International Journal of Theoretical Physics, Vol. 30, No. 2, 1991

Prediction Problem in Quantum Mechanics Is Intractable (NP-Hard)

Vladik Kreinovich,[1] Alejandro Vazquez,[1] and Olga Kosheleva[1]

Received July 23, 1990

It is proved that both the prediction problem and the problem of reconstructing the state from the observations in quantum mechanics are NP-hard.

GENERAL INTRODUCTORY REMARK

We prove that both the prediction problem and the problem of reconstructing the state from given observations in quantum mechanics are in the general case intractable (or, using the precise mathematical notion from complexity theory, NP-hard). This result can be of interest to two groups of readers: those who are well acquainted with the mathematical problems of quantum physics and those who are well acquainted with algorithmic complexity and NP. We do our best to make this text understandable to both. Therefore we include brief explanations of both the quantum mechanics formalism and the formal notion of intractable (NP-hard) problems. Those readers already familiar with one of these notions can simply skip the corresponding part.

1. INTRODUCTION: PREDICTION PROBLEM IN PHYSICAL TERMS

Before we formulate the problems in mathematical terms we want to explain their physical origin. By prediction we mean that for some given object (or system), after performing some measurements, we are able to predict something about its future: namely, what future behavior is possible and what is not. Prediction is what all the physics is for.

For example, we study substances to predict how they will behave in different situations; we study electromagnetic waves in order to find out

[1]Computer Science Department, University of Texas at El Paso, El Paso, Texas 79968.

0020-7748/91/0200-0113$06.50/0

whether some concrete electronic device will work properly or some misbehavior is possible. In quantum physics, we have, e.g., an accelerator, we measure energy, polarization, and maybe some other characteristics of the particles that are emitted by this accelerator. Then we place some target in their way and we want to predict what will happen, e.g., is it possible that 90% of these particles hit the target, etc.?

We show that this prediction problem is in the general case difficult to solve (in a precise mathematical sense).

Another problem that is closely connected with this one is: to determine the real state of the object from known experimental results. This problem is connected with the prediction problem, because often, when we have to predict, we first determine the state of the object and then make predictions based on this state. This is a most natural (direct) way to predict. However, usually experimental results are not sufficient to reconstruct the state uniquely, so we can either produce at least one state consistent with all the observations or try to produce all of them. The simplest possible version of this problem is: to produce at least one state that is consistent with all the observations. We show that even in this simplest form the state reconstruction problem is in general also hard to solve.

2. HOW TO FORMULATE THIS PROBLEM IN MATHEMATICAL TERMS

This section contains the motivation of the formal definitions given in Section 3. So readers who are interested mainly in the mathematical result itself can skip this section and go to Section 3.

In order to formulate the above problems in mathematical terms, let us briefly recall the mathematical formalism of quantum mechanics (see, e.g., von Neumann, 1955), or, to be more precise, parts of this formalism that are relevant to the problems of prediction and state reconstruction. In quantum mechanics possible states of objects and systems are represented by vectors in some abstract (Hilbert) space. If we choose a base for that space, then these states are represented by complex vectors $s = (s_1, s_2, \ldots, s_n, \ldots)$ such that the sum of the squares of all the modules $|s_i|^2$ equal to 1. In the following we always assume that some base is fixed, so by a state we always mean a vector.

In the quantum formalism, experiments or observations are represented by self-adjoint matrices $A = \|A_{ij}\|$, i.e., matrices for which $A_{ji} = A_{ij}^*$ (here z^* means a complex conjugate to z). In classical (nonquantum) physics, if we fix the state of the object and the concrete experiment, then the results of this experiment are uniquely determined. Quantum mechanics is essentially stochastic in the sense that if we repeat the same experiment with several

identical copies of the same system, then, generally speaking, we get different results. The only thing we can determine from these experiments is one or several characteristics of the corresponding probabilistic distribution of the possible experimental results.

