Quantum Computation

Zoya Gavrilov

June 26, 2012

1 Introduction

Quantum computation harnesses the power of nature by relying on the properties of quantum systems to both speed up classical computations, as well as to solve problems that are not classically computable. In essence, quantum computation makes use of the wave nature of particles to obtain *quantum parallelism*. Since *qubits* (quantum bits[1]) can exist in a *superposition* of states, functions operating on qubits are said to simultaneously operate on all the states. Subsequent measurement collapses the state of a qubit to some eigenvalue of the *observable* being measured. The state of a qubit collapses to certain values with probabilities that are functions of the wave amplitude for the qubit. Hence, a quantum computation will proceed as follows: qubits are prepared in certain states[2], they are then operated on by quantum gates (which can be expressed as sequences of unitary operations) which change the state of the system[3], and a single measurement can then be performed as the final step of computation. Observation should occur at the end of all other computations because measurement collapses the state of the system, information is lost, and thus subsequent measurements are not possible[4]. Hence, the goal is to ensure that the computations on the qubits are performed in such a way that the desired answer can be obtained by measuring a single observable of the final system. This is why the design of quantum algorithms requires a fair bit of ingenuity.

2 Some key concepts

- Quantum states are unit vectors in a Hilbert space (a complex, norm-preserving, vector space). The bases used for this space depend on a choice of observables - they are the eigenvectors of the observables. When we say that a measurement collapses the state of a vector, we

[1] The quantum unit of storage which is analogous to the classical bit.

[2] For instance, the measuring instruments can be calibrated to eigenvectors of chosen qubit observables.

[3] The state of the whole system depends not only on the input qubits being directly operated on, but also on other qubits that are in the system or may enter it and cause *decoherence*.

[4] Subsequent measurements are technically possible, but they yield no new information about the system. The idea that it is not possible to measure multiple properties of a particle (because through measurement of one we have lost information about the other) is known as the Heisenberg uncertainty principle.

mean that the vector is projected onto one of the basis vectors with probability equal to the projected norm.

- Performing operations on quantum states is equivalent to rotating the corresponding vectors in Hilbert space. Because such rotation changes the phase of the quantum state, we can further describe these computations by wave equations (Schrodinger interpretation). Equivalently, we can fix the quantum states, and rotate the bases, where the computations would have to be described as functions of the observables (Heisenberg interpretation).

- Quantum operators can be expressed as unitary matrices, the significance of which is that they are reversible computations that preserve vector norms. In other words, these unitary matrices applied to quantum states represent rotations of those states in Hilbert space.

- Measurement need not require a conscious observation. Other quantum particles may be said to 'observe' or 'measure' a quantum state, thereby causing a loss of information termed *decoherence*. This is what makes the physical design of quantum systems very difficult, since the system must be maximally isolated from noise.

3 The Power of Quantum Computation

One important property of quantum systems that is impossible in classical systems is *quantum entaglement*, which refers to the sharing of information by multiple quantum particles, separated by an arbitrary distance. Another way to say this, is that the particles share a quantum state, and hence a computation on, or measurement of, one particle affects the state of the other particle. This is at the root of the *EPR paradox*. This property has many implications for quantum computing (both in terms of computational power but also in terms of difficulty of constructing physical quantum systems). Some applications utilizing this property include game playing (the sharing of quantum information can lead to a higher probability of winning than is possible with classical/probabilistic strategies) and encryption schemes (secure transfer of information across distances).

Another method of leveraging the properties of quantum systems for encryption and security schemes is by making use of the Heisenberg uncertainty principle. For instance, a document or a money bill can be manufactured to contain quantum particles (e.g. photons). Attempting to measure some observable of the system will collapse the state of the system, thus making further attempts at measurement futile - i.e. the whole state of the system would not be physically measurable.

The wave nature of quantum particles (the fact that the particles are found in a superposition of states), is what allows multiple computations to be performed simultaneously. More specifically, say we have a function f that is to be evaluated at multiple values x (i.e. different bit-string inputs). A classical computation would involve a sequence of function invocations. On the other hand, if x is a qubit (and is in 'multiple states at once'), a single function invocation is sufficient to calculate the

result of f applied to different values of x (via *quantum parallelism*). However, the resulting values of f can not be disentagled from one another (they have become a single coherent system), and a single measurement will collapse the whole system's state to one value. As mentioned previously, the quantum algorithm must thus be designed in such a way that the solution to the problem can be interpreted from this single value.

