QUANTUM EXCLUSIVITY
UNIQUELY NON-CLASSICAL
INFORMATION PROCESSING

Selim G. Akl

School of Computing
QUEEN'S UNIVERSITY
Kingston, Ontario, Canada

Online Conference *Theoretical and Foundational Problems in Information Studies*, a part of the IS4SI online Summit 2021, September 12–19, 2021 (is4si.org)

Summary

The property of quantum exclusivity is introduced which refers to computations that are possible to carry out only on a quantum computer, but are impossible, in principle, on a Turing machine.

Exclusively quantum computations invalidate the Church–Turing thesis, and the Extended Church–Turing thesis as well.

These computations also demonstrate the falsity of the Principle of Universality.

This talk aims to establish correct historical precedence, with respect to the violation of the Extended Church–Turing thesis by a quantum computer.

Introduction

On October 23, 2019, an article appeared in *Nature* entitled “Quantum Supremacy Using a Programmable Superconducting Processor”.

A quantum computer had successfully solved a computational problem related to random number generation in 200 s.

The same computation was estimated to require 10,000 years on the fastest classical supercomputer.

Meanwhile ...

Introduction (cont.)

The group in charge of the supercomputer stated that,

according to their calculations,

their machine would take 2.5 days

(not 10,000 years)

to complete the computation in question, in a straightforward way and without any optimization.

The debate is still raging.

Introduction (cont.)

If all of this was not enough controversy,

the authors of the Nature paper concluded by asserting that

their quantum computer had, *for the first time*, violated the **Extended Church–Turing thesis**

according to which any computation by any computer can be **efficiently** simulated on a Turing machine.

Introduction (cont.)

Here I would like to set the record straight concerning previous work on the limitations of the Church–Turing thesis and, by extension, on the Extended Church–Turing thesis.

Quantum exclusivity is introduced as a more powerful property than quantum “supremacy”.

I will describe computations that can be carried out on a quantum computer but are impossible, in principle, on a Turing machine.

Introduction (cont.)

This contradicts the Church–Turing thesis, whereby any computation that can be performed on any computing device can be simulated on a Turing machine.

By direct consequence, **because they cannot be carried out at all**, whether efficiently or inefficiently, on a Turing machine, these computations invalidate the Extended Church–Turing thesis as well.

Introduction (end)

A broader and more important consequence of this result is that the Principle of Universality in computation is also invalid.

It is therefore a fallacy to claim that there exists a finite and fixed Universal Computer, be it the Turing machine, the Random Access Machine, the Cellular Automaton, or any such “universal” model, capable of simulating any computation by any other computer.

Background

WHAT IS COMPUTATION?

‘‘Computation is the evolution process of some environment via a sequence of ‘simple, local’ steps.”

Avi Wigderson, *Mathematics and Computation*, Princeton University Press, 2019.

Background (cont.)

Importance of parallelism

Parallel computation often offers much more than just a faster solution.

We study the implications of parallelism in quantum information theory and show that a parallel approach can make the difference between success and failure in many computational problem cases.

Background (cont.)

Quantum information and quantum computation

Qubit:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

where α and β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$

Measurement:

When we measure a qubit , we get either the result 0 with probability $|\alpha|^2$, or the result 1 with probability $|\beta|^2$.

Background (cont.)

Putting qubits together:

For a system of two qubits, each with basis $\{|0\rangle, |1\rangle\}$, the resulting state space is the set of normalized vectors in the four dimensional space spanned by basis vectors

$$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}.$$

This generalizes in the obvious way to an *n*-qubit system with 2^n basis vectors.

Background (end)

Entanglement:

Multiple-qubit systems can also be in a superposition state.
For example, the vectors:

$$\frac{1}{\sqrt{2}}|00\rangle \pm \frac{1}{\sqrt{2}}|11\rangle \text{ and } \frac{1}{\sqrt{2}}|01\rangle \pm \frac{1}{\sqrt{2}}|10\rangle$$

each describes such a superposition state for a two-qubit system.

We say that the two qubits are *entangled*.

