Theory of Quantum Computing

David Shimkus
Southern Illinois University Edwardsville
April 24, 2023

***Abstract*—Quantum computing is a multi-disciplinary field with interesting ramifications regarding time and space complexity for certain problems. As transistor density reaches near atomic levels of granularity, quantum mechanics and phenomena become more relevant. By embracing these concepts instead of trying to work around them, computer scientists have entered a paradigm shift in how some problems are approached. Unfortunately, practical applications of physical systems are large, complex, fragile, and still in their infancy. Due to the fragile nature of these systems, they are susceptible to noise and error in their computations. Recent advancements in quantum error correction has made great strides in the goal of mitigating this risk. Understanding the computational theories behind these concepts and how they relate to classical computation is critical for the next generation of experiments to reach the next step towards an error-resistant algorithmic physical system.**

***Index Terms*—quantum, error, correction, introduction, theory, computation, Qiskit, simulation, IBM, Google**

I. Introduction

This report is intended to fulfill the requirement to complete a Graduate Research Final Report for Dr. Thoshitha Gamage's CS 454 Theory of Computation Class during the Spring 2023 semester (CRN 17991). While a significant focus area of research narrows to Quantum Error Correction (QEC), this document attempts to align with the requirement to provide topics "relevant" to the course material. A background and historical context is first laid in accordance with how the class progressed from less complex systems to more complex systems. As such, having the prerequisite knowledge of Non-Deterministic Finite State Automata, Push-Dow Automata, Turing Machines, and related materials gives the reader many of the tools necessary to digest the material. There exists a set of slides to go along with this report, but it makes use of much more liberal sources and diagrams. If there was more time to finalize the report, the hand-drawn diagrams and formula would have been translated into the languages, but the in-class presentation slides formatting took precedent.

A. Background

Since the times of ancient philosophers, existential questions have fallen into two categories. There are questions regarding the meaning and purpose of reality, and there are questions regarding the nature of reality. Classical physics dominated the way people perceived the world. By applying physics and logistics principles the theory of computation is born.

Modern theory of computation can trace its roots back almost 100 years ago to Alonzo Church [1]. In 1936 and 1937, Church and Alan Turing arrived at what became known as the Church-Turing Thesis which has formed the foundation of most aspects of classical computing [2], [3]. The abstract model known as a Turing machine is a mathematical concept upon which any classical algorithm has been known to be able to be implemented. Building upon concepts such as Push-Down Automata, the Turing machine concept has been exhaustively used in computer science when discussing computability, complexity, and efficiency.

Around the same time, great advancements in quantum physics were being made. In 1920's and 1930's, famous scientists such as Werner Heisenberg and Paul Dirac were building upon foundational research made in the late 1800's by Michael Faraday, Heinrich Hertz, Max Planck, and others. Radical ideas such as wave-particle duality were being raised, calling into question many long-standing beliefs.

These two disciplines continued in parallel for a time, before physicist Richard Feynman changed everything with a 1982 paper asking if quantum physics can truly be simulated via classical computation [5]. Feynman's argument was that natural physics could never be truly simulated with a traditional "universal" Turing Machine! The very nature of atomic particles are continuous and analog, and can never be fully captured in a discrete set of tape symbols without losing some level of precision. Feynman referred to this as the "hidden-variable" problem where a classical universal device simply cannot represent the results of quantum mechanics [5]. This reasoning seems to be a natural evolution of Turing's stipulation of his computing machine requiring to be operated against "finite" numbers or functions (naturally a bijection of sorts) [3]. Figure 1 below attempts to illustrate this point along a continuous function.

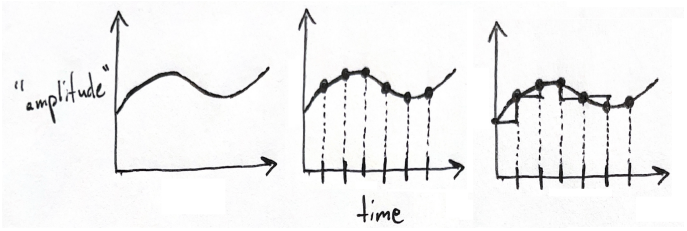

Figure 1. Differences between analog/continuous "amplitude" measurements and digital/discrete measurements. Note the loss of precision as digital (classical) measurements against the continuous function must happen at specific time intervals. The "amplitude" axis is expanded on in subsequent sections.

