Quantum computing

Ante Sosa
Erasmus exchange student
Student number: 70081480
Faculty of Mathematics and Physics
University of Ljubljana

***Abstract*—The main point of this essay is to introduce quantum computation and compare Quantum Turing machine with model of classical Touring machine. To understand the model of quantum computation, it is necessary to be familiar with some basics of quantum mechanics. Therefore, quantum principles will be compared with classical ones.**

1. Introduction

During the 1980s scientists Paul Benioff, Yuri Manin and Richard Feynman took advantage of quantum-mechanical phenomena, such as superposition and entanglement, to construct a new model of computation.

2. Quantum bits

A quantum bit is a unit vector in two dimensional complex vector space for which a particular basis $\{|0\rangle, |1\rangle\}$ has been fixed. The half-angle bracket notation $\rangle$ is conventionally used to indicate qubits, as opposed to ordinary bits. When $|0\rangle$ is measured, the result of measurement is a classical 0, and when $|1\rangle$ is measured, result is a classical 1.

We say that qubit is in a superposition of $|0\rangle$ and $|1\rangle$ if it is equal to $a|0\rangle + b|1\rangle$ where a and b are complex numbers such that $|a|^2+|b|^2 = 1$. Since all measurements are made with respect to the standard basis $\{|0\rangle, |1\rangle\}$, the probability that the measured value is $|0\rangle$ is $|a|^2$ and the probability that the measured value is $|1\rangle$ is $|b|^2$.

Entanglement, by itself, doesn't have classical analog, rather by observing one of two entangled qubits, it can be measured that qubit behave randomly. Entanglement creates a correlation between two random behaviours of qubits. [4] The fact that quantum computers can be in entangled state is the reason for their enormous computing power.

3. Quantum gates

Classical computation can be preformed using a sequence of classical universal gates. Similarly, for quantum computation there is a set of quantum gates, which contains primitive quantum state transformations. Those transformations won't be defined precisely. When transformation is applied on a qubit, depending on specific transformation, it changes state such that it rotates around basis vectors or their linear combinations by some amount of radians. I is the identity transformation, X is negation, Z is a phase shift operation, and $Y = ZX$ is a combination of both. This gates are unitary. Another single-bit transformation is the Hadamard Transformation H. When H is applied on $|0\rangle$, it creates superposition. Also there are gates that operate on two qubits like controlled-NOT gate, C_{not}. Combining controlled-NOT gate and H, two qubits can obtain entangled state.

4. Quantum Touring machine

Quantum Touring machine(QTM) is abstract machine used to model the effect of quantum computer. As with a definition of classical Touring machine(TM), QTM contains: a finite set of states (including initial and halting state), set of input/working alphabet, infinite tape and a single head. Transition function will differ from one defined in TM. It is defined as a collection of unitary matrices that map Hilbert space to itself.

We define the quantum state of the QTM as a unit vector in the Hilbert space $\mathscr{H}$ generated by the configuration space $Q \times \Sigma^* \times \mathbb{Z}$. The specific configuration $C = (q, T, i)$ is represented as the state $|C\rangle = |q\rangle|T\rangle|i\rangle$.

The QTM is initialized to the state $|\psi(0)\rangle = |q_0\rangle|T_0\rangle|1\rangle$, where $T_0 \in \Gamma^*$ is concatenation of the input $x \in \Sigma$ with as many blanks as needed.

At each step, QTM changes states according to some unitary U $|\psi(i+1)\rangle = U|\psi(i)\rangle$. Note that the state at any step k is given by $|\psi(k)\rangle = U^k|\psi(0)\rangle$. Where U can be any unitary transformation that changes the tape only on place where the head is located and moves the head one step to the right or left. Particulary, $\langle q', T', i'|U|q, T, i\rangle = 0$ if $i' = i \pm 1$ and T' is different from T only at position i.

When the QTM reaches halting state q_f the tape is being measured using the computational basis. In each step, the QTM's state is a superposition of all possible configurations.

5. Comparing TM and QTM

Everything that can be computed by QTM can be computed with TM. If we take computational efficiency in consideration, then QTMs are assumed not to be polynomially equivalent to TM. For example, there are some optimization problems that can be

solved in polynomial time with QTM and with TM it is assumed that they can't be solved in polynomial time.

6. Quantum computer

A quantum computer uses a sequence of qubits, which can represent a one, a zero, or any quantum superposition of those two qubit states. Generally, a quantum computer with n qubis can be in arbitrary superposition of up to 2^n. This is such a big difference from normal computer that can only be in one of 2^n states at any time.

7. Conclusion

QTM can be considered as a realistic model of informal notation of algorithm, because it satisfies all of its conditions. The computation process is specified completely in a finite amount of steps. QTM preforms steps, independent of input in real time, using working space.

This is my very first essay on mathematical topic, so there might be some mistakes in form, not valid statements and conclusions. Furthermore, almost every idea represented in this essay is taken from sources in References section and is not my intellectual property. Writing this essay I found out how incredible topic Quantum computation is and would like to conclude quoting D. Deutsch: "Quantum theory is a theory of parallel interfering universes. There are circumstances under which different computations performed in different universes can be combined by Q giving it a limited capacity for parallel processing. " [1][1]

References

[1] David Deutsch *Quantum theory, the Church-Turing principle and the universal quantum computer*. Proceedings of the Royal Society of London A 400, pp. 97-117 (1985)

[2] Wikipedia: Quantum computing, https://en.wikipedia.org/wiki/Quantum_computing

[3] Eleanor Rieffel *An Introduction to Quantum Computing for Non-Physicists*. FX Palo Alto Laboratory, 3400 Hillview Avenue, Palo Alto, CA 94304

[4] IBM Q: Online quantum computer (5-qubit), https://www.research.ibm.com/ibm-q/

[1] Q is universal quantum computer and it is proven in [1] that it can simulate any Touring machine.