

Logic programming as quantum measurement

Roman R. Zapatrin

Friedmann Lab. for Theoretical Physics
SPb UEF, Griboyedova 30/32
191023, St-Petersburg, Russia

June 30, 1995

Abstract

The emphasis is made on the juxtaposition of (quantum theorem) proving versus quantum (theorem proving). The logical contents of verification of the statements concerning quantum systems is outlined. The Zittereingang (trembling input) principle is introduced to enhance the resolution of predicate satisfiability problem provided the processor is in a position to perform operations with continuous input. A realization of Zittereingang machine by a quantum system is suggested.

Introduction

What is the desirable way to broaden the facilities of processors in order to have progress in solving NP-hard problems? The principle of trembling input I am going to put forth in this paper will require a flexibility of processor. That means that it will be assumed that the processor is able to deal with "intermediate outputs", or, in other words, that it will be possible to pass continuously from one input to another. We shall also assume that all possible inputs form a linear space, and that the result depends continuously on input preserving linear combinations.

To elucidate the idea of the principle I suggest to consider the SAT problem. Suppose that, solving some problem, you succeeded to reduce

QUANT-PH-9506041

it to the following one: given a propositional form $P(x_1, \dots, x_n)$ of, say, $n = 100$ variables, you have to check whether there exists an n -tuple (c_1, \dots, c_n) such that $P(c_1, \dots, c_n) = 'true'$.

So, if there is no heuristical methods to prove the theorem

$$\exists x_1, \dots, \exists x_n \quad P(x_1, \dots, x_n)$$

it remains the only (classical) way of solution, namely, to choose at random the values of the input n -tuples, substitute them to the machine calculating the form P , and wait while the 'true' will appear on the output. Or, if you have 2^n such machines, do it simultaneously. When n is large enough, both possibilities are unrealistic, and you have to confirm that there are no classical means to prove this this theorem.

The Zittereingang principle which I am going to put forward could provide the non-constructive solution of the problem. Its basic idea is the following. Instead of preparing and re-preparing the input register at different input states in order to search the witness of $P = 'true'$ we make the input state *tremble*. Then, instead of checking the output value you measure the *derivative* of the output. If the value of P is always NO, the output will not tremble you will have the zero value of the derivative. Whereas there are YESs among output values, the derivative will be nonzero. So, checking the value of the derivative, you can prove or reject the theorem.

To realize this project, I suggest to call on quantum effects.

1 Polarized electrons

The potential Reader of this paper is assumed to be far away from quantum mechanics, so a brief outline of the simplest physical experiment where quantum effects arise seems appropriate. This will be the famous Stern-Gerlach experiment with polarized electrons. The equipment needed for this experiment is depicted at Fig.1.

There will be two possible orientations of the polarizer (w.r.t. the frame at the left margin of Fig.1) and two possible positions for detector within this scheme. So, we shall be able to prepare four sorts of beams:

1. The polarizer P is x -oriented, and the upper beam is chosen.
2. The polarizer P is z -oriented, and the right beam is chosen.

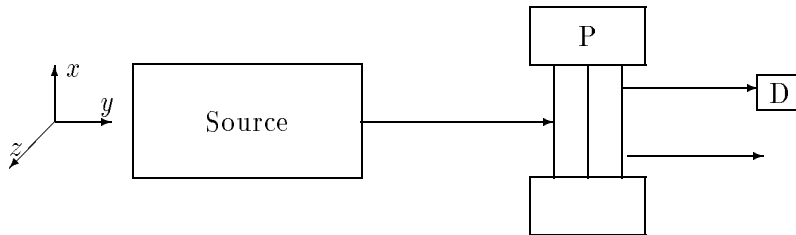


Figure 1: The Stern-Gerlach experiment. The source (cathode) S emits a beam of electrons. The polarizer P splits the initial beam into two. The detector D counts the number of absorbed electrons: whenever an electron is absorbed, the detector clicks.

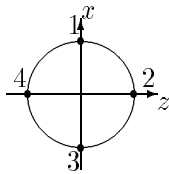


Figure 2: Reminder on state notation: the filled circle denotes the trace of the appropriate beam in the (xz) plane.

3. The polarizer P is x -oriented, and the lower beam is chosen.
4. The polarizer P is z -oriented, and the left beam is chosen.

From now one can consider the new source of electrons *prepared in a definite state*(Fig. 3).

