Completing the physical representation of quantum algorithms provides a retrocausal explanation of the speedup

Giuseppe Castagnoli

Citation: AIP Conference Proceedings **1841**, 020004 (2017); doi: 10.1063/1.4982768
View online: https://doi.org/10.1063/1.4982768
View Table of Contents: http://aip.scitation.org/toc/apc/1841/1
Published by the American Institute of Physics

Articles you may be interested in

The retrocausal tip of the quantum iceberg
AIP Conference Proceedings **1841**, 020005 (2017); 10.1063/1.4982769

How retrocausality helps
AIP Conference Proceedings **1841**, 020001 (2017); 10.1063/1.4982765

Is there really "retrocausation" in time-symmetric approaches to quantum mechanics?
AIP Conference Proceedings **1841**, 020002 (2017); 10.1063/1.4982766

Janus sequences of quantum measurements and the arrow of time
AIP Conference Proceedings **1841**, 020003 (2017); 10.1063/1.4982767

Preface and Acknowledgements: Quantum Retrocausation III
AIP Conference Proceedings **1841**, 010001 (2017); 10.1063/1.4982764

Quantum entanglement in time
AIP Conference Proceedings **1841**, 020007 (2017); 10.1063/1.4982771

Completing the Physical Representation of Quantum Algorithms Provides a Retrocausal Explanation of the Speedup

Giuseppe Castagnoli[1,a)]

[1]*Elsag Bailey ICT Division and Quantum Information Laboratory, Via Puccini 2, 16154 Genova, Italy*

[a)]Corresponding author: giuseppe.castagnoli@gmail.com

Abstract. The usual representation of quantum algorithms, limited to the process of solving the problem, is physically incomplete as it lacks the initial measurement. We extend it to the process of setting the problem. An initial measurement selects a problem setting at random, and a unitary transformation sends it into the desired setting. The extended representation must be with respect to Bob, the problem setter, and any external observer. It cannot be with respect to Alice, the problem solver. It would tell her the problem setting and thus the solution of the problem implicit in it. In the representation to Alice, the projection of the quantum state due to the initial measurement should be postponed until the end of the quantum algorithm. In either representation, there is a unitary transformation between the initial and final measurement outcomes. As a consequence, the final measurement of any $\mathcal{R}$-th part of the solution could select back in time a corresponding part of the random outcome of the initial measurement; the associated projection of the quantum state should be advanced by the inverse of that unitary transformation. This, in the representation to Alice, would tell her, before she begins her problem solving action, that part of the solution. The quantum algorithm should be seen as a sum over classical histories in each of which Alice knows in advance one of the possible $\mathcal{R}$-th parts of the solution and performs the oracle queries still needed to find it – this for the value of $\mathcal{R}$ that explains the algorithm's speedup. We have a relation between retrocausality $\mathcal{R}$ and the number of oracle queries needed to solve an oracle problem quantumly. All the oracle problems examined can be solved with any value of $\mathcal{R}$ up to an upper bound attained by the optimal quantum algorithm. This bound is always in the vicinity of $\frac{1}{2}$. Moreover, $\mathcal{R} = \frac{1}{2}$ always provides the order of magnitude of the number of queries needed to solve the problem in an optimal quantum way. If this were true for any oracle problem, as plausible, it would solve the quantum query complexity problem.

INTRODUCTION

The present work is a defense of the retrocausal interpretation of the quantum computational speedup pursued in [1 – 5]. We show that this interpretation comes from completing the physical representation of quantum algorithms. Since the use of retrocausality in quantum mechanics is controversial, showing that it answers the well accepted requirement of completing the physical description should be of interest.

This discussion is in the context of *oracle computing*. Bob, *the problem setter*, chooses a function out of the set of functions $\{f_{\mathbf{b}}\}$ and gives Alice, *the problem solver*, a black box that computes it. The function identifier **b**, which we call the *problem setting*, ranges over the set of all the possible problem settings σ_B. Alice knows the set of functions but not Bob's choice. She is to find some characteristic of the function computed by the black box (e. g. the period of the function) by performing *function evaluations*. Traditionally, in the literature, the black box is also called the *oracle* and function evaluation the *oracle query*.

The usual representation of quantum algorithms, limited to Alice's problem-solving action, consists of the input-output transformation typical of computations. Alice unitarily sends an input state into an output state which encodes the solution of the problem; then acquires the solution by a final measurement.

This representation is physically incomplete as it lacks the initial measurement: from the foundational perspective pursued in the present work, the complete representation of a quantum process must consist of an initial measurement, a unitary transformation of the measurement outcome, and a final measurement. Also, there is no physical representation of the value of **b**, which of course is essential in determining the quantum process. The value of **b** is naturally

Quantum Retrocausation III
AIP Conf. Proc. 1841, 020004-1–020004-13; doi: 10.1063/1.4982768
Published by AIP Publishing. 978-0-7354-1511-9/$30.00

taken into account in writing the result of function evaluation, but is, so to speak, done by hand from outside the physical process. Here we restore both the initial measurement and the physical representation of **b** by extending the representation of the quantum algorithm to the process of setting the problem.

As we move into uncharted waters, we summarize our retrocausal interpretation of the speedup, anticipating some formalizations. This should make the concepts we will discuss more tangible.

We use as an example the following problem. Bob hides a ball in one of four drawers. Alice is to locate it by opening drawers. This requires opening up to three drawers in the classical case, just one in the quantum case. We are dealing, of course, with the simplest instance of Grover's algorithm [6].

Let the four drawers be numbered $00, 01, 10, 11$ and **b** be the number of the drawer with the ball. Checking whether the ball is in drawer **a** amounts to computing the Kronecker function $\delta_{\mathbf{b}}(\mathbf{a}) \equiv \delta(\mathbf{b}, \mathbf{a})$, which is 1 if $\mathbf{b} = \mathbf{a}$ and 0 otherwise.

In the usual Grover algorithm, the number of the drawer that Alice wants to open **a** (i. e. the argument of function evaluation) is contained in a register A of basis vectors $|00\rangle_A$, $|01\rangle_A$, $|10\rangle_A$, $|11\rangle_A$. This register, under the control of Alice, will eventually contain the solution of the problem. A register V, of basis vectors $|0\rangle_V, |1\rangle_V$, is meant to contain the result of function evaluation modulo 2 added to its former content for logical reversibility.

As anticipated, the value of **b** is not represented physically. One should have it in mind when writing the result of function evaluation. Let us assume it is $\mathbf{b} = 01$. The usual algorithm is limited to the unitary transformation of the input state:

$$|\zeta\rangle_I = \frac{1}{\sqrt{2}} |00\rangle_A (|0\rangle_V - |1\rangle_V)$$

into the output state:

$$\Im_A U_f H_A |\zeta\rangle_I = \frac{1}{\sqrt{2}} |01\rangle_A (|0\rangle_V - |1\rangle_V),$$

where register A contains the solution of the problem – the number of the drawer with the ball 01. H_A is the Hadamard transform on register A. It transforms $|00\rangle_A$ into a uniform quantum superposition of all the possible values of **a**. U_f is function evaluation, performed in *quantum parallelism* [7] for all the possible values of **a**. It leaves the state of register V, $\frac{1}{\sqrt{2}}(|0\rangle_V - |1\rangle_V)$, unaltered when $\mathbf{a} \neq 01$, it changes it into $-\frac{1}{\sqrt{2}}(|0\rangle_V - |1\rangle_V)$ when $\mathbf{a} = 01$. For example, the superposition element $|10\rangle_A (|0\rangle_V - |1\rangle_V)$, for which $\delta(01, 10) = 0$, goes into itself; instead $|01\rangle_A (|0\rangle_V - |1\rangle_V)$, for which $\delta(01, 01) = 1$, goes into $-\ |01\rangle_A (|0\rangle_V - |1\rangle_V)$. The transformation $\Im_A$, applying only to register A, is the so called *inversion about the mean*. It makes the elements of the final state superposition properly interfere with one another. We do not need to go into further detail; all we need to know of the quantum algorithm is already there.

