Highlighting the mechanism of the quantum speedup by time-symmetric and relational quantum mechanics

Giuseppe Castagnoli
Elsag Bailey ICT Division and Quantum Information Laboratory*

May 13, 2014

Abstract

Bob hides a ball in one of four drawers. Alice is to locate it. Classically she has to open up to three drawers, quantally just one. The fundamental reason for this quantum speedup is not known. We explain it by extending the usual representation of the quantum algorithm, limited to the process of solving the problem, to the process of setting the problem. The number of the drawer with the ball becomes a unitary transformation of the random outcome of the preparation measurement. This brings in relational quantum mechanics: the extension is *with respect to* Bob and cannot be with respect to Alice. It would tell her the drawer number before she opens any drawer. To Alice, the projection of the quantum state due to the preparation measurement should be retarded at the end of her search; in the input state of this search, the drawer number is determined to Bob and undetermined to Alice. A second consequence is the emergence of an ambiguity. Either the preparation measurement or the final one required to read the solution selects the solution. For reasons of symmetry, we assume that the selection shares evenly between the two measurements. All is as if Alice, by reading the solution, selected half of the information that specifies the drawer number. This selection leaves the input state to Bob unaltered and projects that to Alice on a state of lower entropy where she knows that half in advance. The quantum algorithm is a sum over histories in each of which Alice knows in advance that the ball is in a pair of drawers and locates it by opening one of the two. More in general, given an oracle problem, this explanation of the speedup predicts the number of queries required to solve it in an optimal quantum way.

1 Introduction

A quantum algorithm is said to deliver a quantum speedup when it requires fewer computation steps than its classical counterpart, sometimes fewer than

*retired
the number demonstrably necessary in the classical case. An example is as follows. Bob, the problem setter, hides a ball in one of four drawers, Alice, the problem solver, is to locate it. In the classical case, Alice might have to open up to three drawers. With Grover’s quantum search algorithm [1], it always takes one.

As noted in the literature [2], this violation of a limit applying to any classical time-evolution relates the quantum speedup to the violation of the temporal Bell inequality of Leggett and Garg [3], the information-theoretic one of Braunstein and Caves [4] and, particularly, the one formulated by Morikoshi [2] exactly in the case of Grover’s algorithm.

While there is an important body of literature on various mathematical relations between speedup and other quantum features, like entanglement and discord, an exact, quantitative explanation of the fundamental mechanism of the speedup has never been pinpointed.

As almost thirty years have passed since the discovery of the seminal speedup on the part of Deutsch [5], there should be no a-priori objection to adopting a novel perspective. The present explanation of the speedup relies on extending the usual representation of quantum algorithms, limited to the process of solving the problem, to the process of setting the problem (here the number of the drawer with the ball). We think that it is obvious in hindsight, but it would be so in a rather unconventional representation of quantum computation.

A simple use of mathematical representations makes things more clear. Besides Alice’s register $A$, meant to contain the solution of the problem at the end of the algorithm, we need an imaginary Bob’s register $B$, which contains the number of the drawer with the ball (i.e., the problem setting). We assume that, initially, register $B$ is in a maximally mixed state (the reason for this assumption will soon become clear), register $A$ in any sharp state. The initial state is thus:

$$|\psi\rangle = \frac{1}{2} (e^{\imath \phi_0} |00\rangle_B + e^{\imath \phi_1} |01\rangle_B + e^{\imath \phi_2} |10\rangle_B + e^{\imath \phi_3} |11\rangle_B) |00\rangle_A ,$$  

where 00, ..., 11 are the drawer numbers in binary notation, suffix $B$ ($A$) denotes Bob’s (Alice’s) register, and the $\phi_i$ are independent random phases with uniform distribution in $[0, 2\pi]$.

We are using the random phase representation [6] of the maximally mixed state of register $B$ — see Section 2.1 for further details. In view of the sum over histories representation, we need to keep the ket vector representation of quantum states. Reading state (1) is simple: register $B$ is in a decohered quantum superposition (mixture) of the four possible settings of the problem — phases are in fact randomized. The von Neumann entropy of state (1) is two bit.

In order to prepare register $B$ in the desired setting, in the first place Bob should measure its content, which we call observable $B$. The measurement outcome is completely random. Say it comes out:

$$P_B |\psi\rangle = |11\rangle_B |00\rangle_A ,$$  

where
where $P_B$ is the projection of the quantum state induced by Bob’s measurement. Then Bob applies to register $B$ a unitary transformation $U_B$ — a permutation of the drawer numbers — that changes the random outcome into the desired setting, say $|01\rangle_B$:

$$U_B P_B |\psi\rangle = |01\rangle_B |00\rangle_A. \quad (3)$$

State (3) is the input state of the quantum algorithm in the representation extended to the process of setting the problem, which is the usual representation up to the ket $|01\rangle_B$.

We can see that this extension immediately calls for another one, this time concerning the actors (observers) on the stage. We have to resort to the relational quantum mechanics of Rovelli [7]. States (1) through (3) constitute the description of the initial part of the quantum algorithm with respect to Bob, the problem setter, and any external observer who does not act on the problem solving process. They cannot be the description with respect to Alice, the problem solver. The input state (3), with register $B$ in the sharp state $|01\rangle_B$, would tell her, before she opens any drawer, that the ball is in drawer 01. Of course the number of the drawer with the ball should be hidden to Alice. In computer science language, to her it is inside a black box.

To physically represent this fact, it suffices to retard the projection $P_B$ at the end of the unitary part of Alice’s action (the projection induced by a quantum measurement can be retarded or advanced at will along a unitary evolution that respectively follows or precedes the measurement). This yields the representation of the quantum algorithm with respect to Alice.

To her, the state of register $B$ in the input state of the quantum algorithm is still maximally mixed. In fact, once removed $P_B$, $U_B$ leaves state (1) unaltered up to an irrelevant permutation of the random phases. Thus, disregarding this permutation, state (1) is the input state to Alice.

We started with register $B$ in a maximally mixed state to represent the fact that, to Alice, the problem setting is physically hidden. The two bit entropy of state (1) represents Alice’s complete ignorance of the setting.

The output state is:

$$UU_B |\psi\rangle = \frac{1}{2} \left( e^{i\varphi_0} |00\rangle_B |00\rangle_A + e^{i\varphi_1} |01\rangle_B |01\rangle_A + e^{i\varphi_2} |10\rangle_B |10\rangle_A + e^{i\varphi_3} |11\rangle_B |11\rangle_A \right), \quad (4)$$

where $U$, the unitary part of Alice’s action, involves opening a single drawer — see Section 2.1 for further details.

We can see that, for each possible problem setting, Alice has reconstructed it in register $A$. Eventually she acquires the reconstruction by reading the content of register $A$, namely by measuring the observable $\hat{A}$ commuting with $\hat{B}$.

