QUANTUM COMPUTING

ELLIOTT ASHBY
PHYSICS AND ASTRONOMY
UNIVERSITY OF SOUTHAMPTON

Abstract. Placeholder for abstract.

Contents

Date: December 2024.

1. Introduction

Animals gain advantages in many ways, one of which is the exploitation of properties of the physical world. This has come to culmination in humans; in 1941 we saw the creation of the first programmable computer, the Z3, by Konrad Zuse, and in the following decades we have continually perfected this technology. The modern computer that we use today is, at its fundamental principals, identical to the Z3, performing binary operations on "bits" (a 1 or a 0) of data in order to encode useful computational results.

The Z3 used electromagnetic relays (600 in the arithmetic unit, 1,400 to store 64 words) and was close in size to the Stibitz BTL Model 1 or a large, floor-to-ceiling bookshelf. [1] In the decades following the Z3, the space required to store and operate computer memory has decreased significantly, and as stated by Moore in 1965, "The complexity for minimum component costs has increased at a rate of roughly a factor of two per year." [2] This has largely held true, thanks to increasingly smaller and smaller manufacturing processes.

As of 2022 the smallest transistors are of the order of 3nm, [3] but when we shrink further down to 2nm or beyond, we begin to approach the size of the atom; at this scale, quantum effects are more pronounced and the transistor can leak current due to gate direct tunnelling. [4] These effects limit the effectiveness of classical computers at this scale, and so we must look to new technologies to push the boundaries of computation.

2. An Overview of Key Concepts

2.1. A Brief History of Quantum Computing.

During the majority of the 20th century up until the early 1980s the fields of quantum mechanics and computer science were, for the most part, separate areas of study despite some crossover such as the application of the laser. But in 1980, Paul Benioff proposed a quantum mechanical model of the computer and computation process [5] and additionally, in the same year, Yuri Manin proposed a similar model. [6] In the following years, Richard Feynman wrote a paper suggesting that the use of quantum phenomena to perform computations could be more efficient for computer physics simulations than classical computers. [7]
Just 2 years following this, in 1984, Charles Bennett and Gilles Brassard continued to merge quantum mechanics and computer science by introducing quantum cryptography [8] showing that a quantum key distribution can be used to secure communications.

Following the proposal of the quantum model of computation, quantum algorithms began to be developed, including Deutsch's algorithm in 1985, [9] the Bernstein-Vazirani algorithm in 1993, [10] and Simon's algorithm in 1994. [11] Building on these papers, Peter Shor published his work on prime factorization quantum algorithms which had real world application breaking the RSA and Diffie-Hellman encryption algorithms. [12] Just 2 years later in 1996, Lov Grover published his algorithm for database search [13] and in the same year Seth Lloyd finally proved Feynman's conjecture that he proposed in 1982 that quantum computers can be

programmed to simulate any local quantum system. [14]

The first quantum computer to be built was in 1998; Isaac Chuang and Neil Gershenfeld along with Mark Kubinec implemented Grover's search algorithm with a 2-qubit (the quantum equivalent to bits) nuclear magnetic resonance (NMR) quantum computer. [15] In the years following, NMR quantum computers would increase in the number of qubits allowing for a 7-qubit quantum computer to run Shor's algorithm in 2001. [16]

Since then, quantum computing has continued to grow, with new technologies and greater numbers of qubits. The most promising of these is the superconducting circuit used as a qubit. Originally proposed in 1999 by Yasunobu Nakamura, Yuri Pashkin and Jaw-Shen Tsai, [17] and shown to be viable for greater application in 2007 by Jelle Plantenberg, P.C. de Groot, C.J.P.M. Harmans and Hans Mooij by demonstrating the controlled-NOT gate, [18] superconducting qubits have become the focus of many large companies such as IBM and Google.

As of 2024, the quantum computer with the most number of qubits is actually not a superconducting quantum computer, but an atomic array quantum computer built by Atom Computing in 2023 [19, 20] with a reported 1,180 qubits. However, since atomic array quantum computers are much newer than superconducting quantum computers, they have less general support for quantum algorithms; the largest superconducting quantum computer as of 2024 is IBM's Condor with 1121 qubits. [21, 22]

The field of quantum computing is still in it's infancy, but with promising results and continued growth, it is likely that quantum computers will become more relevant in the coming years.

