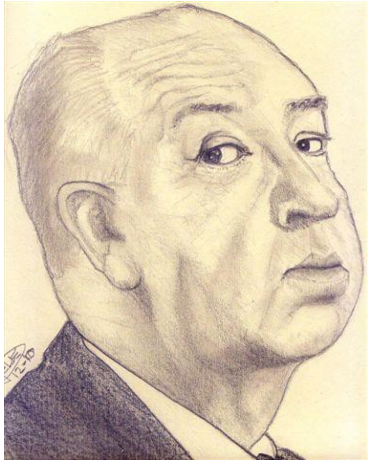
Fundamental mechanism of the quantum computational speedup

Giuseppe Castagnoli

Example of quantum speedup

- 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 she may need to open up to three drawers, in the quantum case it always takes one
- There is a **quantum speed-up**

BOB



00
01
10
11

ALICE

Some jargon

- Drawer and ball problem: ***oracle problem***
- Checking whether the ball is in a drawer: ***function evaluation*** (oracle query)
- b = number of the drawer with the ball; checking whether the ball is in drawer a: computing (evaluating) the Kronecker function $\delta(b, a)$
- Quantum speedup: number of function evaluations required by the quantum algorithm vs number required by the best known classical algorithm

Speedup is poorly understood

- Dozens of speedups discovered
- All by means of ingenuity
- **No fundamental explanation of the speedup**
- **No unified explanation of the amount of speedup**
- A lacuna of quantum computer science
- Quantum cryptography, the other pillar of quantum information, directly relies on the foundations of quantum mechanics

Representation incompleteness

- **Poor understanding** of the speedup: the usual representation of quantum algorithms, limited to the process of solving the problem, is **physically incomplete**
- Drawer number: 01

		meas. $\hat{A}$
$\vert 00\rangle_A$	$\Rightarrow U \Rightarrow$	$\vert 01\rangle_A$

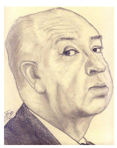
- Quantum register *A:* contains drawer number *a*.
- Alice unitarily changes input state it into an output state that encodes the solution, then acquired by a final measurement
- **Initial measurement: missing**
- **Number of the drawer with the ball: not represented physically**
- **Completing the physical representation explains the speedup**

Three steps

- 1) **extending the usual representation**, limited to the process of solving the problem, to that of setting it
- 2) **relativizing the extended representation** to Alice, who cannot see the problem setting selected by Bob (should be hidden inside the black box)
- 3) **symmetrizing the relativized representation for time-reversal** – to represent the reversibility of the computation process

Step 3) **provides a quantitative explanation of the speedup**

1) extending the representation



meas. $\hat{B}$		meas. $\hat{A}$
$(\|00\rangle_B+\|01\rangle_B+\|10\rangle_B+\|11\rangle_B)\|00\rangle_A$		
$\Downarrow$		
$\|01\rangle_B\|00\rangle_A$	$\Rightarrow \mathbf{U} \Rightarrow$	$\|01\rangle_B\|01\rangle_A$

- Adding a quantum register *B* that contains the number of the drawer with the ball
- Unitary transformation between initial and final measurement outcomes
- Extended representation works for Bob (and any external observer)
- Not for Alice
- Input state $|01\rangle_B|00\rangle_A$ would tell her the number of the drawer with the ball before she begins her problem solving action

Relational quantum mechanics

- Quantum state has meaning to an observer
- Rejects the notion of absolute, or observer independent, state of a system
- E. g. a quantum state could be sharp to an observer and a superposition to another

2) relativizing the representation to Alice

meas. $\hat{B}$		meas. of $\hat{A}$
$(\lvert 00\rangle_B+\lvert 01\rangle_B+\lvert 10\rangle_B+\lvert 11\rangle_B)\lvert 00\rangle_A$	$\Rightarrow \mathbf{U} \Rightarrow$	$\lvert 00\rangle_B\lvert 00\rangle_A + \lvert 01\rangle_B\lvert 01\rangle_A + \lvert 10\rangle_B\lvert 10\rangle_A + \lvert 11\rangle_B\lvert 11\rangle_A$
		$\Downarrow$
		$\lvert 01\rangle_B\lvert 01\rangle_A$

