# 1 Engineering Entanglement: Quantum Computation, Quantum Communication, and Re-conceptualizing Information

Chen-Pang Yeang

## Introduction: the EPR Paradox and Entanglement

Very few issues in the history of quantum mechanics have undergone so many twists as entanglement. According to the received view, the idea of entanglement was proposed as a paradox to challenge quantum mechanics. Albert Einstein, the major opponent of the Copenhagen interpretation, disagreed with Werner Heisenberg and Niles Bohr's denial of physical reality without the intervention of measurement, which they claimed to be an implication of quantum mechanics. From the late 1920s to the early 1930s, Einstein exchanged a series of arguments with Bohr regarding the consistency of the Copenhagen interpretation. The pinnacle of this debate was a thought experiment that Einstein, his assistant Nathan Rosen at the Institute for Advanced Study, and the Russia-born physicist Boris Podolsky came up in 1935.

What is now famous as the Einstein-Podolsky-Rosen (EPR) experiment works as follows: Generate two identical particles at some location and let them move away. According to quantum mechanics, these two particles together constitute a single quantum state that can be expressed by a wave function. Prepare the two particles at a particular quantum state[1] (the "EPR" or "entangled" state) so that they correlate perfectly with each other. For the EPR state, it can be shown that when one makes a momentum measurement at particle 1 and obtains the result $p$, she can be sure that were she to measure the momentum of particle 2 she would get -$p$. Similarly, when she measures the position of particle 1 and obtains $x$, she is guaranteed to get -$x$-$x_0$ from measuring the position of particle 2 ($x_0$ is a constant). In brief, when the two-particle system is at the EPR state, measuring the momentum or position of one particle is sufficient to determine the other particle's momentum or position.

This seemingly straightforward scenario was nonetheless turned into EPR's weapon against the completeness of quantum mechanics. From Heisenberg's interpretation of the uncertainty principle, one cannot determine simultaneously the momentum and position (or any other non-commutating conjugate pair) of a particle, because one measurement would perturb the particle's original state and thus affect the accuracy of the other measurement. In the above thought experiment, however, one can determine particle 2's momentum or position without any measurement-induced perturbation, since all the

[1] The wave function is $\Psi{=}(x_1{,}x_2){=}\int_{-\infty}^{\infty} \mathrm{e}^{i2\pi/h(x_1-x_2+x_0)p}\, dp$ . See Albert Einstein, Boris Podolsky, and Nathan Rosen, "Can quantum-mechanical description of physical reality be considered complete?" *Physical Review*, 47 (1935), 779, equation (10).

measurements are done at particle 1. To EPR, that means both momentum and position are pre-existing physical properties (in EPR's words, "elements of physical reality") of particle 2. Constrained by the uncertainty principle, quantum mechanics cannot yield accurate predictions of the second particle's momentum and position at the same time. But it does not imply (contra Bohr and Heisenberg) that nature prohibits simultaneous determination of both physical quantities. Rather, it indicates that quantum mechanics fails to capture all the elements of physical reality. Quantum mechanics is incomplete.[2]

The entangled state epitomized physicists' efforts to understand the strange, counter-intuitive characteristics of quantum mechanics. Since the founding of the "new" quantum mechanics in the mid-1920s, physicists have tried to grapple with various consequences of the theory that appeared contradictory to the established worldview: An object does not proceed along a trajectory but has the probability to be everywhere. Particles "interfere" with one another to form wavelike patterns. Entities far apart have non-local, spontaneous correlations. Measurement determines physical reality. Entanglement was not the only scenario for illustrating and exploring these odd features of quantum mechanics. Nor did it start as a very conspicuous one. (The EPR paper did not incur much response in the first two decades after its publication.) With a few physicists' rediscovery and elaboration in the 1950s–60s, however, entanglement became one of the most important avenues for the study of quantum logic and the axiomatic foundation of quantum physics.

For instance, the maverick American physicist David Bohm used entanglement in developing his non-local hidden-variable interpretation of quantum mechanics. In 1957, Bohm and his collaborator Yakir Aharonov of Haifa, Israel, reformulated the EPR scenario from its original momentum-position basis into a simpler basis involving spins[3]. In Bohm and Aharonov's version, each of the two particles was described by two quantum states—spin up ($|0\rangle$) and spin down ($|1\rangle$)—instead of the continuous states representing momentum and position. Then the wave function of the EPR state was

$$|\mathrm{EPR}\rangle = \frac{1}{\sqrt{2}}(|0\rangle\,|1\rangle - |1\rangle\,|0\rangle) \tag{1.1}$$

This reformulation of the EPR state turned out to be essential. In his visit to the United States in 1964, the Irish particle physicist John Stewart Bell of CERN discovered a way to respond to EPR's paradox based on the Bohmian entangled state. Bell found that if quantum mechanics were incomplete (as EPR held) and the two particles of the Bohmian entangled state were determined by two sets of unknown parameters independent of each other (i.e., two sets of local hidden variables), then the probabilities of the events for the two particles would follow the so-called "Bell inequalities." However, the probabilities of such events obtained from quantum mechanical calculations did not obey the Bell inequalities. Therefore, any local hidden-variable theory of quantum mechanics must be contradictory.[4]

[2] *Ibid*, 777–780.

[3] David Bohm and Yakir Aharonov, "Discussion of experimental proof for the paradox of Einstein, Rosen, and Podolsky," *Physical Review*, 108 : 4 (1957), 1070–1076.

[4] John S. Bell, "On the Einstein-Podolsky-Rosen paradox," *Physics* 1 (1964), 195–200; reprinted in John S. Bell, it Speakable and Unspeakable in Quantum Mechanics: Collected Papers on Quantum Philosophy (Cambridge: Cambridge University Press, 2004), 14–21.

From Einstein, Podolsky, Rosen, to Bohm, Aharonov, Bell, and their followers in the 1960s–70s, those working on entanglement were preoccupied with understanding the conceptual foundation of quantum mechanics. They treated the entangled state as a model scenario to demonstrate how weird the quantum world is and to interpret why it is the case. To the physicist community, the EPR problem was associated with the meta-theoretical issues of quantum mechanics, such as realism, quantum logic, axiomatic formulation, hidden-variable interpretations, completeness, and measurements.

Nevertheless, an epistemic change has emerged in the past thirty years. Since the 1980s, a number of scholars have revived the study of entanglement for a quite different reason. In addition to the meta-theoretical concerns with the foundation of quantum mechanics, they broadened their attention to the pragmatic aspects of entanglement. Some of them even set aside the question of *why* quantum mechanics is so strange and rather focused on *how to utilize* the strange properties of quantum mechanics. Their answer gave rise to a new field known as quantum information.

How did such an epistemic shift occur? This paper examines the rise and ongoing development of quantum information, the applications of quantum principles to computation, communications, and other information processing problems. Although entanglement is not the only substantial element of quantum information, it nonetheless constitutes the intellectual core of quantum information and has played a key part in the history of this new field. Specifically, entanglement has been transformed from an *explanandum* in the meta-theoretical inquiries of quantum mechanics into a *resource* that facilitates tasks such as parallel computing, teleportation, super-dense coding, and cryptography. In this paper, I will argue that the development of quantum information can be viewed as a process in which scientists and technologists learned how to *engineering* entanglement and related behaviors of single quantum states.

