UIT2205: Quantum Computation
AY 2017/18 Sem 2

Ang Yan Sheng
A0144836Y

Essay 2
On the Future of Quantum Computation

Quantum computation seems to have become a buzzword for the times: popular science articles sensationalise the "exponential speedup" of quantum algorithms without qualification, while experimental implementation of devices that can deliver these promises are slow in coming. Regardless, quantum information theory has already made its mark in diverse fields, from cryptographic protocols such as quantum key distribution, to new interpretations for the laws of physics. In this essay, I will investigate the relationship between the observable universe and quantum information, and to what extent can the universe be considered a quantum computer. In order to focus on the essence of this question, I will study the closely related question of whether the universe can be considered a *classical* computer, present arguments for both sides, and extend the arguments by analogy to the quantum case.

Nielsen and Chuang (2010) identify four basic postulates of quantum mechanics that govern the behaviour of quantum computers (p. 80–96):

1. An isolated physical system is completely described by its *state vector* $|\psi\rangle$, a unit vector in a Hilbert space (the *state space* of the system);
2. The evolution of the state of an isolated physical system is described by a unitary operator U, namely $|\psi_{t_2}\rangle = U\,|\psi_{t_1}\rangle$;
3. A measurement on a physical system is described by a collection $\{A_m\}$ of *measurement operators* satisfying $\sum_j A_j^\dagger A_j = \mathbb{1}$; moreover, given state $|\psi\rangle$ before measurement, the probability of outcome j is
$$p(j|\psi) = \langle\psi|\, A_j^\dagger A_j\, |\psi\rangle,$$
and the state after measurement is
$$|\psi_j'\rangle = \frac{A_j\,|\psi\rangle}{\sqrt{p(j|\psi)}};$$
4. The state space (resp. state vector) of a composite system is the tensor product of the state spaces (resp. state vectors) of the components.

In contrast to a classical computer, which manipulates 0/1 bits with logic gates, according to the rules of Boolean logic, a quantum computer manipulates quantum states, or qubits, using quantum logic gates, according to the rules for quantum systems described above. For now, we will use these as the working definitions of classical and quantum computers, respectively.

There is a trivial sense in which the universe is a quantum computer: it contains one! To clarify this statement, let us look at the classical case. According to this argument, the universe contains (for instance) my laptop, which is definitely a classical computer – it manipulates classical information nontrivially (under the right circumstances: turned on, plugged in to a power supply, etc.). Thus the universe can manipulate classical information, and hence it is a classical computer. Similarly, the universe contains (for instance) the IBM Q, which manipulates quantum information nontrivially (under the right circumstances: correct temperature, etc.). Thus the universe can also manipulate quantum information, and hence it is a quantum computer.

However, further analysis of the above argument reveals that our definition for a 'computer' turns out to be so weak that it is practically useless. To see this, imagine a junkyard containing tonnes of trash, which happens to include a laptop. According to the above argument, the entire junkyard should be considered a classical computer. However, the same argument works if we replace the laptop with a microprocessor chip, or even a single ALU register: given the appropriate conditions, an ALU register can process classical information, if only a few bits. In fact, even if we remove all laptop parts, we can still imagine implementing logic gates with the other pieces of trash – this piece of trash falls if both pieces under it are too small (AND gate), or if one of the pieces is too small (OR gate) – so the junkyard should be considered a classical computer anyway!

Returning to the quantum case, we note that time evolution of a quantum state or wavefunction is governed by Schrödinger's equation, acting as a unitary operator. Hence the passage of time itself can be seen as a nontrivial quantum gate. If we accept that anything that implements a unitary operator is a quantum computer, then any nonempty physical system governed by quantum mechanics is a quantum computer; in particular, since there are no known violations of quantum mechanics, we don't know if there are any physical systems which are *not* quantum computers, according to this definition!

We have shown that our definition of the term 'computer' is close to meaningless (anything which contains even a single logic gate qualifies); this suggests that we should examine our definition of the term 'computer' carefully. We have been using the term in a technical sense to refer to any fixed logical circuit, such as a single ALU gate. Colloquially, we might refer to such a fixed circuit as a 'calculator' instead of a 'computer,' so that the above argument now reads "every physical system, including the universe, is a quantum calculator," a statement that seems much easier to agree with.

