

# Physical-Resource Requirements and the Power of Quantum Computation

Carlton M. Caves,<sup>†</sup> Ivan H. Deutsch,<sup>†</sup> and Robin Blume-Kohout<sup>‡</sup>

<sup>†</sup> Department of Physics and Astronomy, University of New Mexico, Albuquerque, NM 87131–1156, USA

<sup>‡</sup> Theoretical Division, Mail Stop B210, Los Alamos National Laboratory, Los Alamos, NM 87545, USA

E-mail: caves@info.phys.unm.edu

**Abstract.** The primary resource for quantum computation is Hilbert-space dimension. Whereas Hilbert space itself is an abstract construction, the number of dimensions available to a system is a physical quantity that requires physical resources. Avoiding a demand for an exponential amount of these resources places a fundamental constraint on the systems that are suitable for scalable quantum computation. To be scalable, the number of degrees of freedom in the computer must grow nearly linearly with the number of qubits in an equivalent qubit-based quantum computer. These considerations rule out quantum computers based on a single particle, a single atom, or a single molecule consisting of a fixed number of atoms or on classical waves manipulated using the transformations of linear optics.

Submitted to: *J. Opt. B: Quantum Semiclass. Opt.*

PACS numbers: 03.67.Lx, 03.67.Mn

## 1. Introduction

Quantum computation is an alluring long-term goal for quantum optics and the emerging field of quantum information science [1, 2]. In this paper we address the question of what physical resources are required for quantum computation and, in particular, how the required resources scale with problem size. By determining how to avoid a physical-resource demand that increases exponentially with problem size, we establish necessary conditions for a physical system to be a scalable quantum computer.

The initial step in a quantum computation is to store classical information (the input) as some quantum state of the computer. The computer then runs through a carefully controlled sequence of unitary operations and/or measurements (the program). At the completion of the computation, the answer (the output) is stored as classical information that can be read out with high probability by a measurement. The power of a quantum computer lies somewhere in the murky region between the classical input and the classical output—a region where classical, realistic descriptions fail.

Ask for the crucial property of that murky region, and you will get nearly as many answers as there are quantum information scientists: the superposition principle of quantum mechanics and associated quantum interference and quantum parallelism; quantum entanglement; the use of entangling unitary operations; the collapse of the wave function after measurement and associated information-disturbance trade-offs. All of these distinguish quantum systems from classical ones. How are we to decide which is the crucial quantum feature?

We argue that a quantum computer's power stems from the murky region itself: a quantum computer escapes the bounds of classical information processing because there is no efficient realistic description of what happens between the classical input and the classical output. The ability to access arbitrary states in Hilbert space is what leads to situations where there is no efficient realistic description. Optical systems provide one of the most dramatic illustrations of this principle. Classical (coherent-state) linear optics is efficiently simulatable [3]. In contrast, operations with the same linear elements, but supplemented with single-photon sources and counters, can perform universal quantum computation, as shown by Knill, LaFlamme, and Milburn (KLM) [4].

It is difficult to pin down the source of a quantum computer's power because arbitrary states can be accessed in very different physical systems—different hardware—using very different control techniques—different software. Yet no matter how a quantum computation is packaged, we can identify one universal prerequisite: the computer must have a Hilbert space large enough to accommodate the computation. If the computer is to be a general-purpose computer, able in principle to solve problems of arbitrary size, it must have a Hilbert space whose dimension is capable in principle of growing exponentially with problem size. Hilbert space is essential for quantum computation, and the primary resource is *Hilbert-space dimension*.

Hilbert spaces of the same dimension are *fungible*. What can be done in one can be done in principle in any other of the same dimension: simply map one Hilbert space

onto the other, including all the subsystems, operations, and measurements. Which Hilbert space is used to represent and process quantum information becomes important only when further physical considerations are introduced. Though Hilbert spaces are fungible, the physical systems described by those Hilbert spaces are not, because *we don't live in Hilbert space*. A Hilbert space gets its connection to the world we live in through the physical quantities—position, linear momentum, energy, angular momentum—of the system that is described by that Hilbert space. These physical quantities arise naturally from spacetime symmetries and the system Hamiltonian. They are the “handles” that permit us to grab hold of a quantum system and manipulate it, and they are the physical resources that must be supplied to access various parts of the system Hilbert space. The crucial *physical* question for quantum computation is the following: *how much of these resources is required to achieve a Hilbert-space dimension sufficient for a computation?* This is the question we address in this paper.

