Physical consequences of P≠NP

Javier Rodríguez-Laguna
Mathematics Dept., Universidad Carlos III de Madrid, Spain
(Dated: Oct 13, 2010)

Computational complexity theory is applied to *simulations* of adiabatic quantum computation, providing predictions about the existence of quantum phase transitions in certain disordered systems. Moreover, bounds on their entanglement entropy at criticality are given. Concretely, physical consequences are drawn from the assumption that the complexity classes **P** and **NP** differ.

PACS numbers: 02.60.Pn 05.30.Rt 03.65.Ud 89.70.Eg

I. INTRODUCTION

Global optimization is one of the most important computational problems in science and technology. But beyond its practical implications, it is also of deep theoretical interest when viewed from the broader perspective of computational complexity theory[1,2]. Problems are ranged into an intrincate classification by theoretical computer scientists. For example, problems in class **LIN** are specially simple, since they can be solved in linear time by a Turing machine. Of special interest are the complexity classes **P** and **NP**. Problems in **P** can be solved in polynomial time. Problems in **NP**, on the other hand, are characterized by the fact that *every candidate solution* can be evaluated in polynomial time. It is intuitively clear that **P**⊆ **NP**. The important open question is whether **P**=**NP**. It is widely believed by the scientific community that the answer is *no*. The implications of a positive answer to that question would be of utter practical importance. A subset of **NP** with special importance is the set of **NP**-complete problems. Those are problems such that, if a polynomial solution is found for any of them, then all **NP** problems will get immediately a polynomial solution. Therefore, finding a polynomial solution to any **NP**-complete problem would immediately prove **P**=**NP**.

All those complexity classes are defined with respect to an abstract computer, the *Turing machine*. Physical devices designed to solve a particular problem need not be subject to that restriction, i.e.: a **NP**-complete problem *might* be solved in polynomial time by a physical device even if **P**≠**NP**. The reason is that *Nature need not be a Turing machine*. Notwithstanding, *simulations* of physical processes on classical computers are bound by the previous hierarchy of classes, since they are (approximately) Turing machines. If **P**≠**NP**, any attempt to solve a **NP**-complete problem in polynomial time with a simulation of a physical process on a classical computer must fail. The reasons for the failure will be deducible from the simulation details, and insight about the underlying physical process might be obtained.

In this work we apply the results in complexity theory to quantum many-body physics. Also, we will assume that **P**≠**NP**, and extract physical consequences. These consequences might not be found in experiments, thus proving the assumption false. The main thesis is that, if there were no quantum phase transitions (QPT) in certain adiabatic routes, or if they were not of the appropriate kind, a classical computer simulating that physical procedure would be able to solve **NP**-complete problems in polynomial time. Thus, the existence of the aforementioned QPT is proved by contradiction.

This paper is divided as follows. In section II we remind the basics of our model problem: spin-glasses, along with the proposed physical approach to solution: adiabatic quantum computation[3] (AQC), also known as quantum annealing[4]. Section III focuses on our simulation procedure: quantum wavefunction annealing[5]. The main thesis is exposed in section IV, along with the conclusions.

II. THE PHYSICAL SYSTEM: SPIN-GLASSES AND ADIABATIC QUANTUM COMPUTATION

As an example throughout the discussion we will consider the spin-glass problem[6]. Given a graph $\mathcal{G}$ and a set of arbitrary coupling constants J_{ij} attached to each graph link, we define the (classical) spin-glass energy as

$$E = -\sum_{\langle i,j\rangle} J_{ij}\sigma_i\sigma_j \tag{1}$$

Where the σ_i are values in $\{-1,+1\}$ attached to each site. The classical spin-glass problem is to find the values for σ_i which minimize the previous energy. Because of the global Z_2 symmetry the solution is (at least) doubly degenerate.

If the graph is 1D, the problem is in **LIN** and, therefore, in **P**. If it is 2D, a non-trivial construction[7] also renders the problem polynomial. For higher dimensions, or for random graphs of fixed connectivity, the problem is **NP**-complete[8]. Even a 3D graph composed of two flat layers is **NP**-complete[7].

Among the many families of physical algorithms designed for global optimization, we will focus on *adiabatic quantum computation* (AQC)[3], also known as quantum annealing[4,9]. An AQC is implemented by a physical device which establishes an adiabatic route between two hamiltonians, H_0 and H_1, such that the ground state

(GS) of H_0 is easy to obtain and the GS of H_1 provides the solution to some problem. A GS may be difficult to achieve if the low energy spectrum is complex, as it happens in many disordered systems, which is typically the case with H_1. The adiabatic theorem ensures that, if the process is slow enough *and the gap never vanishes*, the ground state of H_1 will be obtained from that of H_0. AQC has been proved to be *universal* in the following sense: the results of any standard quantum computation can be simulated in polynomial time with an AQC[10].