Eventually Alice acquires the solution by measuring the content of A, namely the observable $\hat{A}$ of eigenstates the basis vectors of register A and eigenvalues (correspondingly) 00, 01, 10, 11. Note that this final measurement leaves the quantum state unaltered. Thus, there is a unitary transformation between the initial and final measurement outcomes.

We extend the four drawer instance of Grover algorithm to the process of choosing the number of the drawer with the ball **b**. We need to add a possibly imaginary register B that contains **b**. This register, under the control of Bob, has basis vectors $|00\rangle_B$, $|01\rangle_B$, $|10\rangle_B$, $|11\rangle_B$. We assume that the initial state of register B is a mixture of all the possible drawer numbers. We represent it as a dephased quantum state superposition:

$$|\psi\rangle_B = \frac{1}{2}\left(e^{i\varphi_0} |00\rangle_B + e^{i\varphi_1} |01\rangle_B + e^{i\varphi_2} |10\rangle_B + e^{i\varphi_3} |11\rangle_B\right),$$

where the φ_i are random phases. This *random phase representation* [8] of a maximally mixed state allows us to keep the usual ket vector representation of quantum algorithms. We make a trivial use of it. We can always think that the φ_i are fixed phases so that we are dealing with pure quantum states. Only when we need to compute a von Neumann entropy, we should keep in mind that they are random. The von Neumann entropy of $|\psi\rangle_B$ is 2 bits.

The initial state of the three registers is now:

$$|\psi\rangle_I = \frac{1}{2\sqrt{2}}\left(e^{i\varphi_0} |00\rangle_B + e^{i\varphi_1} |01\rangle_B + e^{i\varphi_2} |10\rangle_B + e^{i\varphi_3} |11\rangle_B\right)|00\rangle_A (|0\rangle_V - |1\rangle_V). \tag{1}$$

Let the observable $\hat{B}$, of eigenstates the basis vectors of register B and eigenvalues (correspondingly) 00, 01, 10, and 11, be the content of register B. (Note, $\hat{A}$ and $\hat{B}$ commute.) At time t_0 Bob measures $\hat{B}$ selecting a problem setting (drawer number) at random, say 10. The state after measurement, at time t_0, is thus:

$$|\psi\rangle_0 = \frac{1}{\sqrt{2}} |10\rangle_B |00\rangle_A (|0\rangle_V - |1\rangle_V) . \tag{2}$$

Then, by the unitary transformation U_B, he sends it into the desired problem setting, say it is still 01. Thus, at time t_1, the state is

$$U_B |\psi\rangle_0 = \frac{1}{\sqrt{2}} |01\rangle_B |00\rangle_A (|0\rangle_V - |1\rangle_V) . \tag{3}$$

This is the input state of the quantum algorithm prepared by Bob – with the ball hidden in drawer 01. Alice unitarily sends it into the output state

$$\Im_A U_f H_A U_B |\psi\rangle_0 = \frac{1}{\sqrt{2}} |01\rangle_B |01\rangle_A (|0\rangle_V - |1\rangle_V) , \tag{4}$$

this at time t_2. Eventually she acquires the solution – the number of the drawer with the ball 01 – by measuring $\hat{A}$.

This extended representation is trivially similar to the usual one. However, there is already an important consequence. Before going to it, we should make a step backward to explicit things that are usually given for granted.

As is well known, the quantum state encapsulates everything that can be known about the quantum system between observations. In this discussion, the question "known by whom?" is essential. We adopt the answer of the Copenhagen interpretation: known by the observer.

Correspondingly, we can say that the quantum state (3), with register B in the sharp state $|01\rangle_B$, is the state to Bob, the problem setter, and any external observer (including ourselves). It tells all of them that the ball is in drawer 01. The consequence we were talking about is that it cannot be the state to Alice, the problem solver. It would tell her the number of the drawer with the ball 01 – the solution of the problem – before she opens any drawer. As well known, the value of $\mathbf{b}$ must be hidden inside the black box that computes $\delta_{\mathbf{b}}(\mathbf{a})$. This is why the box is called *black* in traditional computer science. However, in it, the concealment must be kept in mind, in order to write the right thing at the right moment. Here, we argue, it must be physically represented in quantum computer science, where things must in fact become physical [8].

To represent the concealment physically, we must resort to the relational interpretation of quantum mechanics of Rovelli [9, 10]. According to it, a quantum state has meaning with respect to an observer, like in the Copenhagen interpretation. What the relational interpretation rejects is the notion of absolute, or observer-independent, state of a system. In equivalent terms, it rejects the notion of observer-independent values of physical quantities [10]. This notion "*would be inadequate to describe the physical world beyond the* $\hbar \to 0$ *limit, in the same way in which the notion of observer-independent time is inadequate to describe the physical world beyond the* $c \to \infty$ *limit*" [10].

We refer to [9, 10] for the motivations and consequences of the relational interpretation in quantum mechanics. In the present context, the motivation is that this interpretation allows us to represent physically the concealment of the problem setting to the problem solver; the consequence will be the retrocausal interpretation of the computational speedup.

In relational quantum mechanics, a quantum state can be sharp to an observer and a quantum superposition, or a mixture, to another observer. This gives us the clue to represent the states of the quantum algorithm with respect to Alice.

As is well known, the projection of the quantum state due to a quantum measurement can be postponed at will along a unitary transformation that follows it. To Alice, we postpone the projection due to the initial Bob's measurement until the end of the unitary part of her problem-solving action. We should correspondingly *retard* – i. e. propagate forward in time – the two end states of the original projection by the unitary part in question. By *advancing* a projection, we mean propagating backward in time the two end states of it by the inverse of a unitary transformation that precedes the measurement. The notion of advancing and retarding a quantum state is taken from [11, 12].

By postponing the subject projection, the input state to Alice at time t_1 remains the initial state (1) of time t_0. Of course the unitary transformation U_B (applying to register B between t_0 and t_1 leaves the maximally mixed state of register B unaltered. The 2-bit entropy of the state of register B in the input state of the quantum algorithm to Alice represents her complete ignorance of the problem setting.

This time the unitary part of Alice's action $\Im_A U_f H_A$ sends the input state $U_B |\psi\rangle_I \equiv |\psi\rangle_I$, into the output state:

$$\Im_A U_f H_A U_B |\psi\rangle_I = \frac{1}{2\sqrt{2}} \begin{pmatrix} e^{i\varphi_0} |00\rangle_B |00\rangle_A + e^{i\varphi_1} |01\rangle_B |01\rangle_A \\ +e^{i\varphi_2} |10\rangle_B |10\rangle_A + e^{i\varphi_3} |11\rangle_B |11\rangle_A \end{pmatrix} (|0\rangle_V - |1\rangle_V) . \tag{5}$$

We can see that each possible problem setting is multiplied by the corresponding solution. The final measurement of the content of register A projects the output state on state (4). The measurement outcome is unpredictable to Alice as usual – though not to Bob and any external observer who already know that the number of the drawer with the ball is $\mathbf{b} = 01$.

