A Computer Science approach to elementary Quantum Computing

Arihant Chawla, Deeskshant Hooda, Teekshan Mahajan

Contents

The answer to [why computer science is not a branch of physics departments] isn’t philosophical, it’s historical. Computer scientists back in the day were either mathematicians or electrical engineers. People who would have been computer scientists when there wasn’t such a department went into either math or EE. Physics had its plate full with other things, and to get into physics you had to learn this enormous amount of other stuff which maybe wasn’t directly relevant if you just wanted to hack around and write programs, or if you wanted to think theoretically about computation. Paul Graham has said that computer science is not so much a unified discipline as a collection of people thrown together by accident of history, like Yugoslavia. You’ve got the ”mathematicians,” the ”hackers,” and the ”experimentalists,” and we just throw them all together in the same department and hope they sometimes talk to each other. But I do think (and this is a cliched thing to say) that the boundaries between CS, math, physics, and so on are going to look less and less relevant, more and more like a formality. It’s clear that there’s a terrain, but it’s not clear where to draw the boundaries.

-Scott Aaronson

‘ *Shut up and Calculate*

-David Mermin

1 Introduction

This project aims to look at some of the more elementary quantum information science elements like qubits, quantum gates and phenomenon like quantum entanglment, teleportation, quantum Fourier Transform and Grovers searching algorithm in a computer science friendly way. Undergraduate computer science students often find it intimidating to step into the field of Quantum Computing because of the scary physics. This project also aims to make that easier by explaining these basic phenomena in the language of math, with practically no prerequisite of physics apart from elementary and high school courses. This perspective on the field will hopefully allow more computer scientists and students hold their ground in the field by looking at stuff masked by the digital logic they are comfortable with and some basic knowledge of linear algebra. Even though Quantum Mechanics was discovered by physicists it is not a physical theory in the same sense as electromagnetism or kinematics or even relativity. If it were to be put in the heirarchy of Science it would sit somewhere between Physics and Mathematics. It is the basis on which every other physical theory works. Its not only about matter and waves and probabilities but also about information and amplitudes and quantization of information, something which makes transcending into Information Science theory a no brainer.

2 Literature Review

2.1 Why Havent More Quantum Algorithms Been Found? PETER SHOR

So far, all the quantum algorithms known to offer substantial speed-up over classical algorithms for the same problems fall into one of three classes. The first class uses the Fourier transform to find periodicity. This class contains the factoring and discrete logarithm algorithms [Shor 1997], Simons algorithm [Simon 1997] (the first member of this class to be discovered), and Hallgrens algorithms for Pells equation and certain other number theory problems [Hallgren 2002]. There is, in fact a different way of looking at the factoring algorithm that, although it yields basically the same algorithm, puts it into a setting that emphasizes spectral methods rather than periodicity [Kitaev 1996], but this approach has not yet yielded any new algorithms. The second class contains Grovers search algorithm, which can perform an exhaustive search of N items in $\sqrt{N}$ time [Grover 1997], and a number of extensions of this algorithm (see Grover and Sengupta [2002]). These extensions all have the general flavor of giving a square root improvement in the speed of optimization or search problems. The third class consists of algorithms for simulating or solving problems in quantum physics. This class contains Feynmans original idea [Feynman 1982] of using quantum computers to speed up simulations of quantum physics. While not many theoretical papers have yet been written on this class of algorithms, it is clear that if quantum computers are ever developed, this class will be extremely useful in practice. Feynman came up with his idea of using quantum computers to simulate quantum physics in 1982, Simons algorithm and the factoring algorithm were developed in 1993 and 1994, and Grover came up with his original search algorithm in 1995. Since then, there have been further theoretical developments within each of these classes of algorithms, but no new classes of quantum algorithms have been discovered.