If the corresponding sample is small, the only characteristic that we can efficiently reconstruct from it is the average value of the observable in the analyzed state. According to the quantum formalism, the average value of the observable A in the normalized state s equals the sum of $A_{ij}s_i s_j^*$ for all i, j; this sum is denoted by (As, s). Of course, it is impossible to reconstruct the average precisely when the sample is finite, so in reality from the experiments we get only the estimates for this average (As, s), i.e., values a^-, a^+ such that the average is between them.

If the sample is sufficiently big, we can determine not only the average values, but the probabilistic distribution itself, i.e., the probabilities of different outputs. According to the formalism of the quantum mechanics, every experiment normally has only finitely many possible outcomes (or at least a discrete set of possible outcomes).

Comment. The fact that physical variables like energy or angular momentum that were supposed to be changing continuously and which everyone thought take arbitrary real values can take only finitely many different values is called quantization and its experimental discovery started quantum mechanics.

According to the formalism of quantum mechanics, these possible values are eigenvalues $v_1, \ldots, v_n, \ldots$ of the matrix A, and the probability to obtain the value v_i is $(P_i s, s)$, where P_i is a matrix such that the transformation $s \to P_i s$ is an orthogonal projection of a vector s onto the eigenspace corresponding to v_i.

Of course, in reality we can perform only finitely many experiments, so we have only a finite sample, and from this finite sample we cannot reconstruct the precise values of the probabilities—only frequencies. Frequency is a good approximation to the probability—the greater the sample, the better—but still, as a result of the experiments, we get not the precise value of $(P_i s, s)$, but the lower and upper bounds p^- and p^+ such that $(P_i s, s)$ belongs to the interval $[p^-, p^+]$.

So in all cases the only knowledge about the state s that we get from the experiments is that $(A_i s, s)$ belongs to the interval $[a_i^-, a_i^+]$ for $i = 1, 2, 3, \ldots, m$, where A_i are given matrices and a_i^-, a_i^+ are given numbers.

Due to the stochastic character of quantum mechanics, the notion of prediction is also somewhat different from the classical case: even if we know the state precisely, we cannot predict uniquely the results of future experiments; the only things that we can predict are average values and

probabilities of different results. In reality our knowledge of the state is usually incomplete, so we cannot predict the concrete values of these averages of probabilities, but what we can try to do is to predict whether it is possible that these values (probabilities) will belong to some given interval or not.

Due to the fact that all the measurements and estimates are approximate, we can, without losing any generality, retain only finitely many digits of a_i, so we can consider only the case when a_i^+ and a_i^- are binary rational numbers. In view of that, although we stressed that the precise values of averages and probabilities are unknown, if the sample is sufficiently big so that the resulting precision in the estimate is much greater than the precision of our computer, then both estimates a_i^- and a_i^+ can correspond to equal binary rational numbers. In view of that, we will not suppose that these estimates are different.

The same remark about the approximate character can be applied to the components of the matrices A_i; therefore both the real and the imaginary parts of all their elements can be supposed to be binary rational.

Another remark: in the computer (or in any other storage) we can keep only finitely many real numbers; therefore, although in quantum mechanics some operators are represented by infinite-dimensional matrices, we know only their finite-dimensional part.

One can argue about these restrictions, but due to the fact that we are going to prove a negative result, whether these restrictions are too restrictive or not is not important: for example, if we prove that the problem is intractable in the finite-dimensional case, then of course it means that it is intractable in the general case as well.

So we arrive at the representation of our knowledge in terms of a system of quadratic inequalities. The formalization of our problems is now straightforward. By reconstructing the state, we mean finding the vector x for which all these inequalities are true—to be more precise, computing all the components of this vector with given precision. By predicting the results of future experiments we mean the following problem: given some additional matrices (corresponding to future experiments) and additional intervals, is it possible that for some vector s satisfying the first system of inequalities, all the inequalities from the second system are also valid? In other words, is the joint system of inequalities consistent?

Let us repeat these formulations in purely mathematical terms.