We note that the projection of the quantum state due to the initial measurement, postponed until the end of the quantum algorithm, coincides in the present case with that due to the final measurement.

Either representation, for the fact of comprising initial measurement, unitary evolution, and final measurement, is time-symmetric [13 – 16]. This is so in a strong way as there is a unitary transformation between the initial and final measurement outcomes, what corresponds to the reversibility of the computation process [17 – 20]. There is, as a result, an ambiguity. The final measurement of any $\mathcal{R}$-th part of the solution (i. e. acquiring an $\mathcal{R}$-th part of the information that specifies it) could select back in time a corresponding part of the random outcome of the initial measurement. By selecting back in time we mean that the projection of the quantum state due to the measurement of an $\mathcal{R}$-th part of the solution at time t_2, advanced at time t_0 by the inverse of $\mathfrak{I}_A U_f H_A U_B$, selects a corresponding part of the random outcome of the initial measurement.

Considering for the time being a generic value of $\mathcal{R}$ in the interval $[0, 1]$ is necessary to represent this ambiguity. We will fix the value of $\mathcal{R}$ by comparing it with the number of function evaluations required by the quantum algorithm, as will soon become clear.

We note that $\mathcal{R}$ is a quantitative measure of retrocausality: $\mathcal{R} = 0$ means causality entirely forward in time (i.e. initial measurement outcome entirely selected by the initial measurement); whereas $\mathcal{R} = 1$ indicates causality entirely backward in time (i. e. initial measurement outcome entirely selected by the final measurement); and $0 < \mathcal{R} < 1$ indicates that the selection in question properly shares between initial and final measurements.

The advancement of the projection of the quantum state due to the measurement of an $\mathcal{R}$-th part of the solution, on its way to reaching the time t_0 of the initial measurement, at the intermediate time t_1 projects the input state to Alice, of maximal ignorance of the problem setting and thus of the solution, on one of lower entropy where she knows in advance an $\mathcal{R}$-th part of the solution and a corresponding part of the problem setting – we will give the detailed analysis of this shortly.

Correspondingly, the quantum algorithm should be seen as a sum over classical histories in each of which Alice knows in advance one of the possible $\mathcal{R}$-th parts of the solution and performs the function evaluations still needed to find it – this for the value of $\mathcal{R}$ that explains the algorithm speedup.

In the present four-drawer instance of Grover algorithm, the value of $\mathcal{R}$ that justifies the speedup is $\mathcal{R} = \frac{1}{2}$. Note that $\mathfrak{I}_A U_f H_A$ involves just one function evaluation, compared with three in the classical case. This means that Alice, at time t_1 and in each classical history, knows in advance half of the information that specifies the solution of the problem. Specifically, she knows that the ball is one of a pair of drawers. Opening either drawer allows her to locate it.

Summing up, given an oracle problem, the present retrocausal interpretation of the speedup gives us a physically founded relation between $\mathcal{R}$ and the number of function evaluations needed to solve it in a quantum fashion. It is the number required to classically solve the problem given the advanced knowledge of an $\mathcal{R}$-th part of the solution.

This relation can be applied in two ways. Given a quantum algorithm, we can find the value of $\mathcal{R}$ that justifies its speedup. Conversely, given an oracle problem, we can find the number of function evaluations needed to solve it with retrocausality $\mathcal{R}$. The importance of the relation essentially depends on the following.

All the oracle problems examined can be solved with *any* value of $\mathcal{R}$ up to an upper bound attained by the optimal quantum algorithm. This bound is always close to $\frac{1}{2}$. Conversely, $\mathcal{R} = \frac{1}{2}$ always provides an order of magnitude estimate of the number of function evaluations needed to solve the problem in an optimal quantum way. If this were true for any oracle problem, as is plausible because it holds for a large diversity of problems solvable with quadratic and exponential speedups, this result should be of great practical importance. Further investigations seem warranted.

COMPLETING THE PHYSICAL REPRESENTATION

Here we provide the details of the retrocausal interpretation of the speedup in the four-drawer instance of Grover algorithm. Then we generalize to any number of drawers and eventually to quantum oracle computing.

Time symmetric and relational representations

We have seen that completing the usual representation of the quantum algorithm creates two relational representations, one with respect to Bob, the problem setter, and any external observer, the other with respect to Alice, the problem solver, who cannot see the problem setting. In either representation there is a unitary evolution between the initial and final measurement outcomes. Consequently, the selection of the random outcome of the initial measurement could be partly ascribed to the final measurement. As we are in the context of reversible computation, we consider unjustified the common way of removing this redundancy, which is to ascribe all the selection to the measurement performed first. Sharing the selection between the initial and final measurements should be the reversible way of eliminating the redundancy.

Sharing the selection of the random outcome of the initial measurement between the initial and final measurements

To share the selection of the random outcome of the initial measurement between the initial and final measurements, we must reduce the complete measurements, of $\hat{B}$ and $\hat{A}$, to partial measurements, say of $\hat{B}_i$ and $\hat{A}_j$, satisfying the following conditions: (i) together, they select the random outcome of the initial measurement and (ii) the information selected by either partial measurement performed alone is not selected by the other. The no-redundancy condition (ii) is an application of Occam's razor; we give up the condition that everything is selected by the measurement performed first, not the economic condition that there are no redundant selections.

We quantitatively characterize the sharing by saying that the measurement of $\hat{A}_j$ acquires an $\mathcal{R}$-th part of the information that specifies the solution, with $\mathcal{R} \in [0, 1]$. We wish to acknowledge that the present definition of the retrocausality measure $\mathcal{R}$ was inspired by the work of Dolev and Elitzur on the non-sequential behavior of the wave function highlighted by partial measurement [14]. $\mathcal{R} = \frac{1}{2}$ exactly justifies the speedup of the present instance of Grover algorithm.

To start with, we need a complete definition of the unitary transformation U_B. Let it be:

$$U_B \equiv |11\rangle\langle 00|_B + |10\rangle\langle 01|_B + |01\rangle\langle 10|_B + |00\rangle\langle 11|_B \,,$$

Effectively, U_B changes zeros into ones and ones into zeros.

One way of having $\mathcal{R} = \frac{1}{2}$ compatibly with the above conditions is by assuming that the initial measurement of $\hat{B}$ reduces, for example, to that of $\hat{B}_0$ (the content of the left cell of register B) and the final measurement of $\hat{A}$ to that of $\hat{A}_1$ (the content of the right cell of register A). Note that the outcomes of the complete measurements should be left unaltered, we should only share their selections between the two partial measurements.

Let's see how the two representations of the quantum algorithm develop, starting with that to Bob and any external observer. Here the measurement of $\hat{B}_0$ at time t_0, selecting the left digit of the number contained in register B, must select the 1 of the outcome of the initial measurement $\mathbf{b} = 10$. This projects the initial state (1) on:

$$|\xi\rangle = \frac{1}{2}\left(e^{i\varphi_2}|10\rangle_B + e^{i\varphi_3}|11\rangle_B\right)|00\rangle_A\left(|0\rangle_V - |1\rangle_V\right). \tag{6}$$

At time t_2, state (6) has evolved into:

$$\Im_A U_f H_A U_B |\xi\rangle = \frac{1}{2}\left(e^{i\varphi_2}|01\rangle_B|01\rangle_A + e^{i\varphi_3}|00\rangle_B|00\rangle_A\right)\left(|0\rangle_V - |1\rangle_V\right). \tag{7}$$

Then the measurement of $\hat{A}_1$, selecting the right digit of the number contained in register A, must select the 1 of the number of the drawer with the ball 01. This projects state (7) on the original output state to Bob and external observer (4). Advancing the two ends of the projection by the inverse of $\Im_A U_f H_A U_B$ naturally projects state (6) on the state to Bob and external observer (2).