Quantum mechanics constrains our description of physical systems sufficiently that we can formulate the question of physical-resource demands in a general way. We find that to avoid supplying an amount of some physical resource that grows exponentially with problem size, the computer must be made up of subsystems—degrees of freedom in the simple analysis presented here—whose number grows nearly linearly with the number of qubits required in an equivalent quantum computer. This thus becomes a fundamental requirement for a system to be a *scalable* quantum computer.‡

We emphasize that this requirement is an initial barrier that must be surmounted by proposals for scalable quantum computation, before such proposals confront the difficult and necessary tasks of initialization, control, protection from errors, and readout. Surmounting this initial barrier does not guarantee that a proposal can meet the further requirements; it is a necessary, but by no means sufficient requirement for a scalable quantum computer. The point of this paper is that one can draw general conclusions about the physical systems that can be used for quantum computation just by considering whether the system can efficiently provide the *primary* resource of Hilbert-space dimension, without getting enmeshed in questions about the other necessary requirements for the operation of a quantum computer.

The present paper is an abbreviated version of a more extensive analysis published elsewhere [3]. Here we restrict our consideration to systems of particles that can be described by ordinary quantum mechanics. For these systems, the subsystems can be identified with the *degrees of freedom* of the particles. Though this simple degrees-of-freedom analysis contains the essence of our conclusions—indeed, the essence is summarized succinctly in Figure 1—the original paper extended the analysis to more general systems that require a description in terms of quantum fields. The reader interested in this more general analysis and in a more extensive list of references is

‡ Since in this paper we are interested in comparing how different systems use physical resources, we use the term *quantum computer* for any physical system that has the required Hilbert-space dimension, and we reserve the term *scalable quantum computer* for systems that can provide the required Hilbert-space dimension efficiently.

urged to consult the original paper [3].

## 2. Degrees-of-freedom analysis of resource requirements

### 2.1. Role of Planck's constant

Dimensionless quantities in physics are determined by writing the relevant physical quantities in terms of a relevant scale. For the dimension of a system's Hilbert space, Planck's constant  $h$  sets the scale; the available number of Hilbert-space dimensions is determined by writing an appropriate combination of physical quantities, the *action*, in units of  $h$ .

The analysis of resource demands is particularly simple for systems of particles described by ordinary quantum mechanics, for which the subsystems can be identified with the degrees of freedom of the particles. The quantum state of such a computer is described in a Hilbert space that is a tensor product of the Hilbert spaces of the degrees of freedom.

A degree of freedom corresponds to a pair of (generalized) canonical coordinates, position  $q$  and momentum  $p$ . The physical resources are the ranges of positions and momenta,  $\Delta q$  and  $\Delta p$ , used by the computation. The physically relevant measure of these resources is the corresponding phase-space area or *action*,  $A = \Delta q \Delta p$ . For a degree of freedom that is an intrinsic angular momentum  $J$ , we can use  $\Delta q = 2\pi$  and  $\Delta p = \Delta J$ , thus giving  $A = 2\pi \Delta J$ . The connection to Hilbert space comes from the fact that a quantum state occupies an area in phase space given by Planck's constant  $h$ ; orthogonal states correspond roughly to nonoverlapping areas, each of area  $h$ . Thus the available dimension of the Hilbert space for a single degree of freedom is given approximately by  $A/h$ . The goal of scalability is to avoid having to supply an action resource  $A$  for any degree of freedom that grows exponentially with problem size.

### 2.2. Degrees-of-freedom analysis

We measure the Hilbert-space dimension required for a quantum computation in qubit units: let the problem size for a computation be  $n$ , and let  $N = \mathbf{F}(n)$  be the number of qubits required for the computation, assuming an optimal qubit algorithm that requires only a polynomial number of qubits, an example being Shor's factoring algorithm [2]. Here and below, bold type denotes a function that is bounded above by a polynomial. The Hilbert-space dimension needed for the computation is  $2^N = 2^{\mathbf{F}(n)}$ . Using qubit units, we see that the required Hilbert-space dimension grows exponentially with problem size. We assume that there is no more efficient algorithm in a Hilbert space with some other structure than the qubit tensor-product structure, this being part of our assumption that Hilbert spaces are fungible.

