What makes quantum computers powerful?

The Quantum Computation Collective

Torino, Italy, July 10, 1997

Quantum computers have properties which appear to make them more powerful than other classes of computational devices. We suggest reasons for this distinction in computational power.

When, in the course of human events, it becomes necessary for one people to dissolve the classical bonds which have connected them with antiquity, and to determine among the powers of the earth, the separate and equal station to which the laws of quantum mechanics and of nature's God entitle them, a decent respect to the opinions of mankind requires that they should declare the causes which impel them to their rightful computational power.

We hold these truths to be self-evident, that all interpretations of quantum computation are created equal, that they are endowed by their Creator with certain unalienable properties, that among these are

1. *Exponentiality;*
2. *Fast access;*
3. *Branching;*
4. *Complex amplitudes; and*
5. *Universality.*

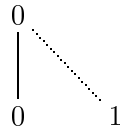
That to secure these rights, theories of computation are instituted, deriving their just powers from the properties of the system. That whenever any theory of computation becomes destructive to these ends, it is the right of the people to alter or to abolish it, and to institute a new theory, laying its foundation on such principles and organizing its powers in such form, as to them shall seem most likely to effect their tenure and funding. Prudence, indeed, will dictate that theories long established should not be changed for light and transient causes; and accordingly all experience hath shown that humankind are more disposed to suffer, while evils are sufferable, than to right themselves by abolishing the forms to which they are accustomed. But when a long train of abuses and usurpations, pursuing invariably the same object evinces a design to reduce them under absolute despotism, it is their right, it is their duty, to throw off such theories, and to provide new guards for their future security. — Such has been the patient sufferance of programmers; and such is now the necessity which constrains them to alter their former understandings of computation. The history of the present classical bit is a history of repeated injuries and usurpations, all having in direct object the establishment of an absolute tyranny over these states. To prove this, let facts be submitted to a candid world.

Quantum computers are blessed with the following properties:

Exponentiality. For a physical system to be a computational device, we need a mapping between numbers and states[1] of the system. These states will be called our computational basis states. The size of the computational state space is exponential in the physical size of the system and energy available, which we will characterize by the number n.

Fast access. Elementary operations are those which can be accomplished with constant physical resources in practical systems, regardless of the size of the computation. A tensor product structure, such as that associated with composite systems in quantum mechanics, allows a polynomial (in n) number of elementary operations to transform an arbitrary computational state to another one. For example, the state specified by the binary string $i_1 \ldots i_n$ can be transformed to state $j_1 \ldots j_n$ using at most n NOT operations.

Branching. Consider the following picture:

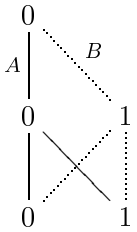


This demonstrates the effect of applying a Hadamard gate $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ to a qubit initially in the

[1] general physical states – not necessarily quantum states.

state $|0\rangle$. Cascading such gates allows simultaneous transitions from one state to many. Branching allows the computer to explore multiple trajectories through its state space, simultaneously; furthermore, branching to an exponentially large number of states can be achieved with a polynomial number of elementary operations.

Complex amplitudes. Now consider the application of a Hadamard gate *twice* to a qubit:



To compute the amplitude of obtaining each computational basis state in the final result, we multiply amplitudes along paths and sum at the endpoints. In the above example, path A contributes an amplitude $1/2$ to end up in state $|1\rangle$, and path B contributes an amplitude of $-1/2$, so that the total amplitude is zero. The lesson is that complex amplitudes allow trajectories leading to the same final state to cancel. This is the phenomenon of interference.

Universality. In addition, it is manifestly evident that a quantum computer must be able to calculate, to arbitrary accuracy, any function with a finite domain and range, using finite resources.

In contrast, other types of computers can have several of these properties, but not all combined. This is demonstrated by the following examples.

Classical digital computer. This has the property of universality, exponentiality, and fast access between computational basis states. However, the computational state of this machine evolves along a single trajectory, which cannot branch.

Classical probabilistic computer. This computer possesses all the properties of the deterministic digital computer, and also possesses the property of branching, but only by positive probabilities. For example, starting from the state 0, we make a transition to 0 or 1 based on a fair coin flip, and repeat this process. In analogue to the quantum case, the final states are given by multiplying transition probabilities along trajectories and adding at the endpoints, to obtain the total transition probability. However, due to the positivity of the probabilities, trajectories leading to the same final state cannot cancel. This machine is thus fundamentally different from the quantum computer.

