Contribution ID: **1225**   Type: **Talk**

Fundamental mechanism of the quantum computational speedup

Thursday 24 August 2017 17:30 (30 minutes)

A paradigmatic example of quantum computational speedup is the simplest instance of the quantum algorithm devised by Grover. Bob, the problem setter, hides a ball in one of four drawers. Alice, the problem solver, is to locate it by opening drawers. In the classical case, Alice needs to open up to three drawers, always one in the quantum case.

The drawer and ball problem is an example of oracle problem. The operation of checking whether the ball is in a drawer is an example of function evaluation. In the case of oracle problems, the quantum speedup comes from comparing the number of function evaluations required to solve the problem quantumly and classically. It should be noted that each speedup has been found by means of ingenuity. Outside the present unconventional approach, there is no fundamental explanation of the speedup, no unification of the various speedups, no way of foreseeing the number of function evaluations needed to solve a generic oracle problem in an optimal quantum way.

We note that the usual representation of quantum algorithms, limited to the input-output transformation typical of computation, is physically incomplete. Alice works on a quantum register A initially in a sharp state unrelated to the problem to be solved. By performing function evaluations interleaved with other unitary transformations, she sends this initial state into an output state that encodes the solution of the problem. Then she acquires the solution by measuring the content of A. The problem setting is not represented physically, namely by a quantum state –it is implicit in the mathematics of function evaluation. Furthermore, the complete representation of a quantum process must include the initial measurement, the unitary transformation of the state after measurement, and the final measurement.

We show that just completing the representation of quantum algorithms explains their speedup. This is done in three steps.

First, we extend the usual representation to the process of setting the problem. We add a possibly imaginary quantum register B meant to contain the problem setting –e. g.the number of the drawer with the ball. We assume that initially this register is in a uniform quantum superposition of all the possible problem settings. The initial state of register A is as before. An initial measurement of the content of B selects a problem setting at random. Ordinarily, Bob would unitarily send it into the desired setting; we jump this transformation for simplicity. Alice unitarily sends the random outcome of the initial measurement into an output state where register B still contains the problem setting selected by Bob and register A the corresponding solution. Then she acquires the solution by measuring the content of A. In view of what will follow, we note that this measurement leaves the quantum state unaltered; there is thus a unitary transformation U between the initial and final measurement outcomes.

Second. The extended representation works for Bob and any external observer, it does not for Alice. The input state of the representation (the outcome of the initial measurement), where register B is in a sharp state, would tell her the setting and thus the solution of the problem before she performs any function evaluation. To her, this setting must be hidden inside the black box that performs the function evaluations. We obtain Alice's view of the extended representation by postponing at the end of her problem-solving action the projection of the quantum state associated with the initial measurement. As well known, this kind of projection can be postponed at will along a unitary transformation that follows the measurement; furthermore, the content of register B and that of register A are commuting observables, so that the projection in question can be postponed after the final Alice's measurement. In particular, the input state of the quantum algorithm to

Alice becomes one of complete ignorance of the problem setting selected by Bob. Now the unitary part of Alice's action yields a superposition of tensor products, each a possible problem settings multiplied by the corresponding solution. The final Alice's measurement of the content of A projects the superposition in question on the product of the problem setting selected by Bob and the corresponding solution. This particular projection is unforeseeable to Alice as usual, it is already known to Bob and any external observer.

Third, we physically represent the reversibility of the computation process between the initial and final measurement outcomes by symmetrizing it for time reversal. This is done by assuming that the initial and final measurements, in presence of one another (contextually), reduce to partial measurements that evenly and without redundancy contribute to the selection of the problem setting and the solution, in all the possible ways in quantum superposition. The selection performed by the initial partial measurement should be propagated forward in time by U; that performed by the final one backward in time by the inverse of U. We note that any uneven sharing would introduce a preferred direction of time unjustified in the present reversible context. This symmetrization leaves the representation to Bob and any external observer unaltered and changes that to Alice. It projects the former input state to her, of complete ignorance of the problem setting and thus of the solution, on a state where she knows half of the information that specifies the solution of the problem she will read in the future. Hiding to Alice the information coming to her from the initial measurement highlights the information coming to her from the final measurement.

An optimal quantum algorithm turns out to be 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 necessary to identify the missing half. This quantitatively explains the quantum speedup and allows to predict the number of function evaluations required to solve a generic oracle problem in an optimal quantum way.

Reference: Castagnoli, G.: Completing the physical representation of quantum algorithms explains their computational speedups. https://arxiv.org/abs/1705.02657

Topic:

Mini-workshop: Quantum Foundations and Quantum Information

Summary

The quantum computational speedup is the fact that quantum algorithms require fewer computation steps that their classical counterparts, sometimes fewer than classically possible. It should be noted that each quantum algorithm has been found by means of ingenuity and that no common mechanism of the computational speedup is known. We show that just completing the physical representation of quantum algorithms highlights the mechanism in question. This is done in three steps: (i) extending the usual representation, limited to the process of solving the problem, to the process of setting the problem, (ii) relativizing the extended representation with respect to the problem solver, who cannot know the problem setting, and (iii) symmetrizing the relativized representation for time-reversal, to physically represent the reversibility of the computation process. The third step projects the input state of the relativized representation, where the problem solver is completely ignorant of the problem setting and thus of the corresponding solution, on one where she knows half of the information that specifies the solution. The quantum algorithm turns out to be a sum over classical histories in each of which the problem solver knows in advance one of the possible halves of the solution and performs the computation steps (function evaluations) needed to find the other half. This explains the quantum speedup and allows to predict the number of steps required to solve any oracle problem in an optimal quantum way.

Author: Dr CASTAGNOLI, Giuseppe (Elsag Bailey, Quantum Information Laboratory)

Presenter: Dr CASTAGNOLI, Giuseppe (Elsag Bailey, Quantum Information Laboratory)

Session Classification: Workshop on Quantum Foundations and Quantum Information

Track Classification: Workshop on Quantum Foundations and Quantum Information