Suppose now that the  $j$ th degree of freedom supplies an action  $A_j$ . The Hilbert space of the entire system is a tensor product of the Hilbert spaces for the degrees of

freedom, so the overall Hilbert space has dimension

$$2^N \sim \frac{A_1}{h} \cdots \frac{A_T}{h} = \frac{V}{h^T}, \quad (1)$$

where  $V$  is the phase-space volume used by the computation. If  $T$  grows more slowly than linearly with  $N$  (within specific logarithmic corrections discussed below), at least one of the actions must grow exponentially with  $N$ , thus requiring an exponential amount of some physical resource. In contrast, if  $T$  grows linearly with  $N$ , no degree of freedom has to supply an increasing amount of action, which makes the system a candidate for a scalable quantum computer.

It is useful to summarize this simple result, as it is the foundation for all our further conclusions. The physical resources are the quantities that label the axes of a (generalized) phase space that has two axes for each degree of freedom. The number of Hilbert-space dimensions available for a computation is proportional to the total phase-space volume. If the number of degrees of freedom grows linearly in  $N$ , the phase-space volume needed to accommodate the Hilbert-space dimension can be folded up into a hypercube in phase space without requiring an exponentially increasing contribution along any direction in phase space. In contrast, if the number of degrees of freedom grows more slowly than linearly in  $N$  (within the logarithmic corrections discussed below), some phase-space direction must supply an exponentially increasing amount of the corresponding physical resource. This simple argument is depicted schematically in Figure 1.

To formulate a more precise statement, we specialize to the case of  $T$  identical degrees of freedom, each of which supplies an action  $A$ . In this situation, the total number of Hilbert-space dimensions satisfies  $(A/h)^T \sim 2^N$ , which gives

$$A/h \sim 2^{N/T}. \quad (2)$$

In order to avoid an exponential resource demand,  $A/h$  must grow polynomially with  $N$ ,§ which means that the number of degrees of freedom increases as||

$$T \sim \frac{N}{\log \mathbf{P}(N)}, \quad (3)$$

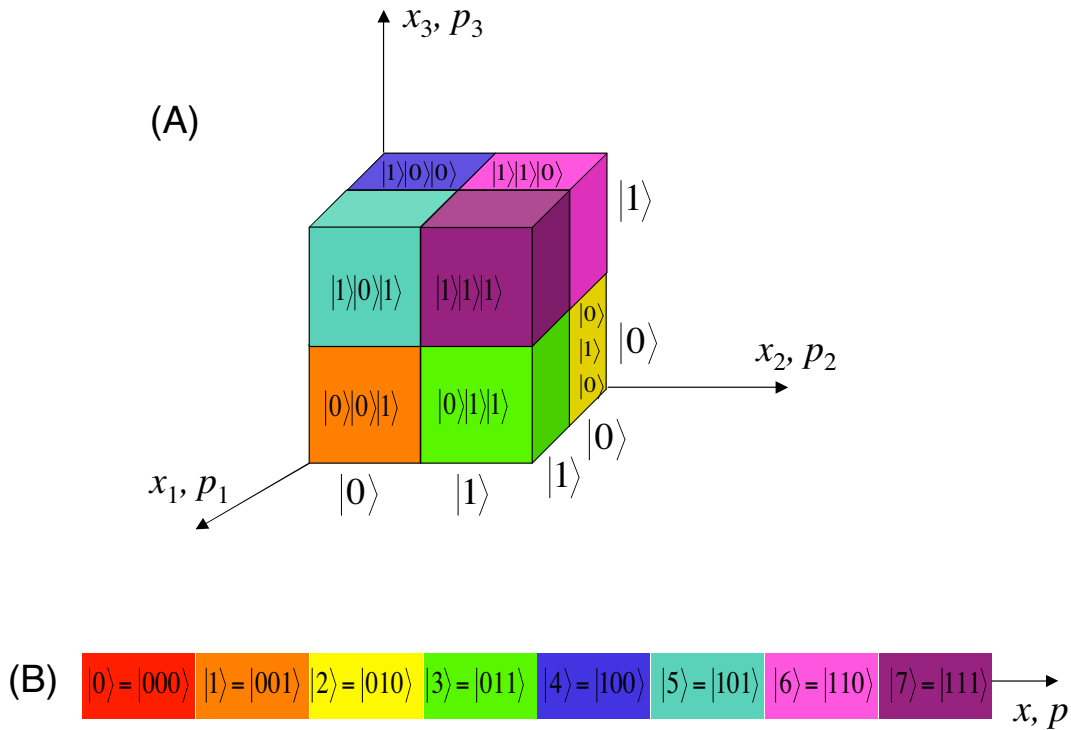
where  $\mathbf{P}(N)$  is a function bounded above by a polynomial. We say that  $T$  grows *quasilinearly* with  $N$  and that the system is *scalable*, having a *scalable tensor-product structure*.