It was clear that to reach true quantum levels of granularity a different type of computation method was needed. What followed was an explosive growth in the field of theoretical

quantum computing. In 1982, David Deutsch produces his landmark work "Quantum theory, the Church-Turing principle and the universal quantum computer" [8]. This work goes on to expand upon inherent parallelism found in quantum computations and illuminates ways in which these ideas can impact classical complexity theory [6].

The physical quantum computers of today are still in their infancy, and might be compared to classical computers in the near decades after Church and Turing's initial works. Physical systems are discussed in greater detail in the "Physical vs. Logical Qubits" section below. Just like with classical computers, quantum computers require error detection and correction to perform computations accurately. Including QEC into automata and grammars is an ongoing area of theoretical research, and is important as input into the practical design of experimental architecture for the decades ahead.

B. Use Cases (Why Should I Care?)

Certain problems are harder to solve than others, and concepts such as time and space complexities for algorithmic solutions to problems remain an important field of study. One might have all of the hardware computing power available in any configuration they might demand, but if the user does not know how to efficiently apply it towards solving some problem(s) then there are fundamental inefficiencies or wasted resources with the overall solution. But what happens when all possible efficiencies for available resources are exhausted? It has long been speculated that humankind is reaching the spatial limits of transistor density for Moore's Law to hold through the coming decades [29]. Exploring alternative methods to reach ever further into the search for efficient solutions to problems must takes other avenues by necessity. One of such models is that of quantum computing, and to a larger extent quantum information processing (QIP).

A broad category in which quantum computing shows tremendous promise is that of combinatorics. Combinatorics is a field of study that touches mathematics, physics, philosophy, and more. It deals with finding "arrangements" or "configurations" of some listing of items that optimizes some goal(s). As more items are added to the list, then there is an exponential increase in possible arrangements. A favorite example of such a problem is the Nondeterministic-Polynomial (NP) hard problem of the Travelling Salesman. However, this particular problem shows extremely small performance gains via quantum methods when compared to classical methods [17], [30]. But there are other problems quantum computing offers performance gains over such as prime number factorization [12], machine learning [31], protein folding [27], and others. To better understand which areas benefit the most from this technology, one must take a closer look at how its results are achieved in principle and theory and once understood drive more results in practice.

II. Quantum Basics

For the purposes of this report, there is one distinctive difference emphasized between classical and quantum mechanics. While studying classical mechanics, one is primarily concerned with everyday objects and the properties thereof such as kinematics, etc. In observing objects in this frame of reference, everything exists at a specific place at a particular time. One might argue that every individual experiences reality phenomenologically differently but this is beyond the scope of this writeup. When dealing with quantum mechanics, one is concerned of how physics behaves at the sub-molecular level of things such as atoms, electrons, photons, etc. With this frame of reference, objects exist in probabilistic "superposition" of multiple places at the same time [4], [32]! At this very small level of detail, classical mechanics does not apply as one's intuition may expect and interesting behaviors begin to arise. The famous thought experiment that begins to illustrate this concept is Schrödinger's Cat, where it was argued that under the experiment's conditions the cat was in a superposition of both alive and dead simultaneously.

A. Qubits and Linear Algebra

There is no such thing as a "pure" quantum computer. All human-operable quantum computers have some element of classical computations intertwined into their architecture. Normally, classical computers input their desired data into the quantum system, coerce the quantum system to execute the desired computations, and then read out the result at the appropriate time [10]. For some instances this may be done in a looping mechanism where consistent inputs or tweaking is necessary. The theory behind how the classical system operates against the quantum system is the focus of this section. Quantum computers do not use regular classical bits that can either take a value of zero or one. Quantum computers use qubits that can be in a superposition of both zero and one simultaneously [8], [9], [32]. These qubits can be implemented in various means such as cold trapped ions [13], nuclear magnetic resonance (NMR) [18], and the more common superconducting qubits [24], [26]. One of the most common ways to illustrate the nature of a universal qubit (regardless of implementation method) is that of a Bloch Sphere [32]. Figure 2 below shows how these qubits can be shown with a type of "spin" indicating a direction, and also begins the discussion surround the Bra-Ket notation.

