International Journal of Engineering, Mathematical and Physical Sciences
ISSN: 2517-9934
Vol:2, No:2, 2008

Impact of the Existence of One-Way Functions on the Conceptual Difficulties of Quantum Measurements

Arkady Bolotin

***Abstract*—**One-way functions are functions that are easy to compute but hard to invert. Their existence is an open conjecture; it would imply the existence of intractable problems (i.e. **NP**-problems which are not in the **P** complexity class).

If true, the existence of one-way functions would have an impact on the theoretical framework of physics, in particularly, quantum mechanics. Such aspect of one-way functions has never been shown before.

In the present work, we put forward the following.

We can calculate the microscopic state (say, the particle spin in the *z* direction) of a macroscopic system (a measuring apparatus registering the particle *z*-spin) by the system macroscopic state (the apparatus output); let us call this association the function *F*. The question is: can we compute the function *F* in the inverse direction? In other words, can we compute the macroscopic state of the system through its microscopic state (the preimage F^{-1})?

In the paper, we assume that the function *F* is a one-way function. The assumption implies that at the macroscopic level the Schrödinger equation becomes unfeasible to compute. This unfeasibility plays a role of limit of the validity of the linear Schrödinger equation.

***Keywords*—**One-way functions, **P** versus **NP** problem, quantum measurements.

I. INTRODUCTION

LET us consider a macroscopic system M (a measuring apparatus) whose macroscopic state Ξ results from the state Q of a microscopic system S interacting with M ; so we can put

$$f : Q \to \Xi \quad . \qquad (1)$$

On the other hand, by the definition of the system $S+M$, its macroscopic state Ξ provides information about the system microscopic state Q, that is, if we know Ξ, we certainly know Q:

$$F : \Xi \to Q \quad . \qquad (2)$$

This implies, that the function F must be *computationally feasible* (otherwise, M cannot be a device for measurement).

For example, assume that in a Stern-Gerlach spin analyzer, if a printer connected to the analyzer prints *one*, the incoming electron has *z*-spin equal to $+1/2$, and if the printer prints *zero*, the electron *z*-spin is $-1/2$. Then if we know the macroscopic state of the analyzer (the printout 1 or 0), it is easy to calculate the analyzer microscopic state (spin up $\left|\uparrow_z\right\rangle$ or spin down $\left|\downarrow_z\right\rangle$ in the *z* direction):

$$F : \{1;0\} \to \left\{\left|\uparrow_z\right\rangle;\left|\downarrow_z\right\rangle\right\}$$

$$\text{defined by } F(\Xi) = \begin{cases} \left|\uparrow_z\right\rangle, & \text{if } \Xi = 1 \\ \left|\downarrow_z\right\rangle, & \text{if } \Xi = 0 \end{cases} \qquad (3)$$

The image of the function $F : \Xi \to Q$ is the set of all possible microscopic states that the function F associates with macroscopic states. Accordingly, the preimage (the inverse image) of F is the function $f : Q \to \Xi$, which determines the set of all possible macroscopic states that the function f associates with microscopic states.

In the physical theoretical framework, it is presupposed that regardless of the system $S+M$ complexity, the preimage $F^{-1} \equiv f$ is feasible to compute as much as the function F itself.

This belief has never been questioned systematically. However, according to the conjecture of the one-way function existence, it could be that the function F is hard to invert, i.e. its preimage f is computationally unfeasible.

One-way functions are mathematical objects, which are based on the conjecture of computationally unfeasible (intractable) problems. That is, the one-way function existence would imply that the complexity classes **P** and **NP** are not equal [1-3].

A problem is in the **P** class if its solution time is bounded by a polynomial.

A problem is assigned to the **NP** class if it is solvable in polynomial time by a nondeterministic Turing machine, or equivalently, if the problem positive solution can be verified in polynomial time given the right information [4,5].