It is instructive to distinguish three cases:

- (i)  $T$  grows more slowly than linearly with  $N$ . If  $T$  grows quasilinearly, as in Eq. (3), then  $A/h \sim \mathbf{P}(N)$ , and the system is scalable. If  $T$  grows more slowly than quasilinearly with  $N$ ,  $A/h$  grows exponentially with  $N$ , leading to an exponential demand for physical resources.

§ We follow the computer-science convention of referring to any superpolynomial growth as exponential.

|| We use base-2 logarithms.



**Figure 1. Using many degrees of freedom to save resources.** Orthogonal basis states for an eight-dimensional Hilbert space are depicted schematically as nonoverlapping phase-space cells in the phase space of three degrees of freedom (A), each of which uses an action  $\sim 2\hbar$ , or in the phase space of a single degree of freedom (B). Phase space is pictured at half its actual dimension by letting the axes represent both the position and momentum coordinates for a degree of freedom; one can think of the axes as measuring the amount of action used by a degree of freedom. To accommodate the eight states, the single degree of freedom requires three times as much action as does each of the three degrees of freedom. If one adds degrees of freedom to (A), the phase-space volume—and hence the Hilbert-space dimension—doubles as each degree of freedom is added and thus grows exponentially with the number of degrees of freedom, whereas the physical resources grow linearly with the number of degrees of freedom and thus logarithmically with the Hilbert-space dimension. The result is a scalable resource requirement. In contrast, for the single degree of freedom in (B), the required resources grow linearly with phase-space volume and Hilbert-space dimension; to achieve the same Hilbert-space dimension as for the scalable case requires physical resources that are exponentially larger. The use of many degrees of freedom, with the number of degrees of freedom growing nearly linearly with the corresponding number of qubits, allows the required phase-space volume to be folded up into a hypercube so that no degree of freedom has to provide an exponential amount of action. As shown, the basis states for both situations can be labeled either by unary or binary numbers, this being an example of the fungibility of Hilbert spaces. The labeling, however, cannot alter the physics: the single degree of freedom is a *physically* unary realization of the Hilbert space, which uses exponential resources asymptotically, whereas the multiple degrees of freedom in (A) provide a *physically* binary realization of the same Hilbert space, which uses resources efficiently.

- (ii)  $T$  grows faster than linearly with  $N$ . In this case,  $A/h$  goes to one as  $N$  increases, implying that each degree of freedom asymptotes to a one-dimensional Hilbert space. This means that the present analysis in terms of independent degrees of freedom breaks down and should be replaced by a counting of the excitations of a quantum field, which properly takes into account the resources used by unoccupied field modes [3].
- (iii)  $T = N/\log D$  grows strictly linearly with  $N$ . For  $D < 2$ , the present analysis breaks down, and we again need the analysis of quantum fields to reach a sensible conclusion [3]. For  $D \geq 2$ , each degree of freedom is a  $D$ -level system, i.e., a *qudit* instead of a qubit. Though this is the special case of quasilinear growth in which  $\mathbf{P}(N) = D$ , we consider it separately because it is the most important scalable case, in that the action supplied by each system,  $A/h \sim D$ , is independent of problem size. Scaling is achieved simply by adding degrees of freedom, without having to change the Hilbert-space dimension supplied by each degree of freedom. We say that this kind of system is *strictly scalable* and has a *strictly scalable tensor-product structure*. Most quantum computing proposals are of this sort.