The discovery of Stern and Gerlach was the following. Suppose that the initial beam is prepared in the state 1. The making it pass through the x -polarizer, one can see that the beam will not split anymore all electrons will go up. That means that whenever an electron is emitted in the state 1 and passes through the filter checking "Whether the state is 1?", the answer will be YES with certainty. Whereas, if the same beam will pass through the z -polarizer, it will split into two. Thus, provided the electron is emitted in state 1, the probability to

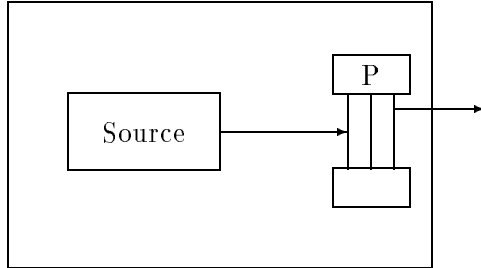


Figure 3: The source of electrons prepared in a definite state.

detect it being in the state 2 is $1/2$, and the same for the state 4 (pip into the reminder at Fig.2 above). These results can be summarized as follows.

Denote by $P(i, k)$ the probability for the electron to be detected in the state k provided it was emitted in the state i . Then

$$P(i, k) = \begin{cases} 1 & , \quad i = k \\ 0 & , \quad i - k = 1(\text{mod}2) \\ 1/2 & \text{otherwise} \end{cases} \quad (1.1)$$

The striking property of quantum mechanics is that the results (1.1) is ALL that we can observe by means of this equipment. It is in principle impossible to measure a pair of properties, say, 1 and 2 simultaneously. Such series of experiments resulted in the famous Bohr's **complementarity principle**: there are physical properties which can not be measured simultaneously. Given two such properties \mathcal{A} and \mathcal{B} , the measurement of \mathcal{A} unavoidably affects the result of measurement of \mathcal{B} . This principle is the fundamental law of the Nature: we can like it or not, but no its violation was yet found.

2 A query model: (quantum theorem) proving

In this section I am going to tackle the problem of determining the initial state of quantum objects. To make the conclusions more transparent, a more complicated quantum system will be studied. It will

have 8 possible initial states: $1, \dots, 8$. At each moment we shall be able to test one of these states. Like in the previous section, we shall have the following outcomes. $P(i, k)$ here means the probability to have the YES reply to the query k provided the initial state of the object was i :

$$P(i, k) = \begin{cases} 1 & , \quad i = k \\ 0 & , \quad i - k = 1(\text{mod}4) \\ 1/4 & \text{otherwise} \end{cases} \quad (2.1)$$

This is the analog of the formula (1.1). This model can be realized by the experiment with ions, analogous to the Stern-Gerlach one, but the filters x and z will split the incoming beam into four. The quantum theorem I am going to prove is formulated as follows.

Suppose we have a source of ions, which emits them by one, and all of them are prepared in *the same initial state*, but we do not know this state. The question is formulated as:

Which is the initial state?

Denote by q the query *Is the state q ?* Looking at the formula (2.1) we can see that after at most 6 steps (emitted ions) the question reduces to the following *Is the state i or k ?* where i is even and k is odd. The algorithm of this reduction is drawn at Fig.4.

Now suppose we stopped on the alternative 12. If we then perform the test, say, 1, the positive reply which is possible in virtue of (2.1) will not clarify the situation in virtue of the formula (2.1). To know the state, we must perform a test, say, 3. If the reply is YES, nothing is clear. Meanwhile, if NO is obtained, it is the solution of the problem: that means that the state is definitely 2. Whereas we see that **there is no upper bound for the number of tests to get the definite answer** irrespective to that the initial state was pure one!

The corollary is that in quantum situation you can have a problem of choice from a finite number of alternatives having no upper bound for its resolution time.

Note that the quasi-quantum query model can be realized by classical automata having nothing quantum in their nature. These are so-called *normalized automata* (Grib and Zapatrin, 1990). From the pure logical point of view normalized automata may be thought of as a sort of "Skolemized quantum systems" grasping only the logical structure of testable properties.