It is worth noting that "engineering" in the history of quantum information has several unconventional senses, all of which are significant in different ways. First, unlike most applied outgrowths of quantum mechanics-microelectronics, chemistry, material science—that deal with macroscopic physical systems with many atoms or molecules, quantum information treats single atoms and coherent quantum states. Thus, the relevant engineering is not doping materials with impurities or changing their statistical mechanical conditions. Rather, it consists of preparing single atoms at simple quantum states, carefully changing these states, and following their amplitude and phase variations. The manipulation of single, coherent quantum states has become an indispensable aspect of engineering. Second, the part theory plays in engineering is no longer restricted to modeling and analysis of some given working systems. In quantum information (as well as in computer and communications sciences), theory is also used to gauge the performance of *all possible* working systems and thus to predict the *fundamental limit* of all solutions to an engineering problem. In other words, engineering consists of figuring out not only what can be done, but also what cannot be done. Third, a major challenge in quantum information is to find how to utilize quantum characteristics such as entanglement. As we will see, a quantum computer or quantum channel does not offer easy access to the information it carries, and often it is not more effective than its classical counterpart. Therefore, some "killer applications" are critical. In fact, the field began to take off only after some specific algorithms, such as quantum factorization and quantum search, were developed in the early 1990s. To this date, we may still characterize quantum information as "an approach looking for problems." In this sense, engineering also included the identification of proper problems.

From the above discussion, it should be clear that the history of quantum information involved multiple intellectual traditions of different communities. The most obvious tradition was the one shared by the physicists working on the EPR paradox and related meta-theoretical issues in quantum mechanics. Yet these physicists/philosophers were by no means the only historical actors in the development of quantum information. There were also down-to-the-earth contributors who cared more about the nitty-gritty details of calculations and experiments than about the philosophical implications: mathematicians and computer scientists preoccupied with universal computing, algorithms, and complexity, information theorists trying to approach the channel capacity with better communications codes, experimental atomic physicists working on purifying and manipulating single atoms, and optoelectronic engineers designing laser circuits. These peoples entered the history of quantum information at different stages.

## Conceiving Quantum Computers

The origin of the idea of quantum computers was closely related to the discussions on universal computation in the first half of the twentieth century. In 1936, the American logician Alonzo Church and the English mathematician Alan Turing independently proposed a solution to David Hilbert's *Entscheidungsproblem.* Their proposal ended up with what is now known as the "Church-Turing thesis:" every "computable" function (i.e., function that can be computed by an algorithm) can be computed by a certain generic procedure. In Turing's version, such a generic procedure was a "universal Turing machine." The Turing machine was a general computing architecture, not a real computer. It comprised a program, a finite-state control, an infinite one-dimensional tape, and a read/write head (see Figure 1). When the machine executed a computing task, the program instructed the finite-state control to move the read/write head according to the machine's internal state and the data being accessed on the tape's cell. The read/write head could read the data on the cell, overwrite the data, or simply skip to the next cell. The Church-Turing thesis asserted that this primitive architecture could perform all the tasks any digital computer could carry out (see Fig. **??**).[5]

The Church-Turing thesis and the universal Turing machine laid out the foundation for modern computer science. However, they also left a longstanding puzzle: Like all the digital computers, the Turing machine performs a discrete sequence of operations that are irreversible—a simple way to understand why it is the case is to observe that all these computing operations can be represented by logic circuits containing AND, OR, and NOT gates; but the AND and OR gates are not reversible operators since they take two inputs but give only one output. Nevertheless, many physical processes in nature (including those in classical and quantum mechanics) are reversible. Thus, why and how is it possible to implement a universal computer with a physical means? An obvious answer is thermodynamics and statistical mechanics, since they describe irreversible physical processes. Yet, the universal Turing machine as an irreversible process has its

[5] Alan Turing, "On computable numbers, with an application to the Entscheidungsproblem," *Proceedings of the London Mathematical Society*, [series 2] 42 (1936–37), 230–265; Michael A. Nielsen and Isaac L. Chuang, *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press, 2000), 122–125.

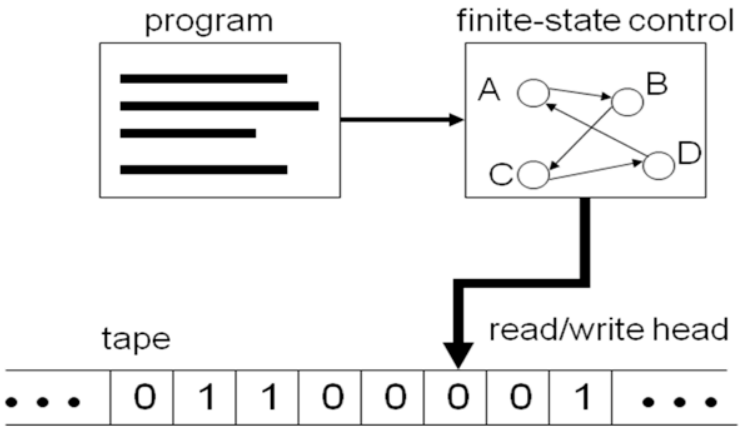

Figure 1.1: Universal Turing Machine

disorderliness (or entropy) decrease with time, which is apparently inconsistent with the second law of thermodynamics. So the problem remains unsolved.

In the 1960s–80s, the close study of this problem led to the expansion of a new area, physics of computation. Rolf Landauer and Charles Bennett at IBM Thomas Watson Research Center, Tommaso Toffoli at MIT Laboratory of Computer Science, and Edward Fredkin at Boston University were the leading figures in this area. It would be beyond the scope of this paper to delve into its immense literature. Suffice to point out that the problem of implementing the irreversible universal computer with a physical process yielded two related problems: Is it possible to make a *reversible* universal computer? Can we simulate every physical process with a universal computer? To deal with the first problem, Bennett, Fredkin, and Toffoli respectively introduced reversible Turing machines and reversible logic circuits.[6] The grappling of the second problem made room for the notion of quantum computers.

The idea of quantum computing began to appear in the 1970s. But perhaps the first influential literatures on this subject were introduced at the conference "Physics and Computation" that Fredkin, Landauer, and Toffoli co-organized at MIT in May 1981. At the conference, both Paul A. Benioff of the Argonne National Laboratory and Richard Feynman, then professor at Caltech, presented this idea. Benioff's was a model of classical Turing-like computation that could be implemented with quantum kinematics and dynamics[7]. Feynman's was something different. He started his presentation by remarking that he wanted to talk about the problem of "simulating physics with computers."[8] Classical physics, according to Feynman, may be efficiently simulated by conventional

[6] Charles H. Bennett, "Logical reversibility of computation," *IBM Journal of Research and Development*, 17 : 6 (1973), 525–532; Edward Fredkin and Tommaso Toffoli, "Conservative logic," *International Journal of Theoretical Physics*, 21 : 3/4 (1982), 219–253.

[7] Paul A. Benioff, "Quantum mechanical Hamiltonian models of discrete processes that earse their own histories: application to Turing machines," *International Journal of Theoretical Physics*, 21 : 3/4 (1982), 177–201.

[8] Richard Feynman, "Simulating physics with computers," *International Journal of Theoretical Physics*, 21 : 6/7 (1982), 467.

digital computers such as the Turing machines, since the relevant physical problems can be described as differential equations and solved numerically by algorithms. And this approach applies to a stochastic physical system as long as some randomized features are introduced into the Turing machines. But the same approach would encounter difficulties in simulating quantum physics, for the quantum wave functions do not represent ordinary probabilities. Instead, they exhibit a variety of strange features pertinent only to quantum mechanics (such as interference, indeterminancy, non-locality, and the violation of the Bell inequalities). In fact, in order to simulate a quantum system, a classical computer needs an exponentially huge memory to cover the entire Hilbert space. (An $N$-level quantum system with $R$ particles has $N^R$ configurations in total.) Therefore, Feynman argued, a more efficient means to simulate quantum physics is the quantum computer. He went further to propose a universal quantum simulator comprising a lattice of spin-up or spin-down particles (like an Ising model) with nearest-neighbor interactions that could be freely specified, and speculated that this system could be used to simulate many quantum field problems.[9]