- **postponing the projection of the quantum state due to the initial measurement** at the end of the unitary part of Alice's action
- Throughout it, Alice remains completely ignorant of number of the drawer with the ball selected by Bob
- Legitimate: degree of freedom of quantum description

3) symmetrizing for time-reversal

- 1) outcome of initial measurement random, 2) unitary transformation between initial and final measurement outcomes
- **Selection of the number of the drawer with the ball by**:
- **1) initial measurement**

meas. $\hat{B}$		
$(\vert 00\rangle_B+\vert 01\rangle_B+\vert 10\rangle_B+\vert 11\rangle_B)\vert 00\rangle_A$		
$\Downarrow$		
$\vert 01\rangle_B\vert 00\rangle_A$	$\Rightarrow \mathbf{U} \Rightarrow$	$\vert 01\rangle_B\vert 01\rangle_A$

		meas. of $\hat{A}$
$(\vert 00\rangle_B+\vert 01\rangle_B+\vert 10\rangle_B+\vert 11\rangle_B)\vert 00\rangle_A$	$\Rightarrow \mathbf{U} \Rightarrow$	$\vert 00\rangle_B\vert 00\rangle_A + \vert 01\rangle_B\vert 01\rangle_A + \vert 10\rangle_B\vert 10\rangle_A + \vert 11\rangle_B\vert 11\rangle_A$
		$\Downarrow$
$\vert 01\rangle_B\vert 00\rangle_A$	$\Leftarrow \mathbf{U}^\dagger \Leftarrow$	$\vert 01\rangle_B\vert 01\rangle_A$

- **2) final measurement**
- **Which measurement?**
- **Neither one alone**: would introduce preferred direction of time, unjustified in a reversible context
- **Share selection evenly between initial and final measurements**

3) symmetrizing for time-reversal

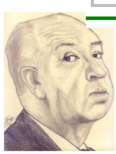
Initial and final measurements reduce to partial measurements that evenly and without redundancy contribute to the selection, e. g.:

- initial measurement of $\hat{B}$, reduced to that of $\hat{B}_l$, selects 0 of 01; outcome propagated forward in time
- final measurement of $\hat{A}$, reduced to that of $\hat{A}_r$, selects 1 of 01; outcome propagated backward in time

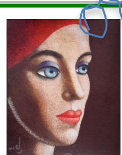
Performing the two propagations in a sequence time-symmetrizes the representation

- Superposition of all the possible ways of sharing

meas. of $\hat{B}_l$		meas. of $\hat{A}_r$
$(\|00\rangle_B+\|01\rangle_B+\|10\rangle_B+\|11\rangle_B)\|00\rangle_A$		
$\Downarrow$		
$(\|00\rangle_B+\|01\rangle_B)\|00\rangle_A$	$\Rightarrow \mathbf{U} \Rightarrow$	$\|00\rangle_B\|00\rangle_A + \|01\rangle_B\|01\rangle_A$
		$\Downarrow$
$\|01\rangle_B\|00\rangle_A$	$\Leftarrow \mathbf{U}^\dagger \Leftarrow$	$\|01\rangle_B\|01\rangle_A$



meas. of $\hat{B}_l$		meas. of $\hat{A}_r$
$(\|00\rangle_B+\|01\rangle_B+\|10\rangle_B+\|11\rangle_B)\|00\rangle_A$	$\Rightarrow \mathbf{U} \Rightarrow$	$\|00\rangle_B\|00\rangle_A + \|01\rangle_B\|01\rangle_A + \|10\rangle_B\|10\rangle_A + \|11\rangle_B\|11\rangle_A$
		$\Downarrow$
$(\|01\rangle_B+\|11\rangle_B)\|00\rangle_A$	$\Leftarrow \mathbf{U}^\dagger \Leftarrow$	$\|01\rangle_B\|01\rangle_A + \|11\rangle_B\|11\rangle_A$