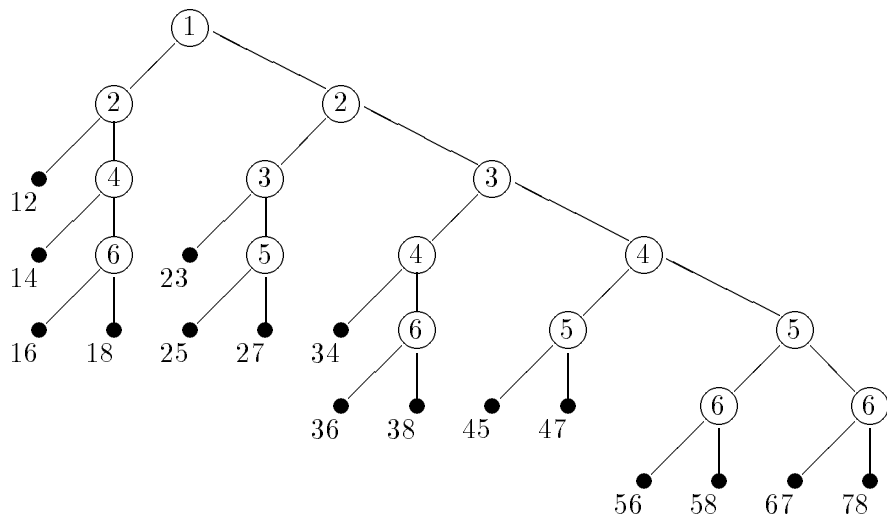


Figure 4: The reduction algorithm. Each node with a number inside is a test. Left edges are associated with YES outcomes, right ones are NOT outcomes. The filled nodes correspond to the reduced questions. For instance, 38 means 3 or 8

3 A piece of quantum mechanics.

The mathematical formalism of quantum mechanics is the steady and rigid machinery verified by enormous number of experiments and applications. I shall briefly introduce its piece needed in the sequel. In quantum mechanics, a physical object is associated with a Hilbert space \mathcal{H} , called *state space*. I shall consider here only finite-dimensional case. A (pure) state of the object is associated with a unit vector $\psi \in \mathcal{H}$. When \mathcal{H} is realized as functional space ψ is just the wavefunction, or "matter wave".

The observable entities are associated with self-adjoint operators in \mathcal{H} . Let A be the operator associated with an observable \mathcal{A} . Since A is self adjoint, it can be decomposed in accordance with the spectral theorem:

$$A = \sum a_i P_i$$

where P_i are mutually orthogonal projectors in \mathcal{H} , and $a_i \in \mathcal{R}$ are possible values of the observable \mathcal{A} . The heart of quantum measurement theory is the

Projection postulate: Let ψ be the initial state of the object. Then the measurement of the observable \mathcal{A} in the state ψ results in:

- The value a_i of \mathcal{A} is obtained with the probability equal to $\| P_i \psi \|^2$. In particular, when ψ is an eigenstate of A , the appropriate value a_i is obtained with certainty
- The state of the object changes after the measurement to the eigenstate associated with the observed value of \mathcal{A} . In particular, when the initial state ψ is the eigenstate of A , the measurement does not change the state of the object.

The new fundamental notion brought by quantum mechanics is that of complementary measurements. In the formalism they are associated with non-commuting operators. Due to the Bohr's principle, such measurements are not performable simultaneously in principle.

The last (but not the least) thing that will be needed is the description of what happens with a quantum mechanical system while one does not touch it, that is, how it *evolves in time*. This is described as:

$$\psi(t) = U(t)\psi(0) = \exp(-iHt)\psi(0)$$

where $U(t)$ is a semigroup of unitary operators representable in the form $\exp(-iHt)$ with a self-adjoint operator H called the *Hamiltonian* of the evolution. In particular, when $\psi(0)$ is an eigenvector of H , the initial state is unchanged up to a factor $\alpha(t)$ such that $|\alpha(t)|^2 = 1$ and the test verifying the state $\psi(0)$ will always give the YES answer.

That is all from quantum mechanics that will be needed for further purposes.

4 Classical Gedankencomputer

In this section I describe the classical computational process as quantum one.

Loading input data. It is supposed that there is a source of physical entities, call them *launches*, having the state space rich enough to encode 2^n input values. As a matter of fact, the state space must be broader to include the START and HALT states to enable the reversibility of the process. The launch enters the input register (measuring device having n yes-no, or 0-1 controls) which prepares it in one of its orthogonal pure states.

Computation is the evolution of the launch within the processor controlled to that extent that before the computation starts the parameters of Hamiltonian responsible for the evolution of the launches are set up (in other words, the program is loaded before the computation). Whereas during the computation no intermediate measurements are performed. Some ideas towards the realization of this process were proposed by Deutsch (1989).

Output is the source of particles (they may not be the initial launches) having only two pure states and produced by the computer in such a way that their states are associated with the calculated values.