On the other hand, a laptop is much more commonly referred to as a 'computer' rather than as a mere 'calculator,' because laptops do not just perform a single specific computational task; software programs allow laptops to perform diverse forms of computation. Hence, there is a stronger sense in which laptops implement classical computation: it is not just a single classical program/gate, but a simulator for *any* classical program/gate (up to a certain size). Thus, what we colloquially call 'computers' are in fact 'calculators' satisfying an additional strong 'universality' condition, which we now turn to investigate.

The canonical model of classical computation is the *Turing machine*, with an infinite tape representing memory, a movable head that reads and writes from the tape, an internal state, and a finite table of transition instructions. A *Turing complete* system of computation is one which can implement or simulate arbitrary Turing machines, assuming unlimited time and memory. By the Church-Turing thesis, any computational algorithm (or computable function) can be implemented by a Turing machine, so a Turing complete system is able to implement any computation. Hence Turing completeness seems like a good candidate to capture the intuitive notion of a 'universal computer.'

However, the assumptions of infinite time and memory imply that no physical implementation of classical computation can be Turing complete, simply because no physical computer has access to an infinite amount of these resources. At the same time, the Turing model of computation does not directly carry over to our notion of quantum computation, which was given in terms of quantum circuits instead of Turing machines. A fixed quantum circuit can only take a fixed number of qubits as input, and thus is already a 'calculator' by our definition. Hence, if we want a useful notion of a 'universal quantum computer', we need an alternative general model of computation, beyond what we have covered in class, which takes into account (a) finiteness of resources; (b) the circuit formulation of computation; and (c) variable size of input.

We turn to a such model of classical computation from circuit complexity theory, as outlined in Vollmer (1999), which is based on Boolean circuits. A *uniform circuit family* (UCF) is a sequence of Boolean circuits $C_1, C_2, \ldots$ satisfying:

1. For each $n \geq 1$, C_n takes n bits of input, uses only AND, OR and NOT gates, and returns n bits of output; and
2. The sequence $C_1, C_2, \ldots$ is computable, ie. there is a fixed Turing machine T such that $T(n)$ outputs the circuit C_n (p. 46).[1]

The UCF model of computation is strictly weaker than the Turing model, since a UCF must give an output for every input, while Turing machines can enter infinite loops. However, Vollmer shows that every total Turing machine (ie. a Turing machine that halts on every input), and in particular every total computable function (ie. a computable function with a well-defined value for every input), can be implemented as a UCF (p. 46–47).

It might seem circular that we are replacing the Turing model of computation with the UCF model, which also includes a Turing machine. However, note that T is only a single instance of a total Turing machine, ie. a 'calculator.' For the following argument, we may even assume certain boundedness conditions on T, such as requiring $O(\log n)$ space or $n^{O(1)}$ time (p. 47). Since many computable functions used in practice are total, with efficiently computable circuit diagrams, the UCF model still captures a large, nontrivial subset of the notion of computability.

We can now give a rigorous definition to what we usually call a 'universal classical computer.' We will say that a physical system is *UCF-complete* if it can implement any finite approximation to a UCF. More specifically, for any UCF given by $(C_1, C_2, \ldots), T$, a UCF-complete physical system should be able to compute C_n using T and implement C_n, for all $n \leq N$, where N is an upper bound on the memory of the physical system. In particular, N should increase without bound ($N \to \infty$) as we increase the size of the physical system.

