Some remarks on consequences of Shor’s Factoring Algorithm

Karl–Georg Schlesinger

Vienna, Preprint ESI 998 (2001)  
February 26, 2001

Supported by Federal Ministry of Science and Transport, Austria
Available via http://www.esi.ac.at
Some remarks on consequences of Shor’s factoring algorithm

Karl-Georg Schlesinger
Erwin Schrödinger Institute for Mathematical Physics
Boltzmanngasse 9
A-1090 Vienna, Austria
e-mail: kgschles@esi.ac.at

Abstract

The algorithm of Shor for factoring integers into primes shows that factoring can be done by a quantum computer in polynomial time. The question if this can also be achieved by a classical Turing machine, i.e. if the Shor algorithm is inherently quantum mechanical or if a classical system could do equally well, is still unresolved but linked to two of the most important open problems of mathematics, the so called NP problem and the Riemann hypothesis. Since the Shor algorithm makes decisive use of quantum interference, the physicist’s first guess would supposedly be that it should not be possible to put an equally powerful classical algorithm in its place. We give a plausibility argument from considerations in quantum mechanics in favour of this view.

1 Introduction

The question if factoring of an integer into primes can be done in a polynomial amount of time by a Turing machine is not only interesting as concerns the security of public key encryption systems but is also linked to two of the most important open problems of mathematics at once. The security of the most common encryption systems is based on the belief that factoring is a “hard” problem, i.e. the amount of time needed to compute the factors grows exponentially with the input data (the number which we want to factor). At
least, this is true for all the algorithms known so far. Suppose now for a
moment that this is not due to our ignorance of finding better algorithms
but that factoring can in principle not be achieved by a Turing machine in
polynomial time. Since factoring into primes is a problem which is known
to be of class $\text{NP}$, this would immediately solve the so called $\text{NP}$ problem
by showing that $\text{P} \neq \text{NP}$ (for the definitions of the complexity classes $\text{P}$
and $\text{NP}$ and the basic results used, here, the reader who is not familiar with
these can consult any of the introductory texts on complexity theory, see e.g.
[BDG]).

But there is another important link of the factoring problem which is even
more surprising since it relates to areas of mathematics which at first sight do
not seem to be related to complexity theory. As was proved by Miller ([Mil]),
the Riemann hypothesis (if valid) would imply that factoring can be done in
polynomial time. So, our above assumption would also immediately refute
the Riemann hypothesis (here, by Riemann hypothesis we will always mean
what is often called the Generalized Riemann hypothesis in the literature).

The general mathematician’s belief gives, of course, a simple answer to our
speculations. The Riemann hypothesis is true, hence factoring into primes
can be done in polynomial time and the fact that we can not do it at the
moment is simply due to our ignorance. On the other hand, we also believe
that $\text{P} \neq \text{NP}$, i.e. there are other problems of class $\text{NP}$ which can really for
principal reasons not be solved in polynomial time but the factoring problem
is simply a badly chosen example to test this case. From the view of pure
mathematics, everything is fine with this belief.

But in 1994 Shor proved by explicitly giving an algorithm (see [Sho]) that
factoring into primes can be done in polynomial time by a quantum com-
puter. So, the question if a classical Turing machine can also do factoring
in polynomial time can now be seen as the question if there exists a classi-
cal system which is equally effective computationally as the Shor algorithm
running on a quantum computer. With this reformulation, it is a physical
question, asking for possible principle limits of realizing properties of a quan-
tum system by a classical one. This type of questions leads to well known no

 go theorems (like the impossibility to describe a quantum system by a local
hidden variables theory) in other situations but none of these can directly
be applied, here. Nevertheless, since the Shor algorithm involves quantum
interference in an essential way, the general physicist’s first guess would sup-
posedly be that a no go theorem for polynomial factoring by a classical device
should also exist in this case.
In conclusion, the Shor algorithm puts a very fundamental question to us: Should we more believe in the Riemann hypothesis or should we give priority to our conviction that the use of quantum interference effects in the Shor algorithm should make polynomial time factoring a truely quantum mechanical phenomenon? The mathematician would supposedly answer that the Riemann hypothesis does not stand alone but our belief in it is tied to a whole conjectural landscape of mathematics in the form of properties of motives, L-functions and the Langlands program. Many physicists would maybe tend to answer on the contrary that the deeply non classical nature of quantum state space has become one of the corner stones of our understanding of nature and that in detailed experiments even the most bizarre features of quantum mechanics have always succeeded over our classical intuitions.