The AQC strategy for the spin-glass problem sets the destination hamiltonian, H_1, as the quantum counterpart of eq. (1), promoting the $\{-1,+1\}$ values of σ_i to spin-1/2 operators[11]:

$$H_0 = -\sum_{\langle i,j\rangle} J_{ij} S_i^z S_j^z \tag{2}$$

To obtain H_0, we add to H_1 a source of quantum fluctuations, such as a uniform transverse magnetic field: $-\Gamma \sum_i S_i^x$. Thus, Γ is the the tunable parameter which connects both hamiltonians and, as a function of it, we obtain the random Ising model in a transverse field (RITF):

$$H(\Gamma) = -\sum_{\langle i,j\rangle} J_{ij} S_i^z S_j^z - \Gamma \sum_i S_i^x \tag{3}$$

where we see that $H(\infty) = H_0$ and $H(0) = H_1$.

Let $|\Psi(\Gamma)\rangle$ denote the ground state of the previous system as a function of Γ, which is only degenerate for $\Gamma = 0$. If $\Gamma \to \infty$, the ground state is found just by making all spins point in the X-direction:

$$|\Psi(\infty)\rangle = \otimes_{i=1}^{N} \left(|+\rangle + |-\rangle\right) \tag{4}$$

In this state, all classical configurations get exactly the same probability, so we may say that it is absolutely disordered. For $\Gamma \to 0^+$, on the other hand, the ground state provides the solution to the classical spin-glass problem.

Thus, the AQC strategy is to take $\Gamma \to \infty$, decrease it until $\Gamma = 0$, and then read the solution. The adiabatic theorem can be applied if the process is slow enough, assuming that the gap never vanishes.

The main difficulty during an AQC is to ensure adiabaticity. The probability of a jump to an excited state decreases exponentially with the energy gap, as reflected by the Landau-Zener formula[11]. Thus, if the system undergoes a phase transition and the energy gap closes, the velocity must be reduced in an appropriate way at that point, thus increasing the computational time.

It is tempting to try to extract conjectures relating the minimal gap along an AQC trajectory and the complexity class of the problem at hand. But these inferences are *not valid*, since the precise nature of the relation between the quantum and the classical complexity classes is not straightforward. Recent results of Altschuler and coworkers[12] cast doubts on the possibility of solving **NP**-complete problems in polynomial time using quantum computation, due to the very narrow gap distribution in disordered systems which can be deduced by Anderson's theorem.

III. THE SIMULATION: QUANTUM WAVEFUNCTION ANNEALING

As it was said before, in order to apply the results of computational complexity theory, we have to analyse algorithms running on Turing machines, not on arbitrary physical devices. Therefore, we will study *simulations* of adiabatic quantum computation running on a classical computer.

A first simulation approach to AQC is the use of path integral Monte-Carlo methods (PIMC)[11]. This technique does not suffer from Landau-Zener level crossings. But if an attempt is made to solve a **NP**-complete problem using it, we find that, at some moment, the system undergoes *critical slowing down*. This forces long relaxation times and reduces the efficiency of the procedure. The exact amount of this reduction is not easy to assess, due to the different complexity classes of probabilistic computation.

A different simulation procedure, quantum wavefunction annealing (QWA) is a fully deterministic classical algorithm and lends itself more easily to analysis[5]. The key feature of QWA simulation is that it computes the full wavefunction of the involved ground states. Roughly speaking, the QWA proceeds in this way:

- 1.- The initial hamiltonian, H_0 (i.e.: for $\Gamma \to \infty$) is diagonalized, obtaining $|\Psi(\infty)\rangle$ trivially.
- 2.- The transverse field Γ is decreased in a certain amount, $\Gamma \to \Gamma - \Delta\Gamma$.
- 3.- The ground state of $H(\Gamma)$ is obtained, *using the previous ground state as a seed*.
- 4.- Return to 2, if $\Gamma > 0$.

If this computation is done in a naive way, the number of stored components is 2^N, thus unfeasible. Instead, the wavefunctions are stored as matrix product states (MPS):

$$|\Psi\rangle = \sum_{s_1 \cdots s_N} \mathrm{Tr}(A^{s_1} \cdots A^{s_N}) \, |s_1, \cdots, s_N\rangle \tag{5}$$

where the A^{s_i} are $2N$ matrices of size $m \times m$. The total number of components in a MPS is, therefore, $2Nm^2$. Of course, m must be chosen *so that the ground state is always accurately represented*.

