Quantum computers and intractable (*NP*-complete) computing problems

Vladimír Černý
Institute of Physics, Comenius University, Mlynská dolina, 842 15 Bratislava, Czechoslovakia
(Received 16 June 1992)

In this paper we discuss physical aspects of intractable (*NP*-complete) computing problems. We show, using a specific model, that a quantum-mechanical computer can in principle solve an *NP*-complete problem in polynomial time; however, it would use an exponentially large energy for that computation. We conjecture that our model reflects a complementarity principle concerning the time and the energy needed to perform an *NP*-complete computation.

PACS number(s): 03.65.Bz, 01.55.+b

INTRODUCTION

In this paper we shall discuss physical aspects of intractable (*NP*-complete) computing problems. A formal mathematical theory of *NP* completeness [1] is based on rigorous definitions of terms such as problem, algorithm, and complexity and, of course, it uses strict mathematical reasoning. However, computers are, after all, physical-world machines, so physical aspects of the problem (in addition to purely mathematical aspects) should be discussed as well. Can one learn something about the frontiers in computation discussing computers as physical-world machines?

The famous open problem of the complexity theory is the $P=NP$ problem. In this paper we shall discuss some physical aspects of this problem. We shall try to solve an *NP*-complete problem in polynomial time. In our discussion we shall, however, use the language of physics rather than rigorous mathematical language. Our constructions will not be strict analogs to mathematical objects.

We shall discuss the famous traveling-salesman problem (TSP): A set of N cities is given with distance $d_{ij} \in \mathbb{Z}^+$ for each pair of cities. The problem is to find the shortest tour through the cities. (Actually we shall discuss a restricted problem where d_{ij} are bounded $d_{ij} < L$ for all N. This is still an *NP*-complete problem.)

There is an easy algorithm for solving the problem: to enumerate all the tours and check the length of each of them. The time needed to perform such an algorithm grows exponentially with N since the number of tours is of the order of $N!$. One does not know whether an efficient algorithm exists for which the computing time would grow only as a polynomial of N. (We refer to more exact formulation of the $P=NP$ problem in Ref. [1].)

A parallel machine evaluating all the $N!$ tours simultaneously would do the calculation in finite time. But if one takes $N!$ processors one gets an exponentially growing space for the computer and an exponentially growing time for the readout. A simple-minded parallelism is of no help.

Naively one would think that a finite system cannot treat an "exponentially large" number of possibilities simultaneously. However, the opposite is true. Quantum-mechanical systems can and in fact do handle an exponentially large number of possibilities at once. We would like to show that this can, in principle, be used for computing.

Quantum-mechanical computers were discussed for example by Deutch [3] and Feynman [4]. Our methods will be similar to those of Feynman [4], although his aim was rather opposite to ours. Feynman has shown that a quantum-mechanical computer can in principle be used to perform the same type of calculation as a standard computer based on logic gates. We shall discuss a complementary problem: whether one can think of, at least in principle, an alternative kind of quantum computing, basically different from computing on a standard machine.

We should stress the words "in principle." In this respect, our discussion will be similar to that of Feynman. We do not want to design a technically possible machine. Our reasoning will be in the spirit of thought experiments. We can work with systems which perhaps do not exist in the actual world but do not contradict any law within certain theory. Such systems are therefore principally acceptable. Our theoretical framework will be the quantum mechanics. We shall show that it is possible to perform an "*NP*-complete" type of computation in "polynomial" time and in polynomial space. We shall construct a specific hypothetical quantum-mechanical model of a TSP solver.

QUANTUM TSP SOLVER

Our hypothetical quantum computer looks like a multislot interference machine with Stern-Gerlach devices on paths between the slots. In this section we shall describe the machine only briefly. Details will be presented in the Appendix.

For a TSP with N cities we shall need a machine consisting of $N-1$ layers $(2,3,4,\ldots,N)$ of slots, each layer having $N-1$ slots $(2,3,4,\ldots,N)$. Therefore, each slot is uniquely identified by two integers i,j. In addition to the slots there is a source ("laser") of particles at the position S and a detector at the position D (see Fig. 1).

