Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer

Reading Report

Nisim Hurst A01012491

Monday 29 October 2018

Abstract

This ground-breaking paper was written by Dr. David Deutsch [1] for the *Proceedings of the Royal Society of London* on 1985, supported in part by a grant from the N.S.F.. First, the paper presents a physical version of the Church-Turing principle that introduces the universal quantum computer. Then, it proceeds to demonstrate why this kind of computer has unique properties that cannot be simulated by a universal turing machine. Finally, the paper evolved into the Deutsch-Jozsa algorithm on 1992.

Hypothesis and Evidence

The author states that a quantum computing model doesn't obey to the simple implicit physical form of the Church-Turing hypothesis. Then the author states there is a useful quantum generalization for the universal Turing machine called the universal quantum computer that have special properties .

Evidence is provided, first in the form of a contrapositive argument based on Karl Popper's epistemology (given the finite nature of the input), then by using mathematical formulæ and *proofs by induction* for establishing some ideosyncratic properties of the universal quantum computer.

Contribution

The first contribution of the article is the distiction it makes for the asymmetry between inputs and outputs of both quantum computing machines and classical stochastic computing machines versus deterministic computing machines. Then it provides a physical finite principle based on the Church-Turing hypothesis, the author calls it the Church-Turing principle. The strong version of the principle is not satisfied by the Turing machine in classical physics. However, it is satisfiable by a new generalization called the universal quantum computer.

A second contribution is a review of the reversible computers using bijective functions, e.g. the Toffoli gate. The author review formulas that describe their architecture in terms of a finite procesor and infinite memory.

A third, (and I think is the greatest) contribution of the article is a set of unique properties of the universal quantum computers:

1. **Random numbers and discrete stochastic systems.** The capacity of truly generating random numbers.
2. **Quantum correlations.** Entangled Bell states can be used for cryptography and teleportation.
3. **Perfect simulation of arbitrary finite physical systems.** Any physical system can be simulated by a universal quantum computer through a series of unitary transformations.
4. **Parallel processing on a serial computer.** All the evaluations of a function can be evaluated in one swoop under a single linear transformation.
5. **Faster computers.** Initialization of a large number of quantum states will allow greater redundancy than classical systems and dismiss the need of classical error code correction.

Finally, the field of quantum complexity theory is proposed by adding to the running time and space complexity the probability of a given result. Q-logical depth is defined the running time of the shortest program to produce a desired state from blank input.

Limitations and Weaknesses

The universal quantum computer properties that have been enumerated in this article doesn't follow a criterion for neither including them nor for ordering them. However, there are some properties conceptually connected e.g. the *random number* section and the *quantum correlations* section.

Future Work

Deutsch points out that any physical process has a equivalent program in a quantum computer. It would be highly desirable to deduce new programs to discover new laws of physics from without knowing beforehand the result.

Also Deutsch's parallelism description herein is the basis for the Deutsch-Jozsa algorithm for computing if a function is balanced or constant developed on 1992.

References

[1] D. Deutsch, "Quantum theory, the church–turing principle and the universal quantum computer," *Proc. R. Soc. Lond. A*, vol. 400, no. 1818, pp. 97–117, 1985.