An Outlook for Quantum Computing

DMITRI MASLOV
National Science Foundation, Alexandria, VA 22314 USA
YUNSEONG NAM
IonQ, Inc., College Park, MD 20740 USA
JUNGSANG KIM
Duke University, Durham, NC 27708 USA, and IonQ, Inc., College Park, MD 20740 USA

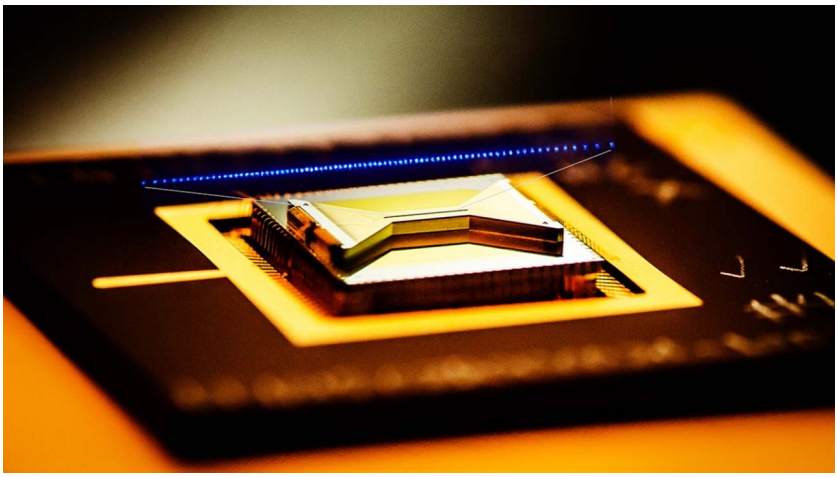

Photo credit: Dr. Kai Hudek, IonQ.

I. WHAT ARE QUANTUM COMPUTERS?

We have ubiquitous presence of computers today, ranging from simple controllers in modern appliances to smartphones in our pockets that provide a wide range of everyday services, to powerful supercomputers and large data centers that carry out the most computationally intensive tasks. These computational machines have a few things in common: for example, the information they handle is stored in bits (0 or 1), and the procedure for processing the information is specified by a program. A great deal is known about the limits of what such computational machines can and cannot do efficiently. There are many important computational problems that are believed to be very difficult to solve using even the most powerful computers, where the resource requirement—whether it is the size of the machine or the time it takes to finish the task—increases exponentially as a function of the problem size.

It was recognized in the 1980s, first by a group of physicists, that the rules of representing and processing information in modern computers are restricted by the laws of classical physics, which govern the behavior of traditional computational machines (thus the term "classical computer"). The applicable laws of physics were expanded greatly in the 20th century with the development of quantum physics that successfully describes the behavior of systems at the atomic and subatomic levels, which classical physics fails to explain. A natural question that arises is whether more computational power can be gained if the laws of quantum physics are exploited, especially in light of realizing that computational resources required to capture the full behavior of quantum systems appear to increase exponentially as the system size grows. Over the last three decades, our understanding of the computational machines that operate on quantum principles (thus the term "quantum computers") has expanded drastically, as the efforts to realize such an exotic computer have made steady yet remarkable progress.

