubits are all "1"

.

.

" $|\hat{e}_{2^n-1}>$: $|1\,1\,1 \ldots 1\,1>$ ← All n qubits are "1"

Since measuring the bit configuration of the qu-register will always collapse any $|\Psi_r>$ into one of these $|\hat{e}_k>$ states, then we can say that these $|\hat{e}_k>$'s constitute the "components" of any possible $|\Psi_r>$ (at least from a mathematical point of view.)

Extending this idea, we are going to assume that these $|\hat{e}_k>$ states conform a rectangular unit basis (orthonormal) of a 2^n dimensional space in which all $|\Psi_r>$'s mathematically exist.

In other words, these $|\hat{e}_k>$'s are going to play a role similar to the one that $\hat{\imath}, \hat{\jmath}, \hat{k}$ play in ordinary 3-D space.

As a vector in this space, any state function $|\Psi_r>$ can be specified by giving their corresponding components respect to each one of the unit basis vectors:

$$|\Psi_r> = \left(\begin{array}{c} \alpha_0 \\ \\ \alpha_1 \\ \vdots \\ \alpha_k \\ \vdots \\ \alpha_2 n_{-1} \end{array}\right) \begin{array}{l} \leftarrow \text{component respect } |\hat{e}_0> \\ \\ \leftarrow \text{component respect } |\hat{e}_1> \\ \\ \leftarrow \text{component respect } |\hat{e}_k> \\ \\ \leftarrow \text{component respect } |\hat{e}_2{}^{n}{}_{-1}> \end{array}$$

This column vector can also be conveniently written as a row:

$$|\Psi_r> \; = \; (\alpha_0 , \alpha_1 \ldots \alpha_k \ldots \alpha_{2^n-1})^T$$

where the superscript "T" stands for the "transpose" operation.

Mathematically, these α_k's can have any value, but in our physical case we are going to impose the restriction that they normalize $|\Psi_r>$. This is, we are going to scale the α_k's so they always make the absolute value of $|\Psi_r> = 1$.

As we mentioned, in general the Ψ(x,y,z,t) are complex functions. Therefore this space where the $|\Psi_r>$'s exist must be complex too. This means that the components α_k's in

$$|\Psi_r> \; = \; (\alpha_0 , \alpha_1 \ldots \alpha_k \ldots \alpha_{2^n-1})^T$$

are in general complex numbers.

Under these circumstances, the magnitude of a $|\Psi_r>$ must be obtained as its inner product with its transpose complex conjugate

$$(|\Psi_r>^*)^T = (\alpha_0^*, \alpha_1^* \ldots \alpha_k^* \ldots \alpha_{2^n-1}^*)$$

The standard (less cumbersome) notation for $(|\Psi_r>^*)^T$ is $<\Psi_r|$, so we can express this inner product as:

$$\langle \Psi_r | \Psi_r \rangle = (\alpha_0^*, \alpha_1^* \ldots \alpha_k^* \ldots \alpha_{2^n-1}^*) \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_k \\ \vdots \\ \alpha_{2^n-1} \end{pmatrix} = \sum_{k=0}^{2^n-1} \alpha_k^* \alpha_k = 1$$

Combining this expression with the previous constrain on probabilities:

$$\sum_{k=0}^{2^n-1} p_k = 1$$

we can write

$$\langle \Psi_r | \Psi_r \rangle = \sum_{k=0}^{2^n-1} \alpha_k^* \alpha_k = \sum_{k=0}^{2^n-1} p_k = 1$$

Thus, we see that the components α_k are closely related to the probability p_k of finding a particular bit configuration:

$$p_k = (\alpha_k{}^*)\, \alpha_k.$$

Conclusion:

No one can deny that all this stuff is quite easy!!!

The obvious restriction on the sum of probabilities being = 1 is nothing more than the norm of an unit vector $|\Psi_r>$ that represents the quantum state function of the whole qu-register in a 2^n dimensional complex vector space, in which the bit-value configuration states $|\hat{e}_k>$ conform an orthonormal basis.

Since the norm of $|\Psi_r>$ must remain equal to 1 at all times in any state evolution process, such process can be visualized as an unitary linear transformation (this is, a rotation) of vector $|\Psi_r>$ in its 2^n dimensional *Hilbert* space.

Easy! Isn't it?

.- Quantum algorithms.

A quantum algorithm consists of a sequence of operations on a qu-register aimed to evolve (unitary linearly transform) its quantum state $|\Psi_r>$ into one which component(s) α_k respect the bit configuration state(s) $|\hat{e}_k>$ associated to the solution of a given problem have been substantially increased.

This way, when the bit configuration is measured, with a higher probability $|\Psi_r>$ will collapse into one of these $|\hat{e}_k>$'s, yielding the desired answer.

Of course, there is not certainty that $|\Psi_r>$ will collapse into a right $|\hat{e}_k>$. If it does not, the whole process must be repeated.

By the way…what is the (formidable) equation that describes the dynamics of the evolution of quantum states?

$$i \hbar \frac{\partial \Psi(x,y,z,t)}{\partial t} = - \frac{\hbar^2}{2m} \nabla^2 \Psi(x,y,z,t) + U(x,y,z,t)\Psi(x,y,z,t)$$

In the sections ahead we will quickly review one of the most important research paper in theoretical Quantum Computing. In it, the author presents a sequence of unitary linear transformations that evolve an initial state function of a qu-register into a final (problem solving) state.

