Generating Real Random Numbers with Uncertainty Principle

ZHANG Jiayi

(*School of physical science and technology*, *Lanzhou university*, 730000, *Lanzhou*, *Gansu*, *China*)

Abstract: The real random number generation is a critical problem in computer science. The current generation methods are either too dangerous or too expensive, such as using decays of some radioactive elements. They are also hard to control. By the declaration of uncertainty principles in quantum mechanics, real probabilistic events can be substituted by easier and safer processes, such as electron diffraction, photon diffraction and qubits. The key to solve the problem of Schrödinger's cat is to identify that the atom stays in different states after and before the decay, and the result of the decay is probabilistic according to the wave packet collapse hypothesis. Same matter is able to possess different kinds of properties such as wave-particle duality due to that it can stay in various states, and which state will the matter stay is determined by the chosen set of physical quantities (or mechanical quantities). One eigenstate of a set of physical quantities can be a superposition of other eigenstates of different sets of physical quantities, and the collapse from a superposition to an eigenstate it contains is really random. Using this randomness, real random number can be generated more easily.

Key words: Uncertainty Principle, Wave Packet, Real Random, Duality, Superposition, Matter Wave

1 The Uncertainty Principle in Quantum Mechanics

Max Planck published his scientific work on blackbody radiation in 1900, quantum physics was consequently introduced. After that, developed by Bohr and Heisenberg, quantum mechanics was created and became one of the main pillars of modern physics. In 1925, Heisenberg invented the "matrix mechanics" which led him into Nobel laureate, which is similar to Schrödinger in 1926 by his "wave mechanics". By quantum mechanics, Heisenberg indicated that there are uncertainties caused by it. For example, by the communication relation of momentum $\vec{p}$ and position $\vec{r}$, i.e., $[p_r, r] = -i\hbar$, the fluctuations of them will be limited by

$$\Delta r \cdot \Delta p_r \geq \frac{\hbar}{2} \quad (1),$$

which means that the concepts about orbits in classical physics will not stand anymore in quantum physics. Every particle would be either a point with unknown movement or a moving wave without certain position. When the stationary particle was released into free movement in space, the momentum will be given randomly from one of the eigenfunctions of momentum and the probability of the particle to have each momentum equals to the square of the parameter before the corresponding eigenfunction in the unfolding polynomial of the particle by the complete eigenfunction set of momentum (which should be timed by dp if the eigenvalue of momentum p is consistent). The similar processes in the alternation of a free moving particle into a stationary point. Other physical quantities that have non-zero commutation relations all have uncertainty relations

$$\Delta A \cdot \Delta B \geq \frac{[A, B]}{2} \quad (2)$$

It is worth mentioning that this uncertainty is a

kind of the nature of matter and is not caused by the affections from measurements. Just like what happened in the case of Schrödinger's cat. (See Appendix A)

However, Schrödinger's cat is still a paradox now, it is necessary to identify what really happens in that case of Schrödinger's cat, before that, one should distinguish the practice and cognitive processes in a measurement.

When a measurement was taken, the atom must choose an eigenstate (to decay or not to decay) to collapse but it also does not need to collapse before the measurement. In uncertainty principle, it cannot be predicted which eigenstate it will collapse into when a state collapses from to an eigenstate it contains. For this cat case, the atom's decay obeys the uncertainty principle. The results are certain to people's daily life, and this seems contradictory with quantum mechanics.

To figure out the way to solve these conflicts, reviewing the processes of collapses from a state to an eigenstate it contains. Let's start with a case of single electron diffraction.

As the picture in Fig. 3 showed, a single electron is propagating from the gun to the screen. Between them there is a wall with two adequately thin slits, and the distance between the two slit is as the wave length of the electrons shot which is calculated by De Broglie formula $\lambda = \hbar k = \frac{h}{p}$, so that electron wave can interfere with itself when passing the two thin slits.