Because no classical algorithm (which is defined to be a sequence of states) can, with a single invocation of a function, obtain an answer that logically depends on multiple evaluations, if quantum computers are made possible, they pose a challenge to the strong Church-Turing thesis which postulates that all algorithmically computable problems are computable on a classical computer (i.e. Turing machine). A quantum computer would then have greater computational power than the Universal Turing Machine, which is supposed to be able to simulate the computation of any (computable) function on all inputs.

Turning this argument around, if there was to exist a Universal Quantum Machine, could it be made to quantum compute everything that's quantum computable? In fact, no. For instance, a quantum computer could not theoretically compute its lowest energy level. Hence, the issue of computational hardness ('quantum-hardness') remains in the quantum case as well.

4 Classical computation $\subset$ quantum computation

Define: $BQP = \{f | f : \{0,1\}^* \rightarrow \{0,1\},\ f \text{ is quantum } p(n) - time\}$
where: f is $p(n) - time$ computable if there is a polynomial-time classical TM (polynomial in n) that can compute f with probability at least $2/3$, on any input of length n.

Lemma: $P \subset BQP$
Proof idea: because every classical TM computation has an equivalent boolean circuit, it is sufficient to show that a boolean circuit can be simulated by a quantum circuit. Each boolean gate has a quantum analog (a reversible unitary operation). To convert a boolean gate to a quantum gate requires polynomially many operations to ensure reversibility of the quantum gate (by adjusting the number of inputs and outputs). Moreover, polynomially many quantum operations are required to then use the outputs of a quantum gate to compute the corresponding output of the classical gate. For instance, whereas a classical gate with input x would compute $f(x)$, the corresponding quantum gate would take inputs x and y and produce outputs x and $yf(x)$ (polynomially many quantum operations could be used to obtain the value of $f(x)$ from $yf(x)$, since y was a known 'scratchpad' qubit, necessary only for the reversiblity of computation).

Corollary: $BPP \subset BQP$
Proof idea: recall that a language L is in BPP if there exists a deterministic TM M that runs in polynomial time on all inputs x, and for $x \in L$, M accepts x with probability at least $2/3$;

for $x \notin L$, M accepts x with probability at most 1/3. In quantum computation, there exists a Hadamard gate that has no classical analog, and acts on qubits to enforce a superposition of states, such that when measured, the qubit has equal probability of being in each of the states. Hence, the addition of a Hadamard gate to the quantum gate repertoire allows the simulation of classical probabilistic computations. The statement of the corollary follows from the definition of BQP.

Is $NP \subset BQP$?
This is still an open problem. In fact, if it could be shown that $NP \not\subset BQP$, then this would imply that $P \neq NP$ (which would be a big result for complexity theorists!), since $P \subset BQP$ (by lemma). Certain quantum algorithms have demonstrated only a quadratic speedup on NP-complete algorithms (such as Grover's algorithm), but this does not necessarily imply $NP \not\subset BQP$. Just as with classical computation, the fact that we have not found polynomial-time algorithms for NP problems is not proof that they do not exist.

5 Conclusion

It is not yet clear whether quantum computers can be made feasible. The same properties that make quantum computations powerful (e.g. entanglement, coherence, etc.) ultimately make their physical instantiations nearly impossible – this is because for controlled quantum computation, the system must be maximally isolated, which is extraordinarily hard to achieve (at least with the techniques and technology available today). On the other hand, if quantum computers were made possible, their practical applications would be abounding - from increasing instrumental precision, to making many currently-infeasible computations, feasible, to providing a new means for security and encryption schemes (not depending on $P \neq NP$). Moreover, since the world around us is just one large quantum system, presumably we should be able to explain nearly everything with quantum phenomena.

References

[1] S. Arora and B. Barak, "Complexity Theory, A Modern Approach", 2009.

[2] David Deutsch, "Lectures on Quantum Computation", 2003.

[3] David P. DiVincenzo, "Quantum Computing: Origins and Directions", 2006.