If we examine Schrödinger's (linear) equation, we can see that in an experimental situation, a specific evolution of $\Psi(x,y,z,t)$ can be implemented in hardware by carefully controlling the functional form of $U(x,y,z,t)$, in order to evolve a given initial state Ψ_o into a desired final one Ψ_f.

.- A factoring problem to be solved.

A popular form of cryptography is based on the difficulty associated with factoring a large number into its prime elements (i.e factors 661 and 887 of number 586,307.)

In 1994 a number of 129 digits was factored using 1600 workstations, and it took them over eight months to do it. At this rate, factoring a number with 1,000 digits would take 10^{25} years, much longer than the age of the universe, (~ 1.5 10^{10} years.)

If an efficient method of factoring large numbers were to be discovered, most of the current encryption schemes would be easily compromised. In 1994 Peter Shor, a scientist at Bell Labs, devised a quantum algorithm that did just that.

.- Shor’s quantum algorithm.

Shor's algorithm hinges on a number theory fact: if “x” is an integer coprime to “N” (this is, *greatest common divisor*, gcd(x,N) =1) then the function F(a) = x^{a}mod[N] is periodic: F(a) = F(a + b r), with “r” the smallest period and b = 0,1,2….

For instance, for N = 91 (=7·13) and x = 3:

a	=	0	1	2	3	4	5	6	7
3^a	=	1	3	9	27	81	243	729	2187
F(a) = 3^a mod[N]	=	1	3	9	27	81	61	1	3

We can observe that for this case r = 6.

Shor's algorithm efficiently finds the smallest period “r”, which is then used as follows:

Since $x^0 = 1$ → $F(0) = x^0 \bmod[N] = 1$. But periodicity implies that also $x^{(0+r)} \bmod[N] = 1$. This expression can be rearranged as

$$(x^r - 1) \bmod[N] = 0$$

which, using the identity $(a^2 - b^2) = (a-b)(a+b)$ gives:

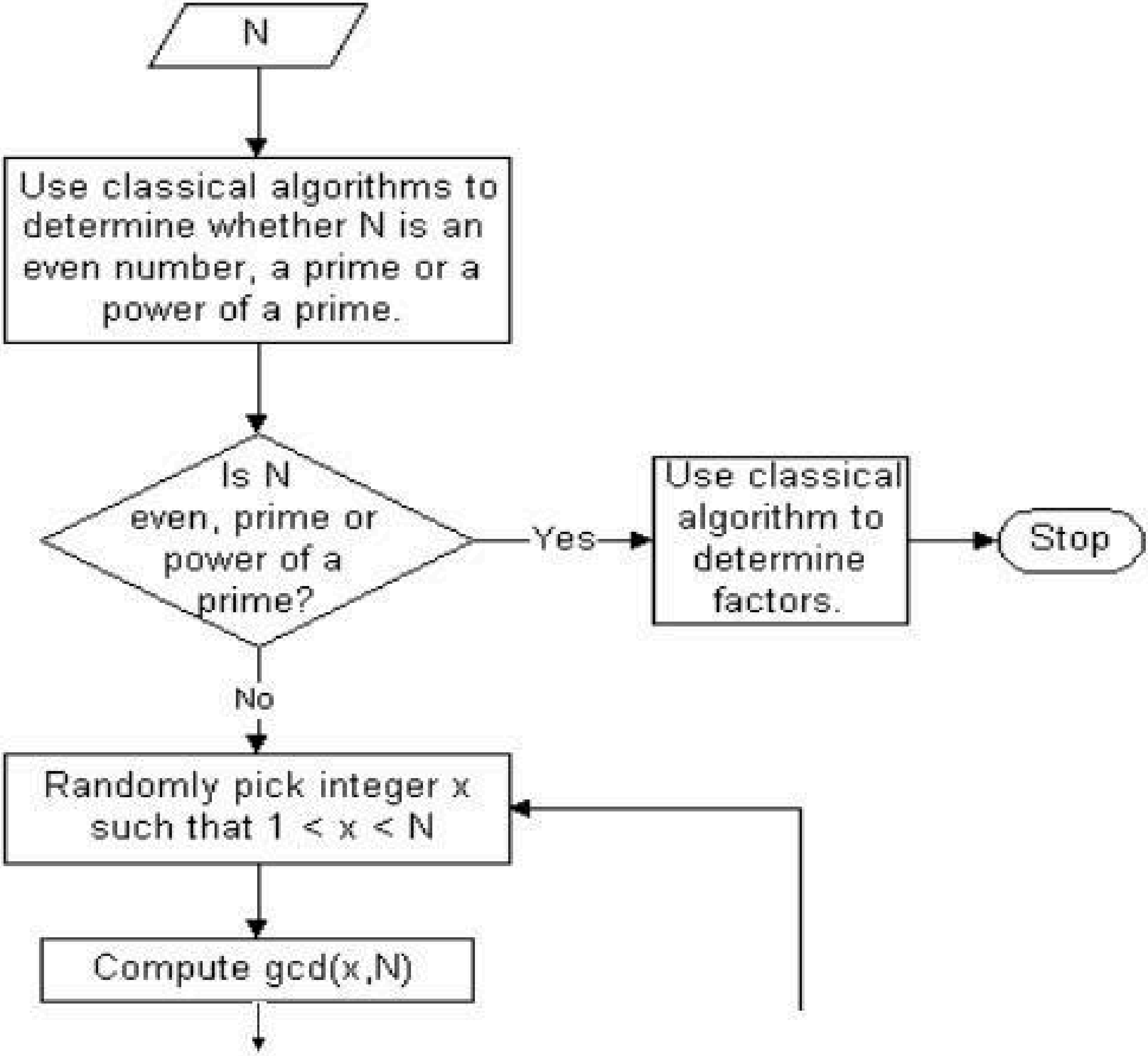
$$(x^{r/2} - 1)(x^{r/2} + 1) \bmod[N] = 0$$