Feynman's quantum machine was more a simulator than a computer in Turing's sense. The individual pushing the idea of quantum computer further toward the Turing-like, algorithmic direction was David Deutsch. Born in Haifa, Israel, Deutsch received his undergraduate education at Cambridge and Oxford and spent some years as a physics graduate student at the University of Texas at Austin. Deutsch's original interest lay in cosmology. While in Austin, he studied quantum field theory in general relativistic space-time. The Austin years shaped his intellectual path. As he later recalled, the scientists that gave him most influence on his work were Dennis Sciama, John Wheeler, and Bryce de Witt, all taught in the Physics Department of UT Austin when Deutsch studied there. De Witt played an especially important part. In Deutsch's own words, "he was the one who introduced me to Everett's many-worlds interpretation of quantum mechanics, and to the wider implications of quantum field theory, and it was because of his take on both the formalism and interpretation of quantum mechanics that I got interested in quantum computers." [10]

Deutsch did not follow his mentors in Texas to pursue cosmology and astrophysics, though. He returned to England, obtained a position as a researcher in the Department of Astrophysics at Oxford University, and started working on quantum computing. In 1985, he published a seminal paper on the topic in *Proceedings of the Royal Society of London.* Entitled "Quantum theory, the Church-Turing principle, and the universal quantum computer," this paper began with a challenge to classical universal computers that was similar to Feynman's: The universal Turing machine can compute every computable function, but can it be used to simulate every finitely realizable physical system? Like Feynman, Deutsch gave a negative answer to the question, owing to various constraints of the classical computation model. To fulfill both the mathematical and the physical universality, Deutsch developed a quantum version of the universal Turing machine. This quantum universal Turing machine contained the same elements as its classical counterpart—a program, a finite-state controller, a tape, and a read/write

[9] *Ibid*, 474–476.

[10] Filiz Peach's interview with David Deutsch in *Philosophy Now*, 30 December 2000 (http://www.qubit.org/people/david/Articles/PhilosophyNow.html); "David Deutsch," in Edge: The Third Culture (http://www.edge.org/3rd_culture/bios/deutsch.html).

head. Contrasting the classical computer, however, the internal states of this quantum computer and its data recorded on the tape memory were both quantum states following the quantum principles such as Hilbert-space expansion, superposition, non-locality, etc. Moreover, all operations of the machine, including the transition from one internal state to another and the writing of a piece of quantum data on the tape, corresponded to unitary operators on quantum states and thus are reversible. Deutsch showed that this quantum Turing machine was able to compute every mathematical function that was computable by a classical Turing machine or a randomized classical Turing machine. Moreover, since the quantum Turing machine was reversible and operates on quantum mechanical principles, it could be used to simulate efficiently the classical and quantum physical systems. Feynman's dream was fulfilled.[11]

The history of quantum computing would have been much more limited if Deutsch had stopped here. Although the universal quantum Turing machine could do anything that classical Turing machines could do, it was not clear at this moment whether this quantum computer could do anything that the classical computers could *not* do (except for simulating quantum physics) or perform any task more efficiently than the classical computers. Without the last two features, the quantum computers were at best equivalent to conventional computers, meaning it did not make sense to explore further the quantum computers from the practical point of view. Deutsch was aware of this problem and had a solution to it. He contended that the quantum computers were not only equivalent to classical computers; they were more efficient than the latter for some kinds of computing tasks (in addition to simulating quantum physics). The fundamental superiority of quantum computers, Deutsch argued, was based upon what he called "quantum parallelism," a basic property of quantum mechanics. Deutsch demonstrated the idea of quantum parallelism with a simple example. In the quantum world, the state of a particle can be a superposition of all basis states. Prepare a particular, "mixed" quantum state in an $N$-state system:

$$|\psi\rangle = \frac{\big(\,|0\rangle + |1\rangle + \ldots + |N-1\rangle\,\big)}{\sqrt{N}} \quad .$$

Couple this particle with another particle at state $|0\rangle$. The composite two-particle system has the quantum state

$$|\psi 0\rangle = \frac{\big(\,|00|\rangle + |10\rangle + \ldots + |N-1,0\rangle\,\big)}{\sqrt{N}} \quad .$$

Deutsch showed that there exists a quantum operation (or a quantum program) that leaves the first "slot" of each term unchanged while registers the result of evaluating a function $f$ at the second "slot:" . Thus the composite state after the operation becomes

$$|\psi 0\rangle \mapsto |\phi\rangle = \frac{\big(\,|0,f(0)\rangle + |1,f(1)\rangle + \ldots + |N-1,f(N-1)\rangle\,\big)}{\sqrt{N}} \quad .$$

This final state has a great computational advantage: It contains all the values of the function $f$ at 0, 1,…, $N-1$ in a single wave function, and this result is obtained only

[11] David Deutsch, "Quantum theory, the Church-Turing principle, and the universal quantum computer," *Proceedings of the Royal Society of London A*, 400 : 1818 (1985), 97–107.

with a single quantum operation. The implication: parallel information processing is possible with a serial quantum computer.[12]

Quantum parallelism and entanglement are the manifestations of the same quantum characteristics: The states of multiple particles can be expressed as linear combinations of the basis states, and the composite resulting state is the sum of couplings between the terms in these linear combinations. Deutsch's identification of the potential applications of these characteristics marked a significant step toward quantum computation. Nevertheless, quantum parallelism was not easy to use as it appeared to be. Although Deutsch's simple example showed the promise of getting $f(0)$, $f(1)$,..., $f(N-1)$ at the output state $|\phi\rangle$ , it was nonetheless difficult to retrieve all these values at the same time, since measuring $|\phi\rangle$ with respect to any of the state $|i, f(i)\rangle$ would inevitably collapse the original form of $|\phi\rangle$ and destroy the information it contained about other $f(.)$'s. This did not mean that quantum parallelism was doomed useless, but it did imply that more careful thoughts and more creative schemes were required to exploit quantum parallelism. Deutsch himself started developing one. Instead of retrieving all the $f(.)$'s, he sought to obtain a global property of $f(.)$ (a property involving multiple evaluations of $f$) from $|\phi\rangle$. With the even simpler binary case in which $N = 2$ and $f$ took only the value of 0 or 1, he demonstrated that the value $f(0) \bigoplus f(1)$ ($\bigoplus$ stands for the logical operation "Exclusive OR") could be determined by certain appropriate measurements of $|\phi\rangle$.[13]

## A Computer Looking for Algorithms

Deutsch became an advocate and devotee of quantum computation after the publication of his 1985 paper. In the second half of the 1980s, he moved to the Mathematical Institute of Oxford and worked on a general theory of quantum logical circuits to replace the less tractable quantum Turing machines. In computer science, a conventional digital computer was constituted of logical circuits with a few building blocks such as wires, sinks, and the AND, OR, and NOT gates. Deutsch's aim was to develop a theory for the necessary building blocks for all quantum logical circuits that shared the essential features of the classical logical circuits. The culmination of this work was a paper published in *Proceedings of the Royal Society of London* in 1989.[14] In this paper, Deutsch started to use the states $|0\rangle$ and $|1\rangle$ as the quantum counterparts of the classical bits 0 and 1. (In 1995, a quantum information theorist Benjamin Schumacher at Kenyon College of Ohio coined the term "qubits" to denote these quantum bits $|0\rangle$ and $|1\rangle$.[15]) Deutsch also proposed a set of elementary building blocks for two-qubit quantum logical operations: the "swap gate" exchanging the order of the first and the second qubits, and the important "controlled-NOT gate" that left the first qubit intact while flipped the second qubit if the first qubit read 1. (This was an analogy of the "Toffoli gate," a reversible two-bit logical operation Toffoli had developed in the 1970s.) In the early 1990s, some one-qubit operations such as the Pauli spin matrices and the so-called "Hadamard matrix" were also added to the repertoire of the quantum logical gates.

[12] *Ibid*, 111–113.

[13] *Ibid*, 112

[14] David Deutsch, "Quantum computational networks," it Proceedings of the Royal Society of London A, 425:1868 (1989), 73–90.

[15] Benjamin Schumacher, "Quantum coding," *Physical Review A*, 51 : 4 (1995), 2747.