Quantum versus classical: Previous work

The Universal Quantum Computer (David Deutsch, 1985)

- Generating 'true' random numbers (Deutsch, 1985)
- Creating entangled states (Deutsch, 1985)
- Quantum speedup (Deutsch and Jozsa, 1992, Shor, 1997)
- Simulating quantum mechanical systems occurring in Nature (Feynman, 1982)

Quantum versus classical: Previous work (end)

- QTM versus DTM versus PTM (Berthiaume and Brassard, 1994, Bernstein and Vazirani, 1997)
- Quantum versus classical complexity (Robinson, 2003)
- Super-turing computations: Computing the uncomputable (Penrose 1989, 1994, Calude and Pavlov, 2002, Kieu, 2003)

Unconventional computations

The information processing tasks we face today or those we discover to take place in Nature often possess attributes which make them unsuitable for a Turing machine.

We call such computations *unconventional*, as opposed to the general pattern exhibited by Turing computations.

Non-universality in computation

Parallelism, in the context of unconventional computations, offers the means to show that a Universal Computer with fixed and finite physical characteristics cannot exist.

Evolving computations, whose characteristics vary during their execution, provide paradigms for which a parallel computing approach is most appropriate, if not vital for the success of the computation.

Evolving computations

Evolution is a fundamental attribute of many systems be they physical, biological, economic, social or of any other nature.

Until recently, information systems whose characteristics change during the computational process itself did not receive much attention.

Five computing paradigms are described, which are labeled *unconventional* precisely because of their dynamic nature.

Five unconventional computation paradigms

Evolving Computational Complexity

- Rank-varying computational complexity
- Time-varying computational complexity

Evolving Computational Variables

- Time-varying variables
- Interacting variables
- Variables obeying a global constraint

Five quantum unconventional computation paradigms

Each of these five unconventional paradigms of computation admits a quantum mechanical instance that requires a parallel approach for a successful outcome.

The QFT: A rank-varying computation

The quantum Fourier transform is a linear operator whose action on any of the computational basis vectors $|0\rangle, |1\rangle, \cdots, |2^n - 1\rangle$ associated with an *n*-qubit register is described by the following transformation:

$$|j\rangle \longrightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n} |k\rangle, \; 0 \leq j \leq 2^n - 1.$$

The QFT: A rank-varying computation (cont.)

If the quantum register is in an arbitrary superposition of the basis vectors $\sum_{j=0}^{2^n-1} x_j|j\rangle$,

then the quantum Fourier transform will rotate this state into another superposition of the basis vectors: $\sum_{k=0}^{2^n-1} y_k|k\rangle$,

in which the output amplitudes y_k represent the discrete Fourier transform of the input amplitudes x_j.

The QFT: A rank-varying computation (cont.)

Classically, we can compute the numbers y_k from x_j using $\Theta(2^{2n})$ elementary arithmetic operations in a straightforward manner and in $\Theta(n2^n)$ operations by using the Fast Fourier Transform algorithm.

In contrast, a circuit implementing the quantum Fourier transform requires only $\Theta(n^2)$ elementary quantum gates.

The QFT: A rank-varying computation (cont.)

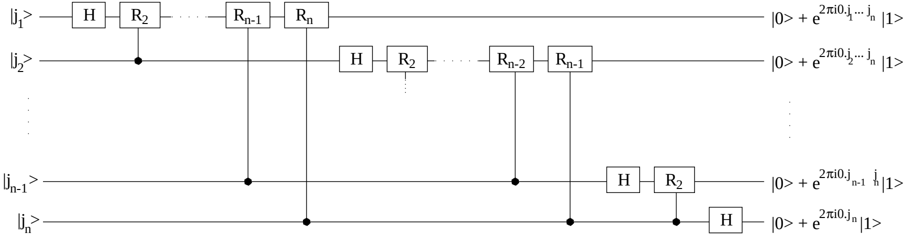
Such a circuit can be easily derived if the QFT is rewritten as a tensor product of the n qubits involved:

$$|j_1 j_2 \cdots j_n\rangle \longrightarrow \frac{(|0\rangle + e^{2\pi i 0.j_n}|1\rangle) \otimes (|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle) \otimes \cdots \otimes (|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle)}{2^{n/2}}.$$

For each qubit, the 0 or π phase induced by its own binary value is implemented through a Hadamard gate.