According to Schrödinger function

$$\hat{\vec{p}}\psi = \vec{p}_0\psi$$
$$-i\hbar\vec{\nabla}\psi = \vec{p}_0\psi$$
$$\psi = e^{i\frac{\vec{p}_0}{\hbar}\cdot\vec{r}} \ ,$$

the electron is a spherical wave when propagating freely in the space. The electrons would apparently be obstructed by the wall and only two spherical waves from two slits would be emitted. This is a case of Young's two micro holes interference. Denoting the two waves as

$$\psi_1 = e^{i\frac{\vec{p}_0}{\hbar}\cdot\vec{r}_1}$$
$$\psi_2 = e^{i\frac{\vec{p}_0}{\hbar}\cdot\vec{r}_2} \ ,$$

the phase difference of them is $\delta = (\vec{r}_1 - \vec{r}_2)\cdot\frac{\vec{p}_0}{\hbar}$, as the Fig.1 shows below, $(\vec{R}_1 - \vec{R}_2)\cdot\vec{p}_0 = 0$ therefore there is no $(\vec{R}_1 - \vec{R}_2)$ in δ. From Fig.3, one can see the probability distribution the same as that of the experimental results in Fig.2.

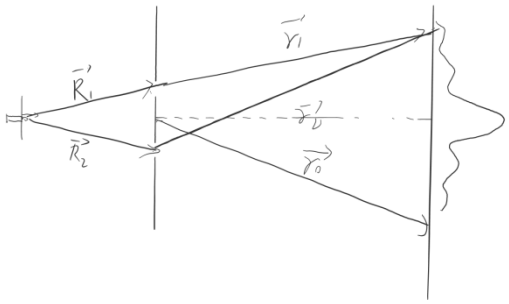

Fig.1 The Interference of Electron-wave through Double-slit, Same Result of Young's Interference

If there is no screen behind, the electron wave would propagate freely infinitely and the wave would constantly be

$$\psi = \psi_1 + \psi_2 \ .$$

When the screen was placed somewhere, the electrons bombarded on it would be pinned down to the screen. Its wave equation would consequently change into

$$\hat{\vec{r}}\psi = \vec{r}_0\psi \quad ,$$

and its solution is

$$\psi = \delta(\vec{r} - \vec{r}_0).$$

In summary, the wave function of the electron changed from

$$\psi = \psi_1 + \psi_2$$

into

$$\psi = \delta(\vec{r} - \vec{r}_0)$$

when propagating from the electron gun into the screen which pinned down it into fixed position. Now one can see that the wave function of the electron is different when freely propagating and when staying at a site of the screen.

Generally, any measurement is analogous to the process showed above. For the single-electron diffraction case, the measurement is to put a screen on the way the electron propagates, and the screen stopped the electrons with their state altered. For general case, any

measurement would change the matter into different state so that the physical quantity of the measured state can be pinned down.

According to the explanation above, the interpretation of Schrödinger's cat paradox should be that the cat stayed at different states before and after the decay of the atom (see appendix A about Schrödinger's cat). And one should distinguish the processes of measurements and the decay of the atom. Whether the atom would decay or not decay will become a fact that influence the life of the cat, but the observation only determines the observer's awareness.

Like a cup of water will change its shape in different containers. The same cup of water will always fix the shape of the container. If one assimilates a superposition $|\psi\rangle$ of a physical quantity $\hat{A}$ to 1kg water in a cup, pouring it into the floor and its shape would naturally turn into a flat shape and the pattern of its planform is usually random and also not regular, then the floor is a container of another shape and could be assimilated as a complete set of the eigenstates of $\hat{A}$ with each position where the particles of water may stay is an eigenstate of $\hat{A}$.

Similar to that, what happens on Schrödinger's cat is that the cat stays in a superposition state of $|Scat\rangle = \frac{\sqrt{2}}{2}(|Dcat\rangle + |Acat\rangle)$. As mentioned above, if classifying every possible pattern of the planform as the picture in Fig.2 showed into two classes: class 1 for more water stays in left half and class 2 for more water in right half, then $|Dcat\rangle\ and\ |Acat\rangle$ can just be corresponded to class 1 and class 2 respectively. All patterns that weight more in left will be marked into class 1 while in right marked into class 2.

