Historical Bibliography of Quantum Computing*

Jill Cirasella
Brooklyn College Library
cirasella@brooklyn.cuny.edu

This bibliographic essay reviews seminal papers in quantum computing. Although quantum computing is a young science, its researchers have already published thousands of noteworthy articles, far too many to list here. Therefore, this appendix is not a comprehensive chronicle of the emergence and evolution of the field but rather a guided tour of some of the papers that spurred, formalized, and furthered its study.

Quantum computing draws on advanced ideas from computer science, physics, and mathematics, and most major papers were written by researchers conversant in all three fields. Nevertheless, all the articles described in this appendix can be appreciated by computer scientists.

Reading Scientific Articles

Do not be deterred if an article seems impenetrable. Keep in mind that professors and professionals also struggle to understand these articles, and take comfort in this epigram usually attributed to the great physicist Richard Feynman: "If you think you understand quantum mechanics, you don't understand quantum mechanics."

Some articles are difficult to understand not only because quantum theory is devilishly elusive but also because scientific writing can be opaque. Fortunately, there are techniques for tackling scientific articles, beginning with these preliminary steps:

- **Read the title.** It may contain clues about the article's purpose or findings.

- **Read the abstract.** It summarizes the article and will help you recognize important points when you read them.
- **Read the introduction and conclusion.** Usually in plain language, the introduction and conclusion will help you decode the rest of the article.
- **Skim the article.** Skim to get a sense of the article's structure, which will help you stay oriented while you read.

Once you understand an article's purpose and structure, you are ready to read the full article. To maximize comprehension and minimize frustration, follow these tips:

- **Read actively.** Take notes while you read. Underline key phrases; mark important passages; record important points; sketch arguments and proofs; and reproduce calculations. (Of course, don't write on anything owned by a library; make copies instead.)
- **Don't dwell.** Skim or skip difficult parts and return to them later. They might make more sense after you have read subsequent sections.
- **Consult the bibliography.** If something confuses you, one of the cited articles might explain it better or provide helpful background information.
- **Read the article multiple times.** You'll understand more with each pass.
- **Know when to stop.** Don't obsess over an article. At some point, you will have gotten as much as you are going to get (for the time being). Some or even most of the article might still elude you; nevertheless, you will know more after reading the article than you did before you started, and you will then be better equipped to read other articles.
- **Talk about the article.** Mull over the article with other students, and ask your professor if you need help. After you have finished the article, keep talking about it. Explain it to your class, to your study group, or even to someone unfamiliar with the field. After all, the best way to learn something is to teach it to someone else!

Models of Computation

Richard Feynman was the first to suggest, in a talk in 1981, that quantum-mechanical systems might be more powerful than classical computers. In this lecture, reproduced in the *International Journal of Theoretical Physics* in 1982 [18], Feynman asked what kind of computer could simulate physics and then argued that only a quantum computer could simulate quantum physics efficiently. He focused on quantum physics rather than classical physics because, as he colorfully put it, "nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy" (p. 486).

Around the same time, in "Quantum mechanical models of Turing machines that dissipate no energy" [3] and related articles, Paul Benioff demonstrated that quantum-mechanical systems could model Turing machines. In other words, he proved that quantum computation is at least as powerful as classical computation. But is quantum computation *more* powerful than classical computation?

David Deutsch explored this question and more in his 1985 paper "Quantum theory, the Church–Turing principle and the universal quantum computer" [14]. First, he introduced quantum counterparts to both the Turing machine and the universal Turing machine. He then demonstrated that the universal quantum computer can do things that the universal Turing machine cannot, including generate genuinely random numbers, perform some parallel calculations in a single register, and perfectly simulate physical systems with finite-dimensional state spaces.

In 1989, in "Quantum computational networks" [15], Deutsch described a second model for quantum computation: quantum circuits. He demonstrated that quantum gates can be combined to achieve quantum computation in the same way that Boolean gates can be combined to achieve classical computation. He then showed that quantum circuits can compute anything that the universal quantum computer can compute, and vice versa.

Andrew Chi-Chih Yao picked up where Deutsch left off and addressed the complexity of quantum computation in his 1993 paper "Quantum circuit complexity" [35]. Specifically, he showed that any function that can be computed in polynomial time by a quantum Turing machine can also be computed by a quantum circuit of polynomial size. This finding allowed researchers to focus on quantum circuits, which are easier than quantum Turing machines

to design and analyze.