Had we focused on the total action resource,

$$TA/h \sim T2^{N/T}, \quad (4)$$

instead of on the action resource per degree of freedom, we would have reached the same conclusions regarding scaling. For a scalable system, the total action resource grows as  $TA/h \sim NP(N)/\log \mathbf{P}(N)$ ; only for strictly scalable systems is the total action resource linear in  $N$ .

### 2.3. Quantum computing in a single atom

An illuminating extreme example of the nonscalable systems in case 1 is the attempt to implement quantum computing in a single atom [5], single molecule with a fixed number of atoms [6, 7], or large spin [8]. Advances in laser spectroscopy with ultrashort pulses have allowed researchers to manipulate and measure the electronic wave function in an atom [9] or both electronic and rotational/vibrational wave functions in a molecule [10] with exquisite precision. It is natural to wonder whether these tools for coherent control of quantum states can be applied to quantum computing.

For illustration, consider the simplest hypothetical model, quantum computing in a hydrogen atom. Characteristic atomic units of length, momentum, and energy are formed from the physically important constants: the electron charge and mass,  $e$  and  $m$ , and the quantum of action,  $\hbar$ . If we ignore spin, Bohr's formula for quantizing the action gives the familiar expressions for the energy, radius, and momentum of a stationary state with principal quantum number  $n$ ,

$$E_n = -\frac{1}{2n^2} \frac{e^2}{a_0}, \quad r_n = n^2 a_0, \quad p_n = \frac{1}{n} \frac{\hbar}{a_0}, \quad (5)$$

where  $a_0 = \hbar^2/me^2$  is the Bohr radius. The dimension of the Hilbert space spanned by all bound states from the ground state up to a maximum principal quantum number  $n$  is

$$\sum_{k=1}^n \sum_{l=0}^{k-1} (2l+1) \sim \frac{1}{3}n^3 \sim \left(\frac{r_n p_n}{\hbar}\right)^3. \quad (6)$$

The final expression has just the form we expect. Without spin the internal states of the hydrogen atom have three degrees of freedom, signaled by the 3 in the exponent and corresponding to the three coordinates of relative motion of the electron and proton. Each degree of freedom is allotted an action  $A \sim r_n p_n$ , which provides enough phase space for  $\sim A/h$  orthogonal states in Hilbert space.

Demanding that the atomic Hilbert space have a dimension  $2^N$  requires that the radial coordinate scale as  $r_n \sim 2^{2N/3}a_0$ . The exponential growth of this coordinate with problem size implies that quantum control in a single atom *cannot* be used for scalable quantum computation. For instance, to implement a quantum computation requiring  $N = 100$  qubits, the atomic radius must be  $r_n \sim 10^{20}a_0 = 6 \times 10^6$  km, about 5 times the diameter of the Sun.

A single atom is an example of a “physically unary” quantum computer, having a limited natural tensor-product structure provided by the small number of physical degrees of freedom. Similar poor scaling will be seen in any implementation consisting of a single particle, a single atom, or a single molecule consisting of a fixed number of atoms. The fungibility of Hilbert spaces means that one can impose an artificial tensor-product structure on the Hilbert space of these systems, equivalent to that of qubits, but this does not obviate the need to provide the physical resources to generate orthogonal quantum states. Without a scalable tensor-product structure corresponding to a division into physical degrees of freedom, the action resources along one or more of the physical coordinate axes must blow up exponentially with problem size, meaning that these systems are not suitable for scalable quantum computation.

This should be contrasted with quantum computing using multiple atoms, containing a physical tensor product structure, such as in an ion trap [11]. Quantum information is stored in two sublevels of each of the ion’s ground states and manipulated with a limited number of vibrational states. A Hilbert space of 100 qubits requires 100 ions in their ground states occupying 100 local positions. Neither the internal nor the external degrees of freedom of the atoms requires physical resources that grow exponentially in order to accommodate a  $2^N$ -dimensional Hilbert space.