2.2 Recent Progress in Quantum Algorithms - Dave Bacon and Wim Van Dam

The discovery that quantum comput- ers could efficiently factor is, even today, difficult to really appreciate. There are many ways to get out of the conundrum posed by this discovery, but all of these will require a funda- mental rewriting of our understanding of either physics or computer science. One possibility is that quantum com- puters cannot be built because quan- tum theory does not really hold as a universal theory. Although disappoint- ing for quantum computer scientists, such a conclusion would be a major discovery about one of the best tested physical theoriesquantum theory. Perhaps there is a classical algorithm for efficiently factoring integers. This would be a major computer science discovery and would blow apart our modern public key cryptography. Or perhaps, just perhaps, quantum com- puters really are the true model of computing in our universe, and the rules of what is efficiently computable have changed. These are the dreams of quantum computer scientists look- ing for quantum algorithms on the quantum machines they have yet to be quantum programmed.

3 Qubits

Any introduction to the subject of quantum computing genereally would begin with a formal definition of qubit. A qubit or a quantum bit is the quantum equivalent of a bit. A bit can store either zero or one, with all the states in between forbidden. A quantum bit has no forbidden state. It is represented as a vector of amplitudes of probabilities which can be either positive, negative, or even complex numbers. This opens up the possibility for storing a larger amount of information in a single qubit.

Physically,a qubit can be thought of as an electron in a Hydrogen atom. There are two possible states an electron in a hydrogen atom can be in the ground and the excited state. The ground state corresponds to the value of the qubit being 0, and the excited state corresponds to 1. We represent the ground state as $|0\rangle$ and excited state as $|1\rangle$. By the basic principles of quantum mechanics, the general state, denoted $|\alpha\rangle$, of an electron is given by a superposition of these two states.

$$|\alpha\rangle = \alpha_1 \ |0\rangle + \alpha_2 \ |1\rangle$$

where α_1, α_2 C and $|\alpha_1|^2 + |\alpha_2|^2 = 1$.

By this we mean that if a measurement is made on the state of the electron, we find it to be $|0\rangle$ with probability $|\alpha_1|^2$ and $|1\rangle$ with probability $|\alpha_2|^2$.

4 Gates

A quantum gate is the equivalent of classical gates like AND, OR, XOR, NOT, NAND, etc. They are basically small quantum circuits working on a small number of qubits. We usually represent quantum gates using matrices. Unlike classical gates, quantum gates need to be reversible. Also the matrices representing them need to be unitary so as to maintain the net probability being unity.

4.1 Hadamard Gate

The Hadamard gate acts on a single qubit. It maps the basis state from $|0\rangle$ to $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|1\rangle$ to $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$. So a measurement will have equal probability of $|0\rangle$ and $|1\rangle$. The matrix representing the Hadamard Gate is

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

4.2 Pauli-X Gate

The Pauli-X gate acts on a single qubit. It is the quantum equivalent of the NOT gate for classical computers. It maps $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$. The matrix representing the Pauli-X Gate is

$$X = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$$

4.3 Pauli-Y Gate

The Pauli-Y gate acts on a single qubit. It maps $|0\rangle$ to $\iota\,|1\rangle$ and $|1\rangle$ to $-\iota\,|0\rangle$. The matrix representing the Pauli-Y Gate is

$$Y = \begin{bmatrix}0 & -\iota\\ \iota & 0\end{bmatrix}$$

4.4 Pauli-Z Gate

The Pauli-Z gate acts on a single qubit. It leaves $|0\rangle$ unchanged and maps $|1\rangle$ to -$|1\rangle$.The matrix representing the Pauli-Z Gate is

$$Z = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$$

4.5 Swap Gate

The swap gate works on a 2 qubit input e.g. $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$ and swaps the two qubits.

The matrix representing the Swap gate is

$$SWAP = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}$$

4.6 Control Gates

Controlled gates act on 2 or more qubits, where one or more qubits act as a control for some operation on the second bit called the target bit. E.g. in the CNOT or Controlled NOT gate the first input acts as control for the second inputs NOT operation, i.e, if the first input is $|0\rangle$ the second input will remain unchanged but if the first input is $|1\rangle$ then an operation Pauli X (equivalent to classical NOT) operation is applied to the target bit. The CNOT gate works on the 2 qubit input $|00\rangle$, $|01\rangle$, $|10\rangle$ or $|11\rangle$ and its matrix is represented

$$CNOT = cX = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

4.7 Toffoli Gate

The Toffoli Gate is a universal 3 qubit gate. It is also called a CCNOT gate because the first two inputs are the control gate and when both of them are equal to $|1\rangle$ we perform a Pauli-X transform on the target bit

$$T = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

4.8 Fredkin Gate

The Fredkin or the C-SWAP gate is a 3 qubit gate that has the first qubit as the control bit which if 1, swaps the other two bits .