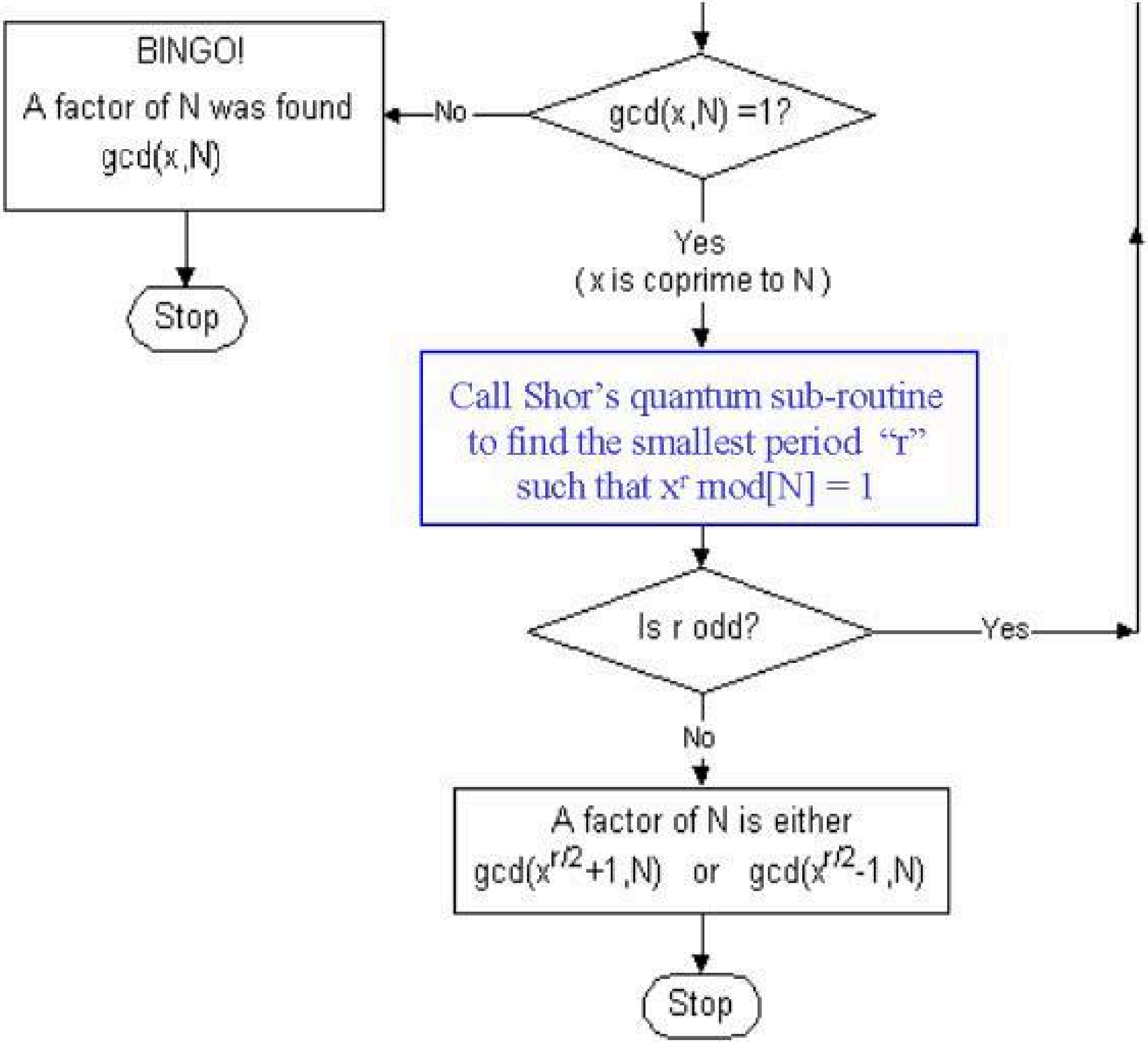
If “r” is even, we can find

$$\gcd(x^{r/2} - 1, N) \quad \text{and} \quad \gcd(x^{r/2} + 1, N)$$

where at least one of them is a non-trivial factor of “N”.

Shor's algorithm in flowchart form:


N
Use classical algorithms to determine whether N is an even number, a prime or a power of a prime.
Is N even, prime or power of a prime?
Yes
Use classical algorithm to determine factors.
Stop
No
Randomly pick integer x such that 1 < x < N
Compute gcd(x,N)



BINGO!

A factor of N was found gcd(x,N)

Stop

No

gcd(x,N) =1?

Yes

(x is coprime to N)

Call Shor's quantum sub-routine to find the smallest period "r" such that $x^r \bmod[N] = 1$

Is r odd?

Yes

No

A factor of N is either $\gcd(x^{r/2}+1,N)$ or $\gcd(x^{r/2}-1,N)$

Stop

.- Shor’s quantum sub-routine.