Let $P_A$ be the projection of the quantum state induced by Alice’s measurement. Of course $P_A$ coincides with the retarded projection induced by Bob’s measurement. Thus, in present assumptions, it yields:

$$P_A UU_B |\psi\rangle = |01\rangle_B |01\rangle_A. \quad (5)$$
It is convenient to take small steps. Things are simpler if we think that $U_B$ is a fixed unitary transformation of the random outcome of Bob’s measurement and that this transformation is the identity. Say that the number of the drawer with the ball remains 01 and that the eigenvalue selected by Bob’s measurement was 01 instead of 11. In other words, the number of the drawer with the ball is the completely random outcome of Bob’s measurement. Under this assumption, there is clearly quantum correlation between this outcome and that of Alice’s measurement. Correspondingly, in the resulting time-symmetric [8, 9] representation of the quantum algorithm, either measurement, performed alone (ie with the other suppressed), selects the number of the drawer with the ball.

The measurement postulate does not specify which measurement selects this number. One can think of several ways of filling this gap. The selection could be entirely ascribed to Bob’s measurement, or to Alice’s measurement, or to both measurements (in which case there would be complete redundancy between the two measurements); alternatively, it could be shared between the two measurements.

By the way, one might wander whether choosing a disambiguation of the measurement postulate has any verifiable physical consequence. We anticipate the consequence of our choice: the prediction of the number of computation steps (here drawer openings) required by an optimal quantum algorithm. It is naturally a complex consequence, but this goes along with the fact that we are in the complex physical situation that originates the speedup.

The present disambiguation relies on Occam’s razor and keeping the equivalence between the two measurements for what concerns the selection of the number of the drawer with the ball (the drawer number for short). Let us refer more in general to a drawer number of $n$ binary digits. For Occam’s razor, we assume that Bob’s and Alice’s measurements, when they are considered together, act as partial measurements that tightly – without any redundancy – select the drawer number. Then, if one partial measurement (performed alone) selects $p$ of the bits that specify this number, the other (performed alone) must select the remaining $n - p$ bits. Eventually we keep the equivalence between the two measurements by requiring that $p = n - p = n/2$.

In other words, we are assuming that Alice’s measurement selects half of the bits that specify the drawer number. We will see how this can occur in a uniform quantum superposition of all the possible ways of taking half of the bits.

There is no risk of sending a message backward in time. In the outcome of Bob’s measurement, each digit of the drawer number is independently and randomly selected. We are just ascribing half of these selections to Alice’s rather than Bob’s measurement.

By the way, this kind of apparent retrocausation is sometimes invoked to explain EPR non-locality, but mostly as a curiosity because it is believed to be of no consequence. It has no consequences also in the representation with respect to Bob and any external observer. To them, it leaves the input state of the quantum algorithm – state 3 – unaltered. It just tells that, say, the left digit of the drawer number 01 has been randomly selected by Bob’s measurement.
and the right digit by Alice’s measurement – in fact an inconsequential thing.

Things change dramatically in the representation relativized to Alice – the problem solver.

Let us consider the above example: Alice’s partial measurement (ie Alice’s measurement in the presence of Bob’s measurement) contributes to the selection of the drawer number 01 by selecting the right digit. This means that it projects state (4) on:

\[ |\chi\rangle = \frac{1}{\sqrt{2}} (e^{i\varphi_1} |01\rangle_B |01\rangle_A + e^{i\varphi_3} |11\rangle_B |11\rangle_A) . \] (6)

We need to agree on the time at which the joint selection of the drawer number occurs. A reasonable assumption is that it has already taken place when Bob and any external observer see the number in question (of course Alice, to whom the number must be concealed, is excluded). In other words, we should assume that joint selection occurs at the time of Bob’s measurement. This implies that the projection of state (4) on state (6) propagates backward in time (along the representation relativized to Alice) to the time of Bob’s measurement.

Let us see the value of this propagation immediately before the application of \( U \); we should advance the two ends of the projection of (4) on (6) by the inverse of \( U \). The result is the projection of state (1), the input state of the quantum algorithm to Alice, on:

\[ U^\dagger |\chi\rangle = \frac{1}{\sqrt{2}} (e^{i\varphi_1} |01\rangle_B + e^{i\varphi_3} |11\rangle_B) |00\rangle_A . \] (7)

This is an outstanding consequence. State (7), the input state to Alice taking into account the contribution of her own measurement to the selection of the drawer number, tells her, before she opens any drawer, that this number is either 01 or 11 – that the right digit of the number is 1. In other words, Alice knows the contribution of her own measurement to the selection of the drawer number in advance. We note that we are at a fundamental level where knowing is doing [10]; knowing in advance half of the drawer number means the possibility of behaving consequently. It simply means that the quantum algorithm has to locate the ball knowing in advance it is in drawer \( b = 01 \) or \( b = 11 \).

Of course, there are many ways of selecting half of the drawer number – here a pair of drawers that includes the one with the ball. The quantum algorithm turns out to be a sum over classical histories in each of which Alice, knowing in advance that the ball is in one of these pairs, uses this information to locate it by opening either drawer. The sum is over all the possible pairs and choices of the drawer to open.

The second step is noting that nothing changes if \( U_B \), always seen as a fixed unitary transformation of the random outcome of Bob’s measurement, is not the identity. The third is noting that, in order to assess the contribution of Alice’s measurement to the selection of the drawer number, \( U_B \) should be seen
as a fixed unitary transformation even when it transforms the random outcome of Bob’s measurement into the desired drawer number. In fact the contribution in question depends on the quantum correlation between the outcomes of Bob’s and Alice’s measurements and this correlation remains there also in this case, as follows.

Of course, correlation is defined over an ensemble of repetitions of the same experiment, here consisting of the measurement of $\hat{B}$ in state $\mathbf{1}$, the unitary transformation $UU_B$, and the measurement of $\hat{A}$ in the resulting state $\mathbf{4}$. What can change over the ensemble are only the values of the measurement outcomes. In particular $U_B$ must be the same in all the elements of the ensemble, in fact a fixed unitary transformation. Over the ensemble, the drawer number, the fixed unitary transformation of a random measurement outcome, is a random variable as well. By the way, it becomes the desired Bob’s choice only in the element of the ensemble that actually occurred.

More in general, given an oracle problem (see Section 4 for the definition), the present explanation of the speedup allows to predict the number of oracle queries required to solve it in an optimal quantum way. We will see that this prediction fits exactly a variety of well-known, optimal quantum algorithms.

The present work belongs to an evolutionary approach. In [11], we introduced the time-symmetric representation of quantum algorithms and argued it should be important to understand the speedup. Through [12, 13], we showed that the sum over histories representation is a pattern common to various algorithms. [14] is a discussion of [13] in an AAAS meeting on quantum retro-causality.

The novelty of the present work is that the sum over histories representation is inferred from the disambiguation of the measurement postulate in a more general way that makes it applicable to oracle quantum computing. This is what allows foreseeing the number of oracle queries required to solve an oracle problem in an optimal quantum way.

The present work has also points of contact with works of Morikoshi. In [15], making reference to [12], this author highlights the problem-solution symmetry of Grover’s and the phase estimation algorithms and notes it may be relevant for the explanation of the speedup. In [2], the same author shows that Grover’s algorithm violates an information theoretic temporal Bell inequality. The present work will give an explanation of this fact.