$$F = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

5 Measurement

Measurement of a qubit is an irreversible process and thus not a gate operation. Once measured the qubit takes either of $|0\rangle$ or $|1\rangle$ depending on the squares of amplitudes, which would have been determinable from thsi measurement if (theoretically) you had infinite copies of the qubits and perform measurement on all of them. The problem with that is by Bell's inequalities what follows is the no cloning theorem.

6 No Cloning Theorem

The No Cloning Theorem states that it is impossible to create an identical copy of an arbitrary qubit. The No Cloning Theorem is the biggest caveat in the application of classical error correction techniques on quantum bits, which at the moment is the biggest problem in the existance of stable quantum machines with large number of qubits.

7 Entanglement

An entangled system is defined to be one whose quantum state cannot be factored as a product of states of its local constituents; that is to say, they are not individual particles but are an inseparable whole. In entanglement, one constituent cannot be fully described without considering the other(s). The state of a composite system is always expressible as a sum, or superposition, of products of states of local constituents; it is entangled if this sum necessarily has more than one term.

Measurements of physical properties such as position, momentum, spin, and polarization, performed on entangled particles are found to be correlated. For example, if a pair of particles is generated in such a way that their total spin is known to be zero, and one particle is found to have clockwise spin on a certain axis, the spin of the other particle, measured on the same axis, will be found to be counterclockwise, as is to be expected due to their entanglement. . Einstein and others considered such behavior to be impossible, as it violated the local realist view of causality (Einstein referring to it as ”spooky action at a distance”) and argued that the accepted formulation of quantum mechanics must therefore be incomplete. Later, however, the counterintuitive predictions of quantum mechanics were verified experimentally in tests where the polarization or spin of entangled particles were measured at separate locations, statistically violating Bell’s inequality, demonstrating that the classical conception of ”local realism” cannot be correct.

Entanglement is considered fundamental to quantum mechanics, even though it wasn’t recognized in the beginning. Quantum entanglement has been demonstrated experimentally with photons,[neutrinos, electrons, molecules as large as buckyballs, and even small diamonds. The utilization of entanglement in communication and computation is a very active area of research.

As an example of entanglement: a subatomic particle decays into an entangled pair of other particles. The decay events obey the various conservation laws, and as a result, the measurement outcomes of one daughter particle must be highly correlated with the measurement outcomes of the other daughter particle (so that the total momenta, angular momenta, energy, and so forth remains roughly the same before and after this process). For instance, a spin-zero particle could decay into a pair of spin $\frac{-1}{2}$ particles. Since the total spin before and after this decay must be zero (conservation of angular momentum), whenever the first particle is measured to be spin up on some axis, the other, when measured on the same axis, is always found to be spin down. (This is called the spin anti-correlated case; and if the prior probabilities for measuring each spin are equal, the pair is said to be in the singlet state.)

7.1 Explanataion

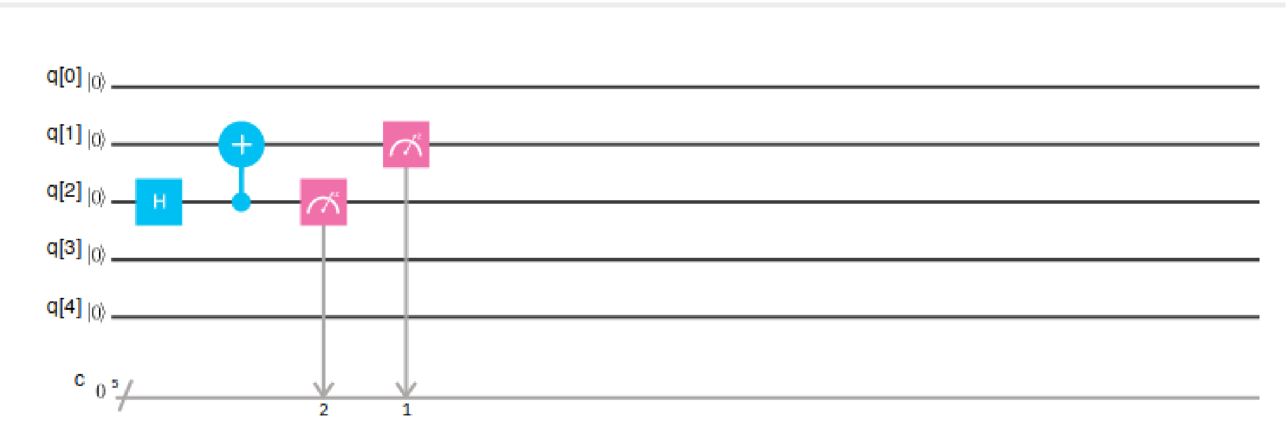
If the tensor product state of two qubits cannot be factored, they are said to be entangled. E.g.