The quantum version of a bit, called a qubit, is encoded by the

Digital Object Identifier 10.1109/JPROC.2018.2884353

two basis states of the quantum system that represents it, $|0\rangle$ and $|1\rangle$. In contrast to a classical bit, which may be in a state of 0 or 1, a qubit may exist in a superposition of the two states $|\psi\rangle = x_0|0\rangle + x_1|1\rangle$, where x_0 and x_1 are the complex coefficients. These coefficients satisfy the normalization condition $|x_0|^2 + |x_1|^2 = 1$, owing to the fact that $|x_0|^2$ and $|x_1|^2$ represent the probabilities of finding the qubit in the state $|0\rangle$ and $|1\rangle$ upon measurement, respectively, and the probabilities must sum up to 1. With n qubits, the composite qubit system is described by a superposition of all possible 2^n basis states as $|\psi_n\rangle = \sum_{i=0}^{2^n-1} x_i|i\rangle$, where the summation runs over all binary representations of n-qubit states (from $|00...0\rangle$ to $|11...1\rangle$), with the normalization condition for the complex coefficients x_i, $\sum_{i=0}^{2^n-1} |x_i|^2 = 1$. Such an n-qubit system description illustrates a direct access to the full computational space that is exponentially large in n. With x_i being complex rather than real numbers, the computational advantage of quantum computers versus classical probabilistic computers comes into play. Similar to the classical logic gate operations, quantum logic gates compute the output states from the input states but allow the input states to be an arbitrary quantum state (such as superposition states). Quantum logic gates are implemented by designing the time evolution of the input quantum states to achieve the desired output states, often by manipulating the external control signals. Mathematically, quantum gates are described by the unitary matrices, and their application is accomplished through multiplication of the respective matrix by the state vector. During the computation, the state of the qubits develops correlations among them where the state of one qubit cannot be described independently of the state of other qubits, known as quantum entanglement. Superposition and entanglement are two unique properties of quantum physics that do not have classical counterparts.

It is experimentally verified that one can take advantage of the superposition and entanglement to perform certain tasks for which no classical methods with comparable efficiency are known. Such demonstrations include the following.

1) *Superposition:* The generation of random numbers, relying on the true probabilistic nature of quantum mechanics, and reducing to the preparation and measurement of the quantum state $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ to obtain the desired random number.
2) *Entanglement:* A game (known as the CHSH game [6], named after its inventors Clauser, Horne, Shimony, and Holt, and equivalent to Bell's inequality) that can be played using entanglement to correlate players' strategies thus enabling a better than the best possible classical strategy.
3) *Superposition and Entanglement:* Testing the properties of small Boolean functions given as a black box, including Deutsch–Jozsa algorithm to distinguish balanced and constant functions, and Grover's algorithm to find a satisfying assignment. The advantage over classical algorithms manifests itself through the ability to query black boxes by superposed and entangled states, therefore extracting the desired information faster than it is possible to do classically.

II. QUANTUM COMPUTING HARDWARE

A. Implementation Challenges

The access to unconventional computational power offered by quantum computers comes at the price of the fragility of quantum systems. Quantum systems tend to quickly lose their quantum nature (quantum coherence) and revert to classical descriptions as the system becomes larger and more complex, due to mainly the interaction with the environment that tends to destroy superposition and entanglement. Utmost care must be taken to isolate the qubits from their environment and ensure that the logic gate operations modify the quantum system as close to the desired outcome as possible. Unlike classical digital logic gates where the output is rather insensitive to small noise at the input, quantum logic gates manipulate the complex coefficients of the superposition states and any error or noise in the gates can accumulate in an analog fashion. To address this problem, quantum error correcting codes (QECCs) were developed that can be used to correct these errors, in a manner similar to how classical error correction works in an analog communication channel. In a QECC, the quantum data (referred to as logical qubits) is redundantly encoded into a larger number of physical qubits, in a way that the errors on the physical qubits can be corrected so long as they occur sufficiently infrequently. Systematic approaches to construct fault-tolerant (FT) quantum computers from faulty components centered around QECC were developed, in close analogy to early days of digital computers based on faulty vacuum tube technology. Current FT quantum computing approaches incur a very large overhead, which is expected to improve as the performance of the component technology advances.