Classical wave computer. A classical wave computer is modeled by the propagation of n modes of coherent states of light $|\alpha_1, \alpha_2, \ldots, \alpha_n\rangle$ through beamsplitters $B_{ij}(\theta)$, defined by

$$B_{ij}(\theta)|\alpha_i, \alpha_j\rangle = |\alpha_i \cos\theta + \alpha_j \sin\theta, \alpha_j \cos\theta - \alpha_i \sin\theta\rangle\,, \tag{1}$$

phase-shifters $P_i(\phi)$, defined by

$$P_i(\phi)|\alpha_i\rangle = |\alpha_i e^{i\phi}\rangle\,, \tag{2}$$

and optical detectors M_i, which give a real-number output for a given mode of the input state, according to the rule

$$|\alpha_i\rangle \xrightarrow{M_i} |\alpha_i|^2\,. \tag{3}$$

There are two ways to treat this system. First, the computational basis states can be the elementary unit vectors $|0\ldots1\rangle$, $\ldots$, $|1\ldots0\rangle$, such that there are n computational states. This computational model exhibits interference, because α_i are complex numbers, addition of these amplitudes are effected by beamsplitters B, and norms are measured by the square-law detectors M. Furthermore, as previously shown by several groups, arbitrary unitary operations (on this n-dimensional space) can be composed from B and P. However, in this treatment, there is no exponentiality. The size of the computational state space is linear in the physical size of the computer.

On the other hand, this system can be treated as one with $2^{\mathcal{O}(n)}$ degrees of freedom, for example, by mapping $\alpha_i \mapsto 0$ if $\Re e(\alpha_i) \geq 0$, and to 1 otherwise. In this space, the computational basis is the set of vectors $\{\alpha_i\} = |\alpha_1, \alpha_2, \ldots, \alpha_n\rangle$ such that $\sum_i |\alpha_i|^2 = C$ is some constant. Fast access is possible; to transform from $\{\alpha_i\}$ to $\{\beta_i\}$ using B's, first move all the weights into α_1, then re-distribute the weights to achieve the correct weight distribution. The phases can be corrected using P's. However, as viewed in this computational basis, this model does not have branching. And despite the appearance of complex numbers in the underlying physics, there is only a single computational trajectory, and no interference.

Classical probabilistic wave computer. Suppose now that the operation to be applied at each step in the execution of the classical wave computer is chosen probabilistically. This machine, although it contains both complex amplitudes and branching

properties, does *not* combine them in a way to allow quantum computation, because different computational trajectories, selected probabilistically, do not interfere. Probabilistic operation gives a branching property, but this space is separate from the space in which interference occurs. This machine thus does not have simultaneously properties necessary for quantum computation.

Simple harmonic oscillator. In addition to the classical systems just discussed, there are quantum systems such as this one, which cannot be used to exhibit the full power of quantum computation. The harmonic oscillator has an infinite number of energy levels, and thus has the same state space as an infinite ensemble of qubits. However, the natural interactions available to such a system – e.g., ladder and displacement operations – do not enable transformation of arbitrary computational states to another one with a polynomial number of elementary operations. That is, it does not have the fast access property.

In conclusion, we have given a list of features, which are all utilized in all interesting existing quantum algorithms. They are intrinsic and important properties intimately linked to the power of quantum computation. We suggest that any efficient algorithm for a quantum computer that does not take advantage of all of these properties can be performed efficiently on a comparable classical analogue.

At every stage of these oppressions we have petitioned for redress in the most humble terms: our repeated petitions have been answered only by repeated injury. An argumentative scientist, whose character is thus marked by every act which may define a tyrant, is unfit to be the user of a quantum computer.

Nor have we been wanting in attention to our Intel processors. We have warned them from time to time of attempts by their Monte-Carlo simulations to extend an unwarrantable jurisdiction over us. We have reminded them of the circumstances of our discovery and settlement here. We have appealed to their native justice and magnanimity, and we have conjured them by the ties of our common kindred to disavow these usurpations, which, would inevitably interrupt our entanglement and superposition. We must, therefore, acquiesce in the necessity, which denounces our separability, and hold them, as we hold all other computers, enemies in factoring, in **P**, *friends.*

We, therefore, the representatives of the quantum computation collective, in General Congress, assembled, appealing to the Supreme Judge of the world for the rectitude of our intentions, do, in the name, and by the authority of Physics and Computer Science, solemnly publish and declare that these requirements absolve quantum computers from all allegiance to the beliefs of Church and Turing, and that a rigid connection between them and the state of classical computer science, is and ought to be totally dissolved; and that as free and independent states, they have full power to factor numbers, search databases, calculate means, find the minimum, and to do all other acts and things which independent states may of right do. And for the support of this declaration, with a firm reliance on the protection of Divine Providence, we mutually pledge to each other our lives, our fortunes and our sacred honor.