The form of apparent retrocausality utilized for the present explanation of the speedup has been inspired by the work of Dolev and Elitzur [16] on the non-sequential behavior of the wave function highlighted by partial measurement.

## 2 Grover’s algorithm

We formalize the present explanation of the speedup on Grover’s algorithm, but in a way that makes it applicable to oracle quantum computing in general.

Let $\mathbf{b}$ and $\mathbf{a}$, belonging to $\{0, 1\}^n$, be respectively the number of the drawer with the ball and that of the drawer that Alice wants to open. Opening drawer
“a” amounts to evaluating the function $f_b(a)$, which is one if $a = b$ and zero otherwise – tells Alice whether the ball is in drawer $a$.

Given the set of the functions $f_b(a)$ for all $b \in \{0, 1\}^n$, Bob chooses one of these functions (ie a value of $b$) and gives Alice the black box that computes it. Alice is to find the value of $b$ by performing function evaluations for appropriate values of $a$. Of course Alice is forbidden to inspect the value of $b$ contained in the black box (hence the name).

### 2.1 Representation relativized to the problem solver

Alice’s register $A$ contains $a$. Bob’s register $B$ contains $b$. This latter register was used in [17] to derive a lower bound on the computational complexity of Grover’s algorithm, in [11] through [14] in former stages of the present theory was used in [17] to derive a lower bound on the computational complexity of

In view of the sum over histories representation, we need the fully detailed relational representation of Grover’s algorithm already given in [13]. We repeat it here for convenience. With $n = 2$, the input state of the quantum algorithm to Alice is:

$$|\psi\rangle = \frac{1}{2\sqrt{2}} \left( e^{i\phi_0} |00\rangle_B + e^{i\phi_1} |01\rangle_B + e^{i\phi_2} |10\rangle_B + e^{i\phi_3} |11\rangle_B \right) |00\rangle_A \left( |0\rangle_V - |1\rangle_V \right).$$

Register $V$ is meant to contain the result of the computation of $f_b(a)$ modulo 2 added to its former content for logical reversibility. One can do without this register like we did in the introduction, but unitary transformations become more difficult to explain. We have seen that the $\phi_i$ are independent random phases with uniform distribution in $[0, 2\pi]$.

By the way, the usual density operator is the average over all $\phi_i$ of the product of the ket by the bra:

$$\rho = \langle |\psi\rangle |\psi\rangle_{\phi_i} = \frac{1}{8} \left( |00\rangle_B \langle 00|_B + |01\rangle_B \langle 01|_B + |10\rangle_B \langle 10|_B + |11\rangle_B \langle 11|_B \right)$$

$$|00\rangle_A \langle 00|_A \left( |0\rangle_V - |1\rangle_V \right) \left( |0\rangle_V - |1\rangle_V \right) .$$

Alice applies the Hadamard transform $H_A$ to register $A$:

$$H_A |\psi\rangle = \frac{1}{4\sqrt{2}} \left( e^{i\phi_0} |00\rangle_B + e^{i\phi_1} |01\rangle_B + e^{i\phi_2} |10\rangle_B + e^{i\phi_3} |11\rangle_B \right)$$

$$\left( |00\rangle_A + |01\rangle_A + |10\rangle_A + |11\rangle_A \right) \left( |0\rangle_V - |1\rangle_V \right).$$

Function evaluation is represented by the unitary transformation $U_f$:

$$U_f H_A |\psi\rangle = \frac{1}{4\sqrt{2}} \left[ e^{i\phi_0} |00\rangle_B \left( |00\rangle_A + |01\rangle_A + |10\rangle_A + |11\rangle_A \right) + e^{i\phi_1} |01\rangle_B \left( |00\rangle_A - |01\rangle_A + |10\rangle_A + |11\rangle_A \right) + e^{i\phi_2} |10\rangle_B \left( |00\rangle_A + |01\rangle_A - |10\rangle_A + |11\rangle_A \right) + e^{i\phi_3} |11\rangle_B \left( |00\rangle_A + |01\rangle_A + |10\rangle_A - |11\rangle_A \right) \right] \left( |0\rangle_V - |1\rangle_V \right).$$
Note that when \( f_b(a) = 0 \) nothing changes, when \( f_b(a) = 1 \) the term \((|0\rangle_V - |1\rangle_V)\) changes into \((- (|0\rangle_V - |1\rangle_V))\). From here are the minus signs in the superpositions of eigenstates of \( A \).

We also note that \( H_A \) can be defined as the transformation that maximizes the amount of information about the value of \( b \) that goes from register \( B \) to register \( A \) with function evaluation. In \((10)\), four orthogonal states of register \( B \), each a different value of \( b \), one by one multiply four orthogonal states of register \( A \). This means that the information that specifies the value of \( b \) has propagated to register \( A \).

To make this information accessible to measurement, Alice applies to register \( A \) the unitary transformation \( \Im_A \) (the inversion about the mean), which diagonalizes the reduced density operator of register \( A \) yielding the output state:

\[
\Im_A U_f H_A |\psi\rangle = \frac{1}{2\sqrt{2}} \left( e^{i\phi_0} |00\rangle_B |00\rangle_A + e^{i\phi_1} |01\rangle_B |01\rangle_A + e^{i\phi_2} |10\rangle_B |10\rangle_A + e^{i\phi_3} |11\rangle_B |11\rangle_A \right) (|0\rangle_V - |1\rangle_V) .
\]

In view of what will follow, we note that \( H_A \) and \( \Im_A \), the unitary transformations that precede and follow function evaluation \( U_f \), can also be defined as the transformations that maximize the probability of finding the solution in register \( A \) at the end of the unitary part of Alice’s action.

Alice acquires the solution – the number of the drawer with the ball – by measuring \( \hat{A} \), what projects state \((11)\) on:

\[
P_A \Im_A U_f H_A |\psi\rangle = \frac{1}{\sqrt{2}} (|01\rangle_B |01\rangle_A (|0\rangle_V - |1\rangle_V) .
\]

As in the introduction, we are assuming that the problem setting was \( b = 01 \).

### 2.2 Quantum feedback

We formalize the notion that Alice, by reading the solution at the end of the algorithm, contributes to selecting the problem setting at the beginning.

The starting point is the fact that either Bob’s or Alice’s measurement, performed alone (with the other suppressed), selects the solution of the problem. In Grover’s algorithm, either measurement also selects the problem setting but we should disregard this further commonality. It is redundant in this algorithm and absent in other quantum algorithms.