Advanced knowledge

meas. of $\hat{B}_l$		meas. of $\hat{A}_r$
$(\|00\rangle_B+\|01\rangle_B+\|10\rangle_B+\|11\rangle_B)\|00\rangle_A$	$\Rightarrow \mathbf{U} \Rightarrow$	$\|00\rangle_B\|00\rangle_A + \|01\rangle_B\|01\rangle_A + \|10\rangle_B\|10\rangle_A + \|11\rangle_B\|11\rangle_A$
		$\Downarrow$
$(\|01\rangle_B+\|11\rangle_B)\|00\rangle_A$	$\Leftarrow \mathbf{U}^\dagger \Leftarrow$	$\|01\rangle_B\|01\rangle_A + \|11\rangle_B\|11\rangle_A$

$$(|01\rangle_B + |11\rangle_B)|00\rangle_A \Rightarrow \mathbf{U} \Rightarrow |01\rangle_B|01\rangle_A + |11\rangle_B|11\rangle_A$$

- Computational complexity of the problem: reduced to finding a ball hidden in one of two drawers $\{01,11\}$
- Solving the reduced problem classically requires just one function evaluation, a fortiori quantumly

Reduced problem

- **Oracle problem can always be solved quantumly with the number of function evaluations required to solve its reduced problem classically**
- **Reduced problem: original one but for the fact that the problem solver knows in advance a part of the problem setting that corresponds to half solution**
- **Found an upper bound to the quantum computational complexity of oracle problem**
- **It holds for any oracle problem and can be computed on the basis of the problem alone**

Quantum superposition

- Taking the superposition of all the time-symmetric transformations rebuilds the original transformation with respect to Alice

$$\left(|00\rangle_B + |01\rangle_B\right)|00\rangle_A \Rightarrow \mathbf{U} \Rightarrow |00\rangle_B|00\rangle_A + |01\rangle_B|01\rangle_A$$

$$+$$

$$\left(|00\rangle_B + |10\rangle_B\right)|00\rangle_A \Rightarrow \mathbf{U} \Rightarrow |00\rangle_B|00\rangle_A + |10\rangle_B|10\rangle_A$$

$$+$$

$$........$$

$$=$$

$$\left(|00\rangle_B+|01\rangle_B+|10\rangle_B+|11\rangle_B\right)|00\rangle_A \Rightarrow \mathbf{U} \Rightarrow |00\rangle_B|00\rangle_A + |01\rangle_B|01\rangle_A + |10\rangle_B|10\rangle_A + |11\rangle_B|11\rangle_A$$

- Symmetrization for time-reversal partitions the transformation with respect to Alice into a **superposition of time-symmetric transformations each solving an instance of the reduced problem**

Upper bound checked on the major quantum algorithms

- Deutsch, Deutsch&Jozsa, Simon, Shor, Grover, Abelian hidden subgroup (12 algorithms)
- All optimal in character
- **Upper bound always coincides with the number of function evaluations required to solve the problem in an optimal quantum way**
- **Conjecture: this holds in general, for any oracle problem**

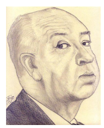
Conjecture

$$(|01\rangle_B + |11\rangle_B)|00\rangle_A \Rightarrow \mathbf{U} \Rightarrow |01\rangle_B|01\rangle_A + |11\rangle_B|11\rangle_A$$

- $\mathbf{U}$ requires just one function evaluation
- By an optimal quantum algorithm, a non-optimal one would require a higher number
- The symbolic description of a quantum process speaks to us in classical logic

Summarizing

- **In all cases, half of the random outcome of the initial measurement (half of the problem setting) selected back in time by final measurement**
- **This tells nothing to Bob, who knows the outcome of the initial measurement to start with**



meas. of $\hat{B}_l$		meas. of $\hat{A}_r$
$(\lvert 00\rangle_B+\lvert 01\rangle_B+\lvert 10\rangle_B+\lvert 11\rangle_B)\lvert 00\rangle_A$		
$\Downarrow$		
$(\lvert 00\rangle_B+\lvert 01\rangle_B)\lvert 00\rangle_A$	$\Rightarrow \mathbf{U} \Rightarrow$	$\lvert 00\rangle_B\lvert 00\rangle_A + \lvert 01\rangle_B\lvert 01\rangle_A$
		$\Downarrow$
$\lvert 01\rangle_B\lvert 00\rangle_A$	$\Leftarrow \mathbf{U}^\dagger \Leftarrow$	$\lvert 01\rangle_B\lvert 01\rangle_A$

