

**A Plausibility Argument for
 $\#P \neq P$ from Physics**

Karl-Georg Schlesinger

Vienna, Preprint ESI 999 (2001)

February 26, 2001

Supported by Federal Ministry of Science and Transport, Austria
Available via <http://www.esi.ac.at>

A plausibility argument for $\#P \neq P$ from physics

Karl-Georg Schlesinger

Erwin Schrödinger Institute for Mathematical Physics

Boltzmannngasse 9

A-1090 Vienna, Austria

e-mail: kgschles@esi.ac.at

Abstract

Quantum computers have been shown to be capable to deal with problems like the factoring of numbers into primes in polynomial time, i.e. they might differ from classical Turing machines with respect to computational complexity, provided $\#P \neq P$. We reverse this conclusion by giving a plausibility argument for $\#P \neq P$ by arguing that - as a consequence of the basic rules of quantum mechanics - classical Turing machines should not be able to emulate quantum computers even if a polynomial time delay for the classical Turing machine is allowed. A generalization of the argument holds also for the case of replacing $\#P$ by NP .

1 Introduction

Quantum computers have been shown to lead to an exponential speed up in time as compared to the best known classical algorithms for some problems like the factoring of numbers into primes (see [Sho 1994]). On the other hand, it can be shown that those problems which can be solved by a quantum computer in polynomial time still belong to the class $\#P$ of classical complexity theory ([Sho 2000]). In conclusion, a quantum computer can only differ from a classical Turing machine with respect to computational complexity if $\#P \neq P$ (So, the still unresolved question if $\#P \neq P$ of complexity

theory is besides other famous problems another example where the question of the relationship between classical and quantum mechanics is touched.). We reverse this conclusion by giving a plausibility argument, based on the fundamental rules of quantum mechanics, to the effect that classical Turing machines should not be able to effectively emulate a quantum computer where we mean by an effective emulation one in which the classical Turing machine is allowed at most a polynomial time delay as compared to the quantum computer. A generalization of the argument holds also for the case of replacing $\#\mathbf{P}$ by \mathbf{NP} .

2 The argument

Observe, first, that a quantum computer is capable to simulate any quantum spin system (i.e. any quantum system with a finite dimensional Hilbert space) in real time, i.e. the simulation of a quantum spin system is clearly in the class of problems which are polynomial in time for a quantum computer. The simulation of a quantum system is therefore a problem in the class $\#\mathbf{P}$ for a classical Turing machine. Now, assume we would have $\#\mathbf{P}=\mathbf{P}$. Especially, the simulation of any quantum spin system would then be possible in an amount of time, depending polynomially on the input data, for a classical Turing machine. It follows therefore that any quantum spin system can equivalently be described as a classical one with a polynomially rescaled time axis.

The discrete state description of a classical Turing machine is, of course, only an idealized one. As a real physical system (which we will call a *physical Turing machine*) it has to be described as a classical mechanical system in space and time coordinates but we can approximate the discrete state description to an arbitrarily high degree of accuracy by a physical Turing machine. The same holds true for the quantum computer which is in reality also not a pure spin system but has a wave function with space and time coordinates. Again, we can approximate the quantum computer to any desired accuracy by a *physical quantum computer*. Note that the accuracy is a fixed prescribed value which one can require to hold for an arbitrarily long prescribed time.

It follows then that the physical quantum computer can be to an arbitrarily high degree of accuracy described as a physical Turing machine with a

polynomial rescaling of the time axis. If we choose the formulation of quantum mechanics as given by Bohm (see [Boh]), where we have a description for the quantum system in terms of trajectories, too, for the physical quantum computer, it follows that we can trace the trajectories of the physical quantum computer with an arbitrarily high accuracy by those of a physical Turing machine. But as a quantum mechanical system, the trajectories of the physical quantum computer have regions with sensitive dependence on initial conditions, especially, they are exponentially divergent (since quantum interference effects are decisive for quantum computation and one can without loss of generality consider a double slit experiment as the prototype of a quantum interference experiment, then. Indeed, in a concrete experimental situation one will normally observe the interference via fringes. But for the double slit one has sensitive dependence on initial conditions because the trajectories entering one of the valleys of the quantum potential are very rapidly driven apart, there. Near the bottom of the valley the quantum potential is nearly quadratic in the coordinate, leading to an exponential acceleration, see e.g. [Hol]). The physical Turing machine, on the other hand, does - by the way it is defined as a stable computing device - not have any sensitive dependence on initial conditions for its trajectories. As a consequence, we can not trace the trajectories of the physical quantum computer by it by employing a polynomial rescaling of time (with an exponential rescaling we could, of course, transform exponentially divergent trajectories into ones which do not have this property). So, this establishes a contradiction and we have to conclude that our assumption that $\#P=P$ is false.