Summing up, the two partial measurements rebuild the selection of the initial measurement outcome while leaving the original quantum algorithm to Bob and any external observer unaltered. In the present example, retrocausality would only say that the right digit of the random outcome of the initial measurement has been selected back in time by the final measurement, an apparently unverifiable thing. Retrocausality is inconsequential in this representation, which is the conventional quantum algorithm up to the representation of Bob's choice.

Things change dramatically in the representation with respect to Alice.

Here the measurement of $\hat{B}_0$ at time t_0 does not alter the original quantum algorithm, since the projection of the quantum state associated with it must anyhow be postponed until the end of the algorithm. We can go directly to the output state to Alice (5), at time t_2, when the measurement of $\hat{A}_1$ acquires the right digit of $\mathbf{a} = 01$. This projects that output state on:

$$|\chi\rangle = \frac{1}{2}\left(e^{i\varphi_1}|01\rangle_B|01\rangle_A + e^{i\varphi_3}|11\rangle_B|11\rangle_A\right)(|0\rangle_V - |1\rangle_V). \tag{8}$$

Also now we should propagate this projection backward in time until it selects, at time t_0, the right digit of the outcome of the initial measurement, namely the 0 of 10.

What is interesting is the value of this backward propagation at time t_1, immediately after U_B and before the unitary part of Alice's action $\Im_A U_f H_A$. We should advance the two ends of the projection of state (5) on state (8) by the inverse of $\Im_A U_f H_A$. The result is the projection of the input state to Alice (1) on the state:

$$H_A^\dagger U_f^\dagger \Im_A^\dagger |\chi\rangle = \frac{1}{2}\left(e^{i\varphi_1}|01\rangle_B + e^{i\varphi_3}|11\rangle_B\right)|00\rangle_A(|0\rangle_V - |1\rangle_V). \tag{9}$$

This is a remarkable consequence. State (9), the input state to Alice under the assumption that the selection of the random outcome of Bob's measurement equally shares between the initial and final measurements, tells her, before she performs any function evaluation, that the number of the drawer with the ball is either $\mathbf{b} = 01$ or $\mathbf{b} = 11$. We will say that Alice *knows in advance* that $\mathbf{b} \in \{01, 11\}$. We take this as a metric notion: advanced knowledge of part of the problem setting or, identically, of the solution brings the solution closer in the metric of quantum computation – we will further discuss this point in the next section.

In the following we will use a convenient notation. Here the set of the problem settings σ_B is $\{00, 01, 10, 11\}$. Alice's advanced knowledge, for example that $\mathbf{b} \in \{01, 11\}$, is thus represented by a subset of σ_B; we will say for short that the measurement of $\hat{A}_1$ in the output state projects σ_B on the subset $\{01, 11\}$, whereas $\mathbf{b} \in \{01, 11\}$ represents Alice's advanced knowledge.

Sum over classical histories

We need to reconcile the notion of advanced knowledge of half of the information that specifies the solution with the fact that such a half can be taken in a plurality of ways.

Moreover, we need an operational interpretation of the advanced knowledge notion. At an elementary level, knowledge is action [21]. Advanced knowledge of half solution on the part of the problem solver means that she can find the solution with a correspondingly reduced number of function evaluations.

We kill two birds with one stone by resorting to Feynman's path integral formulation of quantum mechanics [22]. We see the quantum algorithm as a sum over classical histories in each of which Alice knows in advance one of the possible halves of the solution and performs the function evaluations needed to find the other half. The sum covers all the possible ways of taking half solution.

This explains the speedup of the present instance of Grover algorithm, namely the fact that Alice needs just one function evaluation to find the solution. In each history, Alice knows in advance that the ball is in a pair of drawers. Opening either drawer allows her to locate it.

An example of history is:

$$e^{i\varphi_1}|01\rangle_B|00\rangle_A|0\rangle_V \, H_A \rightarrow e^{i\varphi_1}|01\rangle_B|11\rangle_A|0\rangle_V \, U_f \rightarrow e^{i\varphi_1}|01\rangle_B|11\rangle_A|0\rangle_V \, \Im_A \rightarrow e^{i\varphi_1}|01\rangle_B|01\rangle_A|0\rangle_V .$$

The left-most state is one of the elements of the input state superposition (1). The state after each arrow is one of the elements of the quantum superposition generated by the unitary transformation of the state before the arrow; the transformation in question is specified above the arrow.

In the history we are dealing with, the problem setting is $\mathbf{b} = 01$. Register B is correspondingly in $|01\rangle_B$ throughout the unitary part of Alice's action, which of course does not change the problem setting chosen by Bob. (To this end, register B must be the *control register* of function evaluations. This means that any basis vector of B affects the transformation while remaining unaltered through it; moreover, the other unitary transformations of Alice's action must not apply to B.) Alice performs function evaluation for $\mathbf{a} = 11$ (the content of register A in the second and third state is correspondingly $|11\rangle_A$). The basis vectors of registers B and A always remain unaltered through function evaluation; that of register V also remains unaltered here because Bob's choice is $\mathbf{b} = 01$, and the argument of function

evaluation is $\mathbf{a} = 11$; thus the result of function evaluation is $\delta(01, 11) = 0$ that, (modulo 2) added to the content of register V before function evaluation, leaves it unaltered.

Therefore, we must assume that Alice's advanced knowledge in this history is $\mathbf{b} \in \{01, 11\}_B$. In fact the pair of drawers Alice knows in advance the ball to be in must include the drawer with the ball, namely drawer 01; since she tries function evaluation for $\mathbf{a} = 11$, this must be the number of the other drawer. As the result of function evaluation is zero, she finds that the ball must be in drawer 01.

In summary, each history is characterized by a number of the drawer with the ball, the argument of function evaluation chosen by Alice, a corresponding possible Alice's advanced knowledge, and the result of function evaluation, which tells Alice the solution of the problem.

Grover algorithm with $N > 4$

We now proceed to the case of $N = 2^n$ drawers, where n is the number of bits that specify the drawer number. The input and output states of Grover algorithm relativized to Alice are respectively:

$$|\psi\rangle_I = \frac{1}{2^{n/2}\sqrt{2}} \sum_{\mathbf{b}\in\sigma_B} e^{i\varphi_{\mathbf{b}}} |\mathbf{b}\rangle_B |\mathbf{0}\rangle_A (|0\rangle_V - |1\rangle_V), \tag{10}$$

$$\mathcal{U}U_B |\psi\rangle_I = \frac{1}{2^{n/2}\sqrt{2}} \sum_{\mathbf{b}\in\sigma_B} e^{i\varphi_{\mathbf{b}}} |\mathbf{b}\rangle_B |\mathbf{b}\rangle_A (|0\rangle_V - |1\rangle_V), \tag{11}$$

where $\sigma_B \equiv \{0, 1\}^n$, $\mathbf{0}$ is a bit string of n zeros, and $\mathcal{U} = \left(\Im_A U_f H_A\right)^{k(n)}$, with $k(n) = \frac{\pi}{4 \arcsin 2^{-n/2}} - \frac{1}{2}$. Here $k(n)$ is the number of function evaluations required to solve Grover problem with 2^n drawers; H_A, U_f, and $\Im_A$ are respectively the Hadamard transform, function evaluation, and inversion about the mean of the four drawers case extended to n-qubit registers; their sequence is iterated $k(n)$ times. By the way, we have $k(2) = 1$, in fact the number of function evaluations of the four-drawers case.