If **P** ≠ **NP**, then the solution of **NP**-problems requires (in the worst case) an exhaustive search, while if **P** = **NP**, then asymptotically faster algorithms may exist. Nonetheless, in practice, a **NP**-problem may be tractable if the problem size is relatively small. Besides, a problem might not belong to **P** but

Arkady Bolotin is with Ben-Gurion University of the Negev, Beersheba 84105, Israel (phone: 972-8-6477458; fax: 972-8-6477638; e-mail: arkadyv@bgu.ac.il).

be solved quickly if we accept an approximate or probabilistic solution. In fact, this is a common approach to solve problems in **NP** not known to be in **P** [5].

Even though the existence of one-way functions is still an open conjecture, it would be interesting to analyze its possible impact on some difficult problems in physics and philosophy such as *quantum measurements*.

II. The Problem of Measurement in Quantum Mechanics

In quantum mechanics, any observable quantity corresponds to an eigenstate of a Hermitian operator. The linear combination of two or more eigenstates results in quantum superposition of two or more values of quantity.

The problem naturally arose as to why macroscopic objects do not seem to display quantum superposition. In 1935, Erwin Schrödinger devised a well-known thought experiment, now known as *Schrödinger's cat*, which highlighted this problem [6].

In this experiment, a Geiger counter M monitors a radioactive source S, which is so weak "that perhaps in the course of one hour one of the atoms decays, but also, with equal probability, perhaps none" [6]. Detection of a decaying atom triggers a spray of poisonous gas into the box occupied by a cat. "If one has left this entire system $S+M$ for an hour, one would say that the cat still lives if meanwhile no atom has decayed. The first atomic decay would have poisoned the cat. The psi function for the entire system $S+M$ would express this by having in it the living and the dead cat mixed or smeared out in equal parts" [6].

The essence of the problem is this. We know that superposition of possible outcomes must exist simultaneously at a microscopic level (because we can observe interference effects from there). We know that the cat in the box is dead, alive or dying and not in a smeared out state between alternatives. So, when and how does the model of many microscopic possibilities resolves itself into a particular macroscopic state?

The disappearance of macroscopic superpositions is the major issue; the fact that such superpositions cannot be resolved at any stage within the linear Schrödinger equation may seen as the major difficulty of quantum mechanics [7].

A. Assumption

If we know the macroscopic state Ξ of the system $S+M$ (the cat is dead or alive), we can easily calculate the system microscopic state Q (the radioactive atom has decayed or not decayed).

We will assume that $F:\Xi\to Q$ is a one-way function.

In other words, we will assume that whereas it is easy to compute the microscopic state of the system $S+M$ through its macroscopic state, the inverse operation – given the system microscopic state to find the macroscopic one – is hard.

B. Schrödinger Equation is in **NP**

In quantum mechanics, both microscopic and macroscopic state of the system $S+M$ is described by the system state vector $\left|\Psi\right\rangle$.

As the state of the system $S+M$ changes over time, $\left|\Psi\right\rangle$ is a function of time. The quantitative description of the time evolution of the state vector $\left|\Psi\right\rangle$ is provided by the Schrödinger equation:

$$\hat{H}\left|\Psi\right\rangle = i\hbar\frac{\partial}{\partial t}\left|\Psi\right\rangle \quad , \qquad (4)$$

where $\hat{H}$ is the Hamiltonian operator of the system $S+M$.

Because of the fact that the Hamiltonian typically includes partial derivatives with respect to the position variables, the Schrödinger equation is a difficult linear partial differential equation to solve.

Actually, it happened to be very difficult to find analytical solutions for Hamiltonians of even moderate complexity [8]. The Hamiltonians to which we know analytical solutions, such as the hydrogen atom, the quantum harmonic oscillator and the particle in a box, are too idealized to adequately describe most systems. Therefore, for most systems only *numerical* solutions to the Schrödinger equation can be found.

With that, an exact numerical polynomial-time algorithm for solving the Schrödinger equation for a system of the arbitrary complexity is unknown. This entails, that for a given system, it might be necessary to test each possibility sequentially in order to determine if it is the solution (*exhaustive search*).