For a concrete example, consider a modern CPU. Since the logic gates in the CPU (namely, the ALUs) are programmable, a CPU can implement any Turing machine T with a bound N_1 on its space or time requirements, and any Boolean circuit C_n up to size N_2, where N_1, N_2 only depends on the memory available to the CPU. By increasing the memory, number of ALUs, etc., we can arrange $N_1, N_2 \to \infty$. Hence the modern CPU architecture is UCF-complete. Another example is given by Fredkin and Toffoli (1982), which implements the universal Fredkin gate in reversible classical computation using a billiard ball model. Thus the billiard ball model can implement Turing machines up to size N_1 and logic circuits up to size N_2, with N_1, N_2 dependent on the physical size of and number of billiard balls used in the system. Again, by increasing these parameters, we can have $N_1, N_2 \to \infty$, so the billiard ball model is also UCF-complete. In contrast, any implementation of a fixed Turing machine (or 'calculator') is not UCF-complete, since we cannot simulate arbitrarily large boolean circuits on such a machine. These examples suggest that our notion of UCF-completeity accurately captures the intuitive notion of a 'universal computer,' as opposed to a 'calculator.'

As a corollary, note that within the paradigm of classical physics, it is possible to im-

[1] This condition amounts to the requirement that the family of circuits should have a finite description – without this condition, such a circuit family can even implement Turing uncomputable functions, such as a halting oracle, and would not be an accurate model of a 'computer.'

plement in theory either CPUs with arbitrarily large memory, or arbitrarily large billiard ball computers. Of course, in practice there are clearly problems with trying to construct a kilometre-sized CPU chip or billiard ball computer (which is what the "arbitrarily large" requirement entails). However, these issues are essentially problems in enginnering, and could conceivably be overcome with clever new ways to eg. wire semiconductors, or minimise mechanical friction. The point is that there is no known physical law expressly forbidding the construction of such systems at arbitrarily large scales; hence we can say that the physical universe is, as far as we know, UCF-complete, ie. a 'universal classical computer.'

Returning to the question of whether the universe is a 'universal quantum computer,' we need the quantum version of the UCF model. Let us propose the *uniform quantum circuit family* (UQCF), a sequence of quantum circuits $Q_1, Q_2, \ldots$ such that:

1. For each $n \geq 1$, Q_n takes n qubits of input, uses only single-qubit and CNOT gates, and returns n classical bits of output after measurement; and
2. The sequence $Q_1, Q_2, \ldots$ is efficiently computable (in logarithmic space, or polynomial time, by a Turing machine T).[2]

A physical system which can compute Q_n with T and implement Q_n to arbitrary accuracy, for any UQCF, will be called *UQCF-complete*. By analogy, we can reasonably expect that UQCF-universal systems can implement arbitrary total quantum Turing machines, and thus captures a large subclass of quantum algorithms; however, the definition of a quantum Turing machine, and a rigorous proof of this conjecture, is beyond the scope of this essay.

The problem now becomes: "Is the universe a UQCF-complete physical system?" Namely, for any UQCF given by $(Q_1, Q_2, \ldots), T$, is there a physical system in the universe that can:

1. Compute Q_n using T for $n \leq N$;
2. Implement Q_n for $n \leq N$; and
3. Allow for $N \to \infty$ as the size of the system increases?

It is easy to show that Condition 1 is satisfied: since the universe is UCF-complete, Turing machines with space or time bounds can be implemented as physical systems.

For Condition 2, we need to be able to approximate the single-qubit and CNOT gates to any desired accuracy. However, the Solovay-Kitaev theorem states that any single-qubit gate can be approximated to accuracy ε using only the following quantum gates:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}, \quad \text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

(In other words, $\{H, T, \text{CNOT}\}$ form a universal set for all quantum gates.) Moreover, Dawson and Nielsen (2005) present a classical algorithm to compute such an approximation in $\log^{O(1)}(1/\varepsilon)$ time. By the UCF-completeness of the universe, we conclude that Condition 2 can also be satisfied by some physical system.

For Condition 3, we note that within the paradigm of quantum mechanics, there are no known theoretical obstacles to constructing quantum circuits with arbitrarily many qubits.

[2] Similar to the classical case, this requirement is strictly weaker than being able to implement arbitrary unitary gates on n qubits: Nielsen and Chuang (2010) show that even though every unitary operator can be approximated using single-qubit and CNOT gates (p. 188–194), sometimes exponentially many gates are necessary (p. 198–200).

Hence, under the known laws of physics, the universe can implement any UQCF in principle, limited only by technology and finiteness of resources. In other words, the universe is UQCF-complete, and thus we may consider the universe as a 'universal quantum computer' in this strong sense.