In order to obtain the ground state for a given value of Γ given the ground state for a larger value we use the

density matrix renormalization group (DRMG). This is just a variational scheme within the MPS subspace which allows to have adaptable values of m.

How large will m be? In order to find out, some concepts from quantum information theory are required. Let $S(i)$ be the entanglement entropy between sites $\{1,\cdots,i\}$ and sites $\{i+1,\cdots,N\}$ (in the DMRG literature they are the *left* and *right* blocks). The *maximal* entropy for a DMRG procedure is defined to be $\max_i S(i)$. Then, the value of m scales as $\exp(S)$[13].

Provided that m is large enough to accomodate the desired ground state, DMRG convergence is always achieved in a small number of sweeps, which does not scale with N. Another issue is the speed at which we are allowed to reduce Γ during the procedure. The number of Γ points does not scale with N, either. Of course, it is convenient that the region around criticality gets a higher resolution. Thus, an optimum annealing schedule will monitor the entanglement entropy as a function of Γ. But the key property of the procedure is that convergence is certain and fast if m is large enough and there is significant overlap between the two ground states.

Thus, it can be shown[5,14] that the total computing time of a QWA algorithm is polynomial in m. In fact, under mild assumptions it can be shown to scale like $T_{QWA}(N) \approx Nm^2 \approx N\exp(2S)$. Therefore, entanglement entropy, by itself, controls the efficiency of the procedure.

Other MPS simulation procedures have been proposed for standard quantum computation[14] or AQC[15], in the latter case using real time simulation (which may lead to loss of adiabaticity).

How does this maximal entropy grow with the system size? In homogeneous off-critical systems, the *area law* states that the entanglement entropy between two blocks of a system should grow as the number of broken bonds[16,17]. In disordered systems, on the other hand, the area law does not hold, yet it is a useful guide[18,19].

Let us focus on 1D systems. For a non-critical system it is known that S does not scale with N. But for a critical system, S will scale with the system size. In some cases, the size-dependence of S can be found via conformal field theory[13]. It has been shown that, for many critical 1D problems, $S(N) \approx \alpha\log(N)+\beta$. Thus, $T_{QWA}(N) \approx N^{2\alpha+1}$.

For higher dimension $d>1$, if the area law holds, the entropy will grow with the system size as $S(N) \approx N^{(d-1)/d}$, perhaps with logarithmic corrections at criticality. Therefore, the QWA time will increase exponentially. Nonetheless, for inhomogeneous systems, the area law need not hold.

A key element of the DMRG technique in non-1D system is the *ordering* of the sites, which we call the *DMRG path*. Evidently, a clever DMRG path may decrease the maximal entanglement entropy. A usual strategy is to establish the path so that the number of bonds between the left and right parts is always kept to a minimum[20]. If the area law is fulfilled, this should give a lower entanglement entropy and, therefore, lower m. Unfortunately, this is itself a difficult problem, so no attempt to achieve the global minimum is made, only to get a *good enough* solution.

Some recent works have been devoted to study the efficiency of the computation of MPS. Finding the ground states of a 1D quantum hamiltonian can be even **NP**-complete[21], although they are always nicely approximable[22]. This means that, although the *exact* problem may be **NP**-complete, it is always possible to get an *approximation*, within a factor ϵ of the ground state energy, polynomially both in time and in ϵ. The complexity class which conveys this is called fully polynomial-time approximation scheme (**FPTAS**)[23]. A problem may belong to both classes if the number of metastable states above the true ground state is really huge, within any energy range.

In any case, our scheme for getting the MPS which represents the ground state of our hamiltonian at any step of the adiabatic route is different. The adiabatic route makes it very easy to find the ground state if the entanglement entropy is bounded, *because it has been continuously dragged* from the ground state of H_0. The difficulty, of course, is always to traverse the quantum phase transition which may appear at some stage of this adiabatic route.

IV. PHYSICAL IMPLICATIONS OF COMPLEXITY THEORY

We will start this section by obtaining two very abstract implications of complexity theory in physics. After that, more concrete examples will be studied. Throughout this section we will adopt the notation that a hamiltonian belongs to a complexity class if the obtention of its ground state is a problem in that complexity class.

Let us consider an AQC connecting two hamiltonians H_0 and H_1, such that H_0 is in **LIN** but H_1 is not. E.g., H_1 may be in **P** but with an exponent larger than one, or perhaps with logarithmic corrections. This AQC must find a quantum phase transition (QPT) along the adiabatic path.