Similar to the situation in the early 20th century when the technology to put together a computational machine at modest scales remained elusive, the current status of efforts toward constructing a functional quantum computer is in its early stages. Early research effort emerged in the mid-1990s, in search of the adequate physical system in which to implement the qubits. Over the course of the ensuing two decades, a few physical platforms for qubits, most notably trapped atomic ions and superconducting circuits, have emerged as the leading candidates to construct functional quantum computers. Some small-scale but already fully programmable and universal quantum computers are available to a broader public via cloud

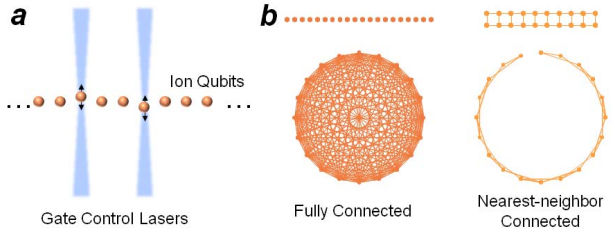

Fig. 1. *(a) Schematic of a small ion trap quantum processor. The linear chain of ions is manipulated using control laser beams that execute quantum logic gates on the ions by inducing their motion based on the qubit state. (b) Connectivity example of two different architectures. The vertices indicate qubits, and the edges correspond to the two-qubit gates that can be operated between the pair of qubits they connect. Available gates in a fully connected architecture of 20 qubits (such as the ion trap processor) (left). 20 qubits arranged in a 2 × 10 lattice with nearest-neighbor gates (right).*

access today, and larger systems with better performance are expected to become available in the coming years. In the early stages, these systems will likely not be large enough to implement FT quantum computations and will operate without the auspices of quantum error correction. Finding practical uses of such noisy intermediate-scale quantum (NISQ) systems will be an important question in transitioning quantum computing technology into a practical industry.

B. Technology Example: Trapped Ions

Trapped atomic ions provide one of the leading physical platforms for implementing a fully functional quantum computer [19], where a programmable quantum computer prototype was demonstrated [7], and its performance was compared with that of a similarly sized superconducting quantum computer [15]. In trapped ions, single atoms with an electron removed (thus, atomic ions) are used to represent the qubit, by selecting two internal states of the atom. Such ions can be trapped, often in the shape of a linear chain, in a structure that provides adequate electromagnetic fields to confine the ions in an ultra-high vacuum environment [Fig. 1(a)]. Modern-day ion traps are made on silicon substrates using microfabrication technology [17], [18].

These atomic qubits are very well isolated from their environments and their quantum properties remain unperturbed for a long time, making them an ideal candidate for qubits. In fact, they are so stable that they are used to define the absolute time reference, known as atomic clocks. Using frequency-stabilized laser light, one can prepare these qubits in a well-defined initial state by optically "pumping" the electron into one of the qubit states with very high probability. One can also measure the qubit with near-perfect accuracy, utilizing the fact that one of the qubit states scatters light and the other does not when it is illuminated with a resonant laser light [12], [19]. The quantum logic gates are realized by illuminating the ion qubits with well-tailored and fully phase-coherent laser beams [Fig. 1(a)] or microwave fields. Similar to the universal gates in traditional logic, it is known that a handful of single-qubit gates and one two-qubit gate are sufficient to implement an arbitrary quantum algorithm [8]. Today trapped ion qubits show the highest gate quality among all qubit technologies, with errors in a few parts per million for single-qubit gate operations [12], and less than one part per thousand for two-qubit gate operations [10].

Besides these device-level advantages, the ion trap approach can provide a processor design with all-to-all connectivity, where two-qubit gates between arbitrary pairs of qubits can be directly implemented [Fig. 1(b)] [7]. Furthermore, communication protocols for constructing modular system architectures have been demonstrated, where multiple quantum computer units are connected to form a larger scalable system [19]. Despite the current promise, continued technical innovation is needed to expand the number of qubits in a quantum computer module, improve the quality of the logic gates among them, and realize scalable expansion using multiple modules.