Having established a formal argument that the universe can implement some form of universal quantum computation, in the form of UQCF-completeness, we conclude this essay by rigorously examining the assumptions that led us to this conclusion.

We have not focused on the accuracy of implementation of arbitrarily large quantum circuits. This is due to a remarkable phenomenon in quantum error-correction, where "provided the noise in individual quantum gates is below a certain constant threshold it is possible to efficiently perform an arbitrarily large quantum computation" (Nielsen and Chuang 2010, p. 493). In other words, under certain assumptions about the noise and architecture in the quantum circuit, it is only necessary to be able to implement the H, T and CNOT gates to within a fixed error threshold (which is numerically around 10^{-5} to 10^{-6}). Hence the problem of accuracy does not grow with increasing circuit size, and thus properly belongs to the domain of engineering.

The argument is also conditional on the assumption that quantum computation, in particular mutual entanglement, is possible for any number of qubits. This is not a problem within the framework of quantum mechanics; in fact, under the interpretation of quantum information theory, it is even possible to talk about the entire universe as a single quantum state, with the process of measurement modelled by *decoherence*, or massive entanglement caused by interaction between a quantum system and the measuring device.

However, for the sake of argument, let us speculate on the validity of quantum physics beyond the current limits of experimental verification. For example, some theorists have proposed a *holographic principle*, motivated by certain black hole phenomena in black holes (Bekenstein 1973), which states that the information content of any physical system is bounded above by a constant times its surface area. Davies (n.d.) has calculated that a system with 400 fully entangled qubits encodes more information than allowed by this principle applied to the entire observable universe. Though the holographic principle remains highly speculative, the prediction about the upper limit of entanglement is fully falsifiable, and will certainly be tested in the industry effort to make larger and larger quantum computers. The important point is that the holographic principle implies that no physical system can implement an n-qubit circuit for $n > 400$, and thus Condition 3 of UQCF-completeness for the universe fails.

Of course, any claim contradicting the central tenets of quantum mechanics can only be speculative at best: quantum mechanics has been one of the most successful physical theories to date, with no known experimental refutations. However, it would be imprudent to suggest that quantum mechanics, or quantum information theory, is the last word on the physical world. Classical mechanics and classical information theory have been successful in describing some aspects of the universe; however, in spite of the Church-Turing thesis, which states that even the IBM Q can be simulated by a Turing machine, the violation of the Bell and CHSH inequalities have demonstrated that the classical framework is inadequate to explain the IBM Q.

Although the universe is UCF-complete, it is not *merely* a universal classical computer, due to its quantum nature. Similarly, although the universe is UQCF-complete (as far as we know), and can be thought of as a universal quantum computer, we should be wary of conceptualising it exclusively, or *merely*, in this framework. Instead, I believe that – much as quantum information theory introduced the radical new ideas that physics is based on generalised probability laws, and that information is even more fundamental than matter – we should look forward to the next paradigm shift, which might introduce even more new, exciting ways of thinking about the universe.

References

Bekenstein, J. D. (1973). “Black Holes and Entropy.” Phys. Rev. Let. D **7**(8):2333–2346. DOI:10.1103/PhysRevD.7.2333

Davies, P. (n.d.). “The implications of a holographic universe for quantum information science and the nature of physical law.” Retrieved from `http://power.itp.ac.cn/~mli/pdavies.pdf`

Dawson, C. M., & Nielsen, M. A. (2005). “The Solovay-Kitaev Algorithm.” arXiv:quant-ph/0505030.

Fredkin, E., & Toffoli, T. (1982). “Conservative Logic.” Int. J. Theor. Phys. **21**(3/4): 219–253. DOI:10.1007/BF01857727

Nielsen, M. A., & Chuang, I. L. (2010). *Quantum Computation and Quantum Information* (10th Anniversary ed.). Cambridge University Press. DOI:10.1017/CBO9780511976667

Vollmer, H. (1999). *Introduction to Circuit Complexity: A Uniform Approach*. Springer-Verlag. DOI:10.1007/978-3-662-03927-4