So, the classical computational process looks as follows.

Installation of program. Let $F(x_1, \dots, x_n)$ be the function whose values are to be calculated. That means that the evolution law for the processor is fixed up in such a way that each pure state prepared by the input register affects the emission of the output launch in one of the final states.

Calculation. The values (x_1, \dots, x_n) of input variables are imposed by appropriate setup of the input controls. Then the launch is emitted. It passes through the input register which prepares it in the pure state $\psi(0)$ and enters the input gate of the processor. By the end of calculation a polarized electron is emitted by the processor. It rushes into the output filter which checks whether the state is HALT (and it certainly will be so since we have organised the evolution within the processor in such a way).

It is essential to note that the Hamiltonian of the processor is such that if the calculation with the same input data is repeated, you are compelled to get the same result. So, on classical input data the described Gedankencomputer works as a deterministic machine.

5 Uncertainty at service

In this section I am going to show how the Gedankencomputer described in the previous section may be converted into Quantum Theorem Prover.

In order to convert the computer to QTP- Quantum Theorem Prover, both classical input and output registers are removed while the processor is kept unchanged. **The input register** is replaced by an apparatus measuring complementary values. The crucial point is the following: *the prepared state must be the superposition of ALL input states with all NONZERO coefficients.* What is needed, is to suppose that the process of computation of each particular value $P(x_1, \dots, x_n)$ is a quantum process.

The launch rushes into the processor, the latter will start working governed by its dynamical laws (=computes P according to the program). Finally, since the quantum evolution is linear, the result will be the superposition of all classical results with the same coefficients. Then, instead of measuring the output value, you make **the output register** be an observable complementary to the classical output.

Which should be this complementary observables? The idea is the following: **we make the input state oscillate (in time or in space, at convenience), and measure the value of the derivative of the output.** Then, since the processor still computes P , we have two alternatives:

1. If there is no x_1, \dots, x_n such that $P(x_1, \dots, x_n)$ is true, then the value of the derivative will be zero
2. If there are x_1, \dots, x_n such that $P(x_1, \dots, x_n)$ is true, then the value of the derivative will be nonzero

The objection against this idea is that the value of the derivative in the case when we have, say, the only satisfying set for P , may be of the order $1/2^n$. To avoid this trouble return to the description of the classical Gedankencomputer. When it is converted to QTP, we have some spare "degrees of freedom" to define the "program" for the processor. Namely, we are confined by only *classical outputs for classical inputs*, and, since the state space of the launch is broader, we are free to define the evolution for *non-classical* input states. This is the main issue making QTP different from other quantum computers (for review on quantum computers see Bennett, 1993).

So, in principle, the satisfiability problem can be solved by QTP at one P -calculation state. There is also a problem of preparation of the superposition of all input states, however it was shown (Deutsch and Jozsa, 1992) that it can be done for polynomial time.

CONCLUDING REMARKS

I endeavored to show how quantum effects such as superposition of states and wave properties of the particles can be used for calculation purposes. The proposed Quantum Theorem Prover is merely an imaginary machine. However, suppose it may exist, it can drastically influence many principles of programming. For example, such problem as SAT: satisfiability of propositional forms is solved on classical computers for the time $T \simeq \exp(n)$, where n is the number of variables. Meanwhile QTP solves it for polynomial time (required for the preparation of the input). Accepting QTPs requires new options in programming languages: the assignment of value should be replaced by the preparation of the input register.

ACKNOWLEDGMENTS

I take this opportunity to mention that the idea of QTP has grown from my attempts to understand what are Labelled Deductive Systems introduced by Dov Gabbay (to appear). The valuable comments made by Richard Jozsa are acknowledged as well as the telecommunication support provided by Pavlov Enterprise (St-Petersburg).

REFERENCES

- Deutsch, D. (1989), *Quantum Computational Networks*, Proceedings of the Royal Society, **A425**, 73
- Grib A.A., Zapatrin R.R.(1990), *Automata Simulating Quantum Logics*, International Journal of Theoretical Physics, **29**, 113
- Deutsch D., Jozsa R.(1992), *Rapid solution of problems by quantum computation*, Proceedings of the Royal Society of London, ser. A, **439**, 553
- Gabbay, D. (to appear), "LDS - Labelled Deductive Systems", Oxford University Press
- Bennett, C.H.(1993), *Quantum Computers: Certainty from Uncertainty*, Nature, **362**, 694