2.2. Limitations of Classical Computers and the Need for Quantum Computing.

2.2.1. *Public-key Cryptography and Factorization of Big Numbers.*

In 1976, Whitfield Diffie and Martin Hellman published their paper on new directions in cryptography, [23] introducing to the general public the concept of public-key cryptography; a method of encryption that uses a pair of keys, public and private, to encrypt and decrypt messages. With the public key, one can encrypt a message that only the private key can decrypt. 2 years later in 1978, Ron Rivest, Adi Shamir and Leonard Adleman published their paper on the "RSA" algorithm, named after their initials, that provides a method for generation of the keys. [24]

The problem of breaking the RSA algorithm is one of finding the prime factors of a large integer. This is difficult to solve for classical computers; the best known algorithm, the general number field sieve (GNFS) [25] runs in sub-exponential time, with a time complexity of:

$$O\left(\exp\left[\left(\frac{64}{9}\right)^{1/3}(\log n)^{1/3}(\log\log n)^{2/3}\right]\right)$$

where n is the number to be factorized. If we were to use an n of 2^{2048}, we would yield a number of operations roughly 1.53×10^{35}. On a 5GHz CPU on a single thread, this would take 9.72×10^{17} years, a long enough time that the RSA algorithm would be considered secure.

However in 1994, Peter Shor published his quantum algorithm for prime factorization [12] now known as Shor's Algorithm. Shor suggests that a quantum computer could be able to factorize a number in polynomial time $O(\log n)$. The fastest current implementation is of $O((\log n)^2(\log \log n))$ [26, 27] yielding a number of operations 1.46×10^7. This is a significant speed up over the GNFS and implies that the RSA algorithm is no longer secure. Among security experts, security through obscurity is not considered a valid form of security, [28] and as such, the need for further research into quantum computing and quantum-resistant cryptography is clear. Shor's Algorithm is discussed further in section 2.6.4.

2.2.2. *Brute-force Search.*

Brute-force search is a method of problem solving that involves systematically generating and testing all possible solutions to a problem. That is to say, brute-force search find the single item that satisfies some condition in a unsorted database of n items. Once a single item has been examined, its ability to satisfy the condition can be determined in one step and as such, the most efficient classical algorithms may only determine the correct item in $O(n)$ time, averaging $n/2$ operations.

In 1996, Lov Grover published his quantum algorithm for database search [13] now known as Grover's Algorithm. Grover's Algorithm is able to find this single item in only $O(\sqrt{n})$ steps, and although not a polynomial time speed up, it is still a significant speed up over classical algorithms. Grover's Algorithm is possible since, quantum mechanical systems can be in a superposition of states and simultaneously evaluate the conditions for multiple items in the database.

A year later in 1997, Grover's Algorithm was shown to be asymptotically optimal by Charles Bennett, Ethan Bernstein, Gilles Brassard and Umesh Vazirani. [29] An algorithm is said to be asymptotically optimal if it, for large inputs, performs at worst a constant factor worse than the best possible algorithm. Grover's Algorithm is discussed further in section 2.6.5.

2.2.3. *Simulation of Quantum Systems.*

REDO—

Can physics be simulated on a classical computer? In 1982, Richard Feynman states that it is certainly not possible to simulate quantum systems on a classical computer without infinite time. [7]

If we wish to simulate a single particle, ψ as a function of x and t, it's probability density can be determined classically using numerical methods. [30] However, if we wish to simulate n particles, the new state of the system is given by some function $\Psi(x_1, x_2, \ldots, x_n, t)$. Describing all of these states would require a k-digit number for every configuration of the system, for every arrangement of the n values of x. Then, if there are N points in space and each point in space has it's own information such as electric fields, n is of order N, so there would be N^N configurations. Since

there are too many variables, it cannot be simulated with a classical computer with a number of elements proportional to N. That is to say, computing this classically would require to discretize x and t to make any results exact. To do this requires the discarding of terms that are too small, for example, if we choose to only take k digits of precision, we must discard probabilities that are less than 2^{-k}. This is not a problem for a small number of particles, but as the number of particles increases to n, the more terms we discard, no matter their validity.