Despite the increasing knowledge on the foundation of quantum computation, the question of application remained: What is the quantum computer useful for? As Deutsch had observed, the idea of quantum computing might not be worth pursuing if there were no algorithm for this computer that was more efficient than the existing approaches to a certain computational task. In other words, a quantum computer must have impressive algorithms with practical potential. The developments of such algorithms in the 1990s marked the real take-off of quantum computation.

The first initiative was taken in Oxford. As early as 1985, Deutsch had come up with a quantum parallel algorithm that solved a simple problem: determining whether $f(0) \bigoplus f(1)$ is 0 or 1. Although this did not address any "real" mathematical problem, it showed a vague but promising direction to go. To expand the algorithm in 1985, Deutsch sought the collaboration of another Oxford alumnus Richard Jozsa. Jozsa received his Ph.D. in physics at Oxford University under the supervision of the mathematical physicist Roger Penrose. Like Deutsch, Jozsa started as a cosmologist but ended up a specialist in the physics of computation. In 1992, the two colleagues published an algorithm, based on Deutsch's 1985 scheme, to solve a less straightforward problem.[16]

The so-called "Deutsch-Jozsa algorithm" tackles the following problem: Consider a binary functions $f$ that takes integer argument from 0 to $2^n - 1$. The function $f$ is either *constant* (0 or 1) for all values of the argument, or *balanced* in the sense that $f(x) = 0$ for half of the $x$ between 0 to $2^n - 1$ and 1 for the other half. The goal is to determine whether $f$ is constant or balanced with the least number of operations. For the classical algorithms, the only general approach to this problem is to check the value of $f(x)$ one by one, and it may take as many as $2^{n-1}+1$ checks before getting the answer. Nevertheless, Deutsch and Jozsa argued, an algorithm using the property of quantum parallelism can significantly reduce the number of operations. Key to the Deutsch-Jozsa approach is to prepare mixed $(n+1)$ qubits exhausting all the quantum states from $|0\rangle$ to $|2^n - 1\rangle$ using the "Hadamard gates" (a Hadamard gate transforms $|0\rangle$ into $\frac{(|0\rangle + |1\rangle)}{\sqrt{2}}$ and $|1\rangle$ into $\frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$). The overall output is then applied to the generalized controlled-NOT operation with $n$ controlling qubits (representing a number $x$) and 1 signal qubit (representing a number $y$). While the first $n$ qubits remain unchanged ($x$), the signal qubit after the gate becomes $y \bigoplus f(x)$. Finally, the first $n$ qubits ($x$) are employed by the Hadamard gates again (see Figure 2 for the exact procedure). Deutsch and Jozsa showed that after all these operations, the first $n$ qubits offer a straightforward test for the nature of $f$—it is constant if all the qubits are zero, and is balanced otherwise.

The strength of the Deutsch-Jozsa algorithm is its few number of operations compared to the conventional solutions to the same problem. While the conventional algorithms may take as many as $2^n/2+1$ steps to determine the nature of $f$, the quantum algorithm takes a single step, for the information about all values of $f$ is contained in the output quantum state. This is a significant saving of computational time, or, the reduction of computational complexity.

The Deutsch-Jozsa algorithm demonstrated the possibility of *engineering* the strange properties of quantum mechanics by turning them into computational resources. But

[16] David Deutsch and Richard Jozsa, " Rapid solutions of problems by quantum computation," *Proceedings of the Royal Society of London A*, 439 : 1907 (1992), 553–558.

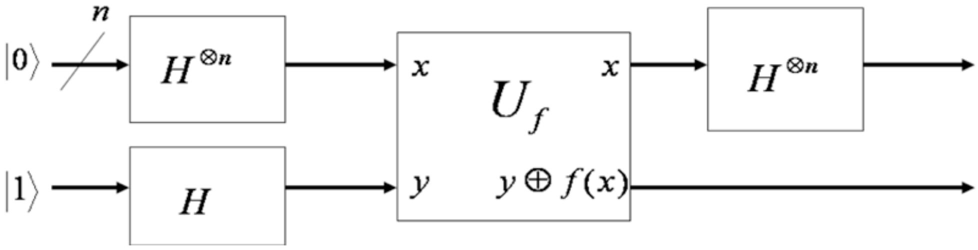

Figure 1.2: Deutsch-Jozsa Algorithm

the problem this algorithm aimed to solve was still artificial as well as insignificant, if not straightforward. Not until the mid-1990s did quantum computing begin to attack some "real-world" problems. Enter the American mathematician Peter Shor.

A native of California, Peter Shor was a mathematical prodigy-he won the International Olympiad and the Putnam Competition while in college. He received his B.S. from Caltech in mathematics and Ph.D. from MIT in applied mathematics. After graduation, he spent a year as a postdoc at the University of California in Berkeley and eventually landed a research position at the AT&T Bell Laboratories. Shor's early mathematical interests focused on statistical and geometrical problems in computer science. His Ph.D. dissertation was about the probabilistic analysis of the "bin-packing" problem: to pack a number of objects with different volumes and shapes into the least number of fixed bins. From the 1980s to the early 1990s, he published in a variety of areas including discrete and computational geometry, applied probability, bin packing and scheduling, and combinatorics.[17] Compared with Deustch and Jozsa, therefore, Shor received less training in quantum physics but was more sensitive to the ongoing development in computer science.

Shor's involvement with quantum computers began in 1994, when he proposed a famous quantum algorithm capable of tackling several important problems in number theory. In a conference paper read at the *IEEE Annual Symposium on Foundations of Computer Science*, Shor claimed that he could use the property of quantum parallelism to solve the so-called "order-finding" problem with a quantum algorithm that had a significantly lower time complexity than the traditional approaches.[18] The order-finding problem can be stated as follows: Consider two positive integers $x$ and $N$, where $N > x$. The order of $x$ modulo $N$ is defined as the smallest positive integer $r$ so that $x^r \equiv 1(\text{mod}N)$ (note that $A \equiv B(\text{mod}N)$ when $A - B$ is a multiple of $N$). The order-finding problem has been considered difficult. So far, no classical algorithms have been developed to solve the problem with the complexity (number of steps) lower than the polynomial orders of $N$. And most available algorithms do not go beyond trying different values of $r$ one by one in the modulo equation. That is, there is not yet an "efficient" classical algorithm to perform order finding.[19]

Shor's approach to this apparently intractable problem relied on Deustch's idea of

[17] http://www-math.mit.edu/ shor/pubs.html.

[18] Peter W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (1994), 124–134.

[19] *Nielsen and Chuang* (2000), 226.

quantum parallelism, an entanglement-like resource to facilitate certain computations. First, Shor noticed that a Fourier transform could be employed on an arbitrary quantum state. Like Deutsch's parallel state that contained all the information about a function, this "quantum Fourier transform" condensed all the spectral data of the input state into the output superposition state. And since the quantum Fourier transform was a quantum operator, it could be implemented with the components of standard quantum circuits such as Hadamard gates and phase rotators. In Shor's circuit for the quantum Fourier transform for $N$ elements, moreover, the number of operations was in the order of $O((\log N)^2)$ , which was considerably lower than the complexity $O(N \log N)$ of the Fast Fourier Transform, the quickest classical algorithm for spectral analysis.[20]

Second, Shor showed that the quantum Fourier transform was a tool to do phase estimation—i.e., estimating the phase $\varphi$ of a given operator $U$'s eigenvalue ($U|u\rangle = e^{i2\pi\varphi}|u\rangle$). The reason that the quantum Fourier transform was useful for such a task was clear: The phase estimation was equivalent to the operation of period finding, which could be done with spectral (Fourier) analysis. Shor developed a circuit constituting of Hadamard gates, a controlled-NOT gate, and a quantum Fourier transformer for the purpose of phase estimation.

Third, phase estimation was quite close to order finding, for both belonged to a general class of period-finding operations. In fact, Shor developed a formulation of the order-finding problem in terms of the phase-estimation problem. Thus, the order-finding problem was solved with a more efficient approach using quantum parallelism, since the major building block of the new approach—the quantum Fourier transform—had a significantly lower complexity than its classical counterparts.