The dependency on the previous qubits is reflected in the use of controlled phase shifts, as depicted in the following figure.

The QFT: A rank-varying computation (cont.)


$|j_1>$
$|j_2>$
$|j_{n-1}>$
$|j_n>$
H
R_2
R_{n-1}
R_n
H
R_2
R_{n-2}
R_{n-1}
H
R_2
H
$|0> + e^{2\pi i 0.j_1 \ldots j_n} |1>$
$|0> + e^{2\pi i 0.j_2 \ldots j_n} |1>$
$|0> + e^{2\pi i 0.j_{n-1} j_n} |1>$
$|0> + e^{2\pi i 0.j_n} |1>$

Quantum circuit performing the discrete Fourier transform.

The QFT: A rank-varying computation (cont.)

In the figure, H denotes the Hadamard transformation

$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

while the gate R_k implements a $\pi/2^{k-1}$ phase shift of the $|1\rangle$ component, according to the unitary transformation

$$R_k \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}.$$

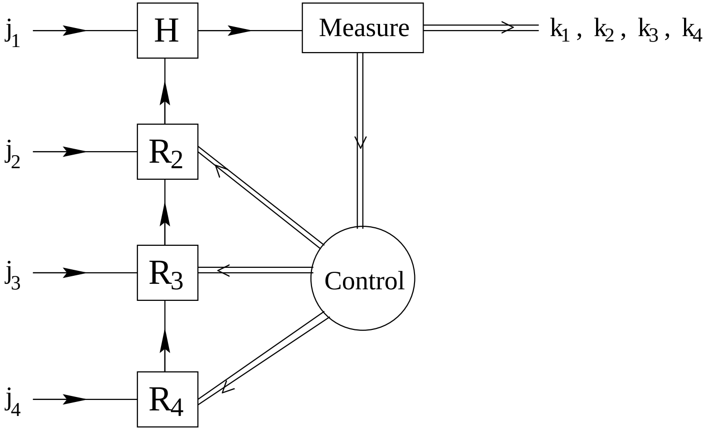
The QFT: A rank-varying computation (cont.)

Can a parallel approach be employed in order to counter this variation in complexity and make all steps take a constant amount of time to execute?

If the Fourier transform step comes right before measuring in a quantum algorithm, then it is possible to devise a parallel solution that can reduce the total running time.

The parallel approach is based on the observation that once a qubit has been measured, all phase shift gates classically controlled by the outcome of that measurement can be applied in parallel. The arrangement for just four qubits, is shown in the following figure.

The QFT: A rank-varying computation (cont.)



Quantum pipeline array for computing the Fourier transform.

For n qubits the computation requires $\Theta(n)$ operations.

The QFT: A time-varying computation

QUANTUM DECOHERENCE

Qubits are fragile entities.

One of the major challenges in building a practical quantum computer is to find a physical realization that would allow us to complete a computation before the quantum states we are working with become seriously affected by quantum errors.

Through interactions with the environment, quantum decoherence occurs, causing qubits to lose their quantum properties and behave classically.

The QFT: A time-varying computation (cont.)

The data stored in a quantum register before a certain time limit δ is significantly different from what the same qubits encode after the decoherence threshold δ.

The coupling between our qubits and their surrounding environment effectively places a hard deadline on the computation.

After this deadline, the input data (variables) will have changed and if the computation is not yet complete, it has inevitably failed.

The QFT: A time-varying computation (cont.)

From this perspective, the computation of the quantum Fourier transform in the presence of decoherence is an example of the paradigm dealing with *time-varying variables*.

As we saw earlier, parallelism can help us cope with variables whose values change over time.

The use of a parallel approach becomes critical when the solution to a certain problem must accommodate a deadline.

The QFT: A time-varying computation (cont.)

The precise value of δ will certainly depend on the particular way chosen to embody quantum information

But if δ lies between the sequential completion time and the parallel completion time, then the quantum pipeline array may be the only way to complete the computation successfully.

In our case, quantum decoherence places an upper bound on the scalability of computing the quantum Fourier transform, and the only chance to reach beyond that limit is through a parallel solution.