Feynman presents that descretizing presents some problems, for example taking the electric field at some point below a certain amount, would in turn suggest that it is not there at all. This is not the case, we know it to be quantized. By descretizing, we are not simulating the correct equations.

This leaves only one option, to simulate quantum systems on a quantum computer. Feynman's conjecture was backed up by Seth Lloyd later in 1996 [14] stating that a mere 30 or 40 qubits would be enough to simulate a quantum simulations of multidimensional fermionic systems like the Hubbard model that prove resistant to conventional computers.

—

2.3. Quantum Bits and Parallelism.

The bit is the smallest building block of information of classical information. Similarly, the qunatum bit or qubit is the equivalent for quantum information theory. [31] While the qubit can be represented by physical systems such as photons, electrons or atoms, for now we will consider the qubit as a abstract concept.

While a classical bit has a state of either 0 or 1, qubits similarly have a state of $|0\rangle$ or $|1\rangle$ which correspond to the classical states respectively. There is one key difference however, instead of being exclusively in one state or the other, a qubit can also be in a linear combination of states. That is to say, a qubit can be represented as:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{2.1}$$

where α and β are complex numbers and $|\alpha|^2 + |\beta|^2 = 1$. These states however, are not observable, to retrieve information from a qubit, it must be measured. Doing so we get either 0, with a probability of $|\alpha|^2$, or 1, with a probability of $|\beta|^2$. An example of this could be for a qubit to be in the following states:

$$|+\rangle = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle \tag{2.2}$$

$$|-\rangle = \frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle \tag{2.3}$$

which we have defined as $|+\rangle$ and $|-\rangle$.

2.4. Quantum Superposition and Entanglement.

2.5. The Thermodynamics of Quantum Computing.

2.6. Quantum Algorithms.

2.6.1. *Deutsch's Algorithm.*

2.6.2. *Bernstein-Vazirani Algorithm.*

2.6.3. *Simon's Algorithm.*

2.6.4. *Shor's Algorithm.*

The RSA algorithm uses 3 large positive integers, e, d and n, where n is the product of 2 large prime numbers, p and q, and for all integers $m(0 \leq m < n)$, both $(m^e)^d$ and m have the same remainder when divided by n. That is to say:

$$(m^e)^d \equiv m \mod n \tag{2.4}$$

where n and e make up the public key, d is the private key, and m is the message. We can then define the encryption and decryption as follows:

$$c \equiv m^e \mod n \tag{2.5}$$

$$m \equiv c^d \mod n \tag{2.6}$$

where c is the cipher text.

The RSA algorithm is said to be secure because breaking it requires recovering m such that (2.5) is true. To do this requires the factorization of n into its prime factors, hence allowing the calculation of d from e and the prime factors of n.

2.6.5. *Grover's Algorithm.*

2.7. Quantum Error Correction.

2.8. Experimental Quantum Computing.

References

[1] Weiss, E.: Konrad Zuse Obituary. In: *IEEE Annals of the History of Computing* 18 (1996), Nr. 2, S. 3–. http://dx.doi.org/10.1109/MAHC.1996.489747. – DOI 10.1109/MAHC.1996.489747

[2] Moore, Gordon E.: Cramming more components onto integrated circuits, Reprinted from Electronics, volume 38, number 8, April 19, 1965, pp.114 ff. In: *IEEE Solid-State Circuits Society Newsletter* 11 (2006), Nr. 3, S. 33–35. http://dx.doi.org/10.1109/N-SSC.2006.4785860. – DOI 10.1109/N–SSC.2006.4785860

[3] Samsung: *Samsung begins chip production using 3NM Process Technology with GAA Architecture.* https://news.samsung.com/global/samsung-begins-chip-production-using-3nm-process-technology-with-gaa-architecture. Version: Jun 2022

[4] Yang, N. ; Henson, W.K. ; Wortman, J.J.: A comparative study of gate direct tunneling and drain leakage currents in n-MOSFET's with sub-2 nm gate oxides. In: *IEEE Transactions on Electron Devices* 47 (2000), Nr. 8, S. 1636–1644. http://dx.doi.org/10.1109/16.853042. – DOI 10.1109/16.853042