Cat is still alive in the superposition state which is analogous to that cup of water still in the cup. After the decoherence of the $|Scat\rangle$ happened at the decay of the atom, the $|Scat\rangle$ would collapse into one of the $|Dcat\rangle\ and\ |Acat\rangle$ which are the eigenstates it consists with the probability equal to $\frac{\left|\frac{\sqrt{2}}{2}\right|^2}{\left|\frac{\sqrt{2}}{2}\right|^2+\left|\frac{\sqrt{2}}{2}\right|^2} = \frac{1}{2}$.

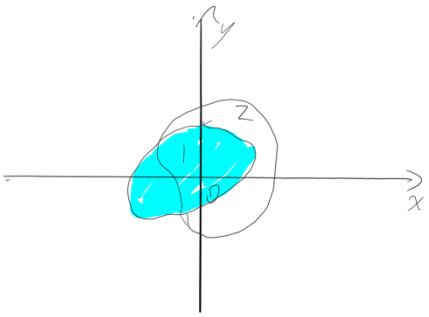

Fig.2 The Blue Pattern of Water Belongs to Class 1 and the Transparent Pattern Belongs to Class 2

In general case, for more concise analogy, if the probabilistic property of the collapse has already been understood, then a superposition $|\psi\rangle$ can just be assimilated to a cup of water in container A with cubic shape connected with multiple tubes steering to different containers, say, B containers, and only one tube can be open for each time, each container that the tubes can lead to should be assimilated to an eigenstate of the measured physical quantity. After that, a collapse is just corresponded to a random opening of one of these tubes, which leads the water into containers of other shapes. The water will change its shape into the shape of B containers when one tube is opened for a time, and this process is analogous to that a superposition collapse into an eigenstate probabilistically.

According to quantum mechanics, the probability of a state ψ collapsing into each eigenstate is $\frac{|c_i|^2}{\sum_i |c_i|^2}$, where c_i is the parameter before each states in the unfolding of the whole state by the complete set of eigenstates of the measured quantity.

$$\psi = \sum_i c_i \psi_i \tag{3}$$

$\{\psi_i\}$ is a set of eigenfunctions of the measured physical quantity, this set should have completeness because of the measurability of physical quantities. In this assimilation, different shapes of the containers assimilate to different sets of physical quantities that are measured. A measurement makes these physical quantities to have definite values (simultaneously for a set of physical quantities), and these confinements that the states should have definite values of every physical quantity in the set of physical quantities of the meas-

urement form something appropriately like various shapes of containers, each set of physical quantities confine the matter into a states of its shape.

Heisenberg's uncertainty principle pointed out that sometimes a physical quantity may be uncertain for a state, and this state is called a superposition of the eigenstates of this physical quantity. According to the arguments above, this does not mean that this physical quantity simultaneously has multiple values, such as an electron at an eigenstate of the energy in an atom cannot be regarded as having multiple positions. The case is that this electron just stays in a state that has no certain position, only changing it into an eigenstate of position can have a definite position, to have such an eigenstate, a measurement of position should be taken and the electron should change its state from energy eigenstate $|\psi_E\rangle$ to a position eigenstate $|\delta(\vec{r})\rangle$. The probability for each $|\delta(\vec{r})\rangle$ depends on $\frac{|C(\vec{r})|\delta(\vec{r})\rangle|^2 d^3\vec{r}}{\langle\psi_E|\psi_E\rangle}$ where $|\psi_E\rangle = \int |\delta(\vec{r})\rangle\langle\delta(\vec{r})|\psi_E\rangle d^3\vec{r}$, $\langle\delta(\vec{r})|\psi_E\rangle = \psi_E(\vec{r}) = C(\vec{r})$. The value of each $\frac{|C(\vec{r})|\delta(\vec{r})\rangle|^2 d^3\vec{r}}{\langle\psi_E|\psi_E\rangle}$ equals to $|\psi_E(\vec{r})|^2\vec{\mathrm{r}}$, that is exactly the statistical interpretation to wave function that put forward by Born.

To make it clear, a superposition is just an independent state that is different from the eigenstates it contains, and this does not mean that it has multiple eigenvalues of the physical quantity which these eigenstates belong to, but just that it stays in a state different from those eigenstates, the set of physical quantities used by the measurement determines what kinds of states the matter would stay. A physical quantity can be uncertain in a state, and an eigenstate of one physical quantity can probably be a superposition state of another quantity's eigenstates.