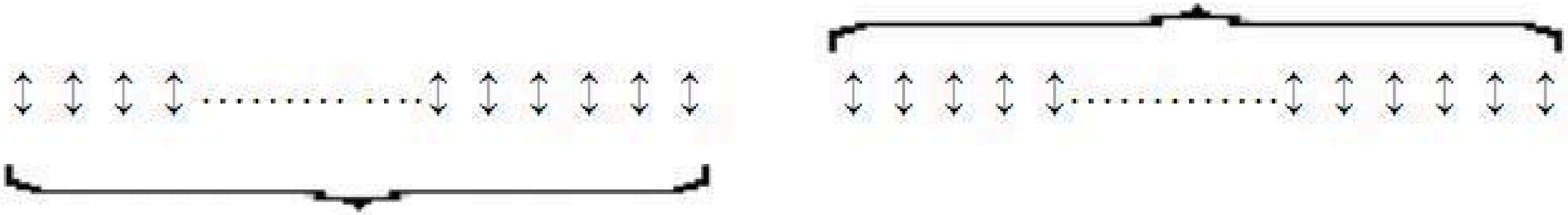
The value of “r” is found by using a quantum register, which will be manipulated as two separated parts, Reg1 and Reg2.

Let’s represent qubits by the symbol ↕ in the following diagram:

N = Number to be factored.

Enough qubits to store number N-1

Reg2



Reg1

“n” qubits, with “n” such that $N^2 <= 2^n < 2N^2$ (“n” qubits can store up to binary number $2^n – 1$.)

Step 1: We start with the qu-register in state $|\Psi_r\rangle = |\hat{e}_0\rangle = |0\ 0\ \ldots\ 0\ 0\rangle$, or $|\Psi_r\rangle = (1,0,0\ldots0)^T$.

Step 2: We transform this $|\Psi_r\rangle$ into a state where the Reg1 component becomes an equally weighted superposition of all the 2^n bit configurations available to Reg1, but at the same time the qubits in Reg2 remain unaltered. After this unitary linear transformation, the new state $|\Psi_r\rangle$ is (with $q = 2^n$):

$$|\Psi_r\rangle = \frac{1}{\sqrt{q}} \sum_{m=0}^{q-1} \left| m \quad 0 \right\rangle \quad \text{or}$$

$$|\Psi_r\rangle = (\alpha_0, \alpha_1 \ldots \alpha_{2^n-1}, 0, 0 \ldots 0)^T$$

$$\text{with } \alpha_0 = \alpha_1 = \ldots \alpha_{2^n-1} = \frac{1}{\sqrt{q}}, \quad q = 2^n$$

Step 3: The second unitary linear transformation to be applied involves the function x^m mod[N]: for each vector |m 0> inside the sum in the previous expression, we compute the associated value x^m mod[N] and store it in the Reg2 area. The resultant state is:

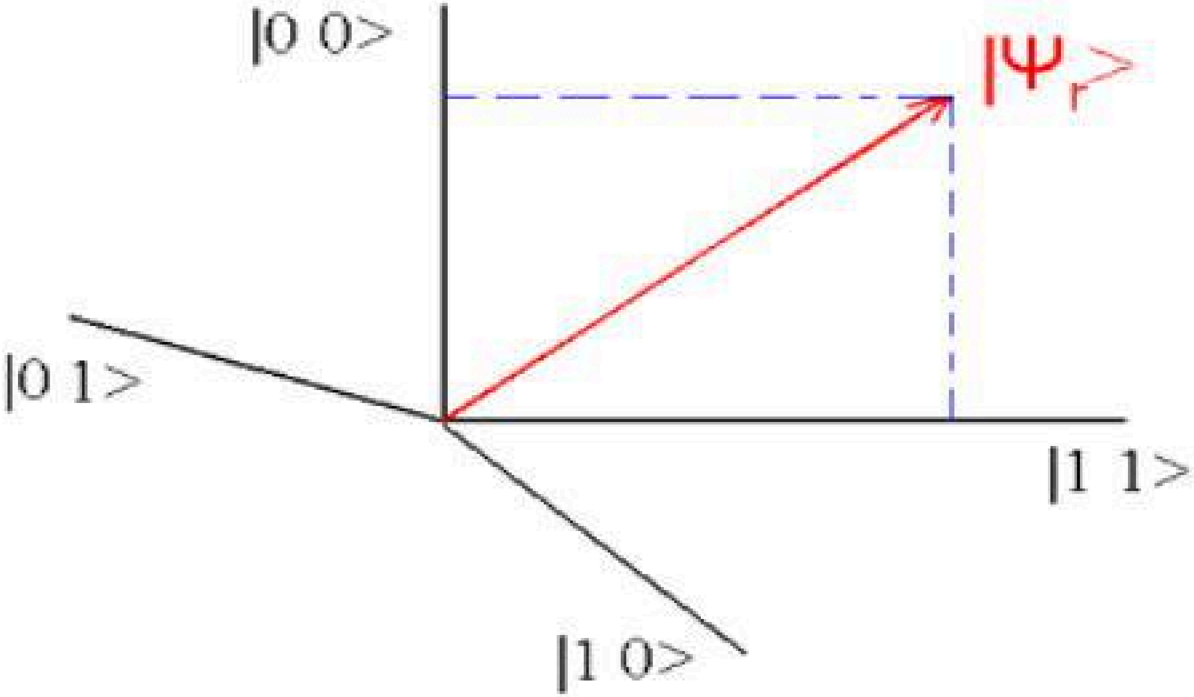
$$|\Psi_r\rangle = \frac{1}{\sqrt{q}} \sum_{m=0}^{q-1} \left| m \quad x^m \bmod N \right\rangle$$

Basically, what we have done is simply a change the basis, from the set of vectors |m 0> to the set |m x^mmod[N] >.

There still are q = 2^n terms in the sum, and $|\Psi_r>$ is still an equally weighted superposition, but now of these different basis states | m x^m mod[N] >.