[5] Benioff, P.: The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. In: *Journal of Statistical Physics* 22 (1980), Nr. 5, S. 563–591. http://dx.doi.org/10.1007/BF01011339. – DOI 10.1007/BF01011339

[6] Manin, Yu. I.: Vychislimoe i nevychislimoe. In: *Sovetskoe Radio* (1980), S. 13–15

[7] Feynman, R. P.: Simulating physics with computers. In: *International Journal of Theoretical Physics* 21 (1982), Nr. 6/7, 467-488. http://dx.doi.org/10.1007/BF02650179. – DOI 10.1007/BF02650179

[8] Bennett, Charles H. ; Brassard, Gilles: Quantum cryptography: Public key distribution and coin tossing. In: *Theoretical Computer Science* 560 (2014), Dezember, 7–11. http://dx.doi.org/10.1016/j.tcs.2014.05.025. – DOI 10.1016/j.tcs.2014.05.025. – ISSN 0304–3975

[9] Deutsch, David: Quantum theory, the Church-Turing principle and the universal quantum computer. In: *Proceedings of the Royal Society of London* A400 (1985), Nr. 1818, 97-117. http://dx.doi.org/10.1098/rspa.1985.0070. – DOI 10.1098/rspa.1985.0070

[10] Bernstein, Ethan ; Vazirani, Umesh: Quantum complexity theory. (1993), 11–20. http://dx.doi.org/10.1145/167088.167097. – DOI 10.1145/167088.167097. ISBN 0897915917

[11] Simon, D.R.: On the power of quantum computation. (1994), 116-123. http://dx.doi.org/10.1109/SFCS.1994.365701. – DOI 10.1109/SFCS.1994.365701

[12] Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. (1994), 124-134. http://dx.doi.org/10.1109/SFCS.1994.365700. – DOI 10.1109/SFCS.1994.365700

[13] Grover, Lov K.: A fast quantum mechanical algorithm for database search. (1996). http://dx.doi.org/10.48550/arXiv.quant-ph/9605043. – DOI 10.48550/arXiv.quant–ph/9605043

[14] Lloyd, Seth: Universal Quantum Simulators. In: *Science* 273 (1996), Nr. 5278, 1073-1078. http://dx.doi.org/10.1126/science.273.5278.1073. – DOI 10.1126/science.273.5278.1073

[15] Chuang, Isaac L. ; Gershenfeld, Neil ; Kubinec, Mark: Experimental Implementation of Fast Quantum Searching. In: *Phys. Rev. Lett.* 80 (1998), Apr, 3408–3411. http://dx.doi.org/10.1103/PhysRevLett.80.3408. – DOI 10.1103/PhysRevLett.80.3408

[16] Vandersypen, Lieven M. K. ; Steffen, Matthias ; Breyta, Gregory ; Yannoni, Costantino S. ; Sherwood, Mark H. ; Chuang, Isaac L.: Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. In: *Nature* 414 (2001), Dezember, Nr. 6866, 883–887. http://dx.doi.org/10.1038/414883a. – DOI 10.1038/414883a. – ISSN 1476–4687

[17] Nakamura, Y. ; Pashkin, Yu. A. ; Tsai, J. S.: Coherent control of macroscopic quantum states in a single-Cooper-pair box. In: *Nature* 398 (1999), Apr, 786-788. http://dx.doi.org/10.1038/19718. – DOI 10.1038/19718

[18] Plantenberg, J. H. ; Groot, P. C. ; Harmans, C. J. P. M. ; Mooij, J. E.: Demonstration of controlled-NOT quantum gates on a pair of superconducting quantum bits. In: *Nature* 447 (2007), Jun, 836-839. http://dx.doi.org/10.1038/nature05896. – DOI 10.1038/nature05896

[19] AtomComputing: *Quantum startup Atom Computing first to exceed 1,000 qubits*. https://atom-computing.com/quantum-startup-atom-computing-first-to-exceed-1000-qubits/. Version: Oct 2023