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\1\end{bmatrix} = \begin{bmatrix}a\\b\end{bmatrix} \otimes \begin{bmatrix}c\\d\end{bmatrix}$$

$$\begin{gathered}\text{ac} = \tfrac{1}{\sqrt{2}}\\ \text{ad} = 0\\ \text{bc} = 0\\ \text{ad} = \tfrac{1}{\sqrt{2}}\end{gathered}$$

This system of equation has no solution. Thus the product state can not be factored and hence the two qubits are in entangled state. This has a 50% chance of collapsing to $|00\rangle$ and 50% chance of collapsing to $|11\rangle$.

7.2 Reaching an entanged state



7.3 Applications

Entanglement has many applications in quantum information theory. With the aid of entanglement, otherwise impossible tasks may be achieved.

Among the best-known applications of entanglement are superdense coding and quantum teleportation Most researchers believe that entanglement is necessary to realize quantum computing (although this is disputed by some).

Entanglement is used in some protocols of quantum cryptography. This is because the ”shared noise” of entanglement makes for an excellent one-time pad. Moreover, since measurement of either member of an entangled pair destroys the entanglement they share, entanglement-based quantum cryptography allows the sender and receiver to more easily detect the presence of an interceptor.

8 Quantum Teleportation

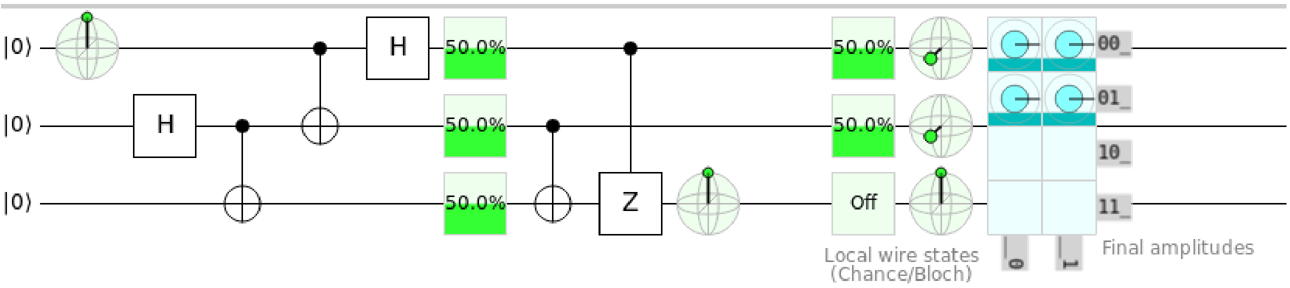
Quantum teleportation is a process by which quantum information (e.g. the exact state of an atom or photon) can be transmitted (exactly, in principle) from one location to another, with the help of classical communication and previously shared quantum entanglement between the sending and receiving location. Because it depends on classical communication, which can proceed no faster than the speed of light, it cannot be used for faster-than-light transport or communication of classical bits. While it has proven possible to teleport one or more qubits of information between two (entangled) atoms, this has not yet been achieved between anything larger than molecules.

Although the name is inspired by the teleportation commonly used in fiction, quantum teleportation is limited to the transfer of information rather than matter itself. Quantum teleportation is not a form of transportation, but of communication: it provides a way of transporting a qubit from one location to another without having to move a physical particle along with it.