III. QUANTUM ALGORITHMS

Quantum computing is perhaps most famously known for its applications that employ Shor's integer factoring [22] and Grover's database search [11] algorithms. Shor's integer factoring solves the fundamental mathematical problem of finding integer factors of an n-bit integer number by a quantum algorithm faster than the best classical algorithm known to date. The quantum computer running Shor's algorithm completes the factoring task in time polynomial in n, whereas the best classical complexity is $\exp(O(\sqrt[3]{n\log^2(n)}))$. This shows a superpolynomial advantage by the quantum algorithm. Shor's integer factoring algorithm and its generalization to finding discrete logarithm over the Abelian groups pose a threat to the widely employed Rivest–Shamir–Adleman (RSA) and elliptic-curve cryptosystems. Grover's algorithm solves the argmax problem—given an unknown Boolean function $f(\cdot)$, find an input assignment x such that $f(x)=1$—using only $O(2^{n/2})$ queries to the black box computing the function f and providing quadratic improvement over best classical strategy. Grover's algorithm can be used to solve hard instances of combinatorial problems.

In addition to Shor's and Grover's algorithms, recently, quantum simulations have also been gaining attention in the context of important applications of quantum computing. First observed by Feynman [9] and Manin [24], a quantum computer is expected to be particularly well-suited for simulating various quantum

mechanical phenomena, akin to how a classical computer is useful for simulating various classical mechanical phenomena. A host of interesting problems that are not otherwise known how to address efficiently with classical computers may be successfully solved with quantum simulations performed on a quantum computer. A few examples include, in increasing order of difficulty and impact, the following:

1) deeper understanding of many-body physics and strongly correlated matter, with possible applications in the design of room-temperature superconductors or materials with favorable electrical properties;
2) high-precision chemistry calculations for developing new catalysts and chemical processes, with important applications such as finding a replacement for the Haber process for nitrogen fixation (NF) used in the synthesis of fertilizers;
3) large-scale, highly accurate molecular dynamics simulations to study problems in protein folding and drug design.

In quantum theory, the Hamiltonian is a formula describing interactions between constituent particles in a complex quantum system, based on the energy associated with each interaction term. Tracking the actual time-dependent evolution of the system subject to these interacting Hamiltonian terms can be extremely complicated due to the exponentially growing number of possible interaction configurations among the particles. Methods for simulating Hamiltonian dynamics on a quantum computer have been developed, which take the Hamiltonian description as the input and simulate the time evolution of the system to extract a relevant quantity of interest (such as the lowest overall energy of the system and corresponding quantum state) to within the specified tolerance. Studies show that two kinds of algorithms for Hamiltonian dynamics simulation appear to be particularly promising [5]: Suzuki–Trotter formulas [2], [23] that rely on breaking down the target evolution into small pieces and expressing the individual evolution terms as quantum circuits, and an asymptotically optimal approach by Low and Chuang [16] that extends signal processing techniques to the quantum scenario.

Despite the advantage provided by quantum algorithms, simulating the Hamiltonian evolution is still a highly demanding task, as illustrated in Fig. 2 containing some of the best-known quantum computing resource estimates. To address this difficulty, a quantum/classical hybrid approach was developed, known as the variational quantum eigensolver (VQE). VQE seeks to find the lowest eigenvalues and eigenstates of a matrix H corresponding to the desired physical Hamiltonian. The approach is based on variational method, which consists of preparing a trial quantum state with some variational parameters, evaluating the energy of the state, and updating the state preparation with new variational parameters to reduce the corresponding energy. The procedure is run in an iterative fashion, guided by a classical optimization strategy, until a solution, such as the lowest energy state, is found. VQE utilizes quantum computers to prepare the trial states from the variational parameters and can dramatically simplify the portion of the simulation task run on a quantum computer. However, it must be repeated a large number of times per trial and needs to be supplied with highly optimized (and often empirical) procedures for designing and iteratively improving the trial states. VQE also runs the risk of being stuck in a local minimum. We note that VQE is a set of strategies rather than a completely specified algorithm, and the rigorous efficacy of this method for achieving a useful answer is not yet known.

Here, we highlighted some of the algorithms and approaches to solving problems on a quantum computer, but many more are known. We refer the interested reader to [13].