With n sufficiently large, $k(n)$ can be approximated by $k(n) \simeq \frac{\pi}{4} 2^{n/2}$. To have this number of function evaluations, according to the present retrocausal interpretation of the speedup, Alice must know in advance that the ball is in a subset of σ_B of about $\frac{\pi}{4} 2^{n/2}$ drawers (σ_B is 2^n drawers). Correspondingly, sharing the selection of the initial random measurement outcome between the initial and final measurements should reduce Alice's ignorance of the number of the drawer with the ball from the original n bit to $\lg_2 \frac{\pi}{4} 2^{n/2}$ bit, namely $(n/2 - 0.348)$ bit. This means that Alice knows in advance $n - (n/2 - 0.348) = (n/2 + 0.348)$ bits of the solution. Dividing by n yields the corresponding value of $\mathcal{R}$, namely $\mathcal{R} \simeq \frac{1}{2} + \frac{0.348}{n}$.

Summing up, when n is greater than 2, the value of $\mathcal{R}$ that explains the speedup of Grover algorithm is slightly greater than $\frac{1}{2}$, reverting to $\frac{1}{2}$ for $n \to \infty$.

It is interesting to see what equation (9), becomes in the case of a generic n. The selection of an $\mathcal{R}$-th part of the solution, with $\mathcal{R} \simeq \frac{1}{2} + \frac{0.348}{n}$, is associated with the projection of state (11) on:

$$|\chi\rangle = \frac{2}{\sqrt{\pi} 2^{n/4}} \sum_{\mathbf{b}\in\sigma'_B} e^{i\varphi_{\mathbf{b}}} |\mathbf{b}\rangle_B |\mathbf{b}\rangle_A (|0\rangle_V - |1\rangle_V),$$

where σ'_B is any subset of σ_B with $\frac{\pi}{4} 2^{n/2}$ drawers. Advancing the two ends of this projection at time t_1, by the inverse of $\mathcal{U}$, yields the projection of the input state to Alice (10) on:

$$\mathcal{U}^\dagger |\chi\rangle = \frac{2}{\sqrt{\pi} 2^{n/4}} \sum_{\mathbf{b}\in\sigma'_B} e^{i\varphi_{\mathbf{b}}} |\mathbf{b}\rangle_B |\mathbf{0}\rangle_A (|0\rangle_V - |1\rangle_V).$$

Here the state of register B represents Alice's advanced knowledge of an $\mathcal{R}$-th part of the solution with $\mathcal{R} \simeq \frac{1}{2} + \frac{0.348}{n}$.

All the above holds for the optimal Grover algorithm. Interestingly, there is always a quantum algorithm that solves Grover's search problem with any value of $\mathcal{R}$ from the zero of a classical algorithm to the $\frac{1}{2} + \frac{0.348}{n}$ of Grover algorithm. This is Long algorithm [24, 25], which can be tuned to solve the problem by opening any number of drawers equal to or above the minimum number required by Grover algorithm. (Long algorithm always yields the solution with absolute certainty, Grover algorithm, with absolute certainty, only for $n = 2$.) It appears as if the value of $\mathcal{R}$ is limited to an upper bound that is slightly more than $\frac{1}{2}$, as attained by the optimal quantum algorithm.

Generalization to quantum oracle computing

Until now, the present retrocausal interpretation has been used to find the value of $\mathcal{R}$ that justifies the speedup of a known quantum algorithm. Now we show how, given an oracle problem, it can be used to compute Alice's advanced knowledge of the solution and thus the number of function evaluations required to solve it with retrocausality $\mathcal{R} = \frac{1}{2}\mathrm{R}{=}1\frac{}{2}$ for simplicity. This exactly justifies the speedup of the quantum algorithms considered in the following and, in all the cases examined, provides the order of magnitude for the number of function evaluations required to solve the oracle problem in an optimal quantum way.

A generic oracle problem can be formulated as follows. We have a set of functions $f_{\mathbf{b}} : \{0,1\}^n \to \{0,1\}^m$ with $m \leq n$. The suffix **b** ranges over the set of all the possible problem settings σ_B. Bob chooses one of these functions (a value of **b**) and gives Alice the black box that computes it. Alice (who knows the set of functions but not the function chosen by Bob) is to find a certain feature of the function (e. g. the value of **b** in Grover algorithm) by performing function evaluations for appropriate values of **a**. We call the feature in question $s(\mathbf{b})$, which is the solution of the problem and a function of **b**.

We provide a more general way of computing Alice's advanced knowledge, which is applicable to any oracle problem. The function of the partial observables $\hat{B}_i$ and $\hat{A}_j$ is the same as in the algorithm of Grover.

First we note that a partial measurement of the content of register A in the output state of the quantum algorithm can always be represented as a partial measurement of the content of register B. This is because, in the state in question, the content of register A is a function of that of B. Therefore, we can replace the measurement of a generic $\hat{A}_j$ by that of a generic $\hat{B}_j$.

At this point we have only the reduced density operator of register B, namely the trace over registers A and V of the state of the three registers. Let us go back to the four-drawers example. In the output state (5) (and in random phase representation), the reduced density operator of register B has the same form of the initial state of register B. We repeat it here for convenience:

$$|\psi\rangle_B = \frac{1}{2}\left(e^{i\varphi_0}|00\rangle_B + e^{i\varphi_1}|01\rangle_B + e^{i\varphi_2}|10\rangle_B + e^{i\varphi_3}|11\rangle_B\right). \tag{12}$$

Measuring $\hat{B}_1$ in the output state selects the right digit of the number of the drawer with the ball 01, projecting $|\psi\rangle_B$ on

$$\frac{1}{\sqrt{2}}\left(e^{i\varphi_1}|01\rangle_B + e^{i\varphi_3}|11\rangle_B\right). \tag{13}$$

Advancing this projection at time t_1 (the time of the input state), by $H_A^\dagger U_f^\dagger \Im_A^\dagger$, leaves it unaltered. In fact the unitary part of Alice's action does not change $|\psi\rangle_B$ or any projection thereof, like that of $|\psi\rangle_B$ on state (13). This is because any content of register B remains unaltered under this part of the action. At time t_1, the projection of (12) on (13) becomes the projection of the input state of register B, of maximal ignorance of the problem setting, on the state of lower entropy (13), which represents Alice's advanced knowledge.

At this point we can introduce a further simplification. The projection in question can be obtained simply by measuring $\hat{B}_1$ in the input state of register B. This selects the right digit of the number of the drawer with the ball 01, projecting (12) on (13).

At this point it is also convenient to move the measurement of $\hat{B}_0$ from the initial to the input state. To Alice, these two states are identical. It suffices to ask that the measurement selects part of the problem setting, no more of the random outcome of the initial measurement.

We end up with the problem of splitting the measurement of $\hat{B}$ in the input state to Alice into two partial measurements, of the generic $\hat{B}_i$ and $\hat{B}_j$, such that they select without any redundancy the problem setting chosen by Bob and evenly contribute to the selection of the solution – and evenly reduce the entropy of the reduced density operator of register A in the output state.