Conversely, if a solution $\left|\Psi\right\rangle$ to the Schrödinger equation is somehow known, then demonstrating the correctness of the solution $\left|\Psi\right\rangle$ can be done easy (i.e. in polynomial time).

In brief, verifying that $\left|\Psi\right\rangle$ is a solution to the Schrödinger equation is much faster than finding $\left|\Psi\right\rangle$ in the first place.

All this suggests that the Schrödinger equation is in the **NP** complexity class.

If it turned out that **P** does not equal to **NP**, it would mean that for a given system the Schrödinger equation *could only be solved by exhaustive search in the worst case*. (Otherwise, if **P** = **NP**, it would mean that there exists an efficient solution method for any Hamiltonian, or, in other words, that the Schrödinger equation is as easy to compute as to verify.)

C. Macroscopic Superposition

The crux of the difficulties with the Schrödinger's cat experiment is the presupposition that the Schrödinger equation can be *computable* (i.e. computed quickly or in a reasonable amount of time) *at any stage* of the measuring chain, which starts with the atom decay and goes on until it reaches the macroscopic state.

If the Schrödinger equation is really computable at any stage, then there is nothing to prevent transformation of "an indeterminacy originally restricted to the atomic domain into macroscopic indeterminacy" [9]. As the recent proof of the "insolubility theorem" goes, by sticking to the linear Schrödinger equation we stuck also with the result that at the end of the measurement process (i.e. at the macroscopic level), there must be "superpositions of macroscopically distinct states of the apparatus, and in general of a macro-system" [10].

Therefore, the assumption proposed in this paper (which entails that the Schrödinger equation – the **NP**-problem – is not in **P**) might be "an additional ingredient" to the theory in order to avoid macroscopic superpositions.

Indeed, form the assumption follows that while for the initial stages of the measuring chain – when the number of degrees of freedom is still limited – the Schrödinger equation can be computable (tractable), *at the macroscopic level it cannot be solved efficiently*.

For example, if constituent quantum particles of the macroscopic measurement apparatus M strongly correlate with each other, then the dimension of the Hilbert space describing M as a system of *N* such particles will scale exponentially in *N*. This makes an exact numerical solution for M unfeasible: every time an extra particle is added to M, the computational resources would have to be doubled.

This brings us to the following question. If a macroscopic solution of the Schrödinger equation is unfeasible, can we describe a macroscopic state of the composite system $S+M$ by a wave function?

The answer to this question depends on how the word "unfeasible" is explained.

For instance, a computationally unfeasible problem might be solved analytically one day. In addition, even if only numerical solutions to the problem are possible, new computing models such as quantum computers may be able to solve it quickly.

However, to solve analytically the Schrödinger equation for a macroscopic system $S+M$ means to solve a system of around 10^{23} simultaneous differential equations. It is difficult even to imagine how this solution would look like. Perhaps humans may not be able to solve such system analytically.

As to numerical solutions, a proof **P** ≠ **NP** would guarantee that a polynomial-time algorithm for a **NP**-problem would never be found.

Furthermore, there is strong evidence that the solution of the Schrödinger equation for an arbitrary macroscopic system is unfeasible even on a quantum computer [11].

Therefore, we believe that the answer to the above question should be negative. That is, if the Schrödinger equation is in **NP** and **P** ≠ **NP**, then we will never be capable of affirming that the system $S+M$ is in a "blurred" state containing simultaneously the dead and alive cat.

D. Wave Function Collapse

Suppose, at time t, when the measuring chain begins, the state of the microscopic system S is represented by the superposition $\sum c_n|\psi_n\rangle$, where $|\psi_n\rangle$ are state vectors corresponding to possible states of S (the decayed and undecayed atom for instance), $\{c_n\}$ is some set of complex numbers; so the initial state of the entire system $S+M$ will be described by

$$|\Psi\rangle = \sum_n c_n |\psi_n\rangle|\phi\rangle \quad , \tag{5}$$

where $|\phi\rangle$ represents the initial state of the measuring apparatus M.