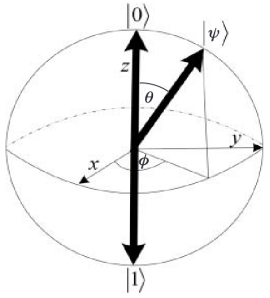

Figure 2. Showing the two formation of the two qubit 00 state by entangling two 0 qubits with a tensor product.

In Figure 2, we can see the "spin arrow" pointing along the Z-axis directly "upwards" correlating to value $|0\rangle$ which is the quantum analog for the classical zero value. Similarly, when the "spin" direction is pointing directly "down" the qubit assumes the $|1\rangle$ value which is the quantum version of a classical bit's one value [32]. Things begin to get interesting when the spin value is neither directly up or directly down, but in some superposition state somewhere between these two values. This intermediate spin can be characterized by to trigonometric angles, θ and ϕ. Through this method, it can be deduced that $0 \leq \phi < 2\pi$ and $0 \leq \theta < \pi$. Figure 3 below further illustrates the breakdown of the qubit and its Bra-Ket notation.

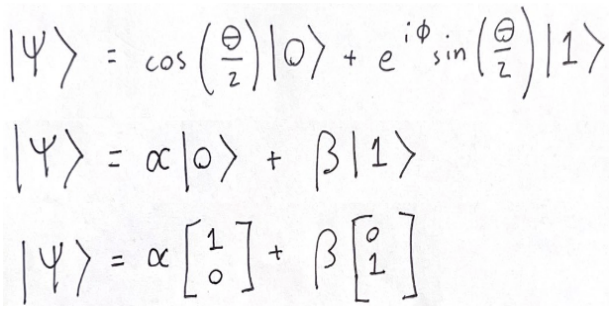

Figure 3. Various ways to represent a qubit's state. Oftentimes the unknowns of each portion are simplified to α and β parameters instead of using the trigonometric functions.

From here, we can see how the value of our qubit represented in this Bra-Ket notation and how it relates to linear algebra. The $|0\rangle$ value correlates to $\binom{1}{0}$ and the $|1\rangle$ value correlates to $\binom{0}{1}$. A helpful tip to try and remember this is the "number on the bottom" of the matrix is the qubits value, but we will soon see that this does not hold throughout all behaviors.

Similar to Schrödinger's Cat, these qubits are exhibit this behavior until they are measured, where they collapse to their $|0\rangle$ or $|1\rangle$ states! They can only be in this superposition state as they are unobserved. The probability that the qubit will collapse to $|0\rangle$ is α and $|1\rangle$ is β.

B. Quantum Entanglement

One of the largest means of "quantum speedup" this technology has stems from the tenet of entanglement. Quantum entanglement occurs when two quantum particles interact with each other in such a way that they both influence each others' "spin angle" and the measurement of one particle not only collapses itself, but the other particle as well [9], [32]. This entanglement can be represented by the tensor product of the qubits in their matrix form. Figure 4 shows a type of shorthand notation of two zero qubits "tensored" together and how the matrix multiplication works out.

Shown here is the first indication of how these quantum systems have the potential to outperform their classical counterparts. Note that with two qubits, the total number of possible states (the resulting vector) is 2^2. With three qubits the vector

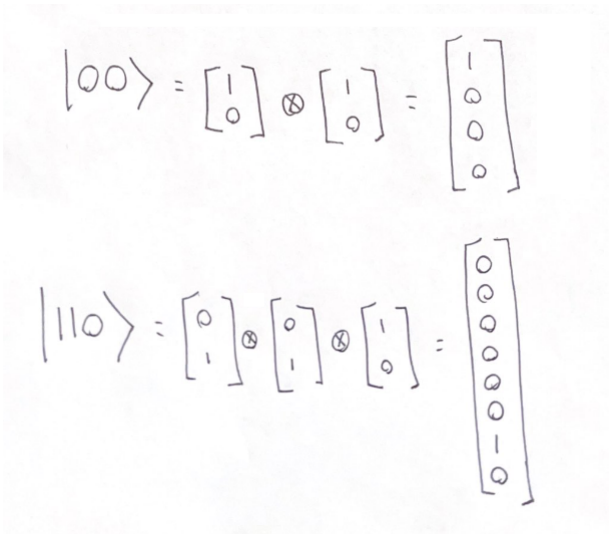

Figure 4. Two $|0\rangle$ qubits entangled with each other, and the three qubit state of $|110\rangle$.