IV. OUTLOOK

The usefulness of a computer is measured by its ability to successfully execute desired computational tasks. In a conventional digital computer, the performance typically boils down to parameters such as the memory size, processing speed, and processor architecture, as the gate errors are generally negligible. In a quantum computer, where the logic gate operation features a nonnegligible probability of error, the performance will be constrained by both the size of the computer (measured by the number of qubits in the system, for example) and the size of quantum circuit (measured by the total number of quantum gates in the algorithm) that the system can execute before the errors accumulate to result in a meaningless outcome. Fig. 2 shows the performance space of quantum computers characterized by these two metrics. As the gate error probability is reduced for a given number of qubits, a wider class of algorithms can be executed on such a processor making it more useful. For NISQ systems, the ability to operate the two-qubit gates between a given pair of qubits within the system [connectivity described in Fig. 1(b)] makes a big difference in performance [15]; a two-qubit gate between qubits that are not directly connected has to be replaced by multiple gates allowed by the connectivity, incurring a large overhead cost in the error probability by the accumulation of gate errors. For FT quantum computers, the connectivity is largely driven by the choice of QECC and its implementation. A much lower error probability can be achieved at the logical qubit level in these systems, at the cost of the fault-tolerance overhead (in physical qubit numbers and logical-qubit level gate execution times) that depends on the choice of QECC.

The quantum computing systems available today (green colored region

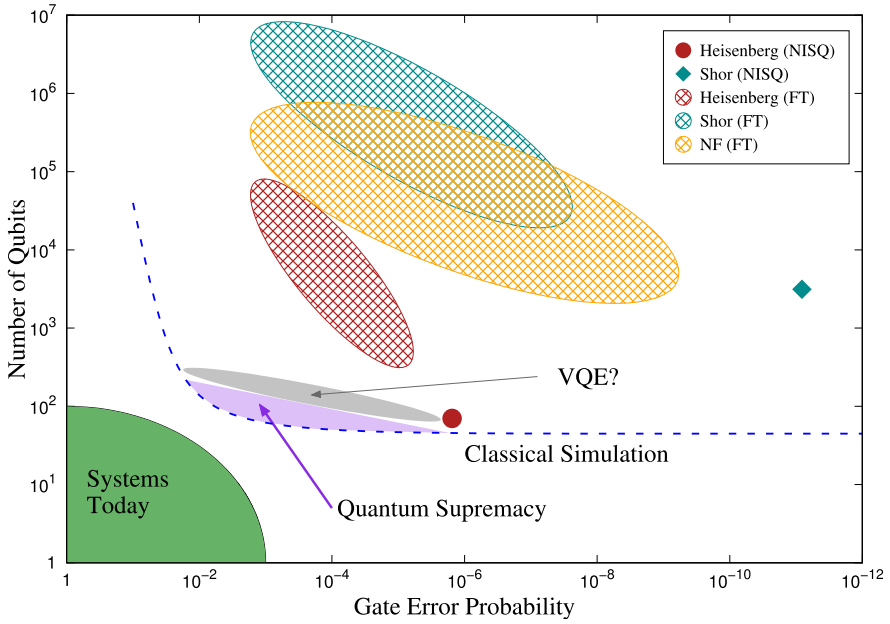

Fig. 2. ***Performance space of quantum computers, measured by the error probability of each entangling gate in the horizontal axis (roughly inversely proportional to the total number of gates that can be executed on a NISQ machine), and the number of qubits in the system in the vertical axis. Blue dotted line approximately demarcates quantum systems that can be simulated using best classical computers, while the green colored region shows where the existing quantum computing systems with verified performance numbers lie (as of September 2018). Purple shaded region indicates computational tasks that accomplish the so-called "quantum supremacy," where the computation carried out by the quantum computer defies classical simulation regardless of its usefulness. The different shapes illustrate resource counts for solving various problems, with solid symbols corresponding to the exact entangling gate counts and number of qubits in NISQ machines, and shaded regions showing approximate gate error requirements and number of qubits for an FT implementation (not pictured are the regions where the error gets too close to the known fault-tolerance thresholds): cyan diamond and shaded region correspond to factoring a 1024-bit number using Shor's algorithm [14], magenta circle and shaded region represent simulation of a 72-spin Heisenberg model [20], and orange shaded region illustrates NF simulation [21].***