3. MATHEMATICAL FORMULATION OF THE PROBLEMS

General Definitions. Suppose some integer N is given. It will be the *dimension* of the state space. By a *norm* $|s|$ of a complex N-dimensional

vector $s = (s_1, s_2, \ldots, s_N)$ we mean the square root of the sum of the squared modules $|s_i|^2$ of its components. By a *state* we understand a complex vector s with a unit norm ($|s| = 1$). *Binary rational* numbers are defined in the usual manner: as numbers represented in the standard computer binary form $c_{-k} \ldots c_{-2}c_{-1}c_0 \cdot c_1c_2 \ldots c_p$ for some k and p, where $c_i = 0$ or 1. By an *observable* A we mean a complex self-adjoint $N \times N$ matrix with elements A_{ij} (self-adjoint means that $A_{ji} = A_{ij}^*$). For every observable A and state s, by (As, s) we mean the sum of $A_{ij}s_is_j^*$ for all i, j. We say that an observable is *efficiently defined* if both real and imaginary parts of all its elements A_{ij} are binary rational.

By a *knowledge* we mean a finite list of triples (A_i, a_i^-, a_i^+), where A_i is an efficiently defined observable, and a_i^-, a_i^+ are binary rational numbers. We say that a state s is *consistent* with the knowledge K if for all the triples from that knowledge the value (A_is, s) belongs to the interval $[a_i^-, a_i^+]$. We say that a knowledge K is *consistent* if there exists a vector x that is consistent with K.

By a *future behavior* we mean a finite set of triples like those in the definitions of the knowledge (so from the mathematical viewpoint these definitions coincide; they differ only in interpretation).

Prediction Problem. Given a knowledge K and a future behavior K', find whether there exists a state x that is consistent both with K and K'.

State Reconstruction Problem. Given a consistent knowledge K and $e > 0$, compute all the components of some vector x consistent with this knowledge, with precision e.

Comment. The first problem is to find whether a given system of quadratic inequalities of special type has any solutions, and the second problem is, in case such a solution exists, to find it.

4. FORMULATION OF THE RESULT

Preliminary Comments. We want to prove that these problems are NP-hard. This notion (see, e.g., Garey and Johnson, 1979) means that if there existed an algorithm allowing one to solve them in polynomial time (i.e., whose running time does not exceed some polynomial of the input length), then the polynomial-time algorithm would exist for practically all discrete problems such as the propositional satisfiability problem, discrete optimization problems, etc.—and it is a common belief that for at least some of these discrete problems no polynomial-time algorithm is possible. So the fact that the problem is NP-hard means that no matter what algorithm we use, there will always be some cases for which the running time grows faster than any polynomial—and therefore for these cases the problem is

intractable. In other words: no practical algorithm is possible that solves the problems of prediction or state reconstruction in all cases.

Theorem. The prediction problem and state reconstruction problem are NP-hard.

5. PROOF

Preliminary Remark. Although in the formulation of the prediction problem we have two separate sets of triples—knowledge K and future behavior K', we never consider them separately; the only thing we are interested in is to find whether there exists an s satisfying all the inequalities from both K and K', i.e., from the union of those lists. So although the division into knowledge and future behavior is physically meaningful, from the mathematical viewpoint the problem can be reformulated as follows: given a set of triples, to find whether it is consistent or not. In the following proof we use this reformulation.

1. First let us prove that the prediction problem is NP-hard. Namely, we show that if it were possible to solve it in polynomial time, then it would be possible to solve in polynomial time a problem that is already known to be NP-hard: the so-called satisfiability problem for 3-CNF (see, e.g., Garey and Johnson, 1979). This problem consists of the following: suppose an integer n is fixed, and a formula F of the type $F_1 \,\&\, F_2 \,\&\, \cdots \,\&\, F_k$ is given, where each of the expressions F_i has the form $a \vee b$ or $a \vee b \vee c$, and $a, b, c, \ldots$ are either $x_1, x_2, \ldots, x_n$ or their negations $\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_n$. If we assign arbitrary logical values ("true" or "false") to n variables $x_1, x_2, \ldots, x_n$, then, applying the standard logical rules, we get the truth value of F. The problem is to find such truth values of x_i for which the truth value of the expression F is "true."