covers 2^3 possible states. It follows that with n qubits the system has an exponential increase in its state space of 2^n! This property is explored in more detail in the next section.

III. Theory of Computation

Even with this newer technology, the scope of problems able to be solved has not changed. As mentioned previously, certain types of combinatorial problems can benefit from quantum speedup, but this does not alter their purview at all. As such, quantum computers do not solve the halting problem! One can even make a certain connection between the "measurement" aspect of the collapsing of the qubit state to a halting type operation. When exactly is the right time to measure and halt the system? There are no definitive answers to this question, only estimations and probabilities can be deduced [22].

A. Quantum Turing Machines

Before describing the nature of the Quantum Turing Machine (QTM), it is critical to understand the Unitary concept and operations against the quantum state. Unitary operations are reversible and are key components to portraying and manipulating the unobservable quantum state(s) [4], [5], [32]. Unitary matrices take the form

$$UU^{\dagger} = U^{\dagger}U = I$$

where I is the identity matrix. The state of the quantum system evolves via unitary operations. This can be thought of as taking this type of notation, where $|\psi\rangle$ is the system at time t, and $|\psi^1\rangle$ is the system at time t+1 after the unitary operation yielding $|\psi^1\rangle$ = U $|\psi\rangle$. The state of a quantum system is Ψ belonging to a "Hilbert Space" which is a complex inner product space usually denoted $\mathcal{H}$.

QTM's follow the same definition of a classical Turing Machine, with caveats in the definitions of its parameters [20].

$$M = (Q, \Sigma, \Gamma, \delta, Q_0, \square, F)$$

Where Q is the states in overall $\mathcal{H}$. Σ is the input alphabet (this can be classical!). Γ is the tape alphabet (also in $\mathcal{H}$). δ can be written as (Q - F) x δ which can be thought of as $\mathcal{H}$ transitions (i.e. via tensor products). Q_0 is the start state (the initial $\mathcal{H}$) and F is the set of final possible $\mathcal{H}$.

The more common method of representing a QTM is by Quantum Circuit Diagrams [11]. These diagrams can help illustrate the flow of the Hamiltonian of the circuit by representing the entanglements between qubits as well as imposed quantum gates. Figure 5 gives a toy example of such a circuit.

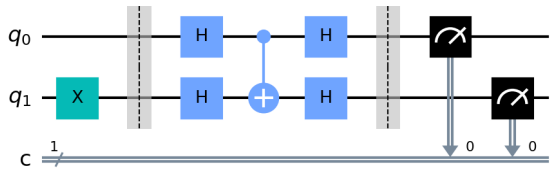

Figure 5. Two qubits entangled with each other, showing the Bit Flip X gate, the Hadamard H gate, and the measurement operation. The Hadamard gate is beyond the scope of this writeup. The c line stands for the classical register upon which the result is measured for human consumption. This diagram was generated with IBM's Python Qiskit library.

B. Inherent Parallelism

The Quantum Entanglement subsection above gives good evidence regarding the inherent quantum speedup due to the parallel nature of these qubits. A single qubit is able to have a superposition of two different states simultaneously, and n qubits can have 2^n states all at the same time.

IV. Error Detection and Correction

It was around the mid 1990's when operational scientists began to take a more serious look at the potential error in quantum systems. During this time some of the first steps were being taken to attempt to build a physical experimental system, and all sorts of questions began to arise. Quantum systems were extremely fragile, and susceptible to different types of noise and decoherence. Known for some time had been the idea of the "no-cloning theorem" which stated that any quantum bit could not be observed or measured without collapsing it into its base or excited state - thereby losing its superposition [7]. Scientists were finding that the environmental particles surrounding the system attempting to be isolated were indeed measuring the qubits in certain ways and by extension introducing unnecessary collapsing errors.