Third, phase estimation was quite close to order finding, for both belonged to a general class of period-finding operations. In fact, Shor developed a formulation of the order-finding problem in terms of the phase-estimation problem.[21] Thus, the order-finding problem was solved with a more efficient approach using quantum parallelism, since the major building block of the new approach—the quantum Fourier transform—had a significantly lower complexity than its classical counterparts.

However, what was the use of solving the order-finding problem beyond satiating the curiosity of some number theorists? Shor argued that the order-finding problem could be applied to tackle two other problems with enormous practical implications: factorization of a large integer and finding the discrete logarithm of a number with respect to a cyclic group. The factorization problem seeks to obtain the factors of an integer equaling to the product of two large prime numbers, whereas the discrete logarithm problem is, roughly, to find the minimum solution $r$ of the equation $x^r \equiv p(\mathrm{mod} N)$ for given $x$, $p$, and $N$. Both problems are crucial in contemporary cryptography. The factorization of the product of two large prime numbers, for instance, has been the theoretical backbone of today's most popular public-key encryption scheme—the RSA algorithm that Ron Rivet, Adi Shamir, and Leonard Adlerman developed in the 1970s. The best classical algorithm to factorize a large number $N$ has the order of complexity no better than $O(N^{1/3})$ , and this intractable time prevents any effective way of breaking the encrypted code. Nevertheless, Shor's quantum algorithm for factorization can achieve a complexity as low as $O((logN)^2 log(logN) log(log(logN)))$, which is improved *exponentially* over the

[20] *Shor* (1994), 127–128.

[21] *Ibid*, 128-129.

classical algorithms. With Shor's algorithm, therefore, the security of most current communications systems is at stake.[22]

The quantum factorization and discrete-logarithm algorithms developed in 1994 were the first algorithms for quantum computers to solve "real-world" problems. Compared with the Deutsch-Jozsa scheme, Shor's algorithms were more "practical." Within two years, the computer scientist Lov Grover proposed another major quantum algorithm for practical applications. Like the factorization and discrete logarithm scheme, this algorithm was also originated from the Bell Laboratories.

Lov Kumar Grover was born in India. After obtaining a Bachelor's degree in Indian Institute of Technology in Delhi, he moved to the United States for further study and work. Grover once taught in the Department of Electrical Engineering at Cornell University, but later left Cornell to join the Bell Laboratories as a researcher. In the mid-1990s, he became aware of Shor's work, probably through the internal communications at the Bell Labs. The idea of using quantum characteristics in algorithm design gave him a clue to solving a problem that had concerned him—the search problem.

Searching a database is a common task in information processing and computer science. Yet this trivial work becomes extremely time consuming when the size of the database is huge. Suppose in a set of $N$ elements there are some element $x$ that satisfies the condition $f(x) = 1$ (the other elements $y$ have $f(y) = 0$). The aim is to find all the $x$'s among the $N$ elements. Since the entire data set does not need to have a regular structure, however, it is difficult to come up with a search scheme that saves time in general. So far, the most efficient classical algorithm is to check the elements one by one, which takes $O(N)$ steps.

Grover got a different idea from quantum computing, though. In 1996, he proposed a quantum search scheme that would reduce the algorithmic complexity from $O(N)$ to $O(\sqrt{N})$. In his own words, "quantum mechanics helps in searching for a needle in a haystack."[23] The central idea underlying Grover's quantum search algorithm is quantum parallelism, too. Since superposition quantum states can carry the information about the $f(.)$ values of all the elements in the data set, we may save significant time by making use of such superposition quantum states. Specifically, Grover's search algorithm begins with the preparation of a superposition state containing all the elements of the data set. Then a series of identical operations are employed on the state. The aim of these iterative operations is to "rotate" the quantum state toward the subspace corresponding to the solution $f(x) = 1$ (Figure 3). Thus, after each iterative operation, the quantum state moves closer to the solution state. Grover showed that it takes about $O(\sqrt{N})$ steps to align the quantum state with the solution state, the objective of the search.[24]

The quantum factorization, discrete-logarithm, and search algorithms developed in the 1990s marked a significant step in the history of quantum computing. Before, quantum computing was either entertained as an alternative formulation to the Turing machine model or exploited to tackle only fabricated problems. Shor's and Grover's quantum algorithms solved "real-world" problems important to pure as well as applied mathematicians. They represented the initial success—at least at the theoretical level—of

[22] Ibid, 130–133; Peter W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal of Computing*, 26 : 5 (1997), 1484–1509.

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

[24] *Ibid*, 326–328.

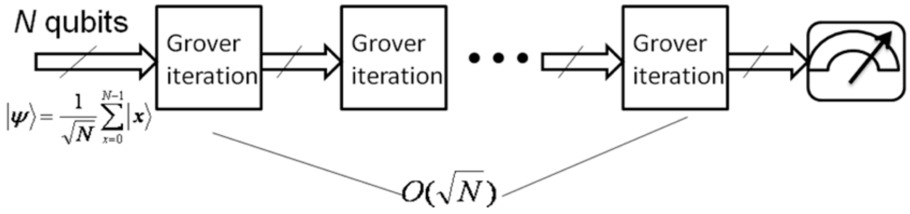

Figure 1.3: Deutsch-Jozsa Algorithm

harnessing the strange properties of quantum mechanics and turning the entanglement-like behaviors of the wave functions into valuable resources for the solution of practical problems. The introduction of the quantum factorization, discrete-logarithm, and search algorithms turned quantum computing from a confined and esoteric subject mainly interested to theoretical physicists into an active research area for mathematicians, computer scientists, and electrical engineers.

## Contemplating Quantum Communications

As physicists and computer scientists were seeking algorithms for quantum computers, another idea of quantum information was being considered. The idea was to use the strange properties of quantum mechanics in the transmission of information. Historically, the research on communications systems had a close relationship with the study of computation—the rise of modern communications engineering in the 1940–60s was owing to the revolution of digital computing, information theory and computer science had shared some common mathematical tools, both areas in the early stage were under the same disciplinary rubric of “information science,” etc. In the case of quantum communications and computing, the connection was built into the core methodology and problematiques. Both exploited and manipulated the fundamental characteristics of wave functions, but with different purposes. Quantum computing aimed at developing efficient algorithms to reduce computational complexity. By contrast, quantum communications set the goal of finding information transmission schemes, or “coding,” with a higher rate, more fault tolerance, and more security. Moreover, while quantum computing utilized a broader realm of quantum phenomena such as parallelism and superposition, quantum communications relied directly on entanglement.

It is natural to connect entanglement with communications problems. The correlation between the two particles of an entangled pair had invited attempts to devise information-transmission schemes. Since Einstein, Podolsky, and Rosen, scholars had disputed about whether information transmission based on the entangled state would lead to unlawful consequences such as superluminal action or time reversal. Yet, most discussions on this topic before the 1970s focused on the consistency and completeness of quantum mechanics. A pioneering effort to turn entanglement into communications resource was made by the American researcher Charles Bennett.

Charles Bennett was a native of Massachusetts. He obtained B.S. from Brandeis University in 1964 and Ph.D. from Harvard University in 1970, both in chemistry. Bennett’s training was physical chemistry; he conducted doctoral dissertation project concerned molecular dynamics. After graduation, he spent two years as a postdoc at Argonne Laboratory and eventually took a position at the IBM Research Center in New York State in 1972. At the time, the IBM Research was a center for exploring cutting-edge computers. For instance, the Corporation had invested on the research into superconducting logical circuits as a hopeful candidate for the computers of the next generation. Rolf Landauer had also established his research group on the physics of computation at IBM. When Bennett joined IBM, he worked under Landauer, who changed his interest from molecular dynamics to the relationship between physics and information. In the 1970s and early 1980s, Bennett contributed to various subjects in the physics of computation, including the formulation of a reversible universal computer and a reinterpretation of "Maxwell's demon" in the context of computation.[25]

Bennett began to pay close attention to entanglement in the early 1980s. The recent success of realizing the EPR experiment in laboratory [26] gave him the motivation of using the entangled states in communications. Bennett's first thought was quantum cryptography, the application of quantum characteristics to encrypting messages. This idea had existed for a while. In the 1970s, a physics student Stephen Wiesner at Columbia University had thought of certain "quantum money" that could withstand counterfeit.[27] Wiesner's proposal was not taken seriously, but Bennett's was. In 1982–84, he collaborated with the computer scientist Gilles Brassard in the Départment d'Information et de Recherche Opérationnelle at Université de Montréal to develop a scheme of quantum cryptography. The key principle of this scheme is that the quantum state of a particle is changed permanently after a measurement. Suppose a person sends a message coded into, say, the polarized state of a photon, to another person. If an eavesdropper is trying to tap this message, then he has to make a measurement of the photon's state, which changes it permanently.