We undertake the promised reduction in several steps.

2. It is known that the satisfiability problem for 3-CNF can be reduced to the problem of solving the system of quadratic equations with the real variables y_i that can take only two possible values 0 and 1. To undertake this reduction, let us introduce for every F_i of the form $a \vee b \vee c$ three new real variables corresponding to a, b, c, and two new real variables for every F_i of the type $a \vee b$. Then the total number of these real variables is three times the number of terms $a \vee b \vee c$ plus two times the number of terms $a \vee b$. The corresponding system of equations is formed as follows: for every term $F_i = a \vee b \vee c$ we add the equation $a + b + c = 1$, where a, b, c are the corresponding variables (respectively $a + b = 1$ for $F = a \vee b$). Then for every pair (a, b) of the new variables that corresponds to some Boolean variable X_i and its negation, we add the equation $ab = 0$.

Let us prove that this system has a solution with values from $\{0, 1\}$ iff the original satisfiability problem has a solution. Indeed, if $x_1, x_2, \ldots$ form the solution of the satisfiability problem, i.e., the truth value of F is "true," then the truth values of all the F_i are also true. So for every $F_i = a \vee \cdots$ at least one of the terms $a, \ldots$ has the truth value "true." Take one of them, and assign to the corresponding real variable the value 1 and to all the others the value 0. Then $a + b + \cdots = 1$ by definition, and $ab = 0$ for a, b that correspond to x_i and $\tilde{x}_i$, because we assign 1 only in case the corresponding logical term has truth value "true," and x_i and $\tilde{x}_i$ cannot both take this truth value.

Conversely, assume that we have found a solution of the above-defined system of quadratic equations. Let us show how to construct the solution of the satisfiability problem. We show how to assign truth values to $x_1, \ldots, x_n$. If at least one of the real variables corresponding to x_i equals 1, then we assign "true;" if at least one real variable corresponding to $\tilde{x}_i$ equals 1, then we assign "false" to x_i; in the remaining cases we assign whatever. The equations $ab = 0$ guarantee that this assignment is correct, i.e., we cannot assign both the values "true" and "false." Then the fact that $a + b + \cdots = 1$ means that at least one of the corresponding terms in F_i "true," so all F_i have the truth value "true," and therefore F is true for these x_i.

3. We have proved that the satisfiability problem can be reduced to the problem of whether some system of quadratic equations has a solution with values from $\{0, 1\}$, i.e., whether there exist such values of the variables $a, b, c, \ldots$ that satisfy all these equations and each of them equals to 0 or 1. Our ultimate goal is to try to reduce the satisfiability problem to the quantum prediction problem. In the latter problem all the conditions on the variables s_i are in terms of quadratic inequalities, so if we want our problem to look like this we must reformulate this additional condition that all the variables take only the values 0 or 1 in terms of quadratic inequalities (in particular, quadratic equations).

This can be done easily, because the condition that $a = 0$ or $a = 1$ is equivalent to the equation $a(1 - a) = 0$. So if we add an equation $a(1 - a) = 0$ for all the variables a to the system, described in step 2, we can make the following conclusion: if the resulting system has a solution in real numbers, then, given this solution, we can easily compute the solution of the original satisfiability problem.

4. This system has both linear and quadratic terms, and we want to reduce the satisfiability problem to the case of quadratic inequalities that have no linear terms. So in order to come closer to the desired form, let us reduce the satisfiability problem to quadratic equations, for which there are no linear terms. Assume M is the total number of variables in the system

constructed in step 3. For convenience, let us denote these variables by y_1, $y_2, \ldots, y_M$. To undertake the desired reduction, let us introduce a new variable y_{M+1}, add a new equation $y_{M+1}^2 = 1$, and change every equation $y_i + y_j + y_k = 1$ to $y_i y_{M+1} + y_j y_{M+1} + y_k y_{M+1} = 1$, and $y_i - y_i^2 = 0$ to $y_i y_{M+1} - y_i^2 = 0$. If $y_1, \ldots, y_M$ is a solution of the old system, then adding $y_{M+1} = 1$, we get the solution of the new system. Conversely, if $y_1, \ldots, y_{M+1}$ form a solution of the new system, then $y_{M+1} = 1$ or -1, and one can easily check that the values $y_i' = y_{M+1} y_i$ satisfy the old system.