Then, at time t', when the measuring chain reaches the macroscopic level, we should look for the solution of the Schrödinger equation in the following form:

$$|\Psi\rangle = \sum_n c_n |\psi_n\rangle|\phi_n\rangle \quad , \tag{6}$$

where $|\phi_n\rangle$ are state vectors corresponding to possible states of M (the printer 1 and 0 output for instance, or, the dead and living cat).

However, according to the proposed assumption, at the macroscopic level the Schrödinger equation is intractable: *it can be solved in theory but cannot be in practice*.

So, we cannot really compute the function (6). This means that in practice the Schrödinger equation cannot predict the state of the system $S+M$ at t' (i.e. at the macroscopic level).

Alternatively, quantum mechanics gives us additional statistical information via the so-called Born statistical interpretation (*the Born's rule*): the probability of the system $S+M$ being registered at t' in one of the possible states represented by $|\psi_n\rangle|\phi_n\rangle$ is

$$\Pr\{|\psi_n\rangle|\phi_n\rangle\} = |c_n|^2 \quad . \tag{7}$$

The rule (7) does not depend on the solution of the Schrödinger equation; and the probability calculation through (7) can be done easy (it is in **P**).

In short, we cannot predict in practice the state of the system $S+M$ at the macroscopic level (because the Schrödinger equation is in **NP**), but we can predict the probability of each possible macroscopic state of $S+M$ (because the statistical interpretation is in **P**).

Graphically, all the above can be presented in a form of the following table.

TABLE I
THE DISAPPEARANCE OF MACROSCOPIC SUPERPOSITIONS
AND THE RELATION BETWEEN THE COMPLEXITY CLASSES **P** AND **NP**

<table>
<tr><td colspan="2" rowspan="3">Size of the problem
(number of degrees of freedom involved)</td><td colspan="3">Complexity classes</td></tr>
<tr><td><b>NP</b>-problem</td><td>≠</td><td><b>P</b>-problem</td></tr>
<tr><td>Schrödinger equation
(time evolution)</td><td></td><td>Born’s probability rule
(observation and measurement)</td></tr>
<tr><td rowspan="2">↓</td><td>Microscopic level</td><td>Feasible</td><td></td><td>Feasible</td></tr>
<tr><td>Macroscopic level</td><td>Unfeasible</td><td></td><td>Feasible</td></tr>
</table>

The vertical arrow (at the left of the table) depicts the direction of the measuring chain. The diagonal arrow shows how quantum superposition resolves: the wave function “collapse” happens when the Schrödinger equation ceases to be tractable.

III. CONCLUSION

According to the most common point of view [12,13], the measurement problem, in a nutshell, runs as follows.

States of quantum mechanical systems are described by wave-like mathematical objects (state vectors) of which sums (superpositions) can be formed. Time evolution (the Schrödinger equation) preserves such sums. Thus, if the given state of an electron S is described by superposition of, say, two state vectors corresponding to spin in *z*-direction equal $+1/2$ and spin in *z*-direction equal $-1/2$, and we let it interact with a measuring apparatus M, the state vector of the entire system $S+M$ will be a sum of two components, one in which the apparatus has coupled to (has registered) *z*-spin $=+1/2$, and one in which the apparatus has coupled to (has registered) *z*-spin $=-1/2$.

The problem is that while we may accept the idea of the microscopic state of the system $S+M$ being described by such sums, we cannot even begin to imagine what it would mean for the macroscopic state of the system $S+M$ to be so described.

We have two choices:

- either the macroscopic state is not described by such a sum, because the Schrödinger equation actually breaks down and needs to be modified (for example, by additional variables [14-16] or nonlinear Hamiltonian terms [16-19]),
- or it is, but then we need to understand what that means, and this requires giving an appropriate interpretation of quantum mechanics (like the history interpretation [21-23] or the “many-worlds interpretation” by Everett [24]).