in Fig. 2) are quite limited in their performance and can be simulated with classical computers (blue dashed line roughly separates classically simulable quantum computers from those impossible to simulate). A "quantum supremacy" experiment is defined to be a task that one can accomplish using a more advanced quantum computer that cannot be simulated with available classical computational resources [4], regardless of its usefulness. Although the exact boundary for quantum supremacy is currently a moving target, it is expected that the number of qubits ($\gtrsim 50$), quantum gate error probabilities ($\lesssim 10^{-3}$) and coherence times ($\gtrsim 10^3$ fold the gate times) required for such an experiment is within reach. While such a demonstration may not be sufficient to signal the practical utility of quantum computers, it proves the fundamental notion that a quantum computer capable of exploring complex quantum systems beyond classical capability is accomplished. The current trajectory of quantum computer development raises the hope that quantum supremacy can be reached in the next few years.

The next major step is to demonstrate that a quantum computer can be used to solve a problem of practical utility that cannot otherwise be addressed. This will likely start from a problem of scientific interest, such as various kinds of quantum simulations, including the dynamics of closed quantum mechanical systems useful in the understanding of many-body physics [20], or studying the structure of or interaction between complex chemical molecules [1]. It is conceivable that such demonstrations can be done before fully FT computers are constructed, which would significantly speed up the growth of utility of quantum computers and encourage further investments.

Once quantum computers are developed to such practical utility, it is highly likely that it will lead to applications of commercial viability. The development of quantum computers beyond this point could mirror the development history of classical digital computers, where the range of applications expanded as the commercial value created in early applications stimulated technology investments. Commercial quantum computers produced at this stage are envisioned to run applications including those based on Shor's and Grover's algorithms, and ultimately solving most complex and resource demanding problems such as those in drug design. Therefore, the demonstration of the practical utility of quantum computers discussed in the previous paragraph can be a trigger

point for a new industry based on quantum computers. We anticipate this point may be reached within the next decade or two.

Crucial to the development of quantum computing technology is not only continued improvements in the qubit hardware technology but also: 1) new advances in quantum computer architectures that can accommodate larger and more complex computational tasks within the available hardware; 2) developments in algorithms and methodologies that map useful problems to quantum computers; 3) the search for and narrowing down the set of practical applications (short and long term; this requires bringing in domain experts); and 4) optimization of software and hardware to boost the performance for selected applications (application-specific integrated circuit-style quantum computers). Drawing from the history of classical computers dating to the early stage in their development, it is likely that the applications of quantum computing that we can think of now and highlighted in this paper will be eclipsed by new applications found while further developing quantum computers. A growing ecosystem of quantum computer developers, users, and an educational system training necessary workforce will be critical in enabling a vibrant future quantum computing industry.

V. CONCLUSION

Now is a very exciting time when programmable quantum computational devices have been demonstrated, yet the practical utility of quantum computers has not been established. The transition of the proof-of-concept devices to useful computational systems faces a set of new technical challenges, ranging from improving and expanding qubit hardware to developing control/operating systems to innovations in algorithms and applications. Pursuing the solutions to these technical challenges defines the demand for the new generation of hardware, software, and application engineers to create and sustain the upcoming quantum computing industry. There is a major opportunity for creative minds to be a part of this future. ■

REFERENCES

[1] R. Babbush, D. W. Berry, J. R. McClean, and H. Neven. (2018). "Quantum simulation of chemistry with sublinear scaling to the continuum." [Online]. Available: https://arxiv.org/abs/1807.09802

[2] D. W. Berry, G. Ahokas, R. Cleve, and B. C. Sanders, "Efficient quantum algorithms for simulating sparse Hamiltonians," *Commun. Math. Phys.*, vol. 270, no. 2, pp. 359–371, 2007.