Since same matter may have different states, the paradox in the explanation of the wave-particle duality can be solved by this argument: when particle stay in momentum eigenstates, they have definite momentums without definite positions, and vice versa. How things have multiple kinds of properties? For same thing can stay in different states, it is therefore able to have different kinds of property in different kinds of states. Multiple kinds of properties of same matter exist in different kinds of states it may stay in.

After all, uncertainty principle reveals that matter can be at various states on which same matter can have different kinds of properties. In that way, same matter can simultaneously have multiple kinds of properties, such as famous wave-particle duality brought up by Bohr. In a superposition of a physical quantity's eigenstates, this quantity will have no certain value, only with the probability distribution of collapsing into each eigenstate if a measurement was taken. It will be interpreted in the next section about what a measurement means to the matter

2 The Collapses of Wave Packets

As mentioned before, uncertainty principle enables matters staying in different states, and the eigenstate of one physical quantity may be a superposition state of another quantity's eigenstates. As the state changing, its properties would also change consequently. This process changing the properties of matter is so-called wave packet collapse.

When a measurement is taken, what people did is just a change to the condition of the state. This makes the state become not stable anymore under the new condition and therefore collapsed into a new state that is stable under this condition. For example, a momentum eigenstate can be decomposed by position eigenstates

$$\int d^3\vec{r}|\vec{r}\rangle\langle\vec{r}|\vec{p}\rangle = |\vec{p}\rangle \tag{5}$$

$$\langle\vec{r}|\vec{p}\rangle = e^{i\vec{r}\cdot\vec{p}} \tag{6},$$

this is a wave packet that has definite momentum but no certain position.

According to $\Delta r \cdot \Delta p \geq \frac{\hbar}{2}$, in this case $\Delta r \to \infty$ due to $\Delta p \to 0$. And when one tries to measure the position of this moving particle, the state $|\vec{p}\rangle$ must collapse into one $|\vec{r}\rangle$ eigenstate with the probability $|\langle\vec{r}|\vec{p}\rangle|^2 d^3\vec{r}$. Between this change from a $|\vec{p}\rangle$ into a $|\vec{r}\rangle$, there is a collapse of the wave packet $|\vec{p}\rangle$. This collapse is a process like things falling from a high place to a low place.

The substantial of measurements in quantum mechanics in fact are alternations of physical quantity sets that should have definite values. Each set of quantities forces the state to have eigenvalues of every quantities of this set. And any state tends to stay in a mutual eigenstate of all the physical quantities of this set.

In a word, the object of a measurement is any state that is stable or unstable when the physical quantities to be measured is determined, and the way of measurement is to change the condition of the objective state so that make it have definite values of the physical quantities that are measured. The objective state can be an eigenstate of other physical quantities, such as an eigenstate of one-dimensional infinite potential trap. The eigenstate of one physical quantity may be a superposition state of another physical quantity's eigenstates.

Different conditions of the state mean measuring by different sets of physical quantities, and different sets of physical quantities render different stages of stable state, i.e., different mutual eigenstates. Which states the matter would stay depends on the sets of physical quantities by which it is measured, and determines which property would the matter perform. Same matter can therefore have multiple kinds of properties and choosing different sets of physical quantities would make it possess different kinds of properties.

The collapse of a wave packet changes the state of this wave packet into one of the eigenstate of the new set of physical quantities according to the intensity proportion of each eigenstate in this state: $\frac{|c_i|^2}{\sum_i |c_i|^2}$ in $\psi = \sum_i c_i \psi_i$, where i can also be a continuous variable and the proportion would be $\frac{|c_i|^2 di}{\int |c_i|^2 di}$. Since this process is totally probabilistic, it is equal to a real classical probabilistic model. And this nature can easily be used to solve a big problem in computational physics: the creation of real random numbers.