[20] Norcia, M. A. ; Kim, H. ; Cairncross, W. B. ; Stone, M. ; Ryou, A. ; Jaffe, M. ; Brown, M. O. ; Barnes, K. ; Battaglino, P. ; Bohdanowicz, T. C. ; Brown, A. ; Cassella, K. ; Chen, C.-A. ; Coxe, R. ; Crow, D. ; Epstein, J. ; Griger, C. ; Halperin, E. ; Hummel, F. ; Jones, A. M. W. ; Kindem, J. M. ; King, J. ; Kotru, K. ; Lauigan, J. ; Li, M. ; Lu, M. ; Megidish, E. ; Marjanovic, J. ; McDonald, M. ; Mittiga, T. ; Muniz, J. A. ; Narayanaswami, S. ; Nishiguchi, C. ; Paule, T. ; Pawlak, K. A. ; Peng, L. S. ; Pudenz, K. L. ; Rodríguez Pérez, D. ; Smull, A. ; Stack, D. ; Urbanek, M. ; Veerdonk, R. J. M. d. ; Vendeiro, Z. ; Wadleigh, L. ; Wilkason, T. ; Wu, T.-Y. ; Xie, X. ; Zalys-Geller, E. ; Zhang, X. ; Bloom, B. J.: Iterative Assembly of ^{171}Yb Atom Arrays with Cavity-Enhanced Optical Lattices. In: *PRX Quantum* 5 (2024), Jul, 030316. http://dx.doi.org/10.1103/PRXQuantum.5.030316. – DOI 10.1103/PRXQuantum.5.030316

[21] IBM: *The hardware and software for the era of quantum utility is here*. https://www.ibm.com/quantum/blog/quantum-roadmap-2033. Version: Dec 2023

[22] AbuGhanem, M.: *IBM Quantum Computers: Evolution, Performance, and Future Directions*. https://arxiv.org/abs/2410.00916. Version: 2024

[23] Diffie, W. ; Hellman, M.: New directions in cryptography. In: *IEEE Transactions on Information Theory* 22 (1976), Nr. 6, S. 644–654. http://dx.doi.org/10.1109/TIT.1976.1055638. – DOI 10.1109/TIT.1976.1055638

[24] Rivest, R. L. ; Shamir, A. ; Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. In: *Commun. ACM* 21 (1978), Februar, Nr. 2, 120–126. http://dx.doi.org/10.1145/359340.359342. – DOI 10.1145/359340.359342. – ISSN 0001–0782

[25] Briggs, M. E.: An Introduction to the General Number Field Sieve. (1998). https://personal.math.vt.edu/brown/doc/briggs_gnfs_thesis.pdf

[26] Beckman, David ; Chari, Amalavoyal N. ; Devabhaktuni, Srikrishna ; Preskill, John: Efficient networks for quantum factoring. In: *Phys. Rev. A* 54 (1996), Aug, 1034–1063. http://dx.doi.org/10.1103/PhysRevA.54.1034. – DOI 10.1103/PhysRevA.54.1034

[27] Harvey, David ; Hoeven, Joris van d.: Integer multiplication in time $O(n\log n)$. In: *Annals of Mathematics* 193 (2021), Nr. 2, 563 – 617. http://dx.doi.org/10.4007/annals.2021.193.2.4. – DOI 10.4007/annals.2021.193.2.4

[28] Scarfone, K. ; Jansen, W. ; Tracy, M.: Guide to General Server Security. In: *NIST Special Publication* 800-123 (2008). http://dx.doi.org/10.6028/NIST.SP.800-123. – DOI 10.6028/NIST.SP.800–123

[29] Bennett, Charles H. ; Bernstein, Ethan ; Brassard, Gilles ; Vazirani, Umesh: Strengths and Weaknesses of Quantum Computing. In: *SIAM Journal on Computing* 26 (1997), Nr. 5, 1510-1523. http://dx.doi.org/10.1137/S0097539796300933. – DOI 10.1137/S0097539796300933

[30] Schrödinger, E.: An Undulatory Theory of the Mechanics of Atoms and Molecules. In: *Phys. Rev.* 28 (1926), Dec, 1049–1070. http://dx.doi.org/10.1103/PhysRev.28.1049. – DOI 10.1103/PhysRev.28.1049

[31] Aaronson, Scott: *Quantum Computing since Democritus*. Cambridge University Press, 2013. – 132 S. https://doi.org/10.1017/CBO9780511976667