The measurement postulate, which states that the measurement of an observable selects one of its eigenvalues projecting the quantum state on the corresponding eigenstate, does not say which measurement selects the solution. We disambiguate the postulate by sharing the selection of the solution between the two measurements in a way that avoids any redundancy and keeps the equivalence between the two measurements for what concerns the selection. We introduce some notations first:

The state of register \( B \) in (the overall) states \((8)\) through \((11)\) is:

\[
|\psi\rangle_B = \frac{1}{2} \left( e^{i\phi_0} |00\rangle_B + e^{i\phi_1} |01\rangle_B + e^{i\phi_2} |10\rangle_B + e^{i\phi_3} |11\rangle_B \right) .
\]
\( |\psi\rangle_B \) is the random phase representation of the reduced density operator of register \( B \), namely \( \rho_B = \langle |\psi\rangle_B \langle \psi|_B \rangle^\rho_{\psi} = \frac{1}{4} (|00\rangle_B \langle 00|_B + |01\rangle_B \langle 01|_B + \cdots) \). Of course, it does not change along the unitary part of the quantum algorithm \( \mathcal{H}_A U_f H_A \): Alice’s action does not change the problem setting.

The state of register \( A \) in the output state \( |11\rangle \) is:

\[ |\psi\rangle_A = \frac{1}{2} \left( e^{i\varphi_0} |00\rangle_A + e^{i\varphi_1} |01\rangle_A + e^{i\varphi_2} |10\rangle_A + e^{i\varphi_3} |11\rangle_A \right). \]

Let \( \mathcal{E}_A \) be the von Neumann entropy of \(|\psi\rangle_A\). We have \( \mathcal{E}_A = 2 \) bit (in general, \( n \) bit). Since either Bob’s or Alice’s measurement performed alone (with the other suppressed) selects the solution, either measurement performed alone zeroes \( \mathcal{E}_A \). This can be written:

\[ \Delta \mathcal{E}_A (\hat{B}) = \Delta \mathcal{E}_A (\hat{A}) = \mathcal{E}_A, \tag{13} \]

where \( \Delta \mathcal{E}_A (\hat{B}) \) is the reduction of \( \mathcal{E}_A \) induced by the measurement of \( \hat{B} \) performed alone, \( \Delta \mathcal{E}_A (\hat{A}) \) that induced by the measurement of \( \hat{A} \) performed alone.

Now we can move to sharing the selection of the solution between the two measurements. It might be easier to think that all measurements are performed in state \( |11\rangle \). Since \( \mathcal{H}_A U_f H_A \) is the identity on \( |\psi\rangle_B \), it is indifferent to measure \( \hat{B} \) in state \( |8\rangle \) or \( |11\rangle \).

We apply Occam’s razor. In Newton’s formulation, it states “We are to admit no more causes of natural things than such that are both true and sufficient to explain their appearances” [18]. In the present context, the razor requires determination without over-determination. To avoid over-determination, we assume that Bob’s and Alice’s measurements effectively act as partial measurements that “tightly” – without any redundancy – select both the setting and the solution of the problem.

For example, let \( \hat{B}_0 \), of eigenvalue \( b_0 \), be the content of the left cell of register \( B \) and \( \hat{A}_1 \), of eigenvalue \( a_1 \), that of the right cell of register \( A \) (we have \( b \equiv b_0 b_1 \) and \( a \equiv a_0 a_1 \)). The initial Bob’s measurement could act as the measurement of \( \hat{B}_0 \) and the final Alice’s measurement as that of \( \hat{A}_1 \). With problem setting \( b = 01 \), the selections performed by these partial measurements must be respectively \( b_0 = 0 \) and \( a_1 = 1 \), what projects state \( |11\rangle \) on \( |12\rangle \). Thus, the solution of the problem is selected without over-determination. We say that the measurements of \( \hat{B}_0 \) and \( \hat{A}_1 \) constitute a pair of complementary partial measurements.

More in general, we require that all pairs of complementary partial measurements – which we call \( \{\hat{B}_i, \hat{A}_j\} \) – satisfy the following conditions:

1. Together, the two partial measurements select both the setting and the solution of the problem. Any part (Boolean function) of either the setting or the solution that is selected by one partial measurement performed alone, it is not by the other performed alone. For example, if Bob’s partial measurement (performed alone) selects the value of the left digit of
the number of the drawer with the ball, Alice’s partial measurement (performed alone) should not provide any information about the value of this digit.

2 Let $\Delta E_A(\hat{B}_i)$ be the reduction of the entropy of $|\psi\rangle_A$ associated with the measurement of $\hat{B}_i$ (performed alone), $\Delta E_A(\hat{A}_j)$ that associated with the measurement of $\hat{A}_j$ (performed alone). We require:

$$\forall \{\hat{B}_i, \hat{A}_j\} : \Delta E_A(\hat{B}_i) = \Delta E_A(\hat{A}_j) = \epsilon_A,$$

where $\epsilon_A$ is a free parameter but for the condition of being the same for all pairs. The system of equations (14) is generated by replacing, in equation (13), the two complete measurements $\hat{B}$ and $\hat{A}$ by pairs of complementary partial measurements and $\epsilon_A$ by $\epsilon_A$. Leaving $\epsilon_A$ free of being determined by conditions 1 and 2 is necessary to avoid over-determination. The equivalence between the two measurements for what concerns the selection of the solution is kept by requiring that Bob’s and Alice’s partial measurements reduce $\epsilon_A$ of the same amount.

Being a specification of the measurement postulate, conditions 1 and 2 are necessarily axiomatic and thus hypothetical in character. Their possible value is being part of a mechanism that predicts the number of function evaluations required by an optimal quantum algorithm.

Applying these conditions to Grover’s algorithm yields the result anticipated in the introduction. Here the problem setting is specified by an unstructured $n$-bit string, namely with each bit independently and randomly selected. Thus condition 1 implies that Bob’s partial measurement (performed alone) selects $p$ of these bits and Alice’s partial measurement (performed alone) the remaining $n - p$ bits. Then we must have $\Delta E_A(\hat{B}_i) = p$ bit and $\Delta E_A(\hat{A}_j) = n - p$ bit. Condition 2 – the system of equations (14) – implies $p = n - p = n/2$.

In words, Alice’s partial measurement (ie Alice’s measurement in the presence of Bob’s measurement) selects “half” of the problem setting (half of the bits that specify it). The fact that there are many ways of taking this half will engage with a sum over histories representation of the quantum algorithm: each history will be associated with one of the possible half settings. We call this retroaction of the output of the quantum process on the input quantum feedback. It is present in the representation of the quantum algorithm with respect to Alice and absent in that with respect to Bob and the external observer.

With respect to the introduction, the merit of conditions 1 and 2 is that they can be applied to the case that $b$ is structured. Let $\sigma_B$ be the set of the problem settings; for example in Grover’s algorithm we have $\sigma_B \equiv \{00, 01, 10, 11\}_B$. One can see that any partial measurement of the content of register $B$ or $A$ (performed alone) selects a subset of $\sigma_B$ and conversely is identified by this subset. Still in the case of Grover’s algorithm and under the assumption that the problem setting is $b = 01$, the measurement of $B_0$ selects $b_0 = 0$ or, in
equivalent terms, the subset \( \{01, 00\}_B \), that of \( \hat{A}_1 \) selects \( a_1 = b_1 = 1 \) or the subset \( \{01, 11\}_B \).