Now we need to make a parenthesis to discuss Entanglement.

This phenomenon is difficult to see because it only happens in the quantum world. Let's try an easy example of two qubits, for which the Hilbert space has only four basis state:



Now, let's consider a state $|\Psi_r>$ that is a superposition of $|0\ 0> + |1\ 1>$ only.

If we measure only one qubit and find it = 1, then consistency demands that the other qubit immediately also becomes = 1 (without being measured!) Same correlation occurs if we find the first qubit to be = 0.

This happens because the original superposition can only collapse to either |0 0> or |1 1>.

Definition:

> "When a quantum system is a state such that measuring one of its sub-systems immediately fixes the other, the system is said to be in an *entangled* state."

Quantum Teleportation, a new area of scientific research, is based on this phenomenon.

Step 4: On the $|\Psi_r>$ obtained in step three:

$$|\Psi_r\rangle = \frac{1}{\sqrt{q}} \sum_{m=0}^{q-1} \left| m \quad x^m \bmod N \right\rangle$$

we measure the bit configuration of the Reg2 part only. Let's say we observe (or that Reg2 collapses to) binary value L.

Since the whole qu-register was *entangled,* this measuring process has the side effect of keeping in the superposition only those states whose Reg1 value is consistent with having the value L in the Reg2 area.

Calling λ this set of (consistent-with-L) values c_v, and n_λ its number of elements, the state of the whole qu-register after this measuring operation becomes

$$|\psi_r\rangle = \frac{1}{\sqrt{n_\lambda}} \sum_{c_v \in \text{set } \lambda} \left| \, c_v \quad L \right\rangle$$

The set λ is a smaller subset of $m = \{0, 1, \ldots q-1\}$.

<u>Step 5</u>: The last unitary linear transformation substitutes each one of the n_λ basis vectors $|c_v\ L>$ by a linear combination of all the basis vectors $|m\ L>$ available to Reg1, involving complex exponential functions (Fourier Transform.)

$$\left|c_v\ L\right\rangle \rightarrow \frac{1}{\sqrt{q}} \sum_{m=0}^{q-1} \left|m\ \ L\right\rangle e^{2\pi i \cdot c_v \cdot m/q}$$

After this transformation, the $|\Psi_r>$ becomes

$$|\Psi_r\rangle = \frac{1}{\sqrt{n_\lambda}} \sum_{\substack{c_v \in \\ \text{set } \lambda}} \left(\frac{1}{\sqrt{q}} \sum_{m=0}^{q-1} \left| m \quad L \right\rangle e^{2\pi i \cdot c_v \cdot m / q} \right)$$

Rearranging the order of summations

$$|\Psi_r\rangle = \sum_{m=0}^{q-1} \left| m \quad L \right\rangle \left(\frac{1}{\sqrt{q}} \frac{1}{\sqrt{n_\lambda}} \sum_{c_v \in \text{ set } \lambda} e^{2\pi i \cdot c_v \cdot m/q} \right)$$

The term in parenthesis can be easily identified as the α_m component of this $|\Psi_r>$ along basis vector $|m \quad L>$. In other words…

… if we now measure the bit configuration in Reg1, the probability of finding a particular |m L> state is

$$p_m = \alpha_m^* \alpha_m = \left| \frac{1}{\sqrt{q}} \frac{1}{\sqrt{n_\lambda}} \sum_{c_v \in \text{set } \lambda} e^{2\pi i \cdot c_v \cdot m/q} \right|^2$$

Conceptually, to sum over a set presents no problem. But in this case, to evaluate this summation over set λ we need to find a suitable <u>index</u>. That we'll do in the next section.

.- “*An index! an index! my kingdom for a index!*”

The set λ of bit values c_v is a subset of the of index values $m = \{ 0,1,\ldots q-1\}$ for Reg1.

Let’s define “ℓ” based on the value “L” measured in Reg2 as:

a) $x^{\ell} \bmod[N] = L$

b) $0 <= \ell < r$

Since $x^{\ell + b r} \bmod[N] = L$, then the set λ of bit values c_v is equal to $\{\ell + b\ r\}$ with $b=0,1,2\ldots b_{max}$. Since $m_{max} = q - 1$, b_{max} must be such that $b_{max}\, r + \ell \sim< m_{max}$.

This is, $b_{max} \sim< (q - 1 - \ell)/ r$.

Incorporating all this in the previous expression for $p_m = \alpha_m{}^* \alpha_m$ we get

$$p_m = \alpha_m^* \alpha_m = \left| \frac{1}{\sqrt{q}} \frac{1}{\sqrt{n_\lambda}} \sum_{b=0}^{\left(\frac{q-1-\ell}{r}\right)} e^{2\pi i \cdot (br+\ell) m/q} \right|^2$$

Taking out all common factors, and approximating $b_{max} = (q - 1 - \ell) / r \approx q/r - 1$ (assuming $q >> 1$ and $\ell \sim r$) we get

$$p_m = \alpha_m^* \alpha_m = \left| \frac{1}{\sqrt{q}} \frac{1}{\sqrt{n_\lambda}} e^{2\pi i \cdot (\ell) m/q} \sum_{b=0}^{\left(\frac{q}{r}-1\right)} e^{2\pi i \cdot (br) m/q} \right|^2$$

This is

$$p_m \propto \left| \sum_{b=0}^{\frac{q}{r}-1} e^{2\pi i \cdot b r m/q} \right|^2$$

In this expression we can clearly see that p_m is much larger for those values of "m" that are multiples of q/r.