- **To Alice, who is shielded from the outcome of the initial measurement, it tells half of it and thus a corresponding half of the solution**

meas. of $\hat{B}_l$		meas. of $\hat{A}_r$
$(\lvert 00\rangle_B+\lvert 01\rangle_B+\lvert 10\rangle_B+\lvert 11\rangle_B)\lvert 00\rangle_A$	$\Rightarrow \mathbf{U} \Rightarrow$	$\lvert 00\rangle_B\lvert 00\rangle_A + \lvert 01\rangle_B\lvert 01\rangle_A + \lvert 10\rangle_B\lvert 10\rangle_A + \lvert 11\rangle_B\lvert 11\rangle_A$
		$\Downarrow$
$(\lvert 01\rangle_B+\lvert 11\rangle_B)\lvert 00\rangle_A$	$\Leftarrow \mathbf{U}^\dagger \Leftarrow$	$\lvert 01\rangle_B\lvert 01\rangle_A + \lvert 11\rangle_B\lvert 11\rangle_A$

Time-symmetrization by reducing initial and final measurements to complementary partial measurements: inspired by the work of Dolev and Elitzur on the non sequential behavior of the wave function highlighted by partial measurement

Positioning

Two main approaches to the quantum speedup:

- **Quantum computer science** (quantum complexity classes and their relations to the classical ones)
- **Relation between speedup and fundamental quantum features** (entanglement/discord)

Positioning – quantum computer science

- **Quantum computer science is analytic** in character
- **The present explanation of the speedup is synthetic**, derived from the foundations
- Like in analytic geometry (mathematics on coordinates) and the synthetic one (derivation of theorems from postulates)
- **Analytic counterpart of the upper bound**
- Difficulty of deriving it?
- **Upper bound vs today's quantum complexity classes**
- If the conjecture that the upper bound is the number of function evaluations required by an optimal quantum algorithm were true, **it would solve the well known open problem of quantum query complexity**

Positioning – relation between speedup and the foundations

- *The speedup appears to always depend on the exact nature of the problem while the reason for it varies from problem to problem* (Vedral, Henderson)
- Present fundamental explanation applies to all oracle problems and is quantitative in character

Conclusion

- **Found an upper bound to the computational complexity of any oracle problem, always coinciding with the number of function evaluations required by the optimal quantum algorithm**
- **Derived in a synthetic way from the foundations of quantum mechanics**

Future work

(1) Checking whether the upper bound always coincides with the number of function evaluations required by the optimal quantum algorithm

(2) Finding oracle problems liable of interesting speedups, classifying quantum complexity of oracle problems (compare with existing quantum complexity classes)

(3) Further studying the fundamental implications of an explanation of the speedup that merges time-symmetric quantum mechanics and quantum information

References

- Aharonov, Y., Cohen, E., Elitzur, A. C.: Can a future choice affect a past measurement's outcome? Ann. Phys. 355, 258-268 (2015).
- Dolev, S. and Elitzur, A. C.: Non-Sequential Behavior of the Wave Function. **arXiv:quant-ph/0102109** (2001)
- Castagnoli, G. and Finkelstein, D. R.: Theory of the quantum speedup. Proc. Roy. Soc. A 1799, 457, 1799-1807 (2001)
- 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)
- Castagnoli, G.: Highlighting the mechanism of the quantum speedup by time-symmetric and relational quantum mechanics. Found. Phys. Vol. 46, Issue 3. 360--381 (2016)
- Castagnoli, G.: On the relation between quantum computational speedup and retrocausality. Quanta Vol. 5, No 1, 34-52 (2016)
- Castagnoli, G.: Completing the physical representation of quantum algorithms explains their computational speedup. **arXiv:quant-ph1705.02657** (2017)