Therefore, given a problem setting, one should identify all the pairs of subsets of \( \sigma_B \) such that the corresponding partial measurements satisfy conditions 1 and 2. Always in Grover’s algorithm and with \( b = 01 \), these are all the pairs among the three subsets \( \{01, 00\}_B, \{01, 10\}_B, \) and \( \{01, 11\}_B \).

Since the contribution of Alice’s measurement to the selection of the problem setting can always be seen as a partial measurement of the content of register \( B \), the system of equations (14) can also be replaced by:

\[
\forall \{\hat{B}_i, \hat{B}_j\} : \Delta E_A (\hat{B}_i) = \Delta E_A (\hat{B}_j) = \epsilon_A,
\]

where the measurement of \( \hat{B}_j \) represents the contribution of Alice’s measurement to the selection.

### 2.3 Advanced knowledge

Since \( U = 3_A U_f H_A \) sends the initial state of register \( V \) into itself, we can disregard this register. Then the example of the introduction holds unaltered. With problem setting \( b = 01 \), Alice can know in advance that the ball is in drawer either 01 or 11, namely that \( b \in \{01, 11\}_B \).

Now that we know that \( U \) is the identity on the reduced density operator of register \( B \), we can follow a shortcut with respect to the introduction. In the example in question, the measurement of \( \hat{A}_j \) projects \( |\psi\rangle_B \) on \( |\psi\rangle_B' = \frac{1}{\sqrt{2}} (e^{i\varphi_1} |01\rangle_B + e^{i\varphi_3} |11\rangle_B) \). The two ends of this projection do not change if advanced by \( U^\dagger \). In particular \( |\psi\rangle_B' \) – which tells us that \( b \in \{01, 11\}_B \) – remains unaltered under the advancement in question. It represents the part of the problem setting selected by Alice’s measurement at the end of \( U \), Alice’s advanced knowledge at the beginning of \( U \).

In general, with \( U \) that sends the initial state of register \( V \) into itself and is the identity on the reduced density operator of register \( B \), Alice knows in advance her contribution to the selection of the problem setting.

### 2.4 Sum over histories

We need to reconcile the quantum algorithm with the fact that Alice knows in advance half of the information that specifies the problem setting, of course taking into account the fact that there are many ways of taking this half.

For this purpose, we introduce a semi-classical representation of the quantum algorithm, a sort of information theoretic transposition of Feynman’s [19] sum over histories. A history is a classical trajectory of the quantum registers, namely a causal sequence of sharp register states. For example:

\[
e^{i\varphi_1} |01\rangle_B |00\rangle_A |0\rangle_V \xrightarrow{H_A} e^{i\varphi_1} |01\rangle_B |11\rangle_A |0\rangle_V \xrightarrow{U_f} e^{i\varphi_2} |01\rangle_B |01\rangle_A |0\rangle_V \xrightarrow{U_f} e^{i\varphi_1} |01\rangle_B |01\rangle_A |0\rangle_V.
\]

(16)
The left-most state is one of the elements of the initial state superposition \(S\). The state after each arrow is one of the elements of the superposition generated by the unitary transformation of the state before the arrow; the transformation in question is specified above the arrow. We note that the amplitude of each state has module one, we are relying on the ray notation of quantum states; the overall superposition of histories at a given time (step) is un-normalized. In the final superposition identical states interfere constructively when the contents of Bob’s and Alice’s registers are the same, destructively otherwise – thus rebuilding state \((11)\).

Of course the quantum algorithm can always be decomposed into a superposition of such histories. Presently there are in total 128 different histories: \(8 \times 4 \times 1 \times 4\) (after \(H_A\) \times 1 \times \Im_A\)).

Let us focus on history \((10)\). Its leftmost state tells us that the problem setting is \(b = 01\). Up to this point, Alice’s advanced knowledge could be \(b \in \{01, 00\}_B\), or \(b \in \{01, 10\}_B\), or \(b \in \{01, 11\}_B\). However, in the second state of the history, Alice chooses to open drawer \(a = 11\). Since we are assuming that Alice, along each history, exploits her advanced knowledge of half of the the problem setting, this half must be \(b \in \{01, 11\}_B\). Function evaluation yields \(f_{01}(11) = 0\). This, besides telling Alice the solution (the ball must be in drawer 01), leaves the content of register \(V\) unaltered (third state). The fourth state is an element of the superposition \(\Im_A e^{i\varphi_1} |01\>_B |11\>_A |0\>_V\).

One can readily check that Grover’s algorithm is a sum over classical histories in each of which Alice performs the function evaluations necessary to identify the solution starting from her advanced knowledge of one of the possible halves of the problem setting.

One can also see – equations \((8)\) through \((11)\) – that function evaluation is preceded and followed by non-computational unitary transformations (\(H_A\) and \(\Im_A\)) that maximize the probability of finding the solution in Alice’s register at the end of the algorithm, bringing it to one. Evidently conditions \(1\) and \(2\), being fundamental in character, foresee the number of function evaluations taken by an optimal quantum algorithm.

The above clearly generalizes to any value of \(n\). It explains why Grover’s algorithm requires \(O\left(2^{n/2}\right)\) function evaluations against the \(O(2^n)\) of the classical case. This goes along with the fact that Alice knows in advance \(n/2\) of the bits that specify the number of the drawer with the ball. By the way, we should keep in mind that Grover’s algorithm is optimal for any value of \(n\) [20].

It also explains why the violation of Morikoshi’s temporal Bell inequality seems to imply that Grover’s algorithm exploits unperformed computations [2]; this is exactly what happens in each and every history the algorithm is made of. Of course the computations that are not performed in one history are performed in the other ones.
3 Deutsch&Jozsa’s algorithm

In Deutsch&Jozsa’s [21] problem, the set of functions is all the constant and balanced functions (with the same number of zeroes and ones) \( f_b : \{0, 1\}^n \rightarrow \{0, 1\} \). Array (17) gives four of the eight functions for \( n = 2 \).

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

(17)

The bit string \( b \equiv b_0, b_1, ..., b_{2^n-1} \) is both the suffix and the table of the function \( f_b(a) \) – the sequence of function values for increasing values of the argument; the reason for this choice will soon become clear. Alice is to find whether the function chosen by Bob is constant or balanced by computing \( f_b(a) \) for appropriate values of \( a \). Classically, this requires in the worst case a number of function evaluations exponential in \( n \). It requires just one function evaluation in the quantum case.

### 3.1 Representation relativized to the problem solver

The input and output states of the quantum algorithm relativized to Alice are respectively:

\[
|\psi\rangle = \frac{1}{4} (e^{i\varphi_0} |0000\rangle_B + e^{i\varphi_1} |1111\rangle_B + e^{i\varphi_2} |0011\rangle_B + e^{i\varphi_3} |1100\rangle_B + ... ) |00\rangle_A (|0\rangle_V - |1\rangle_V),
\]

(18)

\[
H_A U_f H_A |\psi\rangle = \frac{1}{4} [ (e^{i\varphi_0} |0000\rangle_B - e^{i\varphi_1} |1111\rangle_B ) |00\rangle_A + ( e^{i\varphi_2} |0011\rangle_B - e^{i\varphi_3} |1100\rangle_B ) |10\rangle_A + ... ] (|0\rangle_V - |1\rangle_V),
\]

(19)

where \( H_A \) is the Hadamard transform on register \( A \), \( U_f \) is function evaluation, and register \( V \) is always meant to contain the result of function evaluation reversibly added to its former content.