At this point if we measure the bit configuration in Reg1, overwhelming chances are that its quantum state will collapse into any of the bit configuration values m_i such that $m_i = i \cdot q/r$ (with i = 1,2,…r.)

Having this value "m", knowing "q" and that "i" is an integer, the determination of "r" is simple, and with it we can find the factors of N as $\gcd(x^{r/2} - 1, N)$ and $\gcd(x^{r/2} + 1, N)$.

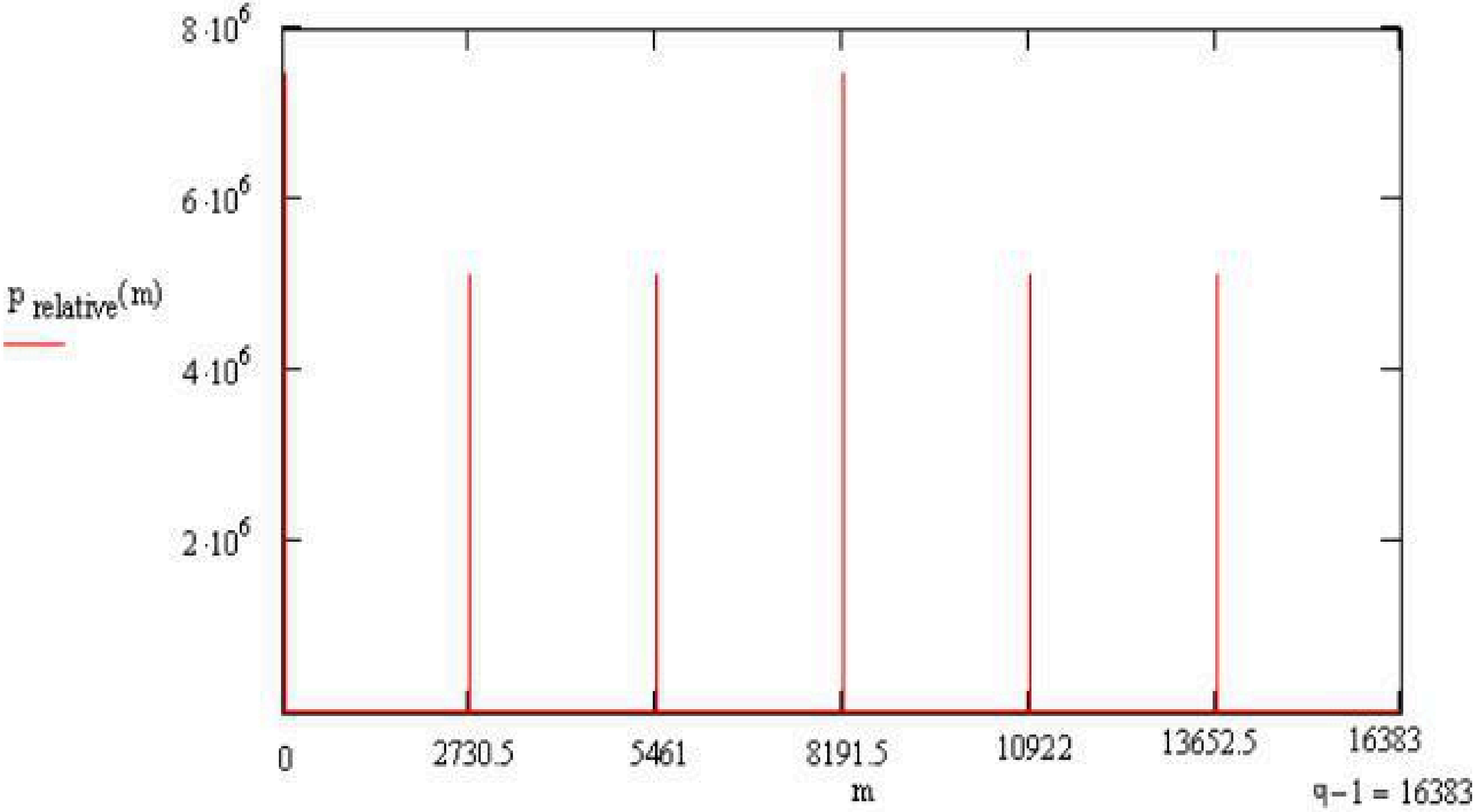
.- **How much larger** are the $p_{(m = i \cdot q/r)}$?

Let’s illustrate this final result with the simple case of $N = 91$, and suppose that we randomly selected $x = 3$ to be used in $F(a) = x^a \bmod[N]$. For these values we already found that $r = 6$.

Since $N^2 = 91^2 = 8281$ and $N^2 < q < 2 N^2$, we need 14 qubits in Reg1 so $q = 2^{14} = 16384$. For this case, $m = 0,1,\dots q - 1$, or $m = 0,1,\dots 16383$.