Also in 1993, Ethan Bernstein and Umesh Vazirani presented "Quantum complexity theory" [6], in which they described a universal quantum Turing machine that can efficiently simulate any quantum Turing machine. (As with so many quantum articles, the final version of the paper did not appear until several years later, in the *SIAM Journal of Computing* [7].) As its title suggests, Bernstein and Vazirani's paper kick-started the study of quantum complexity theory.

Quantum Gates

In 1995, a cluster of articles examined which sets of quantum gates are adequate for quantum computation—that is, which sets of gates are sufficient for creating any given quantum circuit. Of these papers, the one that was cited the most in later works was "Elementary gates for quantum computation" [1], in which Adriano Barenco et al. showed that any quantum circuit can be constructed using nothing more than quantum gates on one qubit and controlled exclusive-OR gates on two qubits. Though that paper was arguably the most influential, other articles were important as well, including "Two-bit gates are universal for quantum computation" [17], in which David DiVincenzo proved that two-qubit quantum gates are adequate; "Conditional quantum dynamics and logic gates" [2], in which Adriano Barenco, David Deutsch, and Artur Ekert showed that quantum controlled-NOT gates and one-qubit gates are together adequate; and "Almost any quantum logic gate is universal" [22], in which Seth Lloyd showed that almost any quantum gate with two or more inputs is universal (i.e., by itself adequate).

Quantum Algorithms and Implementations

In 1992, David Deutsch and Richard Jozsa coauthored "Rapid solution of problems by quantum computation" [16], in which they presented an algorithm that determines whether a function f is constant over all inputs (i.e., either equal to 1 for all x or equal to 0 for all x) or balanced (i.e., equal to 1 for half of the values of x and equal to 0 for the other half). The Deutsch-Jozsa algorithm was the first quantum algorithm to run faster than its classical counterparts. So, even though the problem is somewhat contrived, the algorithm is notable and the article is worth reading. Also worth reading is "Experimental realization

of a quantum algorithm" [13], in which Isaac L. Chuang et al. detailed how they used bulk nuclear magnetic resonance techniques to implement a simplified version of the Deutsch-Jozsa algorithm.

In "Quantum complexity theory" [6] (also mentioned before), Bernstein and Vazirani were the first to identify a problem that can be solved in polynomial time by a quantum algorithm but requires superpolynomial time classically. The following year, Daniel R. Simon introduced a problem that a quantum algorithm can solve *exponentially* faster than any known classical algorithm. His research inspired Peter W. Shor, who then invented two quantum algorithms that outshone all others: polynomial-time algorithms for finding prime factors and discrete logarithms, problems widely believed to require exponential time on classical computers. Simon and Shor both presented their discoveries at the 1994 IEEE Symposium on the Foundations of Computer Science (in "On the power of quantum computation" [30] and "Algorithms for quantum computation: Discrete logarithms and factoring" [26], respectively) and published the final versions of their papers in a special quantum-themed issue of *SIAM Journal of Computing* ([31] and [28], respectively).

Shor's factorization algorithm in particular heightened excitement and even generated anxiety about the power and promise of quantum computing. Specifically, the algorithm caused a furor because it threatened the security of information encrypted according to the widely used cryptosystem developed by Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. RSA cryptography, as it is known, relies on the presumed difficulty of factoring large numbers, a problem that is not known to require exponential time but for which no classical polynomial-time algorithm exists. Rivest, Shamir, and Adleman described the cryptosystem in 1978 in "A method for obtaining digital signatures and public-key cryptosystems" [23], an article that is brief, elegant, and still very relevant to anyone interested in Shor's algorithm, cryptography, or complexity theory.

Of course, to pose a practical threat to RSA cryptography, Shor's algorithm must be implemented on quantum computers that can hold and manipulate large numbers, and these do not exist yet. That said, Isaac L. Chuang and his research team made headlines when they factored the number 15 on a quantum computer with seven qubits. Their 2001 précis of their accomplishment, "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance" [33], is a well-illustrated reminder of just how astonishing Shor's algorithm is.

Another highly influential quantum algorithm is Lov K. Grover's algorithm for searching an unordered list, described in both "A fast quantum mechanical algorithm for database search" [19] and "Quantum mechanics helps in searching for a needle in a haystack" [20]. Unlike Shor's algorithm, Grover's algorithm solves a problem for which there are polynomial-time classical algorithms; however, Grover's algorithm does it quadratically faster than classical algorithms can. With Grover's algorithm, as with the algorithms mentioned earlier, Isaac L. Chuang was at the experimental fore; in 1998, he, Neil Gershenfeld, and Mark Kubinec reported on the first implementation of Grover's algorithm in "Experimental implementation of fast quantum searching" [12].