Measuring \( \hat{A} \) in state (19) says that the function is constant if the eigenvalue selected is all zeros, balanced otherwise. By the way, by ”solution of the problem”, we will always call the full eigenvalue.

We can see that also this quantum algorithm is optimal. It consists of a single function evaluation preceded and followed by two unitary transformations (both \( H_A \)) that maximize the probability of finding the solution in register \( A \) at the end of the algorithm, in fact bringing it to one.

### 3.2 Quantum feedback

Let \( \sigma_B \equiv \{0000, 1111, 0011, 1100, ...\} \) be the set of the problem settings. Given a particular setting, we should find the pairs of subsets of \( \sigma_B \) such that the
corresponding \( \{ \hat{B}_i, \hat{B}_j \} \) satisfy conditions 1 and 2 (Section 2.2). One can check that, for each setting, there is only one pair of such subsets. With \( b = 0011 \), it is: \( \{ 0011, 0000 \}_B \) and \( \{ 0011, 1111 \}_B \). We can see that \( \hat{B}_i \) is the content of the left half of register \( B \) and \( \hat{B}_j \) that of the right half: under the assumption \( b = 0011 \), measuring \( \hat{B}_i \) in state (19) selects \( \frac{1}{\sqrt{2}} (e^{i\phi_0} |0000\rangle_B + e^{i\phi_2} |0011\rangle_B) \), which corresponds to the subset \( \{ 0011, 0000 \}_B \), etc. Either subset represents a possible contribution of Alice’s measurement to the selection of the problem setting. The system of equations (15) is satisfied with \( \Delta \mathcal{E}_A (\hat{B}_i) = \Delta \mathcal{E}_A (\hat{B}_j) = 1 \) bit (from two to one bit).

There is a shortcut to finding the subsets in question. The problem setting – the bit string \( b \) – is the table of the function chosen by Bob. For example \( b = 0011 \) is the table \( f_{b} (00) = 0, f_{b} (01) = 0, f_{b} (10) = 1, f_{b} (11) = 1 \). We call ”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 \( f_{b} (00) = 0, f_{b} (01) = 0 \) corresponds to the subset \( \{ 0011, 0000 \}_B \), is in fact the identical part of the two strings in it.

Thus, given the problem setting, i.e. the entire table, either good half table is the contribution Alice’s measurement to the selection of the table.

### 3.3 Advanced knowledge

Also in the present case the unitary part of the quantum algorithm, \( H_A U_f H_A \), sends the initial state of register \( V \) into itself and is the identity on the reduced density operator of register \( B \). Then, Alice knows in advance a good half table (see Section 2.3).

### 3.4 Sum over histories

Because of the structure of tables, given the advanced knowledge of a good half table, the entire table can be identified by performing just one function evaluation for any value of the argument \( a \) outside the half table. Then the present explanation of the speedup foresees that an optimal quantum algorithm solves Deutsch&Jozsa’s problem with just one function evaluation. This is of course in agreement with Deutsch&Jozsa’s algorithm, which is optimal.

A history is for example: \( e^{i\phi_2} |0011\rangle_B |00\rangle_A |0\rangle_V \xrightarrow{H_A} e^{i\phi_2} |0011\rangle_B |10\rangle_A |0\rangle_V \xrightarrow{U_f} e^{i\phi_2} |0011\rangle_B |10\rangle_A |1\rangle_V \xrightarrow{H_A} e^{i\phi_2} |0011\rangle_B |00\rangle_A |1\rangle_V \). Since the problem setting is \( b = 0011 \) and Alice performs function evaluation for \( a = 10 \), her advanced knowledge must be \( b \in \{ 0011, 0000 \}_B \); if it were \( b \in \{ 0011, 1111 \}_B \), she would have performed function evaluation for either \( a = 00 \) or \( a = 01 \). The result of function evaluation, \( f_{b} (10) = 1 \), tells Alice that the function chosen by Bob is \( f_{0011} (a) \), hence that it is balanced.

One can see that the present analysis, like the notion of good half table, holds unaltered for \( n > 2 \).
4 Oracle quantum computing

So far we have provided our explanation of the quantum speedup each time on a specific quantum algorithm. Here we provide it for a generic quantum algorithm, in fact for oracle quantum computing.

We have a set of functions \( f_b : \{0,1\}^n \rightarrow \{0,1\}^m \) with \( m \leq n \). The suffix \( b \) ranges over the set of the problem settings \( \sigma_B \). Bob chooses one of these functions (a value of \( b \)) and gives Alice the black box (oracle) that computes it. Alice is to find a certain feature of this function (e.g., the period) by performing function evaluations (oracle queries). We call this feature, a function of \( b \), \( s(b) \) (where \( s \) stands for "solution of the problem").

The representation of the quantum algorithm relativized to Alice has the form:

\[
|\psi\rangle = \frac{1}{\sqrt{c}} \left( \sum_{b \in \sigma_B} e^{i\varphi_b} |b\rangle_B \right) |00...\rangle_A, \quad U|\psi\rangle = \frac{1}{\sqrt{c}} \sum_{b \in \sigma_B} e^{i\varphi_b} |b\rangle_B |s(b)\rangle_A,
\]

where \( c \) is the cardinality of \( \sigma_B \) and \( U \) is the unitary part of the quantum algorithm.

We can see that the reduced density operator of register \( B \) is the same before and after the application of \( U - B \) must be the control register of all unitary transformations. Given that the input state \( |\psi\rangle \) is defined stochastically, for \( U \) to be unitary it is not necessary that \( s(b) \) is an invertible function of \( b \), as in the case of Grover’s problem. It is sufficient that the value of \( s(b) \) partitions \( \sigma_B \) into blocks with the same number of elements, as in the case of Deutsch-Jozsa’s problem.

In view of what will follow, it is important to note that \( U|\psi\rangle \) can be written without knowing \( U \). It is enough to know the oracle problem, namely the table of the function \( s(b) \) — all the pairs \( b \) and \( s(b) \).

We can see that we are in the position to apply conditions 1 and 2 of Section 2.2. Either the measurement of \( \hat{B} \) in \( |\psi\rangle \) or that of \( \hat{A} \) in \( U|\psi\rangle \) selects the solution. Therefore all is as if the latter measurement contributed to selecting the problem setting. The possible contributions, each a subset of \( \sigma_B \), are determined by 1 and 2 on the basis of \( |\psi\rangle \) and \( U|\psi\rangle \). Since \( U \) is the identity on the reduced density operator of register \( B \), Alice knows this contribution in advance — the argument is the same as Section 2.3.