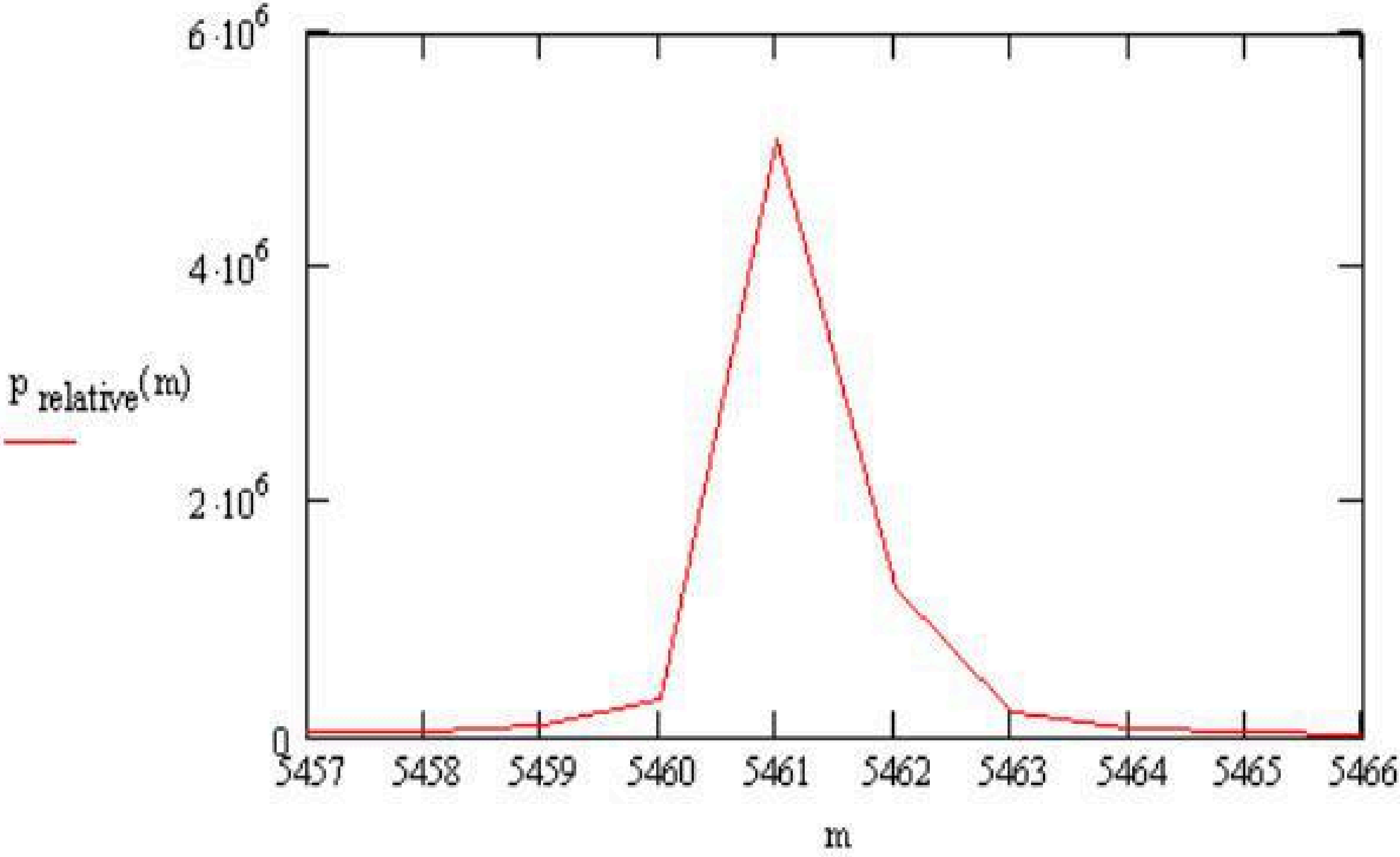
Using suitable scientific software we can define and plot the p_m function we found above as

$$p_{relative}(m) := \left| \sum_{b=0}^{\frac{q}{r}-1} e^{2\cdot\pi\cdot i\cdot b\cdot\frac{r\cdot m}{q}} \right|^{2}$$



We can see that the probabilities for some selected values of "m" are indeed millions of times higher than for the other values. These values of "m" correspond to $m_i = i \cdot q/r$.

A detailed view of how this probability function behaves around m = 5461 is



.- Epilogue.

At this point, some promising experimental success has been achieved in testing quantum computing with a few qubits.

However, a condition for its full development is to have the technology to manipulate state functions to a degree of total control to change and preserve quantum states. Currently we do not have such technology.

But someday we will, and that will open many doors to whole new realms of technological possibilities, when we will be able to fully exploit for practical applications the almost magical nature of the quantum world.

.- References.

To download files containing this presentation, quantumc.doc & quantumc.ppt (as well as other Computer Science material) go to

http://lb109.glendale.edu/compscience/cs165

Other references:

http://www.cs.washington.edu/homes/oskin/Oskin-A-Practical-Architecture-for-Reliable-Quantum-Computers.pdf
http://www.phy.davidson.edu/StuHome/cabell_f/Radial.html
http://www.cs.caltech.edu/~shantz/final.doc
http://www.cs.caltech.edu/~westside/quantum-intro.html
http://stardec.hpcc.neu.edu/~bba/RES/QCOMP/QCOMP.html
http://alumni.imsa.edu/~matth/quant/299/paper.pdf
http://www.research.att.com/~shor/papers/QCalgs.pdf
http://www.cs.bell-labs.com/who/rob/qcintro.pdf
http://xxx.lanl.gov/PS_cache/quant-ph/pdf/0010/0010034.pdf

http://www.iro.umontreal.ca/~paquin/Qu/quantumComp.pdf
http://www.physics.dcu.ie/~jpm/PS407/computing.pdf
http://www.wikipedia.org/wiki/Quantum_computer
http://www.qubit.org/oldsite/intros/comp/comp.html
http://www.fxpal.com/PapersAndAbstracts/papers/ste00.pdf
http://www.doc.ic.ac.uk/~nd/surprise_97/journal/vol4/spb3/
http://www.ra.informatik.uni-stuttgart.de/~ghermanv/Lehre/Seminar/material/Presentation12/report.doc
http://www.wikipedia.org/wiki/Shor%2527s_algorithm
http://www.cafebabe.demon.co.uk/QM/Quantum_Reality.htm

- The Meaning of Quantum Theory: A Guide for Students of Chemistry and Physics. Jim E. Baggott. Paperback, Oxford University Press, Inc., May 1992.