QEC: A time-varying complexity

QUANTUM ERROR CORRECTION

In this example the amount of computational resources required to successfully carry out a certain step are directly proportional with the amount of time elapsed since the beginning of the computation.

Error-correcting codes are employed to maintain a quantum computation error-free.

QEC: A time-varying complexity (cont.)

However, the more time it takes to complete a quantum computation, the more errors are introduced in the process, and consequently, the more time, number of ancilla qubits and higher complexity error-correcting schemes that need to be employed.

Correcting quantum errors is an important task executed alongside the mainstream computation and its complexity is heavily dependent on time.

Steps executed soon after the initialization of the quantum register will require none or low complexity recovery techniques,

while steps executed long after the initialization time may require complicated schemes and heavy resources allocated to deal with quantum errors.

QEC: A time-varying complexity (cont.)

Here too parallelism can help avoid this increase in the complexity of the recovery procedure and ultimately ensure the success of the computation.

If the steps of the algorithm are independent of one another and can be executed in any order, then the most straightforward application of parallelism is to execute all steps simultaneously and thus complete the computation before any serious errors can accumulate over time.

In this way we try to avoid or elude quantum errors rather than deal with them.

But parallelism, in the form of redundancy, can also be used to correct quantum errors.

QEC: A time-varying complexity (cont.)

Error correction via symmetrization relies on the projective effect of measurements to do the job.

The technique uses n quantum computers, each performing the same computation.

Provided no errors occur, the joint state of the n computers is a symmetric one, lying somewhere in the small symmetric subspace of the entire possible Hilbert space.

A clever measurement that projects the joint state back into the symmetric subspace should be able to undo possible errors, without even knowing what the error is.

QEC: A time-varying complexity (cont.)

To achieve this, the n quantum computers need to be carefully entangled with a set of ancilla qubits placed in a superposition representing all possible permutations of n objects.

In this way, the computation can be performed over all permutations of the computers simultaneously.

Then, by measuring the ancilla qubits, the joint state of the n computers can be projected back into just the symmetric computational subspace, without the errors being measured explicitly.

QEC: A time-varying complexity (cont.)

Error correction via symmetrization can be applied repeatedly, at regular time intervals, to avoid the accumulation of large errors and continually project the computation back into its symmetric subspace.

No matter which parallel approach is employed, if the required number of quantum processing units is provided, then the algorithm is successful.

Simulating the same solution on an insufficient number of quantum computers will lead to a gradual accumulation of the quantum errors up to the point where the results of the computation are compromised.

An interacting variables computation

QUANTUM DISTINGUISHABILITY

Given a quantum system composed of n qubits, one can define the following 2^n entangled states of the system:

$$\begin{aligned}
\frac{1}{\sqrt{2}}(|000\cdots0\rangle &\pm |111\cdots1\rangle) \\
\frac{1}{\sqrt{2}}(|000\cdots1\rangle &\pm |111\cdots0\rangle) \\
&\vdots \\
\frac{1}{\sqrt{2}}(|011\cdots1\rangle &\pm |100\cdots0\rangle)
\end{aligned} \tag{1}$$

An interacting variables computation (cont.)

The only chance to differentiate among these 2^n states using quantum measurement(s) is to observe the n qubits simultaneously, that is, perform a single joint (that is, parallel) measurement of the entire system.

Alternatively, suppose that we resort to the *information processing* capabilities of a quantum computer, as opposed to its measurement ones.

An interacting variables computation (cont.)

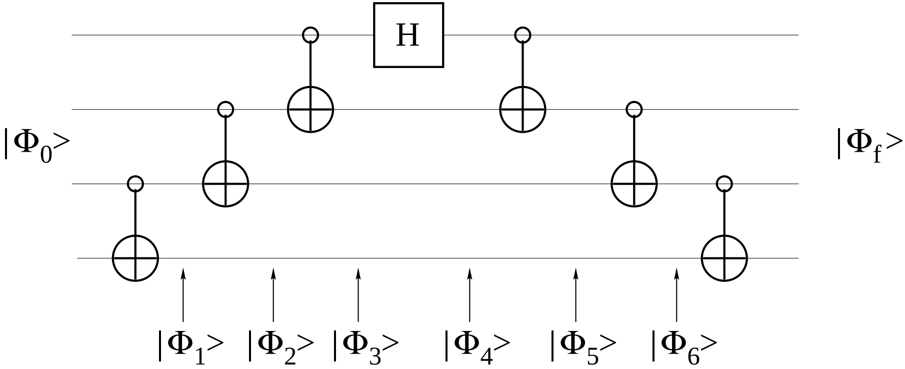
The transformation between the following two orthonormal basis sets for the state space spanned by n qubits:

An interacting variables computation (cont.)

$$\begin{aligned}
\frac{1}{\sqrt{2}}(|000\cdots 0\rangle + |111\cdots 1\rangle) &\longleftrightarrow |000\cdots 0\rangle,\\
\frac{1}{\sqrt{2}}(|000\cdots 0\rangle - |111\cdots 1\rangle) &\longleftrightarrow |111\cdots 1\rangle,\\
\frac{1}{\sqrt{2}}(|000\cdots 1\rangle + |111\cdots 0\rangle) &\longleftrightarrow |000\cdots 1\rangle,\\
\frac{1}{\sqrt{2}}(|000\cdots 1\rangle - |111\cdots 0\rangle) &\longleftrightarrow |111\cdots 0\rangle,\\
&\vdots\\
\frac{1}{\sqrt{2}}(|011\cdots 1\rangle + |100\cdots 0\rangle) &\longleftrightarrow |011\cdots 1\rangle,\\
\frac{1}{\sqrt{2}}(|011\cdots 1\rangle - |100\cdots 0\rangle) &\longleftrightarrow |100\cdots 0\rangle.
\end{aligned} \tag{2}$$

An interacting variables computation (cont.)

can be realized by a quantum circuit comprising only a linear number of controlled-NOT and Hadamard gates, shown below for the case $n = 4$.



Quantum Circuit for Distinguishability Theorem.

Transformations obeying a global constraint

Some computational problems require the transformation of a mathematical object in such a way that

a property characterizing the original object is to be maintained at all times throughout the computation.

Some quantum transformations acting on entangled states may also be perceived as computations obeying a global constraint.

Transformations obeying a global constraint (cont.)

Consider, for example, an ensemble of *n* qubits sharing the following entangled state:

$$\frac{1}{\sqrt{2}}|000\cdots 0\rangle + \frac{1}{\sqrt{2}}|111\cdots 1\rangle.$$

The entanglement characterizing the above state determines a strict correlation between the values observed in case of a measurement: either all qubits are detected in the state 0 or they are all seen as 1.

Transformations obeying a global constraint (cont.)

Suppose that this correlation has to be maintained unaltered, regardless of the local transformations each of the qubits may undergo.

Such a transformation may be the application of a NOT quantum gate to any of the qubits forming the ensemble.

As a result the correlation between the qubits will be altered.

Transformations obeying a global constraint (end)

Parallelism can once again make the difference and help maintain the required entangled state.

If, at the same time one or more of the qubits are "flipped", we also apply a *NOT* gate to all remaining qubits, simultaneously, then the final state coincides with the initial one.

In this way, although the value of each qubit has been switched, the correlation we were interested to maintain remains the same.

Conclusion

Quantum exclusivity was introduced as a more powerful property of computation than quantum "supremacy".

Exclusively quantum computations violate both the Church-Turing Thesis as well as the Extended Church-Turing Thesis.

Conclusion (cont.)

Paradigm	Description	Quantum Example
1. Rank-varying complexity	The complexity of a computational step is a function of its rank.	Quantum Fourier Transform
2. Time-varying complexity	The complexity of a step depends on when it is executed.	Quantum error correction
3. Time-varying variables	Input variables change their values with time.	Quantum decoherence
4. Interacting variables	Input data are interconnected, affecting each other's behavior.	Measuring entangled states
5. Computations obeying a global constraint	A certain global property has to be maintained throughout the computation.	Maintaining entanglement

Exclusively quantum computations.

Conclusion (cont.)

Exclusively quantum computations also demonstrate that a Universal computer cannot exist.

No computer with a finite and fixed number of processors can be universal.

Conclusion (end)

Information is physical and information processing is physical as well!!