At this point we have lost the memory of which was the partial observable originally measured in the output state. It could have been either $\hat{B}_i$ or $\hat{B}_j$. Therefore, the measurement of either $\hat{B}_i$ or $\hat{B}_j$ projects the state of register B in the input state on an instance of Alice's advanced knowledge. We also say it projects σ_B

To find the pairs $\hat{B}_i$ and $\hat{B}_j$ that satisfy the above conditions, it is enough to know the input and output states of registers B and A in the representation with respect to Alice, it is not necessary to know the unitary transformation in between. (Of course, there can always be such a unitary transformation because the output $\mathbf{b}, s(\mathbf{b})$ conserves the memory of the input **b**.) In fact, to satisfy the condition that the measurements of $\hat{B}_i$ and $\hat{B}_j$ in the input state select

without redundancy the problem setting chosen by Bob, it is enough to consider the input state. The projection of $|\psi\rangle_B$ associated with either partial measurement, moved as it is from the input state to the output state, determines the corresponding reduction of the entropy of the reduced density operator of register A. (We should keep in mind that, in the output state, the content of register A is a function of that of B.) To satisfy the other condition, we should require that $\hat{B}_i$ and $\hat{B}_j$ are such that the entropy reductions in question are even.

The input and output states in turn can be written solely on the basis of the oracle problem, namely of all the pairs $\mathbf{b}$ and $s(\mathbf{b})$. In conclusion, we can compute Alice's advanced knowledge and, thus, the number of function evaluations required to solve the problem with retrocausality $\mathcal{R} = \frac{1}{2}$ solely on the basis of the problem itself. Going forward, we call this method of assessing the number of function evaluations required to solve an oracle problem with retrocausality $\mathcal{R} = \frac{1}{2}$ the *advanced knowledge rule*. In the following, we apply it to a variety of oracle problems.

DEUTSCH&JOZSA, SIMON, AND THE ABELIAN HIDDEN SUBGROUP ALGORITHMS

In this section we apply the advanced knowledge rule to compute the number of function evaluations required to solve (with retrocausality $\mathcal{R} = \frac{1}{2}$) the oracle problems addressed by the other major quantum algorithms. We will see that the number foreseen by the advanced knowledge rule is always that of the actual quantum algorithm. This also means that the exponential speedups of these algorithms, which are all optimal, are explained by $\mathcal{R}$

Deutsch&Jozsa algorithm

In the Deutsch&Jozsa's problem, Bob chooses the function out of the set of all the constant and *balanced* functions (ones with the same number of zeroes and ones) $f_{\mathbf{b}}(\mathbf{a}) : \{0,1\}^n \rightarrow \{0,1\}$. Array (14) gives the tables of four of the eight functions for $n = 2$:

$\mathbf{a}$	$f_{0000}(\mathbf{a})$	$f_{1111}(\mathbf{a})$	$f_{0011}(\mathbf{a})$	$f_{1100}(\mathbf{a})$	...
00	0	1	0	1	...
01	0	1	0	1	...
10	0	1	1	0	...
11	0	1	1	0	...

(14)

We use the table of the function – the sequence of function values for increasing values of the argument – as the suffix of the function. Alice knows the set of functions but not Bob's choice, and is to find whether the function chosen by Bob is constant or balanced by computing $f_{\mathbf{b}}(\mathbf{a})$ for appropriate values of $\mathbf{a}$. Classically, this requires in the worst case a number of function evaluations exponential in n. It requires just one function evaluation in the case of Deutsch&Jozsa algorithm [26].

We apply the advanced knowledge rule to compute the number of function evaluations required to solve Deutsch&Jozsa's problem with retrocausality $\mathcal{R} = \frac{1}{2}$. The state of registers B and A in the overall input (or, identically, initial) and output states of the quantum algorithm to Alice are:

$$\frac{1}{2\sqrt{2}}\left(e^{i\varphi_0}|0000\rangle_B + e^{i\varphi_1}|1111\rangle_B + e^{i\varphi_2}|0011\rangle_B + e^{i\varphi_3}|1100\rangle_B + ...\right)|00\rangle_A \tag{15}$$

$$\frac{1}{2\sqrt{2}}\left[\left(e^{i\varphi_0}|0000\rangle_B - e^{i\varphi_1}|1111\rangle_B\right)|00\rangle_A + \left(e^{i\varphi_2}|0011\rangle_B - e^{i\varphi_3}|1100\rangle_B\right)|10\rangle_A + ...\right]. \tag{16}$$

The pairs "problem setting - solution", namely $(\mathbf{b}, s(\mathbf{b}))$, are here $(0000, 00)$, $(1111, 00)$, $(0011, 10)$, etc. $s(\mathbf{b})$ is an intermediate solution. Measuring $\hat{A}$ in the output state (16) says that the function is constant if $s(\mathbf{b})$ is all zeros, balanced otherwise. Note that states (15) and (16) could be written solely on the basis of the oracle problem, namely of the pairs $(\mathbf{b}, s(\mathbf{b}))$. We do not need to know the unitary transformation in between, namely the unitary part of the quantum algorithm.

To start with, we should split in all possible ways the initial measurement of $\hat{B}$ into two partial measurements, of $\hat{B}_i$ and $\hat{B}_j$, that satisfy the advanced knowledge rule. Given the problem setting of a balanced function, there is only one pair of partial measurements of the content of register B compatible with this rule. With problem setting, say, $\mathbf{b} = 0011$, $\hat{B}_i$ must be the content of the left half of register B and $\hat{B}_j$ that of the right half. The measurement of $\hat{B}_i$ yields all zeros, that of $\hat{B}_j$ all ones.

In fact, a partial measurement yielding both zeroes and ones would provide enough information to identify the solution – the fact that $f_{\mathbf{b}}$ is balanced. Then the cases are two. If the other partial measurement does not contain both zeros and ones, it would not identify the solution; this would violate the requirement that the two partial measurements evenly contribute to the selection of the solution. If it did, the two partial measurements would be redundant with one another. Given that either partial measurement must yield all zeroes or all ones, it must concern the content of half register. Otherwise either the requirement of even contribution to the selection of the solution would be violated or the problem setting would not be completely determined, as is readily checked.

One can see that, with $\mathbf{b} = 0011$, the measurement of $\hat{B}_i$, performed alone, projects σ_B on the subset $\{0011, 0000\}_B$, that of $\hat{B}_j$ on $\{0011, 1111\}_B$. In either case the reduction of the entropy of ρ_A in the output state (16) is 1 bit (from 2 to 1 bit). Either subset represents a part of the problem setting that Alice knows in advance. The case of the problem setting of a constant function is analogous. The only difference is that there are more pairs of partial measurements that satisfy the above said conditions. (See [4].)

There is a shortcut to finding the subsets of σ_B that represent Alice's advanced knowledge. Here the problem setting – the bit string $\mathbf{b}$ – is the table of the function chosen by Bob. For example $\mathbf{b} = 0011$ is the table $f_{\mathbf{b}}(00) = 0, f_{\mathbf{b}}(01) = 0, f_{\mathbf{b}}(10) = 1, f_{\mathbf{b}}(11) = 1$. We call a *good half table* any half table in which all the values of the function are the same. One can see that good half tables are in one-to-one correspondence with the subsets in question. For example, the good half table $f_{\mathbf{b}}(00) = 0, f_{\mathbf{b}}(01) = 0$ corresponds to the subset $\{0011, 0000\}_B$, is the identical part of the two bit-strings in it. Thus, given a problem setting, i.e., an entire table, either a good half table, or identically the corresponding subset of σ_B, is a possible instance of Alice's advanced knowledge.

Because of the structure of tables, given the advanced knowledge of a good half table, the entire table, and thus the solution, can be identified by performing just one function evaluation for any value of the argument $\mathbf{a}$ outside the half table.

Summing up, the advanced knowledge rule says that Deutsch&Jozsa's problem can be solved with just one function evaluation. This is in agreement with Deutsch&Jozsa algorithm, what it also means is that the speedup of this algorithm is explained by quantum retrocausality $\mathcal{R} = \frac{1}{2}$; in fact the rule in question presupposes $\mathcal{R} = \frac{1}{2}$. Note that this algorithm, because it requires just one function evaluation, is necessarily optimal.