There are $(N-1)^{N-1}$ possible trajectories for a particle to get from S to D through the slots. A trajectory is uniquely identified by listing the slots on it; for example,

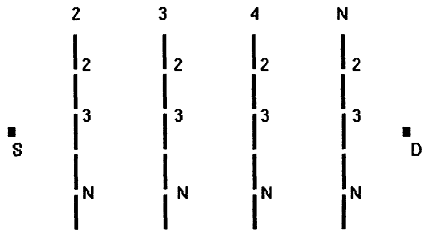

FIG. 1. A multilayer interference machine—the TSP solver.

the trajectory in Fig. 2 is

$$S,(2,2),(3,4),(4,3),(5,5),D \ .$$

It is clear that the layer identifiers can be omitted. Therefore, the same trajectory can be described as

$$S,2,4,3,5,D \ . \tag{1}$$

The trajectory (1) can be seen as a code for the traveling-salesman's tour through five cities provided one identifies the points S and D with the start and the end of the tour (city 1). The trajectory (1) represents the route 1,2,4,3,5,1.

However, there are trajectories through the slots which do not correspond to legal TSP routes, as, for example,

$$S,3,2,2,5,D \ .$$

This is not a legal TSP route since the city 2 was visited twice and the city 4 was omitted.

Our next task will be to get rid of "illegal" trajectories and to introduce the dynamics in such a way that the particle which goes through our machine senses the length of the corresponding TSP route.

To meet these demands we shall need particles with certain internal degrees of freedom which would interact with our machine. We shall use internal degrees of freedom similar to isospin. We should stress again that we work here in a hypothetical world, so we can invent any internal degrees of freedom, even if no corresponding particles exist (are known) in the real world.

We assume that the internal states of our hypothetical particles can be described by the following ket-vector notation:

$$|k;c_2,c_3,c_4,\ldots,c_N;p\rangle \ ,$$

where $k\in\{0,1,2,3,\ldots,NL\}$, $c_i\in\{0,1\}$, and $p\in\{0,1\}$.

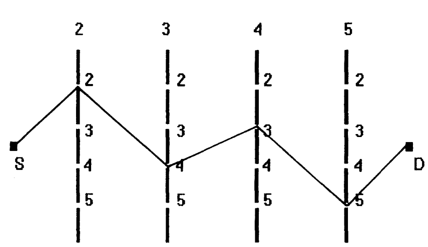

FIG. 2. A trajectory corresponding to a TSP route.

The quantum number k will be used to measure the "number of kilometers" on the route and the numbers c_i will signal whether the ith city was visited or not. The quantum number p has no relation to TSP. It will be used as an auxiliary degree of freedom to implement the desired dynamics.

Now we are ready to describe how the machine would work. Let us consider a piece of trajectory between two slots in neighboring layers,

$$(i,m)\to(i+1,n) \ .$$

This would correspond to a part of the traveling-salesman (TS) route between the cities m and n.

Let us assume that when the particle gets through the slot (i,n) the quantum number c_n will be changed as

$$c_n=0\to c_n=1 \ . \tag{2}$$

Let us also assume that our particle does not move between the slots through free space, but through some field arranged in such a way that the quantum number k increases on this piece of trajectory between the slots (i,n) and $(i+1,m)$ as

$$k\to k+d_{nm} \ , \tag{3}$$

where d_{nm} is the distance between the cities n and m. We shall discuss the corresponding dynamics in the Appendix.

Now assume that all the particles produced in the source S are initially in the state

$$|0;0,0,\ldots,0;0\rangle \ .$$

Then after going through the machine, the particles will be in the state

$$\sum_{\text{trajectories}} |k;c_2,c_3,c_4,\ldots,c_N;p\rangle_{\text{trajectory}} \ . \tag{4}$$

Some of the trajectories in this sum correspond to legal TS routes. It is easy to see that they are those for which all the c quantum numbers are equal to 1. This is guaranteed by the rule (2). For those trajectories, the value of the quantum number k in the corresponding vector in (4) is equal to the length of the corresponding TS route.

Now let us imagine that we shall put a filter to the point D which filters our (suppresses) all the states except those with all the c's equal to 1. Then the state of particles getting out of the machine would be

$$\sum_{\text{TS routes}} |\text{length}_{\text{route}};1,1,\ldots,1;p\rangle_{\text{TS route}} \ . \tag{5}$$

The corresponding filter should consist of a series of Stern-Gerlach-like devices sensitive to quantum numbers c absorbing states with $c=0$. The spirit of our discussion is similar to that used by Feynman in his lectures [2].