Consequently, the received message differs from the sent message. With some protocol that the sender and the recipient exchange via another non-quantum channel, such a discrepancy can be detected. And since this discrepancy marks eavesdropping, both parties can drop the message of concern. In general, this procedure guarantees only the non-eavesdropped messages to get through. Encryption upholds![28] With the help of Bennett colleague John Smolin, Bennett and Brassard supervised the building of an experimental demonstration for quantum cryptography at IBM in 1989.[29]

Bennett and Brassard's quantum cryptographic protocol applied quantum principles to protect the security of communications. More fundamentally, they had shown that

[25] http://www.research.ibm.com/people/b/bennetc/chbbio.html.

[26] Alain Aspect, Phillipe Grangier, and Gérard Roger, "Experimental realization of Einstein-Podolsky-Rosen-Bohm Gedanken Experiment: a new violation of Bell's inequalities," *Physical Review Letters*, 49 : 2 (1982), 91–94; Alain Aspect, Jean Dalibard, and Gérard Roger, "Experimental tests of Bell's inequalities using variable analysis," *Physical Review Letters*, 49 : 25 (1982), 1804–1807; M.A.Horne and Anton Zeilinger, "Einstein-Podolsky-Rosen interferometry, new techniques and ideas in quantum measurement theory," D.Greenberger (ed.), *Annals of the New York Academy of Sciences*, 480 (1986), 469.

[27] Stephen Wiesner, "Conjugate coding," *SIGACT News*, 15 (1983), 77.

[28] Charles H. Bennett and Gilles Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Proceedings of IEEE International Conference on Computers Systems and Signal Processing, (Bangalore India, December 1984)* 175–179.

[29] http://www.research.ibm.com/people/b/bennetc/chbbio.html; Charles H. Bennett and Gilles Brassard , "The dawn of a new era in quantum cryptography: the experimental prototype is working," *ACM SIGACT News*, 20 (1989), 78–83.

one might use quantum states of particles as particular "channels" for information transmission; for instance, one could code the information into the polarized states of photons and send out the photons as information carrier. What are the characteristics of such quantum channels? In addition to encryption, what are the advantages of employing the quantum channels? Can they help increase the rate of information transmission, arguably the primary raison d'être of communication engineering? In the early 1990s, Bennett and his collaborators discovered a few interesting ways of manipulating the EPR states that offered clues to answer the above questions. Specifically, they found means to appropriate entanglement in implementing effective information-transmission systems.

The first finding came in 1992. Bennett and Stephen Wiesner suggested that a specific way of manipulating an EPR state led to a high-rate information transfer. Later known as "superdense coding," Bennett and Wiesner's scheme worked as follows (Figure 4): Suppose Alice wants to send a two-bit piece of information to Bob, who is far away from her. Either Alice or Bob or a third person prepares a two-particle entangled state:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle\,|0\rangle + |1\rangle\,|1\rangle) \tag{1.2}$$

(Note this state is different from the one Bohm and Bell used in (1). Yet both states exhibit the perfect correlation between the two particles that the EPR condition demands.) Now, deliver the first qubit of $|\psi\rangle$ to Alice and the second qubit to Bob. Since both qubits are from the same EPR state, they should have a perfect correlation even though they are possessed by two individuals far apart. After each of them obtains the respective qubit, Alice performs one of the four operations on the qubit she gets, and these operations can be numerated with two binary numbers:

| | | |
|---|---|---|
| 00 | no operation | $\alpha\,|0\rangle + \beta\,|1\rangle \mapsto \alpha\,|0\rangle + \beta\,|1\rangle$ |
| 01 | phase flip | $\alpha\,|0\rangle + \beta\,|1\rangle \mapsto \alpha\,|0\rangle - \beta\,|1\rangle$ |
| 10 | state swap | $\alpha\,|0\rangle + \beta\,|1\rangle \mapsto \beta\,|0\rangle + \alpha\,|1\rangle$ |
| 11 | phase flip+state swap | $\alpha\,|0\rangle + \beta\,|1\rangle \mapsto \beta\,|0\rangle - \alpha\,|1\rangle$ |

The operation Alice performs on her qubit depends on the message she intends to send to Bob: If she wants to send 00, then she leaves the qubit intact; if she wants to send 01, then she performs phase flip, etc. After the operation, Alice sends the qubit to Bob via a quantum channel. Upon receiving Alice's qubit, Bob possesses two entangled particles with the overall quantum state having one of the four possibilities:

| | | |
|---|---|---|
| 00 | $|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle$ | |
| 01 | $|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle$ | |
| 10 | $|\phi\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle$ | |
| 11 | $|\phi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle$ | (3) |

Since the states in (3) are orthogonal to each other, Bob can devise a measuring instrument to distinguish $|\phi\rangle$ perfectly among the four possibilities. By measuring the quantum state of the two entangled particles, therefore, Bob can figure out whether Alice sends $00, 01, 10$, or 11, meaning that he is able to retrieve the information Alice transmits. Moreover, the transmission of this *two-bit* information is achieved with the communication of only one qubit from Alice to Bob. In other words, the rate of information transmission is doubled using EPR and the quantum channel! In 1992, Bennett and Wiesner published their scheme in *Physical Review Letters*.[30]

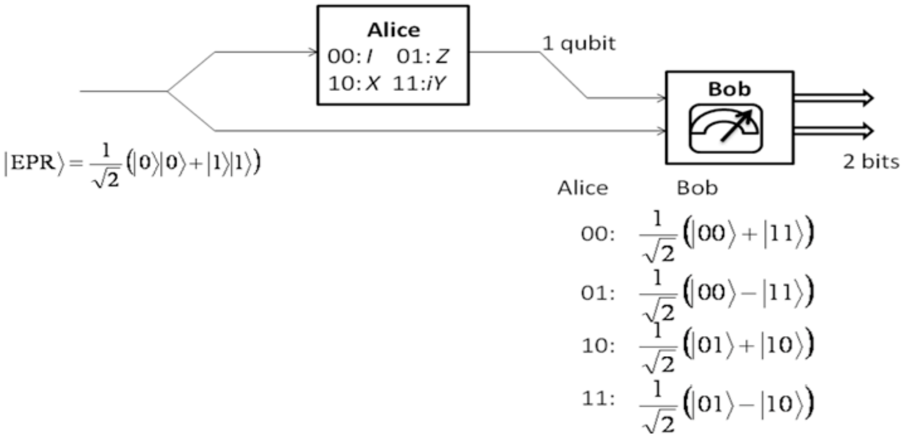
Alice
00:$I$ 01:$Z$
10:$X$ 11:$iY$
1 qubit
Bob
2 bits
$|\mathrm{EPR}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle + |1\rangle|1\rangle\right)$
Alice Bob
00: $\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$
01: $\frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)$
10: $\frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$
11: $\frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$

Figure 1.4: Superdense Coding

Bennett and Wiesner's proposal turned out to be only the first step toward a more unintuitive result in quantum communications. In the 1992 paper, they pointed out that the essence of their scheme was to split the two qubits of an EPR pair, manipulate a qubit at one side, and return the result of manipulation in some way to the other side. The superdense coding was just a special case of a more generic procedure like that. The paper also discussed the conditions in which some "ancilla," an additional quantum state, was coupled with one qubit of the EPR pair. The incorporation of the ancilla gave the communications system more freedom to manipulate, which facilitated the production of more novel effects. An immediate one was "quantum teleportation," the faithful transport of a quantum state from one place to another.