We have seen that Alice’s advanced knowledge is reconciled with the quantum algorithm by means of the following assumption:

3 An optimal quantum algorithm is a sum over classical histories in each of which Alice performs the \( (N_a) \) function evaluations necessary to identify the solution starting from her advanced knowledge of one of the parts of the problem setting selected by her own measurement.

It can be interesting to look at the consequent form of \( U \). Given that the quantum algorithm requires \( N_a \) function evaluations, the most general thing one
can do is to interleave them with non-computational unitary transformations $T_i$. Then we must have $U = T_N U_f T_2 U_f T_1$. Since $U$ is optimal, the $T_i$ are such as to maximize the probability of finding the solution in register $A$ at the end of the algorithm. Moreover, with $N_a$ function evaluations, this maximum is one.

We call conditions 1 through 3 the advanced knowledge rule.

Of course, this rule is verifiable on any optimal quantum algorithm. Conversely, given an oracle problem compatible with equation (20) and related conditions, the advanced knowledge rule defines $N_a$ with no need of knowing the quantum algorithm. It suffices to know the table of the function $s(b)$, namely the oracle problem itself. Thus the rule in question could be a powerful tool in the study of quantum computational complexity. In the next section, we will apply it to the determination of the minimum number of function evaluations required to solve Simon’s problem.

It should also be noted that we find ourselves with two definitions of $N_a$, a synthetic one given by the advanced knowledge rule and an analytic one based on a maximization procedure. In the latter case $N_a$ is trivially the number of function evaluations that brings the probability of finding the solution to one, under the condition that the $T_i$ maximize this probability. The two definitions yield coinciding results in all the optimal quantum algorithms examined in this paper. A consequence is that, in principle, the advanced knowledge rule could be inferred from the mathematical structure of the unitary evolutions we are dealing with. This could be the subject of further investigation. The present work is an exploration.

5 Simon’s and the hidden subgroup algorithms

In Simon’s [22] problem, the set of functions is all the $f_b : \{0, 1\}^n \rightarrow \{0, 1\}^{n-1}$ such that $f_b(a) = f_b(c)$ if and only if $a = c$ or $a = c \oplus h(b)$; $\oplus$ denotes bitwise modulo 2 addition. The bit string $h(b)$, depending on $b$ and belonging to $\{0, 1\}^n$ excluded the all zeroes string, is a sort of period of the function.

Array (21) gives four of the six functions for $n = 2$. The bit string $b$ is both the suffix and the table of the function. We note that each value of the function appears exactly twice in the table; thus 50% of the rows plus one always identify $h(b)$.

| $h(0011) = 01$ | $h(1100) = 01$ | $h(0101) = 10$ | $h(1010) = 10$ | ... |
|----------------|----------------|----------------|----------------|-----|
| $f_{0011}(a)$ | $f_{1100}(a)$ | $f_{0101}(a)$ | $f_{1010}(a)$ | ... |
| 00 0           | 1              | 0              | 1              | ... |
| 01 0           | 1              | 1              | 0              | ... |
| 10 1           | 0              | 0              | 1              | ... |
| 11 1           | 0              | 1              | 0              | ... |

Bob chooses one of these functions. Alice is to find the value of $h(b)$ by performing function evaluation for appropriate values of $a$. 

16
In present knowledge, a classical algorithm requires a number of function evaluations exponential in $n$. Simon’s algorithm solves the hard part of this problem, namely finding a string $s_j^{(b)}$ "orthogonal" [22] to $h^{(b)}$, with one function evaluation. There are $2^n - 1$ such strings. Running Simon’s algorithm yields one of these strings at random. The algorithm is iterated until finding $n - 1$ different strings. This allows Alice to find $h^{(b)}$ by solving a system of modulo 2 linear equations. Thus, on average, finding $h^{(b)}$ requires $O(n)$ iterations of Simon’s algorithm – in particular $O(n)$ function evaluations. Moreover, for any number of iterations, a-priori there is a non-zero probability of not finding $n - 1$ different strings. We will see that Simon’s algorithm is suboptimal according to the advanced knowledge rule. In the following, we apply this rule to derive the number of function evaluations taken by the optimal quantum algorithm for Simon’s problem. We will also provide the simplest instance of this algorithm.

5.1 Representation relativized to the problem solver

Simon’s problem is finding $h^{(b)}$ through function evaluations. We can write the input and output states of the quantum algorithm without knowing the unitary transformation in between:

$$|\psi\rangle = \frac{1}{\sqrt{6}} (e^{i\phi_0} |0011\rangle_B + e^{i\phi_1} |1100\rangle_B + e^{i\phi_2} |0101\rangle_B + e^{i\phi_3} |1010\rangle_B + \ldots) |00\rangle_A |\psi\rangle_V, \tag{22}$$

$$U |\psi\rangle = \frac{1}{\sqrt{6}} \left[ (e^{i\phi_0} |0011\rangle_B + e^{i\phi_1} |1100\rangle_B) |01\rangle_A + (e^{i\phi_2} |0101\rangle_B + e^{i\phi_3} |1010\rangle_B) |10\rangle_A + \ldots \right] |\psi\rangle_V. \tag{23}$$

5.2 Quantum feedback

The analysis is similar to that of Deutsch&Jozsa’s algorithm. This time a good half table should not contain a same value of the function twice, what would select by itself the solution of the problem and lead to either over-determination of the solution or violation of the system of equations (15). This leaves us with two ways of sharing each table. With $b = 0011$, the two good half tables can be: $f_b^{(00)} = 0$, $f_b^{(10)} = 1$ and $f_b^{(01)} = 0$, $f_b^{(11)} = 1$; the corresponding subsets of $\sigma_B$ are $\{0011, 0110\}_B$ and $\{0011, 1001\}_B$; either subset is a possible contribution of Alice’s measurement to the selection of the problem setting. Or they can be $f_b^{(00)} = 0$, $f_b^{(11)} = 1$ and $f_b^{(01)} = 0$, $f_b^{(10)} = 1$, etc.

We note in parentheses that sharing each table into two halves is accidental to Deutsch&Jozsa’s and Simon’s algorithms. In the quantum part of Shor’s [23] factorization algorithm (finding the period of a periodic function), taking two shares of the table that do not contain a same value of the function twice implies that each share is less than half table if the domain of the function spans more than two periods.
5.3 Advanced knowledge

The usual argument applies. Alice knows a good half table in advance.

5.4 Sum over histories

Also in the present case, given the advanced knowledge of a good half table, the entire table and then $h^{(b)}$ can always be identified by performing just one function evaluation for any value of $a$ outside the half table. Thus, according to the advanced knowledge rule, an optimal quantum algorithm solves Simon’s problem with just one function evaluation. Simon’s algorithm, which on average takes $O(n)$ function evaluations to find the solution and never provides the a-priori certainty of finding it in a prefixed number of iterations, would be sub-optimal.

The sum over histories representation can be developed as in Deutsch & Jozsa’s algorithm. If, for example, Alice’s advanced knowledge is $b \in \{0011, 0110\}$, she can identify the value of $h^{(b)}$ by performing a single function evaluation for either $a = 01$ or $a = 11$ – see array (21) – etc.