The reason can be stated as follows. Let us assume that no quantum phase transition is found on the way. Then, we can use a classical computer to run a QWA simulation of the AQC procedure. This simulation will take time $T_{QWA}(N) \approx N\exp(2S)$. If no QPT is found along the adiabatic path, the maximal entropy S will be bounded (i.e.: will not scale with N) and, therefore, the QWA results in a linear algorithm to achieve the ground state of H_1, against the assumption.

In the same line, we state that, if H_0 is **P** and H_1 is **NP**-complete, and **P**$\neq$**NP**, then any AQC connecting the two hamiltonians will find a QPT whose maximal entropy will grow faster than logarithmically.

Again the reason is easy to state. If the maximal entropy grows logarithmically, $S \approx \alpha\log(N)$, then the

QWA time will scale as $T_{QWA} \approx N \exp(2S) \approx N^{2\alpha+1}$. Therefore, the ground state of the H_1 hamiltonian would be found in polynomial time, against the assumption.

In general terms, we may say that the adiabatic connection of two hamiltonians with different complexity classes puts restrictions on the physics along the path. Nature's way to avoid violations of the results of complexity theory in AQC's is the *creation* of QPT of certain kinds. It can be regarded as a kind of *quantum censorship* to prevent us from solving hard problems easily.

In the spin-glass example, the obtention of the ground state of the RITF hamiltonian when $\Gamma \to \infty$ is a trivial problem, taking time $O(1)$. In 1D, the obtention of the classical spin-glass minimum energy state is obviously in **LIN**. Our results do not apply in this case, since QWA takes always time $\geq N$.

In 2D, on the other hand, a prediction can be done. Solving the 2D classical spin-glass problem is in **P**. Therefore, a QPT must exist for some value of Γ. But we only can state that the maximal entropy must grow, *at least*, logarithmically. In fact, recent results[19] (cleverly exploiting the properties of the infinite randomness fixed point[24], IRFP) show that it grows with a modified area law: for a block division cutting l links, the entropy scales as $s(l) \approx l \log(\log(l))$. Maximal entropy, as it is defined in this work, would be $S(N) \approx N^{1/2} \log(\log(N))$, thus rendering the time for the QWA simulation exponential. Our theorem is, therefore, too weak.

Nonetheless, the previous expression for the block entropy in a 2D quantum spin-glass is based on the average number of clusters cut by the block division. A well designed DMRG path might never cut more than one cluster at a time, just sweeping them one by one. In that case, the maximal entropy might grow much more slowly with system size. But, in order to obtain such a path, one should *first* solve the classical problem. Therefore, again, our result is not violated.

In 3D, or for random graphs of fixed connectivity, the **NP**-completeness of the problem forces the QPT to have entropy growing faster than $\log(N)$. In this case, the result is not surprising.

Other analysis[25] have studied the entanglement entropy along typical standard quantum computations, and our general statements also hold. For example, the entropy along Grover's algorithm remains bounded, which is consistent with the fact that the problem under consideration (unsorted search) is in **LIN**. Also, an AQC to solve the exact cover problem (which is **NP**-complete) found a QPT with $S \approx N$. Shor's algorithm also shows a similar behaviour, although it is not clear which is the complexity class of the problem under study (i.e.: integer factorization).

New predictions are easily made for AQC of problems which have never been studied. Thus, an AQC designed to test planarity of a graph, or 2-colorability need not find a QPT, since these problems belong to class **LIN**. But an AQC which orders a set of numbers, or which performs the fast Fourier transform, will find a QPT, since their running time is larger than linear. The maximal entropy in those cases might increase very slowly with size, since the (average) running time for the best algorithms are $T \approx N \log(N)$, so our only bound is that S should scale at least like $\log(\log(N))$. On the other hand, if **P**$\neq$**NP**, any attempt to solve the traveling salesman problem, or 3-SAT, will always find a QPT with the maximal entropy growing faster than logarithmically.

V. CONCLUSIONS

We have shown how to derivate physical inferences from computational complexity theory. If a physical process is devised in order to solve some problem, simulating that process in a computer is an algorithm to achieve the solution. The efficiency of this algorithm may be restricted by complexity theory, and this restriction is due to have some physical counterpart which applies to the real physical system.

Concretely, consider two hamiltonians, H_0 and H_1, linked by an adiabatic route. If the obtention of their ground states belongs to different complexity classes, this process may constitute an adiabatic quantum computation. Simulation of this process on a classical computer can not violate the time bounds which are established by complexity theory on the solution of the respective problems. Therefore, a quantum phase transition (QPT) will appear in the process in order to avoid such violation, with given specific growth rates for the entanglement entropy. Thus, another view is provided of the ubiquity of quantum phase transitions in disordered systems.