This is almost the conclusion. We shall still add an additional Stern-Gerlach-like device to the point D, this time sensitive to the quantum number k. It should split a stream of outgoing particles into NL streams according to the value of k (Fig. 3). If we add particle detectors to each of the NL streams then the detector in the stream

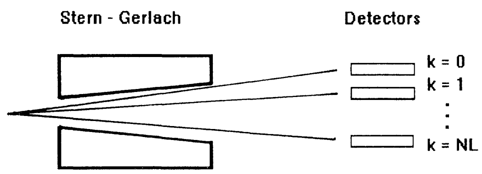

FIG. 3. A Stern-Gerlach-like device measuring the minimal value of k.

corresponding to value $k=M$ would fire if there exists a TS route with the length equal to M. Out of the detectors which fire, one can find the one with lowest corresponding k. It signals the minimal TS route.

PROBLEM OF MEASUREMENT

We should, however, discuss the detection of the minimal k value more carefully. According to orthodox quantum mechanics, each particle which goes through our machine is in the superposition of states as given by the sum (5). A single particle senses all the trajectories and in this way a single particle "knows" the minimal value of k. The TSP solution is hidden in the final state of a single particle which goes through our machine. A particle certainly needs only "polynomial time" to get through the machine, so the particle "knows" the TSP solution in polynomial time. Can we arrange that we (and not only the particle) know the solution, too? The problem is how to measure (in the sense of measurement in quantum mechanics) the minimal value of k present in the superposition (5).

There are (by the order of magnitude) $N!$ states in the superposition (5) and it may happen that only one of them corresponds to the minimal value of k. Therefore we are looking for a state which is present in the superposition with extremely low amplitude, of the order of $1/\sqrt{N}!$. According to the postulates of quantum mechanics it is possible to detect the presence of such an amplitude in one act of measurement only with a probability $1/N!$. So if our detectors have to fire with a reasonable probability, we have to push through our machine a large number of particles simultaneously. This is in principle possible if the particles are bosons so that one can form a classical field out of them in the same way that laser light is formed by a large number of coherent photons.

However, our "laser" should be very energetic: we require that the intensity of the classical field correspond to $N!$ bosons. Unfortunately, this means that we need "exponentially large" energy. So the "calculation" itself can be done in polynomial time, but reading the result expends an exponentially large energy.

CONCLUSIONS

We have discussed one particular model, but we cannot avoid the feeling that the result is perhaps more general. It seems like a sort of complementarity principle with respect to energy and time needed for an NP-complete computation. The opposite situation has been extensively discussed: it was shown that one can compute with zero energy if one does not mind slow computation [4–6]. Here we have the other end: fast computation but with extremely large energy.

Have we observed here a new principle, or is it a consequence of some known laws of nature, e.g., the second law of thermodynamics? Can one learn something from the model presented here to get hints on how to approach the "mathematical" $P=NP$ problem? We do not know. We have presented our simple model more as an opening point in a discussion rather than as a solution to the problem.

ACKNOWLEDGMENTS

The author is indebted to J. Ftáčnik, M. Mojžiš, J. Pišút, and P. Prešnajder for useful discussions.

APPENDIX

We shall now discuss technicalities about the dynamics which leads to required behavior as given in Eqs. (2) and (3). We shall start with Eq. (2). Since it concerns only one quantum number c_n, we can suppress all the other quantum numbers as well as the index n in the notation. Let us assume that in the slot there is a field which interacts with the "quantum number" c and the corresponding Hamiltonian is

$$H_1=\omega_1(a^\dagger+a)\ ,$$

where $a^\dagger$ and a are the creation and annihilation operators defined as

$$a^\dagger|0\rangle=|1\rangle,\quad a^\dagger|1\rangle=0\ ,$$

$$a|0\rangle=0\ ,\quad a|1\rangle=|0\rangle\ .$$

Then

$$\exp(-iH_1t_1)|0\rangle=\cos(\omega_1t_1)|0\rangle-i\sin(\omega_1t_1)|1\rangle\ .$$

If one arranges the value of ω_1 and the time t_1 of flight of the particle through the field in the slot in such a way that $\omega_1\cdot t_1=\pi/2$, then Eq. (2) is satisfied.