One can see that the present analysis, like the notion of good half table, holds unaltered for $n > 2$. Interestingly, also in the Deutsch&Jozsa problem there is always a quantum algorithm that solves it for any value of $\mathcal{R}$ from the zero of a classical algorithm to that of the optimal quantum algorithm – trivially in this case. The quantum algorithm for $\mathcal{R} = 0$ is any logically reversible classical algorithm in quantum notation, that for $\mathcal{R} = \frac{1}{2}$ is the optimal Deutsch&Jozsa algorithm. The same will apply to the quantum algorithms of the following section.

Simon and the Abelian hidden subgroup algorithms

Simon's problem consists in finding the "period" (up to bitwise modulo 2 addition) of a periodic function $f_{\mathbf{b}}(\mathbf{a}) : \{0,1\}^n \to \{0,1\}^{n-1}$. See [4] for details. Array (17) gives the tables of four of the six functions for $n = 2$:

$\mathbf{a}$	$f_{0011}(\mathbf{a})$	$f_{1100}(\mathbf{a})$	$f_{0101}(\mathbf{a})$	$f_{1010}(\mathbf{a})$	...
00	0	1	0	1	...
01	0	1	1	0	...
10	1	0	0	1	...
11	1	0	1	0	...

(17)

Note that each value of the function appears exactly twice in each table; thus 50% of the rows plus one always identify the period. Alice is to find the period of the function by performing function evaluation for appropriate values of $\mathbf{a}$.

Currently, a classical algorithm requires a number of function evaluations exponential in n. The quantum part of Simon algorithm [27] solves with just one function evaluation the hard part of this problem, which is finding a bit string *orthogonal* to the period. Again, see [4] for details.

We consider the following input and output states of registers B and A in the quantum algorithm to Alice:

$$\frac{1}{\sqrt{6}}\left(e^{i\varphi_0}|0011\rangle_B + e^{i\varphi_1}|1100\rangle_B + e^{i\varphi_2}|0101\rangle_B + e^{i\varphi_3}|1010\rangle_B + ...\right)|00\rangle_A\,, \tag{18}$$

$$\frac{1}{\sqrt{6}}\left[\left(e^{i\varphi_0}|0011\rangle_B + e^{i\varphi_1}|1100\rangle_B\right)|01\rangle_A + \left(e^{i\varphi_2}|0101\rangle_B + e^{i\varphi_3}|1010\rangle_B\right)|10\rangle_A + ...\right]. \tag{19}$$

In the output state, register A contains the period of the function identified in register B. Note that state (19) is not the output state of the usual Simon algorithm, where each period would be replaced by a mixture of the bit-strings orthogonal to it – one should then iterate the algorithm until finding a number of different strings sufficient to identify the period. Writing an output state with these mixtures would mean relying too much on our knowledge of Simon algorithm. We prefer to write the output state corresponding to the end problem, which is finding the period. We will see that this makes no difference in the end when comparing Simon algorithm with the present explanation for the speedup.

Here a good half table, which represents an instance of Alice's advanced knowledge like in Deutsch&Jozsa algorithm, is any half table where the values of the function are all different from one another (see [4]). In this way the half table does not allow one to find the period (here the solution of the problem). Since 50% of the rows plus one identify the period, this can always be identified by performing just one function evaluation for any value of the argument **a** outside the half table.

In summary, the advanced knowledge rule says that finding the period of the function, thus also any bit-string orthogonal to it, can be solved with just one function evaluation. This is in agreement with the usual Simon algorithm and says that the speedup of this algorithm is explained by $\mathcal{R} = \frac{1}{2}$. It also says that there should be a quantum algorithm (slightly) more efficient than that of Simon, that finds the period of the function with one function evaluation and no iterations. In [4] we have given this algorithm for the simplest case $n = 2$; finding such an algorithm for $n > 2$ should be the object of further study.

The present analysis, like the notion of good half table, holds unaltered for $n > 2$. It should also apply to the generalized Simon's problem and to the Abelian hidden subgroup problem. In fact, the corresponding algorithms are essentially Simon algorithm. In the Abelian hidden subgroup problem, the set of functions $f_{\mathbf{b}} : G \to W$ map a group G to some finite set W with the property that there exists some subgroup $S \leq G$ such that for any $\mathbf{a}, \mathbf{c} \in G$, $f_{\mathbf{b}}(\mathbf{ac})$ if and only if $\mathbf{a} + S = \mathbf{c} + S$. The problem is to find the hidden subgroup S by computing $f_{\mathbf{b}}(\mathbf{a})$ for the appropriate values of **a**. Now, a large variety of problems solvable with a quantum speedup can be re-formulated in terms of the Abelian hidden subgroup problem. Among these we find: the seminal Deutsch's problem, finding orders, finding the period of a function (thus the problem solved by the quantum part of Shor's factorization algorithm), discrete logarithms in any group, hidden linear functions, self-shift equivalent polynomials, Abelian stabilizer problem, graph automorphism problem [28].

DISCUSSION

It is natural to ask whether Alice's advanced knowledge of part of the solution she will read at the end of her problem solving action implies that information is sent back in time. The same question applies to the related fact that part of the outcome of the initial measurement, at time t_0, is selected back in time by the final measurement, at time t_2. Our answer is negative as long as, in either case, such an information could not be measured.

At the beginning of Alice's action, at time t_1, the information in question would be contained in register B. It would imply a reduction of the entropy of B, namely of the number of problem settings in superposition. By definition, the observer Alice cannot measure the content of register B at time t_1. The fact that this content is concealed to her is the premise of the present retrocausal interpretation of the speedup. Bob and any external observer do measure the content of register B at time t_0 and could repeat the measurement at time t_1, without affecting the quantum state. At time t_0, they see a completely random measurement outcome and have no way of knowing whether part of it is selected back in time by the final measurement. At time t_1, they would see the problem setting as freely chosen by Bob. In either case, no information coming from the future can be identified in the measurement outcome.

Here we would like to add a common sense consideration. The idea that Alice, in each classical history, knows in advance part of what she will read in the future might anyway conflict with our sense of physical reality. Our advice for the time being would be to stick to the quantum computation context, where Alice's advanced knowledge has a precise meaning and admits an apparently harmless metric interpretation. Another important question is whether the time-symmetric and relational interpretations of quantum mechanics are necessary to derive the present results; for example the advanced knowledge rule. An upstream question is, of course, whether these interpretations are necessary to quantum mechanics.

Rovelli drew an analogy between the relational interpretation and Einstein's special relativity theory – in both cases a physical quantity must be relativized to its observer. After noting the revolutionary impact of the 1905 Einstein's paper on special relativity, Rovelli [10] writes: *The formal content of special relativity, however is coded into*

the Lorentz transformations, written by Lorentz, not by Einstein, and before 1905. So, what was Einstein's contribution? It was to understand the physical meaning of the Lorentz transformations.... We could say – admittedly in a provocative manner – that Einstein's contribution to special relativity has been the interpretation of the theory, not its formalism: the formalism already existed. Elitzur expressed a similar consideration about the time symmetric interpretations of quantum mechanics [29]: even if they were pure interpretations, adding nothing to the formalism, they did allow and could allow us to see things that would be otherwise very difficult to see.