The work on quantum teleportation in 1993 resulted from a multinational collaboration involving the U.S., Canada, Israel, and France. The participants included Bennett, Brassard, Brassard's colleagues Claude Crépeau (who was also affiliated with the École Normale Supérieure in Paris) and Richard Jozsa at the Université de Montréal (Jozsa had moved to Montréal in 1985), Asher Peres at Technion-Israel Institute of Technology, and William Wootters at Williams College.[31] Their starting point was the longstanding question whether the long-range correlation between the two elements of an EPR pair can be used in information transfer. Since Einstein, scholars had focused on resolving any scenario that might violate the laws of physics. An example is the demonstration that instantaneous information transfer is impossible with an EPR pair, which saves the premise of relativity that nothing travels faster than light. Yet, Bennett *et al.* were not concerned with the meta-theoretical problems of compromising EPR with existing

[30] Charles H. Bennett and Stephen J. Wiesner, "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states," *Physical Review Letters*, 69 : 16 (1992), 2881–2884.

[31] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters, "Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels," *Physical Review Letters* 70 : 13 (1993), 1895–1899.

physical laws. Instead, they were interested in what can be done with entanglement. Although the EPR state cannot be used to perform instantaneous information transfer, they argued, it can facilitate perfect transmission, or more precisely, a faithful reproduction, of a quantum state. Here is the scheme of Bennett *et al.* to achieve quantum teleportation (Figure 5).

Suppose two far separated individuals Alice and Bob share an EPR pair. Like the case of superdense coding, Alice possesses one qubit while Bob owns the other qubit of the entangled state $|\mathrm{EPR}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$. Alice's task is to transmit to Bob a quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ that she possesses but does not have any knowledge of (i.e., she does not know the values of $\alpha$ and $\beta$). To achieve this end, Alice interacts her qubit of the EPR pair with the unknown quantum state $|\psi\rangle$. Her exact operations consist of a controlled-NOT gate taking $|\psi\rangle$ as the controlled qubit and a Hadamard gate on $|\psi\rangle$. Although these gates operate on $|\psi\rangle$ and Alice's qubit of $|\mathrm{EPR}\rangle$, they modify the joint quantum state of $|\psi\rangle$ and $|\mathrm{EPR}\rangle$, because Bob's EPR qubit and Alice's EPR qubit are perfectly correlated. After simple quantum mechanical calculations, it can be shown that the resultant joint state is the superposition of four distinct terms: Alice's qubits are $|00\rangle$ while Bob's qubit is $\alpha|0\rangle + \beta|1\rangle$, Alice's qubits are $|01\rangle$ while Bob's qubit is $\alpha|1\rangle + \beta|0\rangle$, Alice's qubits are $|10\rangle$ while Bob's qubit is $\alpha|0\rangle - \beta|1\rangle$, Alice's qubits are $|11\rangle$ while Bob's qubit is $\alpha|1\rangle - \beta|0\rangle$. This result indicates that Bob now possesses all the information needed to reconstruct $|\psi\rangle$, and he can do so as long as he knows the exact state of Alice's qubits. So Alice's next step is to measure her two qubits to see whether the outcome $M_1M_2$ is $00, 01, 10$, or 11. Then she transmits these two classical bits $M_1$ and $M_2$ via a classical channel to Bob. Upon receiving $M_1$ and $M_2$, Bob decides which operation to take against his qubit: no action at all for 00, a state swap for 01, a phase flip for 10, a state swap and a phase flip for 11. In all the four conditions, Bob's qubit output is guaranteed to be $\alpha|0\rangle + \beta|1\rangle$, a faithful reproduction of the original $|\psi\rangle$.

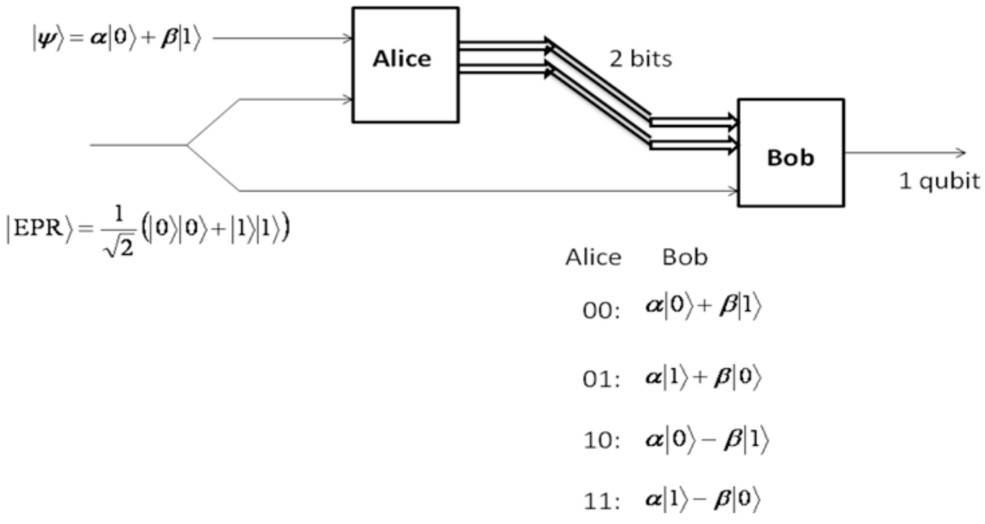
$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
Alice
2 bits
Bob
1 qubit
$|\mathrm{EPR}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$
Alice
Bob
00: $\alpha|0\rangle + \beta|1\rangle$
01: $\alpha|1\rangle + \beta|0\rangle$
10: $\alpha|0\rangle - \beta|1\rangle$
11: $\alpha|1\rangle - \beta|0\rangle$

Figure 1.5: Quantum Teleportation

The quantum teleportation provides a prototypical case for quantum communications.

Its arrangement exhibits certain important features common to a lot of more sophisticated quantum communication schemes. First, entanglement is the crucial resource for the system. The protocol of the system starts with two communicative parties sharing different elements of an EPR pair. Often the message is coded on a separate quantum state rather than an EPR qubit. Yet the message state has to “interact” with the EPR qubit in some algorithmic manner in order to exploit EPR’s correlation property. Second, the access to the quantum information is a tricky issue. Unlike classical information processing, the transmitter and receiver of a quantum communications system cannot freely copy a message or read a message without disturbing it. In the case of teleportation, for instance, Alice does not have any knowledge of the information she sends to Bob. Nor can she keep a copy of the message state afterwards, for the message state is collapsed after the measurement. Carefully designed, quantum-algorithmic-like operations are necessary in the management of information flow. Finally, “classical” channels may play an important part in quantum communications. Sometimes a quantum channel has to be augmented with conventional digital transmission in order to take full advantage of entanglement.

## Quantum Information: What’s Next?

From the 1980s to the mid-1990s, the pioneering works of Deutsch, Jozsa, Shor, Grover, Bennett, Brassard, Wiesner, and a few others had opened up the field of quantum information. The Deutsch-Jozsa, factorization, discrete logarithm, and search algorithms showed the promise of quantum parallelism in tackling computational problems. The ideas of quantum cryptography, superdense coding, and teleportation demonstrated the potential of entanglement in communications engineering. By the beginning of the twenty-first century, quantum information science had become a cutting-edge area with many participants from diverse disciplines and all parts of the world. An online “who’s who” for quantum information science features more than two hundred scholars from North America and Europe as well as East Asia, Middle East, and Latin America. The people studying quantum information had expanded into a significant, international community. What are their research agendas? What do they try to do? What is the next after the surge of innovations in the 1980s–90s?