As it turns out, it might be another choice. If the Schrödinger equation is in **NP**, and **P** ≠ **NP**, then we need neither to modify the Schrödinger equation, nor to seek a new interpretation of quantum mechanics. At the macroscopic level of the measuring chain, the Schrödinger equation becomes unfeasible to solve, and so macroscopic states cannot be in practice described by quantum superpositions.

REFERENCES

[1] Goldreich, O. Modern Cryptography, Probabilistic Proofs, and Pseudorandomness. Springer, 1999.

[2] Sipser M. Introduction to the Theory of Computation. PWS Publishing, Section 10.6.3: One-way functions, 1997, pp. 374–376.

[3] Papadimitriou C. Computational Complexity. 1st edition, Addison Wesley, Section 12.1: One-way functions, 1993, pp.279–298.

[4] Greenlaw, R., Hoover, H. J., and Ruzzo, W. L. Limits to Parallel Computation: P-Completeness Theory. Oxford, England: Oxford University Press, 1995.

[5] Cook, S. The P versus NP Problem http://www.claymath.org/millennium/P_vs_NP/Official_Problem_Description.pdf.

[6] Schrödinger, E. Die gegenwartige Situation in der Quantenmechanik, Naturwissenschaftern. 23: 1935, pp. 807-812; 823-823, 844-849. English translation: John D. Trimmer, Proceedings of the American Philosophical Society, 124, 1980, pp. 323-38.

[7] Laloë F. Do we really understand quantum mechanics? Strange correlations, paradoxes, and theorems. Am. J. Phys., Vol. 69, No. 6, 2001, pp. 655-701.

[8] Griffiths D. Introduction to Quantum Mechanics (2nd ed.). Prentice Hall, 2004.

[9] Schrödinger E. Proc. Cambridge Philos. Soc. 31, 1935, 555; 32, 1936, 446.

[10] Bassi, A., and Ghirardi, G.C. A general argument against the universal validity of the superposition principle. Phys. papers A, 275, 2000, 373-381.

[11] Lui, Y.-K., Christiandl, M., Verstraete, F. Quantum Computational Complexity of the N-Representability Problem: QMA Complete. Phys. Rev. Letters 98, 2007, 110503(4).

[12] Wheeler J. and Zurek W. (eds). Quantum Theory and Measurement. Princeton University Press, 1983.

[13] Krips H. Measurement in Quantum Mechanics. In Stanford Encyclopedia of Philosophy, http://plato.stanford.edu/entries/qt-

measurement/. First published Tue Oct 12, 1999; substantive revision Wed Aug 22, 2007.

[14] Wigner E. P. On hidden variables and quantum mechanical probabilities. Am. J. Phys. 38, 1970, 1005–1009.

[15] Wiener N. and Siegel A. A new form for the statistical postulate of quantum mechanics. Phys. Rev. 91, 1953, 1551–1560.

[16] Siegel A. and Wiener N. Theory of measurement in differential space quantum theory. Phys. Rev. 101, 1956, 429–432.

[17] Bohm D. and Bub J. A proposed solution of the measurement problem in quantum mechanics by a hidden variable theory. Rev. Mod. Phys. 38, 1966, 453–469.

[18] Pearle P. Reduction of the state vector by a non-linear Schrödinger equation. Phys. Rev. D 13, 1976, 857–868.

[19] Ghirardi G. C., Rimini A., and Weber T. Unified dynamics for microscopic and macroscopic systems. Phys. Rev. D 34, 1986, 470–491.

[20] Diosi L. Quantum stochastic processes as models for state vector reduction. J. Phys. A 21, 1988, 2885–2898.

[21] Griffiths R. B. Consistent histories and the interpretation of quantum mechanics. J. Stat. Phys. 36, 1984, 219–272.

[22] Gell-Mann M. and Hartle J. Classical equations for quantum systems. Phys. Rev. D 47, 1993, 3345–3382.

[23] Omnés R. Understanding Quantum Mechanics. Princeton U.P., Princeton, 1999.

[24] Everett III H. Relative state formulation of quantum mechanics. Rev. Mod. Phys. 29, 1957, 454–462.