There are of course more quantum algorithms than those discussed earlier. However, there are far fewer than researchers had hoped there would be by now, and research in quantum algorithms has not kept pace with research in other aspects of quantum computing and quantum information. In 2003, Peter W. Shor addressed this stagnation in a short article called "Why haven't more quantum algorithms been found?" [29]. Although unsure of the answer to that question, Shor offered several possible explanations, including the possibility that computer scientists have not yet developed intuitions for quantum behavior. The article should be required reading for all computer science students, whose intuitions are still being formed.

Quantum Cryptography

As mentioned before, Shor's factorization algorithm has yet to be implemented on more than a few qubits. But if the efficient factorization of large numbers becomes possible, RSA cryptography will need to be replaced by a new form of cryptography, one that will not be foiled by classical or quantum computers. Conveniently, such a method already exists; in fact, it was developed before Shor invented his factorization algorithm. Coincidentally, it too relies on quantum mechanics.

The cryptographic method in question is quantum key distribution, which was introduced in 1984 by Charles H. Bennett and Gilles Brassard in "Quantum cryptography: Public key distribution and coin tossing" [4] and is thus commonly referred to as BB84. In short, quantum key distribution is secure not because messages are encrypted in some difficult-to-decrypt way but rather because eavesdroppers cannot intercept messages undetected, regardless of computational resources.

Although quantum key distribution is the most famous cryptographic application of quantum mechanics, it is not the only one, and it was not the first. In the 1960s, Stephen Wiesner conceived of two applications: a way to send two messages, only one of which can be read, and a way to design money that cannot be counterfeited. His ideas were largely unknown until 1983, when he described them in an article called "Conjugate coding" [34].

Needless to say, the papers mentioned earlier were not the only milestones in the development of quantum cryptography. Curious readers should consult these two installments of *SIGACT News*' "Cryptology column": "Quantum cryptography: A bibliography" by Gilles Brassard [9] and "25 years of quantum cryptography" by Gilles Brassard and Claude Crépeau [10]. Since the publication of those articles, quantum cryptography has matured from theory and experiments to commercially available products; developments are frequently announced by manufacturers such as MagiQ Technologies (http://www.magiqtech.com/), id Quantique (http://www.idquantique.com/), and Smart Quantum (http://www.smartquantum.com/).

Quantum Information

Secure channels of communication are of course crucial, but security is not the only consideration in the transfer of information. Accordingly, quantum cryptography is just one of several topics in the burgeoning field of quantum information. Other topics include quantum error correction, fault-tolerant quantum computation, quantum data compression, and quantum teleportation.

Information needs to be protected not just from eavesdroppers but also from errors caused by channel noise, implementation flaws, and, in the quantum case, decoherence. Peter W. Shor, a trailblazer not just of quantum algorithms but also of quantum error correction and fault-tolerant quantum computation, was the first to describe a quantum error-correcting method. In his 1995 article "Scheme for reducing decoherence in quantum computer memory" [27], he demonstrated that encoding each qubit of information into nine qubits could provide some protection against decoherence. At almost the same time but without knowledge of Shor's article, Andrew M. Steane wrote "Error correcting codes in quantum theory" [32], which achieved similar results. Very shortly thereafter, Shor and A.R. Calderbank presented improved results in "Good quantum error-correcting codes exist" [11]. In the late 1990s, when research on quantum error correction and fault-tolerant

quantum computation ballooned, Shor, Steane, and Calderbank remained among the major contributors.

Error is not the only thing information theorists strive to reduce; they also seek to reduce the space required to represent information. The landmark paper on the classical representation and compression of data was "A mathematical theory of communication" by Claude E. Shannon [25], the "father" of information theory. In this 1948 paper, Shannon showed that it is possible, up to a certain limit, to compress data without loss of information; beyond that limit, some information is necessarily lost. (Seminal in so many ways, this paper also laid the groundwork for classical error-correcting codes.)

Almost 50 years later, Benjamin Schumacher developed a quantum version of Shannon's theorem. Schumacher first described his finding in an article called "Quantum coding," which he submitted to *Physical Review A* in 1993 but which was not published until 1995 [24]. In the (unfortunate but not uncommon) lag between submission and publication, he and Richard Jozsa published "A new proof of the quantum noiseless coding theorem" [21], which offered a simpler proof than the original article.

Not everything in quantum information theory has a precedent in classical information theory. In 1993, Charles H. Bennett et al. dazzled the scientific community and delighted science fiction fans by showing that quantum teleportation is theoretically possible. In "Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen Channels" [5], they described how an unknown quantum state could be disassembled and then reconstructed perfectly in another location. The first researchers to verify this method of teleportation experimentally were Dik Bouwmeester et al., who reported their achievement in 1997 in "Experimental quantum teleportation" [8].