Quantum teleportation provides a mechanism of moving a qubit from one location to another, without having to physically transport the underlying particle to which that qubit is normally attached. Much like the invention of the telegraph allowed classical bits to be transported at high speed across continents, quantum teleportation holds the promise that one day, qubits could be moved likewise.

An important aspect of quantum information theory is entanglement, which imposes statistical correlations between otherwise distinct physical systems. These correlations hold even when measurements are chosen and performed independently, out of causal contact from one another, as verified in Bell test experiments. Thus, an observation resulting from a measurement choice made at one point in spacetime seems to instantaneously affect outcomes in another region, even though light hasn't yet had time to travel the distance; a conclusion seemingly at odds with special relativity (EPR paradox). However such correlations can never be used to transmit any information faster than the speed of light, a statement encapsulated in the no-communication theorem. Thus, teleportation, as a whole, can never be superluminal, as a qubit cannot be reconstructed until the accompanying classical information arrives.

8.1 Teleportation Protocol



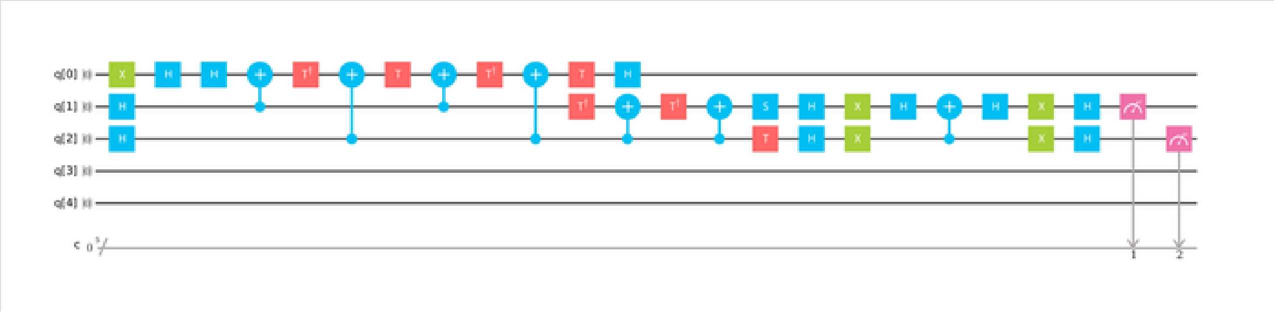
9 Grover's Algorithm

9.1 Introduction

Grovers algorithm as initially described enables one to find (with probability ¿ $frac12$) a specific item within a randomly ordered database of N items using O($\sqrt{N}$) operations. By contrast, a classical computer would require O(N) operations to achieve this. Therefore, Grovers algorithm provides a quadratic speedup over an optimal classical algorithm. It has also been shown that Grovers algorithm is optimal in the sense that no quantum Turing machine can do this in less than O($\sqrt{N}$) operations.

While Grovers algorithm is commonly thought of as being useful for searching a database, the basic ideas that comprise this algorithm are applicable in a much broader context. This approach can be used to accelerate search algorithms where a quantum oracle can be constructed that distinguishes the needle from the haystack. The needle and hay need not be part of a database. For example, it could be used to search to two integers 1 ¡ a ¡ b such that ab = n for some number n, resulting in a factoring algorithm Of course, the performance of Grovers algorithm would not match the performance of Shors algorithm for this purpose.

9.2 Implementation



1. Aharonov, D., Ben-Or, M. Fault-tolerant quantum computation with constant error rate. In Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing (1997). ACM, 176188.

2. Aharonov, Y., Davidovich, L., Zagury, N. Quantum random walks. Phys. Rev. A 48, 167 (1993).

3. Ambainis, A. Quantum walk algorithm for element distinctness. SIAM J. Comput. 37 (2007), 210.

4. Ambainis, A., Kempe, J., Rivosh, A. Coins make quantum walks faster. In Proceedings of the 16th Annual ACM SIAM Symposium on Discrete Algorithms (2005), 1099

5. Aspuru-Guzik, A., Dutoi, A., Love, P.J., Head-Gordon, M. Simulated quantum computation of molecular energies. Science 309, 5741 (2005).