Closely related to unary systems with a single particle are implementations of quantum algorithms that use superposition and interference of classical linear waves. Classical linear optics (electromagnetic waves) provides an example that can be easily implemented in the laboratory. The wave amplitudes are described in a complex vector space, just like the Hilbert space of a quantum system, so it might appear that such classical-wave processors are candidate quantum computers. The problem is that they will *always* scale poorly when the necessary physical resources are taken into account [3]. A classical wave is essentially a many-particle copy of a single-particle wave function.

The linear-optics transformations of a classical wave are in one-to-one correspondence with the unitary transformations of the single-particle wave function. A single photon has only three motional degrees of freedom and one polarization degree of freedom. Thus a classical-wave computation requires an exponential number of orthogonal states, or modes, in the single-particle phase space, a demand inherited from a single-particle unary machine.

### 3. Role of entanglement

Entanglement is a distinctive feature of quantum mechanics. It is clearly a resource for such quantum information protocols as teleportation, yet its role in quantum computation remains unclear. Some claim it is the property that powers quantum computation [12, 13], while others downplay its significance [14, 15]. The situation has been clarified considerably by the recent work of Jozsa and Linden [16], who showed that for a qubit quantum computer—the extension to qudits is straightforward—entanglement among all the qubits is a prerequisite for an exponential speed-up over a classical computation. The Jozsa-Linden proof proceeds by showing that if entanglement extends only to a fixed number of qubits, independent of problem size, the computation can be simulated efficiently on a classical computer.

The Jozsa-Linden argument *assumes* a strictly scalable tensor-product structure. The global entanglement that accompanies exponential speed-up is a consequence of assuming this tensor-product structure and an initial pure state. Consider a computation with an exponential speed-up on a qubit quantum computer. Mapped onto a unary machine, the same computation produces *no* entanglement. Whether run on the unary computer or the qubit computer, the computation accesses arbitrary states—i.e., arbitrary superpositions—in the computer’s Hilbert space and has no efficient description in the realistic language of classical computation. Hilbert spaces are fungible! Global entanglement is a result of running the computation on a quantum computer with a tensor-product structure; for such a computer, arbitrary superpositions lead to entanglement among all the parts, because the states without such global entanglement occupy only a tiny corner of Hilbert space [12, 13]. On a physically unary computer, the same arbitrary superpositions have no entanglement.

The global entanglement in a quantum computation is thus a consequence of the need to save resources, which is what dictates a strictly scalable tensor-product structure to start with. A weak statement is that global entanglement is a measure of the computer’s ability to economize on physical resources. A stronger conclusion is that global entanglement is indeed the key quantum *resource* that allows a scalable quantum computer to avoid an exponential demand for physical resources. For a pure-state quantum computer, such as those considered here, entanglement is what allows the arbitrary superpositions required for quantum computation to be folded into a compact hypercube in phase space, as illustrated in Figure 1.¶

¶ In their analysis, Jozsa and Linden were careful to point out that although entanglement among all

This line of reasoning, based on consideration of pure-state quantum computation, is supported by what is known about mixed-state quantum computation. An example is provided by liquid-state nuclear magnetic resonance (NMR) [17, 18]. In NMR the qubits are the active nuclear spins within each molecule in the liquid sample, and each molecule is an independent quantum computer, which runs an independent version of the computation. Mixed states don't have any effect on the analysis of this paper, which shows that to avoid an exponential resource demand requires a scalable tensor-product structure—in NMR this means that the number of qubits per molecule must increase linearly, just as in a pure-state qubit computer—but the further argument that entanglement follows from accessing arbitrary states in a system with a tensor-product structure, does not work for mixed states [16]. Indeed, with present polarizations, the states accessed in NMR are known to be unentangled up to about 23 qubits [19, 20, 21] and, for bigger numbers of qubits, are likely to be far less entangled than in a corresponding pure-state quantum computer.

In a mixed-state quantum computer, the previous connection between physical resources and entanglement is severed, but a new connection arises to take its place. The paucity of entanglement in mixed-state quantum computing betrays another resource problem. This resource problem comes about from the need to read out the output reliably in the presence of the noise produced by the mixed state and results in a demand for a number of repetitions of the computation that increases exponentially with problem size. In NMR this resource problem shows up as a demand for an exponentially increasing number of molecules. This mixed-state resource problem, which is apparently independent of the phase-space considerations that we apply to quantum computers in this paper, provides further evidence for the importance of entanglement in avoiding exponential resource demands in quantum computation.