Worth noting is the more robust Steane codes that built upon the foundation laid by Shor, and lattice-based correction methods, but these are outside the scope of this review [15], [19], [21], [25].

A. Errors and Noise

There are three main types of errors that can be exhibited against a physical qubit, and they are the (1) Bit Flip, (2) Sign Flip, or (3) the Bit and Sign Flip [32]. The sign flip can also be known as a phase flip or shift [16]. Figure 5 shows how a $|0\rangle$ qubit undergoes a bit flip to a $|1\rangle$ after having a bit flip operation performed against it. The sign flip is harder to visualize as it can happen on either the α or β parts of the superposition, but a general example of a sign flip is for a $|1\rangle$ qubit to go to a $-|1\rangle$ state.

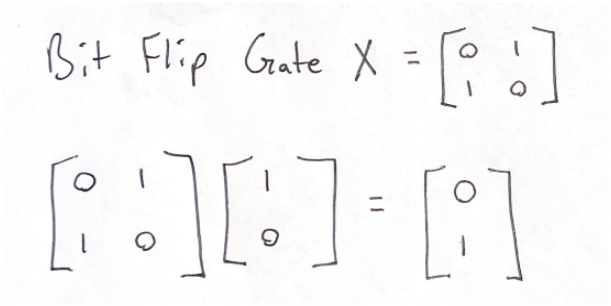

Figure 6. A bit flip gate can be used to illustrate the effects of noise inducing a bit flip onto a qubit.

Scientists set out to devise ways to account for these widely apparent errors by not only detecting them when they occurred, but to correct them. Asher Peres is the first to publish a work regarding quantum error correction (QEC) [9], but only produces an error correction code for a single type of error at first (the bit flip). Peter Shor produces the first QEC code that accounted for all the different types of errors in 1995 [11], [14] and paved the way towards fault-tolerant QEC.

B. Physical and Logical Qubits

There are different types of QEC codes used for different scenarios, but it is sufficient for this report just to understand how they are performed, and to look at the Shor nine qubit QEC. Akin to a classical parity check, scientists are able to "spread" a source qubit's spin value ($|\psi\rangle$) across multiple "ancilla" qubits [23]. After the information is spread out via entanglement, quantum logic gates are applied to the different data qubits that enforce different parts of spin integrity. As mentioned, the most common universal code is the three qubit code, which is easier to understand as there are three types of errors, therefore scaling nicely for simplicity. Again, it is not necessary to understand the fine details of this method, but to be aware that by spreading this information across multiple qubits one arrives at one can be described as a "logical" qubit made up of many different entangled physical qubits. These logical qubits in theory have fault-tolerant properties, making them highly desirable to be utilized for computations. The tradeoff is that there are spatio-temporal overheads such as additional computations needed to perform the corrections and of course the additional ancilla qubits. Figure 7 shows both a bit flip gate X and a sign flip gate Z in green, illustrating a "noisy" channel, and how the Shor Code is able to correct the

data value against qubit Q_0 using eight other entangled qubits and gate operations.

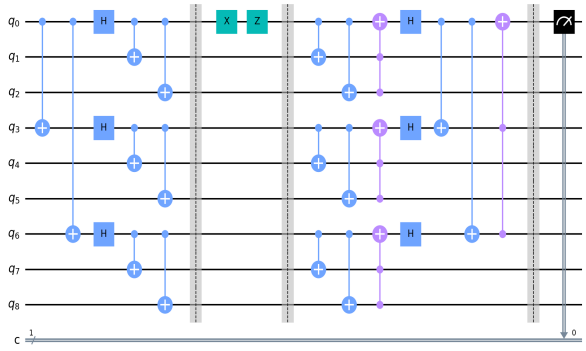

Figure 7. The first logical qubit designed with the nine qubit QEC Shor Code.