Physical realizations of quantum computers and quantum communications systems have been a primary concern for those working in this area. Deutsch and Jozsa’s, Shor’s, and Grover’s algorithms, as well as Bennett et *al.*’s EPR-related communications protocols existed only on papers when they were proposed. Since the 1990s, physicists and engineers have tried to implement these ideas in laboratories. It would be a daunting task to trace the numerous experimental endeavors on quantum information in this paper. Suffice to observe that the implementation of quantum computers and communication systems has been built upon a different set of knowledge and skills from conventional computer engineering, electronic engineering, and material science. Unlike the computers and electronics we are using today, quantum computers and communications systems are difficult to realize using semiconductor materials. In fact, the making of these quantum information devices seems to concern not the choice and engineering of specific materials, but the ability to manipulate single atoms and photons and prepare pure quantum states. Thus, atomic physics and optoelectronics have played more important parts in quantum information experiments than condensed-matter physics and semiconductor electronic engineering.

The first notable success of quantum information experiments came from the physical implementation of simple quantum communications schemes. In 1996, researchers at the Universität Innsbruck in Austria and Los Alamos National Laboratories reported production of the superdense coding phenomenon in laboratory. In 1997–98, the Innsbruck group, and the research teams at the Università Roma, Italy, and Caltech succeeded in the experimental realization of quantum teleportation.[32] All these physicists used photons (more specifically, laser) in their implementation of quantum communication schemes. The choice of laser had good historical reasons: After the invention of laser in the 1960s and the development of optical fibers in the 1970s, optoelectronics had become a major means of high-bandwidth digital communications. In the process of designing efficient fiber networks, optoelectronic engineers and applied physicists had accumulated rich knowledge and skills in preparing and handling pure quantum states of photons such as the coherent state and the squeezed state. These became handy techniques for the experimenters working on EPR. In fact, the first successful laboratory productions of the EPR pairs in the early 1980s were accomplished by atomic physicists using laser apparatus. By the 1990s, therefore, the EPR photon-pair generator consisting of beam splitters and nonlinear parametric amplifiers had become an available device for the quantum information experimenters.

Although optoelectronics may be an effective way of implementing quantum communications systems, its applications in quantum computers have encountered some problems. Some have argued that photons are more difficult to interact with and to store than atoms, so a more feasible quantum computer should be made of the latter. In the mid-1990s, researchers proposed to use trapped ions to implement quantum computers. A technique invented in the 1970s by the German atomic physicists Hans Dehmelt and Wolfgang Paul, respectively, the ion trap utilized an electromagnetic field to confine charged particles within a small volume.[33] The ion trap was originally adopted to the studies of atoms or smaller elementary particles, and hence were more familiar to atomic physicists and particle physicists. This technique was brought to quantum computing, because it offered means to prepare and manipulate atomic particles at simple quantum states. Another popular candidate for the physical implementation of quantum computers is Nuclear Magnetic Resonance (NMR). NMR was another product of the mid-century boom of atomic physics (like laser and ion traps). Chemists and biomedical engineers had spent decades to elaborate and improve the device; by the 1990s, it had become a mature laboratory technology. Since a proposal in 1995, the NMR quantum computer has attracted much attention of quantum information scientists. The major advantage of NMR over ion traps or laser is that NMR functions at the macroscopic level: the data is registered at thousands or even millions of spinning nuclei instead of a few atoms or photons. But this advantage is also NMR's serious shortcoming: it is much more difficult to control the quantum state of a sea of spinning nuclei than that of several

[32] D. Bouwmeester, J.W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A, Zeilinger, "Experimental quantum teleportation," *Nature*, 390 : 6660 (1997), 575–579; D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu, "Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Physical Review Letters*, 80 : 6 (1998), 1121–1125; A. Furusawa, J.L. S¯rensen, S.L. Braunstein, C.A. Fuchs, H.J. Kimble, and E.S. Polzik, "Unconditional quantum teleportation," *Science*, 282 (1998), 706–709.

[33] http: //nobelprize.org/nobel_prizes/physics/laureates/1989/index.html.

atoms or photons. Recently, quantum information scientists have also proposed to extend the candidacy to superconductors, quantum dot, and ordinary semiconductors. But none of these approaches—including optoelectronics, ion traps, and NMR—has reached the stage of practicality. To date, there has not yet been a quantum computer with more than a few qubits, let alone a machine with sufficient qubits indispensable to realize the strength of the factorization, discrete logarithm, and search algorithms.

A major problem for the physical implementation of quantum computers and communications systems is noise. A single, coherent quantum state is very easy to collapse by a slight interaction with its environment. While experimenters' challenge is to maintain the purity of quantum states and remove the sources of noise, theorists' task is to develop algorithms, schemes, and protocols that are more robust to noise. Since the mid-1990s, much of the theoretical work on quantum information science has focused on this issue. Shor's factorization algorithm, Grover's search scheme, and Bennett *et al.*'s superdense coding, for instance, all perform well in an idealized world. But how would they function in the real, noise-infected world? Can we find ways to save their performance with the presence of disturbance? A popular topic among quantum information scientists is quantum error-correction codes. Peter Shor in 1995 and Andrew Steane of Oxford University in 1996 respectively devised error-correction codes for qubits. Similar to classical error-correction codes, their approaches were to interact the data qubits and some redundant qubits with quantum operations equivalent to parity check.[34] The ideas of quantum error-correction coding inspired theoretical works along several directions: In quantum computing, it led to the development of fault-tolerant computing gates that guarantee at least some degrees of performance for quantum algorithms in a noisy environment.

In quantum communications, the similarity between quantum error-correction codes and classical error-correction codes has encouraged theorists to construct a comprehensive quantum communications science analogous to the existing classical communications science. The most important development has been the building of a quantum information theory parallel to the Shannon-like information theory. Like Shannon's followers, the quantum information theorists are seeking the capacity of a quantum channel and consequently the best possible performance of a quantum communication system. They are also looking for the applications of the knowledge about channel capacity to the efficient design of error-correction, data-compression, and cryptographic codes. As of 2007, scholars believe that they still know "only a little of quantum information theory."

Quantum information devices are not yet a reality, if not an impossibility. Despite conspicuous financial support from NSF, DARPA, and other major funding agencies around the world, they remain research ideas and crude experimental prototypes that at best show uncertain promises.[35] Will there eventually be quantum computers or communications systems? Is the entire field a hype or hope? Although our task is not to

[34] A famous example is Peter Shor, "Fault-tolerant quantum computation," *Proceedings of the 37th Annual Symposium on Foundations of Computer Science* (1996), 56–65. Also see *Nielsen and Chuang* (2000), 425–499.

[35] Rolf Landauer, IBM's chief physicist of computation considered by many as a godfather of quantum computation, once suggested that all papers on quantum computing should carry a footnote: "This proposal, like all proposals for quantum computation, relies on speculative technology, does not in its current form take into account all possible sources of noise, unreliability and manufacturing error, and probably will not work." Seth Lloyd, "Obituary: Rolf Landauer (1927–99)," *Nature*, 400 : 6746 (1999), 720.

answer these questions, we can nonetheless observe from such questions what kind of pursuit have the studies of quantum information become. In this paper, I trace how the research into the foundation of quantum mechanics has evolved into an expanded technological project. The process started with physicists/philosophers' epistemological and ontological questions about entanglement, non-locality, and interference—what they are, how to understand them, *etc.* Gradually, however, the central research agendas were amended to pragmatic questions such as how to produce, manipulate, and make use of them. With the introduction of specific quantum algorithms and quantum communications protocols, entanglement and related properties had been turned from puzzles to be explained into resources for information processing. Engineering entanglement has become equally important to, if not dominated over, pondering the interpretation of quantum mechanics. Does this epistemic transformation indicate that quantum mechanics has reached a mature stage so that we stop worrying about its conceptual foundation and feel comfortable using it? I don not know. But I believe this story tells us as much about the technological nature of today's scientific practice as about our understanding of quantum mechanics.