More Milestones?

Quantum computing continues to entice and engross researchers, who will no doubt continue to ask challenging questions, discover inventive and elegant solutions, identify stumbling blocks, and achieve experimental triumphs. To learn how to apprise yourself of developments, consult Appendix D, "Keeping abreast of quantum news: Quantum computing on the Web and in the literature."

References

[1] A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P.W. Shor, T. Sleator, J.A. Smolin, and H. Weinfurter. Elementary gates for quantum computation. *Physical Review A*, 52(5):3457–3467, 1995.

[2] A. Barenco, D. Deutsch, A. Ekert, and R. Jozsa. Conditional quantum dynamics and logic gates. *Physical Review Letters*, 74(20):4083–4086, 1995.

[3] P. Benioff. Quantum mechanical models of Turing machines that dissipate no energy. *Physical Review Letters*, 48(23):1581–1585, 1982.

[4] C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179, Bangalore, India, December 1984.

[5] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W.K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels. *Physical Review Letters*, 70(13):1895–1899, March 1993.

[6] E. Bernstein and U. Vazirani. Quantum complexity theory. In *STOC '93: Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing*, pages 11–20, 1993.

[7] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM Journal on Computing*, 26(5):1411–1473, 1997.

[8] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger. Experimental quantum teleportation. *Nature*, 390:575–579, 1997.

[9] G. Brassard. Cryptology column – quantum cryptography: A bibliography. *SIGACT News*, 24(3):16–20, 1993.

[10] G. Brassard and C. Crépeau. Cryptology column – 25 years of quantum cryptography. *SIGACT News*, 27 (3):13–24, 1993.

[11] A.R. Calderbank and P.W. Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54(2):1098–1105, 1996.

[12] I.L. Chuang, N. Gershenfeld, and M. Kubinec. Experimental implementation of fast quantum searching. *Physical Review Letters*, 80(15):3408–3411, 1998.

[13] I.L. Chuang, L.M.K. Vandersypen, X. Zhou, D.W. Leung, and S. Lloyd. Experimental realization of a quantum algorithm. *Nature*, 393:143–146, 1998.

[14] D. Deutsch. Quantum theory, the Church–Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London, Series A*, 400(1818):97–117, 1985.

[15] D. Deutsch. Quantum computational networks. *Proceedings of the Royal Society of London, Series A*, 425(1868):73–90, 1989.

[16] D. Deutsch and R. Jozsa. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London, Series A*, 439(1907):553–558, 1992.

[17] D.P. DiVincenzo. Two-bit gates are universal for quantum computation. *Physical Review A*, 51(2):1015–1022, 1995.

[18] R.P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6/7):467–488, 1982.

[19] L.K. Grover. A fast quantum mechanical algorithm for database search. In *STOC '96: Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, pages 212–219, 1996.

[20] L.K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Physical Review Letters*, 79(2):325–328, 1997.

[21] R. Jozsa and B. Schumacher. A new proof of the quantum noiseless coding theorem. *Journal of Modern Optics*, 41(12):2343–2349, 1994.

[22] S. Lloyd. Almost any quantum logic gate is universal. *Physical Review Letters*, 75(2):346–349, 1995.

[23] R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[24] B. Schumacher. Quantum coding. *Physical Review A*, 51(4):2738–2747, 1995.

[25] C.E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 623–656, 1948.

[26] P.W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual IEEE Symposium on the Foundations of Computer Science*, pages 124–134, 1994.

[27] P.W. Shor. Scheme for reducing decoherence in quantum computer memory. *Physical Review A*, 52(4):R2493–R2496, 1995.

[28] P.W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[29] P.W. Shor. Why haven't more quantum algorithms been found? *Journal of the ACM*, 50(1):87–90, 2003.

[30] D.R. Simon. On the power of quantum computation. In *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science*, pages 116–123, 1994.

[31] D.R. Simon. On the power of quantum computation. *SIAM Journal on Computing*, 26(5):1474–1483, 1997.

[32] A.M. Steane. Error correcting codes in quantum theory. *Physical Review Letters*, 77(5):793–797, 1996.

[33] L.M.K. Vandersypen, G. Breyta, M. Steffen, C.S. Yannoni, M.H. Sherwood, and I.L. Chuang. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature*, 414(6866):883–887, 2001.

[34] S. Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983.

[35] A.C-C. Yao. Quantum circuit complexity. In *Proceedings of 34th Annual IEEE Symposium on Foundations of Computer Science*, pages 352–361, 1993.