Besides this, there are problems which are known to be in NP and have been shown to be solvable by a quantum computer in polynomial time (e.g. the factoring of a given number into primes, see [Sho 1994]). Let us assume now that $NP=P$, i.e. a classical Turing machine would be able to solve these problems in polynomial time, too. As we have seen, no polynomial rescaling of the time parameter can turn quantum interference effects into classical ones, i.e. we can without loss of generality assume that the quantum and the classical computer arrive at the conclusion just at the same time (This is the essential point of our argument since the usual no go theorems for a classical description of quantum systems apply to equal time axis, only. With the help of our considerations in the framework of the Bohm interpretation, we can get rid of polynomial time rescalings, now, since no polynomial rescaling allows to get away from sensitive dependence on initial conditions.). In contrast to the $\#P$ case, it is not implied, here, that we can simulate the whole quantum

mechanical time development by a classical system. But still we would get the outcome of a quantum interference process by purely classical means since the Shor algorithm makes decisive use of quantum interference. This is not possible by a classical theory satisfying *locality* (which can be assumed for the classical Turing machine, of course, e.g. it can be assumed to use basically only the electromagnetic interaction) as follows from well known no go theorems (see e.g. [Neu]).

Remark 1 *One might be tempted to argue that the process of extracting the information of the prime factors from the observation of the quantum state in the Shor algorithm destroys a lot of information, i.e. it would be an irreversible process and the existence of a classical algorithm determining the prime factors (in equal time than the quantum one) would not necessarily imply that the classical algorithm determines also the outcome of the quantum interference experiment. But without loss of generality, the classical algorithm may be assumed to operate reversibly. So, this would imply that we have an irreversible and a reversible physical process, both starting from a state where an integer number is given and both arriving at a state where we have the prime factors stored on the tape of a Turing machine. But irreversibility would mean that the two states have different entropy while reversibility would require the entropies to be equal. But this is a contradiction and we conclude that there has - in principle - to be a possibility to determine the result of the quantum interference experiment from the prime factors. So, if there is a classical algorithm determining the prime factors (in equal time than the quantum one), we have a classical system giving information which is equivalent to the outcome of a quantum interference experiment (on the side of the quantum system equivalent transformations on the information after measuring it are always allowed and can be considered as irrelevant for the question of no go theorems). Hence, we can apply the no go theorems.*

Since factoring into primes is known to be polynomial in time if the Generalized Riemann hypothesis is true (see [Mil]), this leads also to a physical argument against the validity of the Generalized Riemann hypothesis.

Acknowledgements:

I thank H. Grosse for discussions on the topics involved. Besides this, I thank the Deutsche Forschungsgemeinschaft (DFG) for support by a research

grant and the Erwin Schrödinger Institute for Mathematical Physics, Vienna, for hospitality.

References

- [Boh] D. Bohm, Phys. Rev. **85**, 166 (1952), Phys. Rev. **85**, 180 (1952).
- [Hol] P. R. Holland, *The quantum theory of motion*, Cambridge University Press, Cambridge 1993.
- [Mil] G. L. Miller, *Riemann's hypothesis and tests for primality*, J. Comput. System Sci. **13**, 300-317 (1976).
- [Neu] J. v. Neumann, *Mathematische Grundlagen der Quantenmechanik*, Springer, Berlin 1932.
- [Sho 1994] P. W. Shor, *Algorithms for quantum computation: discrete logarithms and factoring*, 35th Annual Symposium on Foundations of Computer Science (Santa Fe, 1994), 124-134, IEEE Comput. Soc. Press, Los Alamitos 1994.
- [Sho 2000] P. W. Shor, talk at the AMS conference *Mathematical Challenges of the 21st century*, Los Angeles, August 2000.