3 Specific Generations of Real Random Numbers

The collapse of wave packets, as argued before, is totally probabilistic. For this reason, the generation of real random numbers can just focus on which kind of collapse is convenient to use.

a) Qubits in quantum computers

Quantum computer is a kind of computer that uses superposition states to make computation instead of using only one eigenstate among the superposition. And the time it saves may be as long as the age of the universe or even longer than that. The reason why it can manage this is because that a classical computer needs to compute each eigenstate one by one, the more eigenstates needed to be computed, the more time is needed. If there are enough large number of eigenstates to compute, then the algorithm would be impossible to realize. But for a quantum computer, with the use of qubits which consist of all the eigenstates that need to be compute, all the states can be computed simultaneously, therefore those banned algorithms for classical computers would be feasible to realize and an enormous amount of time can be saved. A qubit is a superposition state of classical bits, a collapse from a qubit to a bit obeys the classical probabilistic distribution, thus, a real random number can be created through this process.

b) Boson sampling of a single photon

The same as the qubits, this is also a case of wave packets collapse. And different result of the collapse can create different number, therefore, a real random number can be generated in this process where each result of the sampling was mapped to different numbers.

c) Programmed electronic screen

The electron-wave will interfere with each other even when there is only one electron, and this indicates that an electron itself should be in a form of wave when it is propagating to the screen, while it changed into a particle when stopped at the screen. As a result, the position of the electrons shot on a screen would be random while their distribution satisfies the intensity distribution of the wave of their motions.

In most cases, the sampling of single wave packet collapse is too hard to realize due to the microscopic property of quantum world. To make it easier to operate, one can make a screen that is able to precisely

record the positions of each electron hitting on it. Confining the number of the electrons to be recorded of each shooting into a certain amount, an inhomogeneous diffraction pattern would be created on the screen after each time of shooting electrons into the screen through some slits, which makes them diffract with a wanted waveform that enables one to plan the map between the generated pattern on the screen and the number it corresponds to. For example, if the diffraction pattern is a double-slit diffraction as the Fig.2, then a map can be defined like this: if there are more electrons on the upside of the screen, then the real random number to be created is 1; If more electrons emerge on the downside of the screen, then the real random number will be 0. With a series of 0 and 1, a real random binary number can be created, a real random number in tens can consequently be generated. One can design various kind of real random number generation model like what was done in this example.

d) Collapses of Schrödinger's Cats

As mentioned above, each time of the decay of the atom is a collapse of a wave packet, and whether the cat is dead or alive is really probabilistic. The superposition of the cat before the decay of the atom is

$$|Scat\rangle = \frac{\sqrt{2}}{2}(|Dcat\rangle + |Acat\rangle) \qquad (7),$$

the dead cat and the alive cat respectively have a probability of 50% to be created after the decay. If every dead cat is mapped onto 0 and alive cat is mapped onto 1, then a serious of binary number can be generated if we use enough number of Schrödinger's cats. This number will also be a real random number. The only pity is that the radioactivity of the atom will do harm to human and this cannot be used in practice.

4 Conclusion and Perspective

With the approvement of uncertainty principle and the probabilistic process of wave packet collapse, a real random number can simply be created by a collapse from a superposition to an eigenstate it consists of. The collapse of a qubit into a bit, the sampling of a single photon, the incomplete pattern of certain numbers of electrons' diffraction, and even the diffraction of light can be used to generate real random numbers. And people do not need to worried about the high price or high risk to health when generating real random numbers in these ways.

In modern computer science, artificial intelligence can only be realized by pseud random numbers. Such as the AI that can work out the heliocentric theory in one day which is developed by Renato Renner, what will happen if applying real random numbers into these AI? As it is known, human's actions are totally probabilistic. If AI have the property of probabilistic, it may replace the human being and become a more advanced kind of human.