C. Experimental Results

Using the IBM provided Qiskit Python library, one is able to connect directly to IBM's cloud systems to perform quantum computations. Some of these systems use simulated quantum bits, and some of them use physical quantum bits implemented with transmon superconducting chips. Building Jupyter notebook systems on my personal home computer allowed me to run simulations and produce the diagram results listed in this report. Upon the confirmation of the program completion the output can be read and acknowledged that the Shor Code did indeed correct both types of errors introduced against the source physical qubit Q_0. Worth noting is that for the physical quantum system backends provided by IBM the queue time was multiple hours with varying degrees of results. More information and testing is needed regarding this, and some preliminary numbers are outlined in the slide presentation.

V. Limitations and Next Steps

As noted in the previous sections, physical quantum systems have a variety of limitations. At most, only systems with a couple of hundred of physical qubits exist today. Due to their fragile nature, physical qubits are required to be encoded into logical qubits via entanglement and gate operations to reliably perform meaningful computation. It is currently unclear whether or not these logical qubits can be entangled with one another in such a way that they can perform the computational basis upon which to run quantum algorithms. With physical and simulated systems advancing year after year, the future is bright for this particular area of research and will be of great importance to many industries and humankind.

Acknowledgment

Thanks are due to Southern Illinois University Edwardsville's Computer Science faculty adviser, Dr. Thoshitha Gamage for his guidance during this research.

References

[1] A. Church, "A Set of Postulates for the Foundation of Logic," The Annals of Mathematics, vol. 33, no. 2, p. 346, Apr. 1932, doi: 10.2307/1968337.

[2] A. Church, "An Unsolvable Problem of Elementary Number Theory," American Journal of Mathematics, vol. 58, no. 2, p. 345, Apr. 1936, doi: 10.2307/2371045.

[3] A. M. Turing, "On Computable Numbers, with an Application to the Entscheidungsproblem," Proceedings of the London Mathematical Society, vol. s2-42, no. 1, pp. 230–265, 1937, doi: 10.1112/plms/s2-42.1.230.

[4] C. H. Bennett, "Logical Reversibility of Computation," IBM J. Res. Dev., vol. 17, no. 6, pp. 525–532, Nov. 1973, doi: 10.1147/rd.176.0525.

[5] R. P. Feynman, "Simulating physics with computers," Int J Theor Phys, vol. 21, no. 6–7, pp. 467–488, Jun. 1982, doi: 10.1007/BF02650179.

[6] P. Benioff, "Quantum Mechanical Models of Turing Machines That Dissipate No Energy," Phys. Rev. Lett., vol. 48, no. 23, pp. 1581–1585, Jun. 1982, doi: 10.1103/PhysRevLett.48.1581.

[7] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," Nature, vol. 299, no. 5886, pp. 802–803, Oct. 1982, doi: 10.1038/299802a0.

[8] D. Deutsch, "Quantum theory, the Church–Turing principle and the universal quantum computer," Proc. R. Soc. Lond. A, vol. 400, no. 1818, pp. 97–117, Jul. 1985, doi: 10.1098/rspa.1985.0070.

[9] A. Peres, "Reversible logic and quantum computers," Phys. Rev. A, vol. 32, no. 6, pp. 3266–3276, Dec. 1985, doi: 10.1103/PhysRevA.32.3266.

[10] R. P. Feynman, "Quantum mechanical computers," Found Phys, vol. 16, no. 6, pp. 507–531, Jun. 1986, doi: 10.1007/BF01886518.

[11] A. Chi-Chih Yao, "Quantum circuit complexity," in Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science, Palo Alto, CA, USA, 1993, pp. 352–361. doi: 10.1109/SFCS.1993.366852.

[12] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in Proceedings 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 1994, pp. 124–134. doi: 10.1109/SFCS.1994.365700.

[13] J. I. Cirac and P. Zoller, "Quantum Computations with Cold Trapped Ions," Phys. Rev. Lett., vol. 74, no. 20, pp. 4091–4094, May 1995, doi: 10.1103/PhysRevLett.74.4091.

[14] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," Phys. Rev. A, vol. 52, no. 4, pp. R2493–R2496, Oct. 1995, doi: 10.1103/PhysRevA.52.R2493.