The present derivation was performed using the MPS and the DMRG, which are not specially well suited for multidimensional systems, due to its left-right division of the system for every step. Different generalizations of MPS exist, such as multiscale entanglement Ansatz[26] (MERA) or projected entangled pair states[27] (PEPS), which are altogether labeled as tensor product states[28] (TPS). We expect that usage of these more sophisticated tools will provide stronger predictions on the nature of the QPT found when performing a quantum adiabatic computation.

ACKNOWLEDGMENTS

This work has been supported by the Spanish government by grants FIS2009-11654 and FIS2009-12964-C05-1. The author wants to acknowlege very useful discussion with G. Sierra, I. Rodríguez, E.H. Kim and S.N. Santalla.

[1] C. Papadimitriou, *Computational Complexity* (Addison Wesley, 1994).

[2] S. Aaronson, G. Kuperberg, and C. Granade, "Complexity zoo," (2010), `http://qwiki.stanford.edu/wiki/Complexity_Zoo`.

[3] E. Farhi, J. Goldstone, S. Gutmann, J. Lapan, A. Lundgren, and D. Preda, Science **292**, 472 (2001).

[4] A. Das and B. K. Chakrabarti, Rev. Mod. Phys. **80**, 1061 (Sep 2008).

[5] J. Rodríguez-Laguna, Journal of Statistical Mechanics: Theory and Experiment **2007**, P05008 (2007).

[6] K. Binder and A. P. Young, Rev. Mod. Phys. **58**, 801 (1986).

[7] F. Barahona, J. Phys. A: Math. Gen. **15**, 3241 (1982).

[8] F. Liers, M. Palassini, A. K. Hartmann, and M. Jünger, Phys. Rev. B **68**, 094406 (2003).

[9] A. Das and B. K. Chakrabarti, *Quantum Annealing and Related Optimization Methods*, Lecture Notes in Physics (Springer Verlag, 2005).

[10] D. Aharonov, W. van Dam, J. Kempe, Z. Landau, S. Lloyd, and O. Regev, in *Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science* (2004) pp. 42–51, ISBN 0-7695-2228-9.

[11] G. E. Santoro, R. Martoňák, E. Tosatti, and R. Car, Science **295**, 2427 (2002).

[12] B. Altshuler, H. Krovi, and J. Roland, "Anderson localization casts clouds over adiabatic quantum optimization," (2009), `arXiv:0912.0746v1`.

[13] G. Vidal, J. I. Latorre, E. Rico, and A. Kitaev, Phys. Rev. Lett. **90**, 227902 (2002).

[14] G. Vidal, Phys. Rev. Lett. **91**, 147902 (Oct 2003).

[15] M. C. Bañuls, R. Orús, J. I. Latorre, A. Pérez, and P. Ruiz-Femenía, Phys. Rev. A **73**, 022344 (Feb 2006).

[16] M. Sredniki, Phys. Rev. Lett. **71**, 666 (1993).

[17] J. Eisert, M. Cramer, and M. B. Plenio, Rev. Mod. Phys. **82**, 277 (Feb 2010).

[18] A. Sen(De), U. Sen, J. Dziarmaga, A. Sanpera, and M. Lewenstein, Phys. Rev. Lett. **101**, 187202 (Oct 2008).

[19] Y.-C. Lin, F. Iglói, and H. Rieger, Phys. Rev. Lett. **99**, 147202 (Oct 2007).

[20] J. Rodríguez-Laguna, Journal of Physics A: Mathematical and Theoretical **40**, 12043 (2007).

[21] N. Schuch, I. Cirac, and F. Verstraete, Phys. Rev. Lett. **100**, 250501 (Jun 2008).

[22] N. Schuch and J. I. Cirac, Phys. Rev. A **82**, 012314 (Jul 2010).

[23] G. Ausiello, P. Crescenzi, G. Gambosi, V. Kann, A. Marchetti-Spaccamela, and M. Protasi, *Complexity and Approximation: Combinatorial optimization problems and their approximability properties* (Springer-Verlag, 1999).

[24] D. S. Fisher, Phys. Rev. B **51**, 6411 (1995).

[25] R. Orús and J. I. Latorre, Phys. Rev. A **69**, 052308 (May 2004).

[26] G. Vidal, Phys. Rev. Lett. **101**, 110501 (Sep 2008).

[27] N. Schuch, M. M. Wolf, F. Verstraete, and J. I. Cirac, Phys. Rev. Lett. **98**, 140506 (Apr 2007).

[28] T. Nishino, Y. Hieida, K. Okunishi, N. Maeshima, Y. Akutsu, and A. Gendiar, Progress of Theoretical Physics **105**, 409 (2001).