The retrocausal interpretation of the speedup lends itself to the same kind of consideration. The number of function evaluations required to solve an oracle problem in an optimal quantum way, presumably given in order of magnitude by the advanced knowledge rule, should also be implicit in the mathematics of unitary transformations, as follows. In the most general case, the transformation that represents the unitary part of Alice's problem solving action is (in the appropriate Hilbert space) a sequence of function evaluations, each preceded and followed by a suitable unitary transformation. In principle, these transformations could be seen as the unknowns of the problem of finding the optimal quantum algorithm. They should have variable matrix elements up to the unitarity of the transformation and the condition of not changing the problem setting. For a given number of function evaluations, we should find the values of these variables that maximize the probability of finding the solution with the final measurement; then repeat the procedure each time with that number increased by one; and stop when the probability of finding the solution reaches one. We would have obtained analytically the number of function evaluations required by the optimal quantum algorithm. The same number, in the order of magnitude and in a synthetic way, could be given by the advanced knowledge rule.

However, the analytic way is likely impracticable; it is so in present knowledge. In this case the synthetic one, based on the time-symmetric and relational interpretations, could provide a significant shortcut; it does in all the cases examined.

In the spirit of the above remarks, we assert that the retrocausal interpretation of the speedup is the correct (most compelling) physical interpretation of the mathematics of quantum algorithms. Although an interpretation, it would not be without consequences – physical meaning can be important, of course. Until now there was no fundamental explanation of the speedup, no unification of the quadratic and exponential speedups, no solution to the so called quantum query complexity problem, namely, that of estimating the number of oracle queries (function evaluations) required to solve an oracle problem in an optimal quantum way. The retrocausal interpretation provides a fundamental, quantitative, explanation of all kinds of speedup and promises to solve the quantum query complexity problem with the advanced knowledge rule.

CONCLUSION

The usual representation of quantum algorithms is limited to the process of solving the problem, namely to the input-output transformation typical of computation. The process of setting the problem and the initial measurement are missing. Completing the representation yields two time-symmetric and relational representations, one with respect to Bob (the problem setter) and any external observer, the other with respect to Alice (the problem solver), to whom the problem setting should be concealed.

In either representation, there is a unitary transformation between the random outcome of the initial measurement and the outcome of the final measurement. As a consequence, the final measurement of any $\mathcal{R}$-th part of the solution could select back in time a corresponding part of the initial measurement outcome. Considering a generic value of $\mathcal{R}$ in the interval $[0, 1]$ is mandatory for a complete analysis of this situation.

This is without consequences in the representation with respect to Bob and any external observer, which is a trivial extension of the usual quantum algorithm. In the representation with respect to Alice, it tells her, before she begins her problem-solving action, an $\mathcal{R}$-th part of the solution. Correspondingly, the quantum algorithm should be seen as a sum over classical histories in each of which Alice knows in advance one of the possible $\mathcal{R}$-th part of the solution and performs the function evaluations still required to find it, this for an appropriate value of $\mathcal{R}$.

In all the oracle problems examined, the value of $\mathcal{R}$ can vary from zero, which corresponds to the number of function evaluations required to solve the problem by a classical algorithm, to the maximum of the optimal quantum algorithm. This maximum is always in the vicinity of $\frac{1}{2}$. Additionally, $\mathcal{R} = \frac{1}{2}$ provides the order of magnitude for the number of function evaluations required by the optimal quantum algorithm. If this held for any oracle problem, the quantum query complexity problem would be solved. This conjecture would seem to be justified, as the sample of oracle problems examined is very diversified and covers both the quadratic and exponential speedups.

Further investigations of this conjecture seem warranted in the interests of both quantum computation and the foundations of quantum mechanics.

ACKNOWLEDGMENTS

I wish to thank David Ritz Finkelstein for many fruitful discussions in the development of the present approach to quantum speedup.

REFERENCES

[1] G. Castagnoli and D. R. Finkelstein, Proc. Roy. Soc. A **457**, 1799-1807 (2001).
[2] G. Castagnoli, Phys. Rev. A **82**, 052334-052342 (2010).
[3] G. Castagnoli, "Probing the mechanism of the quantum speed-up by time-symmetric quantum mechanics," in *Quantum Retrocausation II*, Proceedings of the 92nd Annual Meeting of the Pacific Division of the
American Association for the Advancement of Science, D.P. Sheehan, Ed. (San Diego, CA, 2011).
[4] G.Castagnoli, Found. Phys. Vol. **46**, Issue 3, 360–381 (2016).
[5] G. Castagnoli, Quanta Vol. **5**, No 1, 34-52 (2016).
[6] L. K. Grover, "A fast quantum mechanical algorithm for database search" in Proc. 28th Annual ACM Symposium on the Theory of Computing, (ACM press New York 1996) pp. 212-219.
[7] D. Deutsch, Proc. Roy. Soc. A **400**, 97-117(1985).
[8] D. Bohm and D. A. Pines, Phys. Rev. **92**, 626-636 (1953).
[9] C. Rovelli, Int. J. Theor. Phys. **35**
[10] C. Rovelli "Relational Quantum Mechanics" (2011) http://xxx.lanl.gov/pdf/quant-ph/9609002v2
[11] J. A. Wheeler and R. P. Feynman, Rev. Mod. Phys. **17**, 157 (1945).
[12] J. Cramer, Rev. Mod. Phys. **58**, 647 (1986).
[13] Y. Aharonov, P. G. Bergman, and J. L. Lebowitz, Phys. Rev. B **134**, 1410-1416 (1964).
[14] S. Dolev and A. C. Eitzur, "Non-sequential behavior of the wave function" (2001) arXiv:quant-ph/0102109 v1.
[15] Y. Aharonov , S. Popescu, and J. Tollaksen, Physics Today November issue, 27-32 (2010).
[16] Y. Aharonov, E. Cohen, D. Grossman, and A. C. Elitzur "Can a Future Choice Affect a Past Measurement's Outcome?" (2012) arXiv:1206.6224
[17] R. Landauer "Irreversibility and heat generation in the computing process" IBM Journal of Research and Development; 5 (3), 183–191 (1961), doi:10.1147/rd.53.0183.
[18] D. R. Finkelstein "Space-time structure in high energy interactions" in *Fundamental Interactions at High Energy*, edited by
[19] T. Gudehus, G. Kaiser, A. Perlmutter, (Gordon & Breach, New York, 1969) pp. 324-338, https://www.researchgate.net/publication/23919490_Space-time_structure_in_high_energy_interactions
[20] C. H. Bennett, Int. J. Teor. Phys. **21** 905-940 (1982).
[21] E. Fredkin and T. Toffoli, Int. J. Theor. Phys. **21** 219-253 (1982).
[22] D. R. Finkelstein, (private communication).
[23] R. Feynman and A. R. Hibbs, *Quantum Mechanics And Path Integrals* (McGraw-Hill, New York, 1965).
[24] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, SIAM Journal on Computing Vol. **26** Issue 5, 1510-1523 (1997).
[25] G. L. Long, Phys. Rev. A **64** 022307-022314 (2001).
[26] F. M. Toyama, W. van Dijk, and Y. Nogami, Quantum Information Processing **12**, 1897-1914 (2013).
[27] D. Deutsch and R. Jozsa, Proc. Roy. Soc. A **439**, 553-558 (1992).
[28] D. Simon ,"On the power of quantum computation," in Proceedings of the 35th Annual IEEE Symposium on the Foundations of Computer Science (1994) pp. 116-123.
[29] P.Kaye, R. Laflamme, and M. Mosca "An Introduction To Quantum Computing" (Oxford University Press, 2007) pp.146-147.
[30] A. C. Eitzur, (private communication).