[15] A. M. Steane, "Error Correcting Codes in Quantum Theory," Phys. Rev. Lett., vol. 77, no. 5, pp. 793–797, Jul. 1996, doi: 10.1103/PhysRevLett.77.793.

[16] A. Barenco, T. A. Brun, R. Schack, and T. P. Spiller, "Effects of noise on quantum error correction algorithms," Phys. Rev. A, vol. 56, no. 2, pp. 1177–1188, Aug. 1997, doi: 10.1103/PhysRevA.56.1177.

[17] E. Bernstein and U. Vazirani, "Quantum Complexity Theory," SIAM J. Comput., vol. 26, no. 5, pp. 1411–1473, Oct. 1997, doi: 10.1137/S0097539796300921.

[18] D. G. Cory et al., "Experimental Quantum Error Correction," Phys. Rev. Lett., vol. 81, no. 10, pp. 2152–2155, Sep. 1998, doi: 10.1103/PhysRevLett.81.2152.

[19] E. Knill, R. Laflamme, and L. Viola, "Theory of Quantum Error Correction for General Noise," Phys. Rev. Lett., vol. 84, no. 11, pp. 2525–2528, Mar. 2000, doi: 10.1103/PhysRevLett.84.2525.

[20] C. Moore and J. P. Crutchfield, "Quantum automata and quantum grammars," Theoretical Computer Science, vol. 237, no. 1–2, pp. 275–306, Apr. 2000, doi: 10.1016/S0304-3975(98)00191-1.

[21] D. Kribs, R. Laflamme, and D. Poulin, "Unified and Generalized Approach to Quantum Error Correction," Phys. Rev. Lett., vol. 94, no. 18, p. 180501, May 2005, doi: 10.1103/PhysRevLett.94.180501.

[22] A. Hagar, "The Curse of the Open System," in The Complexity of Noise, Cham: Springer International Publishing, 2010, pp. 5–21. Accessed: Mar. 12, 2023. doi: /10.1007/978-3-031-02514.

[23] S. J. Devitt, W. J. Munro, and K. Nemoto, "Quantum error correction for beginners," Rep. Prog. Phys., vol. 76, no. 7, p. 076001, Jul. 2013, doi: 10.1088/0034-4885/76/7/076001.

[24] W. D. Oliver and P. B. Welander, "Materials in superconducting quantum bits," MRS Bull., vol. 38, no. 10, pp. 816–825, Oct. 2013, doi: 10.1557/mrs.2013.229.

[25] A. D. Córcoles et al., “Demonstration of a quantum error detection code using a square lattice of four superconducting qubits,” Nat Commun, vol. 6, no. 1, p. 6979, Apr. 2015, doi: 10.1038/ncomms7979.
[26] A. P. M. Place et al., “New material platform for superconducting transmon qubits with coherence times exceeding 0.3 milliseconds,” Nat Commun, vol. 12, no. 1, p. 1779, Mar. 2021, doi: 10.1038/s41467-021-22030-5.
[27] L. Luo, “Quantum theory on protein folding,” Sci. China Phys. Mech. Astron., vol. 57, no. 3, pp. 458–468, Mar. 2014, doi: 10.1007/s11433-014-5390-8.
[28] L. Zhu et al., “Adaptive quantum approximate optimization algorithm for solving combinatorial problems on a quantum computer,” Phys. Rev. Research, vol. 4, no. 3, p. 033029, Jul. 2022, doi: 10.1103/PhysRevResearch.4.033029.
[29] D. Etiemble, “Technologies and Computing Paradigms: Beyond Moore’s law?,” 2022, doi: 10.48550/ARXIV.2206.03201.
[30] S. Jain, “Solving the Traveling Salesman Problem on the D-Wave Quantum Computer,” Front. Phys., vol. 9, p. 760783, Nov. 2021, doi: 10.3389/fphy.2021.760783.
[31] I. Convy et al., “Machine learning for continuous quantum error correction on superconducting qubits,” New J. Phys., vol. 24, no. 6, p. 063019, Jun. 2022, doi: 10.1088/1367-2630/ac66f9.
[32] N. S. Yanofsky and M. A. Mannucci, Quantum computing for computer scientists. Cambridge: New York: Cambridge University Press, 2008.