6. Bell, J.S. On the Einstein Podolsky Rosen paradox. Physics 1, (1964), 195.

7. Buhrman, H. palek, R. Quantum verification of matrix products. In Proceedings of the 17th Annual ACM- SIAM Symposium on Discrete Algorithms (2006), 880.

8. Childs, A.M., Cleve, R., Deotto, E., Farhi, E., Gutmann, S., Spielman, D.A. Exponential algorithmic speedup by quantum walk. In Proceedings of the 35th ACM Symposium on Theory of Computing (2003), 5968.

9. Farhi, E., Gutmann, S. Quantum computation and decision trees. Phys. Rev. A 58 (1998), 915.

10. Farhi, E., Goldstone, J., Gutmann, S. A quantum algorithm for the Hamiltonian NAND tree. Eprint arXiv:quant-ph/0702144, 2007.

11. Feynman, R. Simulating physics with computers. Intl. J. Theor. Phys. 21 (1982), 467488.

12. Grover, L. A fast quantum mechanical algorithm for database search. In Proceedings of the 28th Annual ACM Symposium on the Theory of Computation (New York, 1996). ACM, 212219.

13. Hffner, H., Hnsel, W., Roos, C.F., Benhelm, J., al kar, D.C., Chwalla, M., Krber, T., Rapol, U.D., Riebe, M., Schmidt, P.O., Becher, C., Ghne, O., Dr, W., Blatt, R. Scalable multiparticle entanglement of trapped ions. Nature 438 (2005), 643.

14. Hallgren, S. Polynomial-time quantum algorithms for pells equation and the principal ideal problem. In Proceedings of the 34th Annual ACM Symposium on the Theory of Computation (New York, 2002). ACM, 653658.

15. Kedlaya, K.S. Quantum computation of zeta functions of curves. Comput. Complex. 15, 119 (2006).

16. Kitaev, A. Quantum error correction with imperfect gates. In Quantum Communication, Computing and Measurement (New York, 1997). Plenum, 181188.

17. Knill, E., Laflamme, R., Zurek, W.H. Resilent quantum computation. Science 279 (1998), 342345.

18. Knill, E., Laflamme, R., Zurek, W.H. Resilient quantum computation: error models and thresholds. Proc. Roy. Soc. Lond. Ser. A 454 (1998), 365384.

19. Leibfried, D., Knill, E., Seidelin, S., Britton, J., Blakestad, R.B., Chiaverini, J., Hume, D.B., Itano, W.M., Jost, J.D., Langer, C., Ozeri, R., Reichle, R., Wineland, D.J. Creation of a six-atom Schrdinger cat state. Nature 438 (2005), 639.

20. Magniez, F., Santha, M., Szegedy, M. Quantum algorithms for the triangle problem. In Proceedings of the 16th Annual ACM SIAM Symposium on Discrete Algorithms (2005), 1109.

21. Nielsen, M.A. Chuang, I.L. Quantum Computation and Quantum Information. Cambridge University Press, New York, 2000.

22. Regev, O. Quantum computation and lattice problems. In 43rd Symposium on Foundations of Computer Science (IEEE Computer Society, 2002), 520529.

23. Rivest, R.L., Shamir, A., Adleman, L. A method of obtaining digital signatures and public-key

cryptosystems. Commun. ACM 21 (1978), 120126.
24. Shor, P.W. Algorithms for quantum computation: Discrete log and factoring. In Proceedings of the 35th Annual Symposium on the Foundations of Computer Science. S. Goldwasser, ed. (Los Alamitos, CA, 1994). IEEE Computer Society, 124134.
25. Shor, P.W. Fault tolerant quantum computation. In Proceedings of the 37th Symposium on the Foundations of Computer Science (Los Alamitos, CA, 1996), IEEE, 5665.
26. Woehr, J. Online interview A Conversation with Christos Papadimitriou. Dr. Dobbs J. July Dave Bacon is an assistant research professor in the Department of Computer Science and Engineering, Department of Physics, at the University of Washington, Seattle.