5. So we have reduced the satisfiability problem to the problem of solving the system of quadratic equations with no linear parts. We want to reduce the system to one that corresponds to the prediction problem in quantum mechanics. There we have complex variables s_i—and we have real variables y_i, but this is not a contradiction, because real numbers are a particular case of complex ones. However, two things are different: first, the quadratic equations in the quantum case are of the special form (As, s) for self-adjoint A, and, second, there is the additional demand that $|s|^2 = 1$. We show in two steps how to reduce the quadratic equations we get to these kinds of equations.

The absence of the linear parts means that each equation can be represented in the following form: the sum of terms proportional to $y_i y_j$ for some i, j ($i = j$ or $i > j$) is equal to some fixed value a (0 or 1). If we denote the coefficients at $y_i y_j$ by a_{ij} and set $a_{ij} = 0$ if there is no such term in the equation, then this equation takes the following form: the sum of the terms $a_{ij} y_i y_j$ (for all i less than or equal to j) is equal to a. There is a standard way to represent this equation in terms of $(Ay, y) = a$ for some symmetric matrix A: just take $A_{ii} = a_{ii}$ and $A_{ij} = A_{ji} = \frac{1}{2} a_{ij}$ for $i < j$. The matrix A is real and symmetric, and hence self-adjoint. It is also easy to check that all the coefficients of the matrix A are either 0 or 1 or $\frac{1}{2}$—all of them binary rational, so all these matrices are efficiently defined observables in the sense of Section 3.

6. So we have already reduced the satisfiability problem to the problem of whether a given system of quadratic equations $(Ay, y) = a$ has a solution. This is not yet a quantum prediction problem, because in that problem we look only for solutions that are states ($|s|^2 = 1$), and in our system it is not necessarily true that $|y|^2 = 1$. So we need a further reduction.

Some estimates for $|y|^2$ can be deduced from this system of equations: namely, for every variable it is true that $y_i = 1$ or 0, so $|y|^2$ (the sum of $M+1$ terms $|y_i|^2$) is not greater than $M+1$. So if we take $s = cy$, where c is a small constant [so that $c^2(M+1) < 1$], then $|s|^2$ will be less than 1. Every equation $(Ay, y) = a$ is equivalent to $(As, s) = c^2 a$, so we have reduced the initial NP-hard problem to the problem of finding s_i that satisfy the system of the quadratic equations $(As, s) = a'$ and we know that all possible solutions of

this system satisfy the inequality $|s|^2 < 1$. Let us now add one more variable s_{M+2} and the additional equation $s_1^2 + s_2^2 + \cdots + s_{M+1}^2 + s_{M+2}^2 = 1$. If this new system has a solution, then $S_1, \ldots, s_{M+1}$ form the solution of the old system. Conversely, if $s_1, \ldots, s_{M+1}$ is a solution of the old system, then we can take s_{M+2} equal to the square root of $1 - s_1^2 - s_2^2 - \cdots - s_{M+1}^2$ (we have already proved that it is positive); then the resulting vector will satisfy all the quadratic equations and also the additional equation $|s|^2 = 1$.

7. This system is almost completely in the desired form; the only thing that we still have to check is that all the estimates a^-, a^+ (in our case, numbers $a' = ac^2$) are binary rational numbers. Here $a = 0$ or 1; so we must take c such that c^2 is binary rational. For example, we can take $c = 2^{-k}$, where k is so big that $c^2 = 2^{-2k} < 1/(M+1)$. This choice of c completes the reduction.