#### **4. Conclusion**

Our contention in this paper is that the fundamental requirement for a scalable quantum computer is set by the need to economize on physical resources in providing the primary resource of Hilbert-space dimension. To avoid an exponential demand for physical resources, the number of degrees of freedom must grow quasilinearly with the equivalent number of qubits. This requirement means that a scalable quantum computer must have a robust tensor-product structure. Systems without such a tensor-product structure are not suitable for scalable quantum computation.

Physical systems that don't scale properly, such as liquid-state NMR, Rydberg atoms, or molecular magnets, are still worth studying for a variety of reasons. First and foremost, a large number of qubits is necessary for exponential speed-up, it is not sufficient: as shown by Gottesman and Knill [2], there are sequences of quantum gates that can be simulated efficiently on a classical computer even though they entangle all qubits. This does not undermine the conclusion that entanglement is necessary for avoiding an exponential resource demand, but it does suggest that some other quantity, presumably closely related to entanglement, might characterize more completely the ability of a quantum computer to economize on physical resources.

foremost, they embody fundamental physical questions that are worth investigating in their own right, regardless of their relevance to quantum information science. Second, they can be used to develop new technologies for control, readout, and error correction in quantum systems. These new technologies might have applications to quantum-information-processing jobs outside quantum computation, and they might be transferable to scalable quantum computers. Finally, the scalability criteria formulated in this paper are asymptotic requirements. They are useful for assessing the physical resources required for a general-purpose quantum computer to do problems of increasing size. Yet even for this purpose, they are imperfect tools, because no real computer is expected to do problems of arbitrary size. Non-scalable systems might be able to provide sufficient Hilbert-space dimension for special-purpose quantum computations that need only a limited number of qubits, such as simulation of other quantum systems [22].

Hilbert space is essential for quantum computation. Yet it is an odd sort of thing to need. It is not a physical object, but rather a mathematical abstraction in which we describe physical objects. A Hilbert space gets a physical interpretation—a connection to the external world—only through the physical system that we describe in that Hilbert space. The connection is made through privileged observables—the generators of space-time symmetries, e.g., position, momentum, angular momentum, and energy—which determine a set of physical degrees of freedom for the system. This connection made, we can determine how the physical resources, measured in terms of phase-space actions constructed from the privileged observables, must grow in order to provide the Hilbert-space dimension needed for a quantum computation.

Our degrees-of-freedom analysis can be applied to the physical resources required by a classical computer. Generally the subsystems in a classical computer consist of many physical degrees of freedom. If each distinguishable configuration of a subsystem occupies a fixed phase-space volume, then our analysis shows that the physical resources required by the classical computer grow exponentially unless the number of subsystems grows quasipolynomially with problem size. But the phase-space scale in the classical analysis is not fundamental, instead being set by noise and the resolution of measuring devices. This makes the classical analysis of resource requirements dependent on other features of a classical computer. The difference for a quantum computer is that Planck's constant sets a fundamental scale, which makes the resource requirements presented here prerequisites for scalable quantum computation, prior to the other necessary requirements for a quantum computer's operation.

## **Acknowledgments**

This work was partly supported by the National Security Agency (NSA) and the Advanced Research and Development Activity (ARDA) under Army Research Office (ARO) Contract No. DAAD19-01-1-0648 and by the Office of Naval Research under Contract Nos. N00014-00-1-0578 and N00014-99-1-0247. This work grew in large part out of discussions at the Institute Theoretical Physics of the University of California,

Santa Barbara, where the authors were in residence during the fall of 2001. The authors received support from the ITP's National Science Foundation Contract No. PHY99-07949.