[3] R. Babbush *et al.*, "Encoding electronic spectra in quantum circuits with linear T complexity," *Phys. Rev. X*, vol. 8, no. 4, p. 041015, 2018.

[4] S. Boixo *et al.*, "Characterizing quantum supremacy in near-term devices," *Nature Phys.*, vol. 14, pp. 595–600, Apr. 2018.

[5] A. M. Childs, D. Maslov, Y. Nam, N. J. Ross, and Y. Su, "Toward the first quantum simulation with quantum speedup," *Proc. Nat. Acad. Sci.*, vol. 115, no. 38, pp. 9456–9461, 2018.

[6] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," *Phys. Rev. Lett.*, vol. 23, no. 15, pp. 880–884, 1969.

[7] S. Debnath, N. M. Linke, C. Figgatt, K. A. Landsman, K. Wright, and C. Monroe, "Demonstration of a small programmable quantum computer with atomic qubits," *Nature*, vol. 536, pp. 63–66, Aug. 2016.

[8] D. P. DiVincenzo, "Two-bit gates are universal for quantum computation," *Phys. Rev. A, Gen. Phys.*, vol. 51, no. 2, p. 1015, 1995.

[9] R. P. Feynman, "Simulating physics with computers," *Int. J. Theor. Phys.*, vol. 21, nos. 6–7, pp. 467–488, 1982.

[10] J. P. Gaebler *et al.*, "High-fidelity universal gate set for $^{9}Be^{+}$ ion qubits," *Phys. Rev. Lett.*, vol. 117, no. 6, p. 060505, 2016.

[11] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th STOC*, 1996, pp. 212–219.

[12] T. P. Harty *et al.*, "High-fidelity preparation, gates, memory, and readout of a trapped-ion quantum bit," *Phys. Rev. Lett.*, vol. 113, no. 22, p. 220501, 2014.

[13] S. Jordan. *Quantum Algorithm Zoo*. Accessed: Jul. 7, 2018. [Online]. Available: https://math.nist.gov/quantum/zoo/

[14] S. A. Kutin. (2006). "Shor's algorithm on a nearest-neighbor machine." [Online]. Available: https://arxiv.org/abs/quant-ph/0609001

[15] N. M. Linke *et al.*, "Experimental comparison of two quantum computing architectures," *Proc. Nat. Acad. Sci. USA*, vol. 114, no. 13, pp. 3305–3310, 2017.

[16] G. H. Low and I. L. Chuang, "Optimal Hamiltonian simulation by quantum signal processing," *Phys. Rev. Lett.*, vol. 118, no. 1, p. 010501, 2017.

[17] J. T. Merrill *et al.*, "Demonstration of integrated microscale optics in surface-electrode ion traps," *New J. Phys.*, vol. 13, p. 103005, Oct. 2011.

[18] D. L. Moehring *et al.*, "Design, fabrication and experimental demonstration of junction surface ion traps," *New J. Phys.*, vol. 13, p. 075018, Jul. 2011.

[19] C. Monroe and J. Kim, "Scaling the ion trap quantum processor," *Science*, vol. 339, no. 6124, pp. 1164–1169, 2013.

[20] Y. Nam and D. Maslov. (2018). "Low cost quantum circuits for classically intractable instances of the Hamiltonian dynamics simulation problem." [Online]. Available: https://arxiv.org/abs/1805.04645

[21] M. Reiher, N. Wiebe, K. M. Svore, D. Wecker, and M. Troyer, "Elucidating reaction mechanisms on quantum computers," *Proc. Nat. Acad. Sci. USA*, vol. 114, pp. 7555–7560, Jul. 2017.

[22] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th FOCS*, 1994, pp. 124–134.

[23] M. Suzuki, "General theory of fractal path integrals with applications to many-body theories and statistical physics," *J. Math. Phys.*, vol. 32, no. 2, pp. 400–407, 1991.

[24] Y. I. Manin, "In Vychislimoe i nevychislimoe [computable and noncomputable]," *Sov. Radiol.*, pp. 13–15, 1980.