8. So for every propositional formula F in the 3-CNF form we have constructed a quantum prediction problem such that F is satisfiable iff this problem is solvable. Therefore, if we have an algorithm for deciding whether quantum prediction problems are solvable or not, we immediately get an algorithm for solving the satisfiability problems—or, in mathematical terms, that the quantum prediction problem is NP-hard.

9. Let us now prove that the state reconstruction problem is also NP-hard. Suppose that there exists an algorithm that solves the state reconstruction problem and its running time is always limited by some polynomial $P(n)$, where n is the length of the input data. Let us show that we are now able to solve satisfiability problems in polynomial time.

Indeed, suppose we have a formula F in the 3-CNF form. Following the above scheme, let us construct a quantum prediction problem corresponding to F. The total number of variables s_i in that problem is $M+2$, where M is limited from above by the length n of the formula F; the number of equations that come from $a+b+c=1$ is also at most n; and there are no more than M^2 equations coming from $ab=0$; so the total number of the equations is bounded by a constant times n^2. Hence the number B of bits necessary to store the data of this problem is bounded by Cn^2. In formulating this problem there was a tiny ambiguity about choosing c. Let us choose $c = 2^{-k}$, where k is the minimal one, for which $c^2 < 1/(M+1)$; so k is of order $\log_2 M$.

Let us take $e = c/4$ and apply the state reconstruction algorithm. Simultaneously with this algorithm, start running a timer that will stop this algorithm after $P(B)$ steps. So this combined algorithm will stop in any case after $P(B)$ steps, i.e., taking into consideration that $B < Cn^2$, in the time bounded by a polynomial of n.

In case the prediction problem has a solution, this algorithm will produce the approximate values S_i to some solution s_i of the prediction

problem, i.e., produce the real values S_i such that $|S_i - s_i| < e$ for all i. We show that this precision is sufficient to reconstruct the solution of the satisfiability problem from S_i. Indeed, the truth values are assigned to the variables x_i of the propositional formula F depending on whether the variables y_i in the above construction are equal to 0 or 1. In terms of $s_i = cy_i$ this means that we have to check whether s_i is equal to 0 or c. If we know S_i such that $|S_i - s_i| < c/4$, then in the first case $S_i < c/4$, in the second case $S_i > 3/4c$; so by comparing every S_i with $c/2$, we get all the information that is necessary for reconstructing Boolean variables.

In view of that, we can propose the following algorithm for checking whether it is possible to assign truth values to x_i so that F is true: namely, we first run the above-described combined algorithm. If it does not generate any S_i at all, this means that the quantum prediction problem has no solution at all: because otherwise this combined algorithm would produce its solution. If it generates some S_i, reconstruct truth values for x_i from them and substitute them into the given formula F. If the resulting truth value for F is "true," this means that the formula is satisfiable in the sense that such truth values exist. If the resulting truth is "false," this means that the formula is not satisfiable, because otherwise the quantum prediction problem would be solvable, and our algorithm would generate its solution, for which, as we have already proved, the corresponding truth values of x_i lead to "true" for F.

So if we have a polynomial algorithm for state reconstruction, then we get a polynomial algorithm for satisfiability. Hence the state reconstruction problem is also NP-hard. QED

ACKNOWLEDGMENTS

One of the authors (V.K.) is greatly thankful to Vladimir Lifschitz (Stanford) and Yuri Gurevich (Ann Arbor, Michigan) for valuable comments on the first version of this paper (Kosheleva and Kreinovich, 1989).

REFERENCES

Garey, M., and Johnson, D. (1979). *Computers and Intractability: A Guide to the Theory of NP-Completeness*, Freeman, New York.

Kosheleva, O. M., and Kreinovich, V. Ya. (1989). Quantum prediction problem is intractable, Center for New Informational Technology "Informatika", Leningrad, Technical Report.

Von Neumann, J. (1955). *Mathematical Foundations of Quantum Mechanics*, Princeton University Press, Princeton, New Jersey.