Now let us discuss Eq. (3). We shall first develop an apparatus which will change the state of the particle going through it as

$$|k\rangle\to|k+1\rangle\ . \tag{6}$$

We shall need the auxiliary quantum number p to arrange the change of state (6) as a sequence of changes (now we skip the c quantum numbers in our notation),

$$|k;p=0\rangle\to|k+1;p=1\rangle\to|k+1;p=0\rangle\ . \tag{7}$$

To perform the first change of state, we let the particle interact with some external field with Hamiltonian

$$H_2=\omega_2(b^\dagger d^\dagger+bd)\ ,$$

where

$$b^\dagger|k;p\rangle=|k+1;p\rangle\quad\text{for } k<L\ ,$$

$$b^\dagger|k;p\rangle=0\quad\text{for } k=L\ ,$$

$$b|k;p\rangle=|k-1;p\rangle \quad \text{for } k>0 \,,$$
$$b|k;p\rangle=0 \quad \text{for } k=0 \,,$$
$$d^{\dagger}|k;p=0\rangle=|k;p=1\rangle, \quad d^{\dagger}|k;p=1\rangle=0 \,,$$
$$d|k;p=0\rangle=0, \quad d|k;p=1\rangle=|k;p=0\rangle \,.$$

Then

$$\exp(-iH_2t_2)|k;0\rangle=\cos(\omega_2t_2)|k;0\rangle -i\sin(\omega_2t_2)|k+1;1\rangle \,.$$

Choosing ω_2 and t_2 (time of flight through the field) so that $\omega_2t_2=\pi/2$, we get the required change of state

$$|k;0\rangle\rightarrow|k+1;1\rangle \,.$$

The next required change of p back to $p=0$ is easily done using interaction with Hamiltonian

$$H_2'=\omega_2'(d^{+}+d)$$

and time of flight t_2' such that $\omega_2't_2'=\pi/2$.

However, one must be very careful here. If the times t_2 and t_2' are not tuned very accurately we will get a small admixture of a state with wrong quantum numbers k and p. But this is dangerous: in the end we look for a state with exponentially small amplitude. Even an exponentially small admixture of state with "wrong" quantum numbers can lead to a wrong result. It is not acceptable to assume that the time tuning can be that fine. Fortunately one can use the auxiliary p variable to test whether the state was changed properly. All one need do is to add after the first change of state $|k;0\rangle\rightarrow|k+1;1\rangle$ a filter which would absorb any admixture of state $|k;0\rangle$.

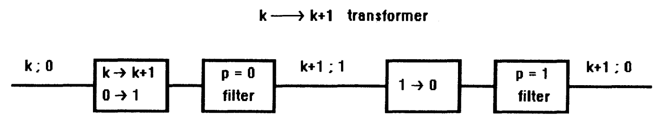

FIG. 4. Sequence of steps implementing the "$k\rightarrow k+1$" change of state.

This can be achieved by testing the value of p alone: Hamiltonian H_1 keeps strict correlation between the values of p and k. This is actually the most important reason why we introduced the auxiliary variable p. We cannot test for the correctness of the value of $k+1$ since we do not know the value of k. Again after the change of state $|k+1;1\rangle\rightarrow|k+1;0\rangle$ we have to introduce a filter which absorbs admixture of state $|k+1;1\rangle$ in order that we be sure to have the correct value $p=0$ before entering the next $k\rightarrow k+1$ apparatus. The whole $k\rightarrow k+1$ apparatus is presented in Fig. 4.

Now we know how to arrange the necessary change of state $k\rightarrow k+d_{nm}$ between the slots n and m: we put d_{nm} pieces of "$k\rightarrow k+1$" devices on the trajectory between the slots m and n. Such devices should be put everywhere on trajectories between any pair of slots in our machine. The filters in these devices decrease the luminosity of our quantum computer (some of the particles do not go through), but since we need exponentially large luminosity anyhow, this is not important. It should also be stressed that the total number of "$k\rightarrow k+1$" transformers needed to build the TSP solver grows only polynomially with N, so our quantum computer is only "polynomially large" both in space and in time.

[1] For a review see, e.g., M. R. Garey and D. S. Johnson, *Computers and Intractability, A Guide of the Theory of NP Completeness* (Freeman, San Francisco, 1979).

[2] R. P. Feynman, R. B. Leighton, and M. Sands, *The Feynman Lectures on Physics, Vol. 3* (Addison-Wesley, Reading, MA, 1963).

[3] D. Deutch, Proc. R. Soc. London, Ser. A **400**, 97 (1985).

[4] R. P. Feynman, Found. Phys. **16**, 507 (1986).

[5] C. H. Bennett, IBM J. Res. Dev. **6**, 525 (1979).

[6] T. J. Toffoli, J. Comput. Syst. Sci. **15**, 213 (1979).