- Tao Of Physics: An Exploration of the Parallels Between Modern Physics & Easter Mysticism, fourth edition. Fritjof Capra. Shambhala Publications, Inc.

.- Appendix A

This is quite different to some interpretation that circulates around about the electron being everywhere. Such interpretation is logically inconsistent because when its location is measured, the electron is always found in a given single location (x,y,z)

In Quantum Mechanics language, a given position is a eigenvalue of the Position operator and eigenvalues are single values.

This absurd view of the electron being “everywhere” comes from the inability of some physicists to conceive that a quantum entity can exist without been anywhere.

.- Appendix B.

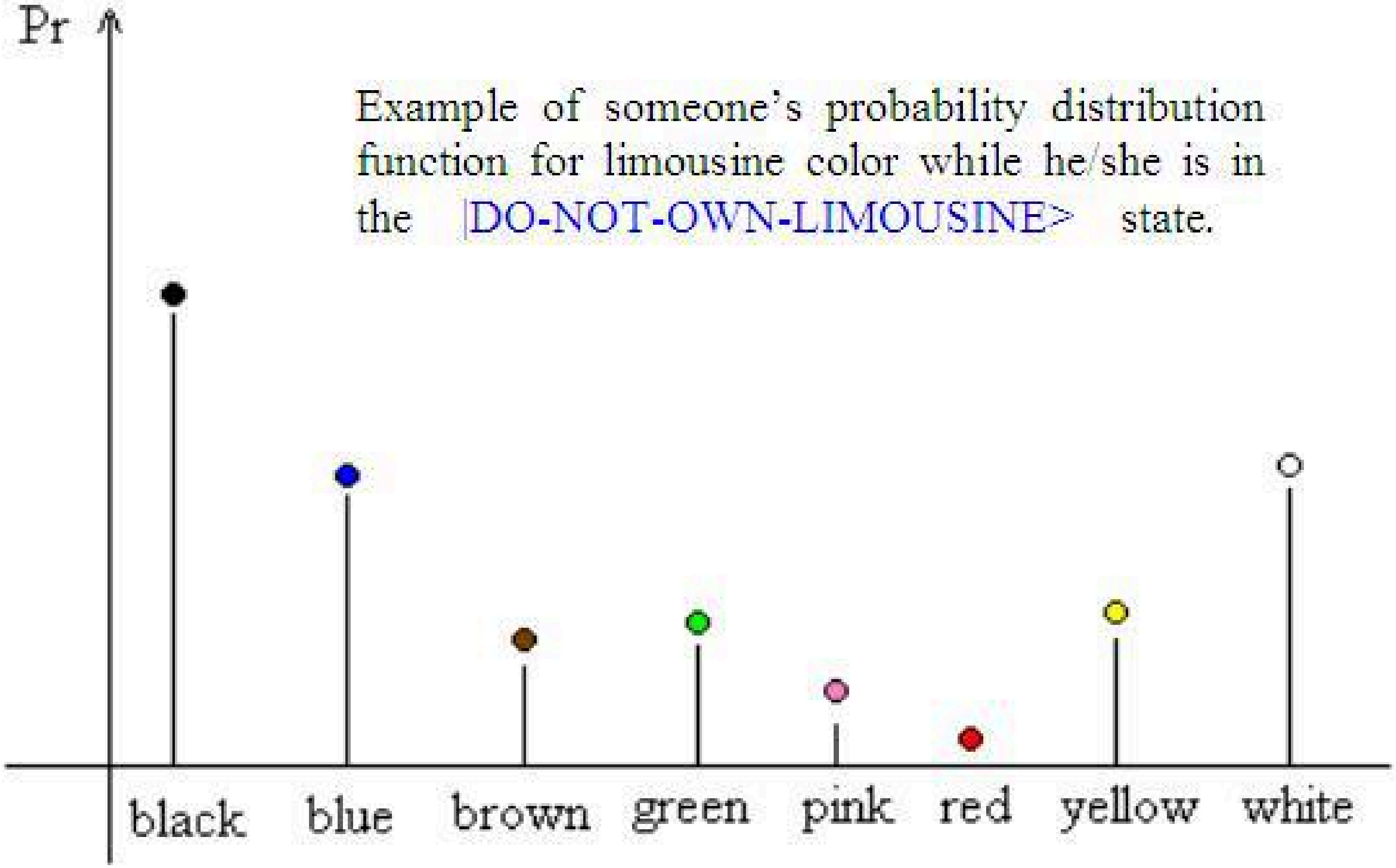
This is not as weird as it seems. Actually, there are situations in our normal life that follow this pattern of behavior.

Suppose we asked the reader “what is the color of your limousine?” He/She may answer “I do not own a limousine,” or in other words,

“I am in a |do-not-own-a-limousine> state.”

But in such state the reader certainly presents a probability distribution for limousine color (reflecting his/hers liking.)

Should the reader change to a |own-a-limousine> state, the color to be adopted (or chosen) will follow that probability distribution that he/she presents in the current state.



Example of someone's probability distribution function for limousine color while he/she is in the |DO-NOT-OWN-LIMOUSINE> state.

This probability distribution would manifest if a change to a |OWN-LIMOUSINE> state occurs.