## References

- [1] *Quantum Information Science: An Emerging Field of Interdisciplinary Research and Education in Science and Engineering*, Report of NSF Workshop, October 28–29, 1999, Arlington, VA, <http://www.nsf.gov/cgi-bin/getpub?nsf00101>.
- [2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, England, 2000.
- [3] R. Blume-Kohout, C. M. Caves, and I. H. Deutsch, "Climbing Mount Scalable: Physical-resource requirements for a scalable quantum computer," *Found. Phys.* **32**, pp. 1641–1670, 2002.
- [4] E. Knill, R. Laflamme, and G. J. Milburn, "A scheme for efficient quantum computation with linear optics," *Nature* **409**, pp. 46–52, 2001.
- [5] J. Ahn, C. Weinacht, and P. H. Bucksbaum, "Information storage and retrieval through quantum phase," *Science* **287**, pp. 463–465, 2000.
- [6] R. Zadayan, D. Kohen, D. A. Lidar, and V. A. Apkarian, "The manipulation of massive ro-vibronic superpositions using time-frequency-resolved coherent anti-Stokes Raman scattering (TFRCARS): From quantum control to quantum computing," *Chem. Phys.* **266**, pp. 323–351, 2001.
- [7] V. V. Lozovoy and M. Dantus, "Photon echo pulse sequences with femtosecond shaped pulses as a vehicle for molecule-based quantum computation," *Chem. Phys. Lett.* **351**, pp. 213–221, 2002.
- [8] M. N. Leuenberger and D. Loss, "Quantum computing in molecular magnets," *Nature* **410**, pp. 789–793, 2001.
- [9] M. W. Noel and C. R. Stroud, Jr., "Excitation of an atomic electron to a coherent superposition of macroscopically distinct states," *Phys. Rev. Lett.* **77**, pp. 1913–1916, 1996.
- [10] H. Rabitz, R. de Vivie-Riedle, M. Motzkus, and K. Kompa, "Whither the future of controlling quantum phenomena," *Science* **288**, pp. 824–828, 2000.
- [11] D. Kielpinski, C. Monroe, and D. J. Wineland, "Architecture for a large-scale ion-trap quantum computer," *Nature* **417**, pp. 709–711, 2002.
- [12] A. Ekert and R. Jozsa, "Quantum algorithms: Entanglement-enhanced information processing," *Phil. Trans. R. Soc. London A* **356**, pp. 1769–1782, 1998.
- [13] R. Jozsa, "Entanglement and quantum computation," in *The Geometric Universe: Science, Geometry, and the Work of Roger Penrose*, S. A. Huggett, L. J. Mason, K. P. Tod, S. T. Tsou, and N. M. J. Woodhouse, eds., pp. 369–379, Oxford University Press, Oxford, England, 1998.
- [14] S. Lloyd, "Quantum search without entanglement," *Phys. Rev. A* **61**, Art. No. 010301(R), 1999.
- [15] P. Knight, "Quantum information processing without entanglement," *Science* **287**, pp. 441–442, 2000.
- [16] R. Jozsa and N. Linden, "On the role of entanglement in quantum computational speed-up," *Proc. Roy. Soc. London A* **459**, pp. 2011–2032, 2003.
- [17] D. G. Cory, R. Laflamme, E. Knill, L. Viola, T. F. Havel, N. Boulant, G. Boutis, E. Fortunato, S. Lloyd, R. Martinez, C. Negrevergne, M. Pravia, Y. Sharf, G. Teklemariam, Y. S. Weinstein, and W. H. Zurek, "NMR Based quantum information processing: Achievements and prospects," *Fortschr. Phys.* **48**, pp. 875–907, 2000.
- [18] J. A. Jones, "NMR quantum computation: A critical evaluation," *Fortschr. Phys.* **48**, pp. 909–924, 2000.
- [19] S. L. Braunstein, C. M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack, "Separability of

- very noisy mixed states and implications for NMR quantum computing,” *Phys. Rev. Lett.* **83**, pp. 1054–1057, 1999.
- [20] N. C. Menicucci and C. M. Caves, “Local realistic model for the dynamics of bulk-ensemble NMR information processing,” *Phys. Rev. Lett.* **88**, Art. No. 167901, 2002.
- [21] L. Gurvits and H. Barnum, “Separable balls around the maximally mixed multipartite quantum states,” unpublished, [arXiv.org e-print quant-ph/0302102](https://arxiv.org/abs/quant-ph/0302102).
- [22] S. Lloyd, “Universal quantum simulators,” *Science* **273**, pp. 1073–1078, 1996.