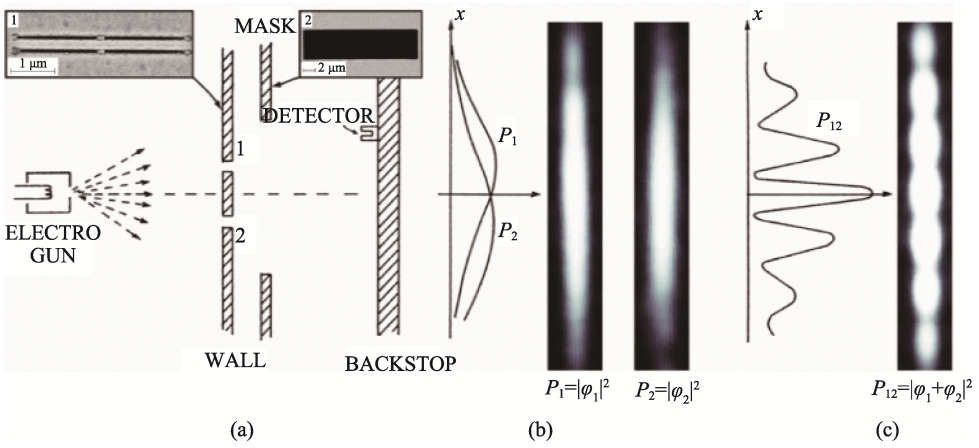

Fig.3 Single Electron Diffraction

Quantum mechanics brought us into a question of what makes a man. What's the difference between a man and a thing? For our human's world is so interesting, it is hoped that AI can just be some kinds of animals but not human.

Appendix

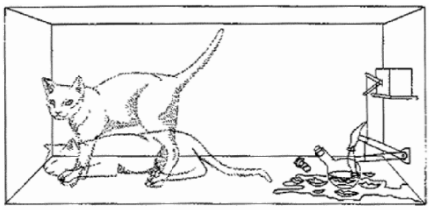

Fig.4 Schrödinger's Cat

Schrödinger's cat is confined in a black box together with a radioactive atom which has 50% probability to decay and 50% not to decay. If the atom decays, the α particle will trig the Geiger-counter and the hammer will therefore hit a flask of prussic acid killing the cat; if the atom does not decay, the cat will survive.

The paradox is, for the atom stay in a superposition of decay and not decay, the cat will also stay in a superposition of being dead and being alive, this contradicts with our daily life, what on earth happened? How can the cat be dead and alive simultaneously?

References

[1] Heisenberg. *The physical principles of the quantum theory*. (translated by Eckart and F. C. Hoyt. [M]. p1-15.

[2] A. Zecca. Diffraction of Gaussian wave packets by a single slit. [J]. *Eur. Phys. J. Plus* (2011) 126: 18

[3] Daniela Frauchiger1 & Renato Renner1. Quantum theory cannot consistently describe the use of itself. [J]. *Nature communications*.

[4] Raoul Nakhmanson. Wavepacket and its collapse. [J].

[5] Bækkegaard, L. B. Kristensen, n. J. S. Loft, c. K. Andersen, D. Petrosyan& n. t. Zinner. Realization of efficient quantum gates with a superconducting qubit circuit. [J]. *Nature reports*.

[6] D. Sen. The uncertainty relations in quantum mechanics. [J]. *CURRENT SCIENCE*, VOL. 107, NO. 2, 25 JULY 2014.

[7] Roger Bach, Damian Pope, Sy-Hwang Liou and Herman Batelaan. Controlled double-slit electron diffraction. [J]. *New Journal of Physics 15* (2013) 033018.

[8] Bochu Qian. *Quantum Mechanics*. [M]. Higher Education Press, Beijing.

[9] Davide Castelvecchi. AI COPERNICUS 'DISCOVERS' THAT EARTH ORBITS THE SU. [J]. *Nature* | Vol 575 | 14 November 2019

[10] DAVIDE CASTELVECCHI. Quantum puzzle baffles physicists. [J]. *NATURE* | VOL 561 | 27 SEPTEMBER 2018.

[11] Michael A. Nielsen, Issac L. Chuang. *Quantum Computation and Quantum Information*. [M]. Tsinghua University Press.

Author Biographies

ZHANG Jiayi, born in Lanzhou, Gansu in 1995. He graduated from theoretical physics major of Lanzhou University in 2017 and entered the graduate school of Lanzhou university in 2019 via national entrance examination of graduate school. He is now a master student studying in theoretical physics, his study interest includes every science subject especially mathematics and theoretical physics, such as group theory, quantum physics and relativity.

Email: zhangjiayi19@lzu.edu.cn