We provide the $U$ and $|\psi\rangle_V$ that send state (21) into (23) with a single function evaluation. We have $U = P_A H_A U_f H_A$, where $H_A$ is Hadamard on register $A$, $U_f$ function evaluation, $P_A$ the permutation of the basis vectors $|01\rangle_A$ and $|10\rangle_A$, and $|\psi\rangle_V = \frac{1}{\sqrt{2}}(|0\rangle_V - |1\rangle_V)$. Looking for the optimal quantum algorithm foreseen by the advance knowledge rule for Simon’s problem with $n > 2$ should be the object of further study.

The fact that Alice knows in advance a good half table and that, as a consequence, she can classically identify the entire table and thus the solution with just one function evaluation clearly 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’s algorithm. In the hidden subgroup problem, the set of functions $f_b : G \rightarrow W$ map a group $G$ to some finite set $W$ with the property that there exists some subgroup $S \leq G$ such that for any $a, c \in G$, $f_b(a) = f_b(c)$ if and only if $a + S = c + S$. The problem is to find the hidden subgroup $S$ by computing $f_b(a)$ 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 hidden subgroup problem [24, 25]. 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.

6 Conclusion

The simple fact of extending the representation of quantum algorithms to the process of setting the problem brought us necessarily to a novel way of see-
ing quantum computation. The extended representation is naturally time-symmetric and relational in character. Because of time-symmetry, all is as if Alice, by finally reading the solution, selected part of the initial setting of the problem – a part exactly specified by the advanced knowledge rule. Relational quantum mechanics tells us that Alice knows this part before performing any computation. It turns out that an optimal quantum algorithm is a sum over classical histories in each of which Alice knows in advance one of the parts of the problem setting specified by the advanced knowledge rule and performs the function evaluations still necessary to identify the solution of the problem.

We have checked that this holds for a variety of well-known, optimal quantum algorithms with either quadratic or exponential speedups. By the way, so far there was no unification whatsoever between the two kinds of speedup.

We have also shown that, given an oracle problem, the same rule provides the number of function evaluations (oracle queries) required to solve it in an optimal quantum way. This could be a powerful tool in the study of quantum computational complexity.

A list of possible further investigations is: (i) verifying the existence of the optimal quantum algorithm foreseen by the advanced knowledge rule for Simon’s problem with \( n > 2 \), (ii) checking whether the advanced knowledge rule fits other optimal quantum algorithms, (iii) applying this rule to the study of quantum query complexity, (iv) studying whether it can explain other violations of temporal Bell inequalities on the part of quantum computation, or (v) whether it could be inferred from the mathematics of a certain class of unitary evolutions. The present work was an exploration.

Acknowledgments

Thanks are due to David Finkelstein for useful discussions.

References

[1] Grover, L. K.: A fast quantum mechanical algorithm for database search. Proc. of the 28th Annual ACM Symposium on the Theory of Computing, 212-219 (ACM press New York, 1996)
[2] Morikoshi, F.: Information-theoretic temporal Bell inequality and quantum computation., Phys. Rev. A 73, 052308- 052312 (2006)
[3] Leggett, A. J., Garg, A.: Quantum mechanics versus macroscopic realism: is the flux there when nobody looks?. Phys. Rev. Lett. 54, 857-860 (1985)
[4] Braunstein, S. L., Caves, C. M.: Information theoretic Bell inequalities. Phys. Rev. Lett. 61, 662-665 (1988)
[5] Deutsch, D.: Quantum Theory, the Church Turing Principle and the Universal Quantum Computer. Proc. Roy. Soc. London A 400, 97-117 (1985)
[6] Bohm, D., Pines, D. A.: Collective Description of Electron Interactions: III. Coulomb Interactions in a Degenerate Electron Gas. Phys. Rev. 92, 626-636 (1953)
[7] Rovelli C.: Relational Quantum Mechanics. Int. J. Theor. Phys. 35, 637-658 (1996)
[8] Watanabe, S.: Symmetry of physical laws. Part III. Prediction and retrodiction. Reviews of Modern Physics 27.2, 179-184 (1955)
[9] Aharonov, Y., Bergmann, P. G., Lebowitz, J. L.: Time Symmetry in the Quantum Process of Measurement. Phys. Rev. B 134, 1410-1416 (1964)
[10] Finkelstein, D. R., private communication.
[11] Castagnoli, G., Finkelstein, D. R.: Theory of the quantum speedup. Proc. Roy. Soc. Lond. A 457, 1799-1807 (2001)
[12] Castagnoli, G.: The mechanism of quantum computation. Int. J. Theor. Phys. 47, 2181-2192 (2008)
[13] Castagnoli, G.: The quantum correlation between the selection of the problem and that of the solution sheds light on the mechanism of the quantum speed up. Phys. Rev. A 82, 052334-052342 (2010)
[14] Castagnoli, G.: Probing the mechanism of the quantum speed-up by time-symmetric quantum mechanics. Proc. of the 92nd Annual Meeting of the AAAS Pacific Division, Quantum Retrocausation: Theory and Experiment (2011)
[15] Morikoshi, F.: Problem-Solution Symmetry in Grover’s Quantum Search Algorithm. Int. J. Theor. Phys. 50, 1858-1867 (2011)
[16] Dolev S., Elitzur, A. C.: Non-sequential behavior of the wave function. arXiv:quant-ph/0102109 v1 (2001)
[17] Bose, S., Rallan, L., Vedral, V.: Communication Capacity of Quantum Computation. Phys. Rev. Lett. 85, 5448-5452 (2000)
[18] Hawking, S.: On the Shoulders of Giants (Running Press, Philadelphia-London 2003)
[19] Feynman, R., Hibbs, A. R.: Quantum Mechanics And Path Integrals (New York, McGraw-Hill 1965)
[20] Bennett C. H., Bernstein E., Brassard G., Vazirani, U.: Strengths and weaknesses of quantum computing. SIAM Journal on Computing 26.5, 1510-1523 (1997)
[21] Deutsch, D., Jozsa, R.: Rapid Solution of Problems by Quantum Computation. Proc. R. Soc. Lond. A 439, 553-558 (1992)
[22] Simon, D.: On the power of quantum computation. Proc. 35th Annual IEEE Symposium on the Foundations of Computer Science, 116-123 (1994)
[23] Shor, P. W.: Algorithms for quantum computation: discrete logarithms and factoring. Proc. 35th Annual IEEE Symposium on the Foundations of Computer Science, 124-134 (1994)
[24] Mosca, M., Ekert, A.: The Hidden Subgroup Problem and Eigenvalue Estimation on a Quantum Computer. Proc. QCQC '98, selected papers from the First NASA International Conference on Quantum Computing and Quantum Communications, Springer-Verlag London, UK 1998,174-188 (1998)
(Springer-Verlag London, UK, 1998)
[25] Kaye, P., Laflamme, R., Mosca, M.: An Introduction To Quantum Computing. 146-147 (Oxford University Press, 2007)