To avoid misunderstanding: As long as we can not apply a no go theorem on the physical side of the argument, there is, of course, no contradiction in the strict logical sense between the two positions. But there is a tension in the sense of which kind of belief will turn out to be the more fundamental one. The Shor algorithm either challenges our belief in the Riemann hypothesis or it might lead to a deep lesson about quantum mechanics in the sense that, as concerns computational complexity, quantum systems might be much more close to classical ones than we would think before hand.

In the rest of this paper, we will give a plausibility argument in favour of the general physicist's belief by some basic considerations in quantum mechanics.

2 The argument

Why can we not apply the usual no go theorems to the situation at hand? Suppose, factoring into primes could also be done in polynomial time by a classical Turing machine. Then there would be a classical device achieving the same results as the Shor algorithm on a quantum computer by at most a polynomial rescaling of time. We have to allow for this polynomial rescaling of time because two physical devices which are computationally equivalent can - by definition of the computational equivalence - always differ by such a rescaling. But it is the rescaling of the time axis which prevents the application of the quantum mechanical no go theorems to the situation (because they apply only to the case of equal time parameters for the quantum and
classical systems). Suppose, first, that we could do without this rescaling and describe both systems - the quantum mechanical and the classical one - by precisely one and the same time parameter. We can also assume without loss of generality that the classical system satisfies locality because we know that we can realize a classical Turing machine e.g. by using only electromagnetic interactions (we can even assume that we realize it by a particle billiard ball system, see [FT]). But we can not achieve the same results as those of a quantum interference experiment by a classical theory satisfying locality (see e.g. [Neu]). Observe that in a concrete experimental situation, the interference effect is e.g. observed by fringes in an interferometer, i.e. without loss of generality we may assume that we deal with the double slit as the prototype of interference experiment.

**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 in the way we did above.

In conclusion, if we could assume without loss of generality that we have identical time parameters for the classical and the quantum systems, we could
apply the no go theorems. We will now argue that we can, indeed, do this.

For convenience, we adopt the Bohm-de Broglie interpretation of quantum mechanics for this (see [Boh], [Hol]) because it allows for a description of the quantum system in terms of particle trajectories, too, and therefore leads to an easy handling of some dynamical aspects, especially, of some properties under rescaling of the time parameter. What we will argue for is that we can not get rid of quantum interference effects by polynomial rescalings of the time parameter. We take, again, the double slit as the prototypical example.

Describing the double slit experiment in the Bohm-de Broglie interpretation, we get regions with sensitive dependence on the initial conditions for the trajectories (because the quantum potential is near the bottom of its valleys approximately quadratic, therefore leading to an exponential divergence of trajectories, see e.g. [Hol]). But we can not get rid of this by a polynomial rescaling of time (of course, by an exponential rescaling one could turn exponentially diverging trajectories into ones not having this property). So, even after a polynomial rescaling of time, we still have sensitive dependence on initial conditions in the same regions as before and therefore a quantum potential of qualitatively the same nature. Especially, concerning computational accessibility, the system has not changed at all by the polynomial rescaling. So, we can, without loss of generality, always neglect such rescalings, here.

**Remark 2** That this point - that sensitive dependence on initial conditions can not be scaled away by polynomial rescalings of the time parameter - is essential is also shown by the fact that with this consideration done - without invoking the well known no go theorems - we can give an argument in favour of the weaker (as compared to the NP problem) \( P \neq \#P \) case (see [Sch] where the whole discussion is written down from a slightly different perspective).

In conclusion, we get a plausibility argument for the view that the polynomial time nature of the Shor algorithm should be an inherently quantum mechanical effect which can not be reproduced classically.

**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


