ELSEVIER

Physica D 120 (1998) 43–47

PHYSICA D

Teleportation as a quantum computation ★

Gilles Brassard [a,*], Samuel L. Braunstein [b,1], Richard Cleve [c,2]

[a] *Département IRO, Université de Montréal, CP 6128, succursale centre-ville, Montréal, Qué. Canada H3C 3J7*

[b] *Abteilung für Quantenphysik, Universität Ulm, 89069 Ulm, Germany, and SEECS, University of Wales, Bangor, Gwynedd LL57 1UT, UK*

[c] *Department of Computer Science, University of Calgary, Calgary, Alta. Canada T2N 1N4*

Abstract

We present a simple implementation of quantum teleportation in terms of primitive operations in quantum computation.

PACS: 03.65.Bz; 03.65.–w; 89.70.+c; 89.80.+h

Keywords: Quantum teleportation; Quantum circuits; Entanglement; Bell measurements; Goulash

1. Introduction

Among the many exciting new applications of quantum physics in the realm of information processing, we are particularly fond of quantum cryptography, quantum computing and quantum teleportation [11,13,15]. Quantum cryptography allows for the confidential transmission of classical information under the nose of an eavesdropper, regardless of her computing power or technological sophistication [2,3,5]. Quantum computing allows for an exponential amount of computation to take place simultaneously in a single piece of hardware [18,20]; of particular interest is the ability of quantum computers to factorize numbers very efficiently [29] and to carry out an exhaustive search quadratically faster than classical computers [18,22], with dramatic implications for classical cryptography [12,14]. Quantum teleportation allows for the transmission of quantum information to a distant location despite the impossibility of measuring or broadcasting the information to be transmitted [4]. Each of these concepts had a strong overtone of science fiction when they were first introduced.

If asked to rank these ideas on a scale of technological difficulty, it is tempting to think that quantum cryptography is the easiest while quantum teleportation is the most outrageous – especially when it comes to teleporting goulash [24]! This ranking is correct with respect to quantum cryptography, whose feasibility has been demonstrated by several prototypes capable of reliably transmitting confidential information over distances of tens of kilometers [23,25,26,31]. The situation is less clear when it comes to comparing the

★ This research was presented at the Fourth Workshop on Physics and Computation, Boston, 23 November 1996.

* Corresponding author. E-mail: brassard@iro.umontreal.ca.
Supported in part by Canada's NSERC, Québec's FCAR and a Killam Research Fellowship from the Canada Council.

[1] E-mail: schmuel@sees.bangor.ac.uk.
Supported in part by a Humboldt Fellowship and by EPSRC grant no. GR/L91344.

[2] E-mail: cleve@cpsc.ucalgary.ca.
Supported in part by Canada's NSERC and the US National Science Foundation under grant PHY94–07194.

0167-2789/98/$19.00
PII: S0167-2789(98)00043-8

technological feasibility of quantum computing with that of quantum teleportation.

On the one hand, quantum teleportation can be implemented with a quantum circuit that is much simpler than that required for any nontrivial quantum computational task: the state of an arbitrary qubit (quantum bit) can be teleported with as few as two quantum exclusive-or (controlled-not) gates [1], as we explain in this note. Thus, quantum teleportation is significantly easier to implement than even the simplest of quantum computations if we are concerned only with the complexity of the required circuitry.

On the other hand, quantum computing is meaningful even if it takes place very quickly – indeed its primary purpose is increased computational speed – and within a small region of space. Quite the opposite, the interest of quantum teleportation would be greatly reduced if the actual teleportation had to take place immediately after the required preparation. Thus, although working prototypes of quantum teleportation have recently been demonstrated [8,9], quantum teleportation across significant time and space will have to await a technology that allows for the efficient long-term storage [17,28,30] and purification [6,7] of quantum information. Nevertheless, it may be that short-distance quantum teleportation will play a role in transporting quantum information inside quantum computers. Thus we see that the fates of quantum computing and quantum teleportation are inseparably entangled!

2. Quantum teleportation

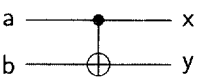
Recall that any attempt at measuring quantum information disturbs it irreversibly and yields incomplete information. This makes it impossible to transmit quantum information through a classical channel. Recall also that the purpose of quantum teleportation [4] is to circumvent this impossibility so as to allow the faithful transmission of quantum information between two parties, conventionally referred to as Alice and Bob.

In order to achieve teleportation, Alice and Bob must share prior quantum entanglement. This is usually explained in terms of Einstein–Podolsky–Rosen nonlocal quantum states [19] and Bell measurements, which makes the process rather mysterious. The purpose of this note is to show how to achieve quantum teleportation very simply in terms of quantum computation. Of course, the uncanny power of quantum computation draws in parts on nonlocal effects inherent to quantum mechanics. The quantum teleportation circuit described in Section 4 is not really different in principle from the original idea [4] since it uses quantum computation to create and measure nonlocal states. Nevertheless it sheds new light on teleportation, at least from a pedagogical point of view, since it makes the process completely straightforward to anyone who believes that quantum computation is a reasonable proposition. Moreover, this circuit could genuinely be used for teleportation purposes inside a quantum computer.

3. The basic ingredients

We shall need two basic ingredients: the quantum exclusive-or gate (also known as controlled-not), which acts on two qubits at a time, and the Walsh–Hadamard gate, which acts on a single qubit. Let $|0\rangle$ and $|1\rangle$ denote basis states for single qubits and recall that pure states are given by linear combinations of basis states, such as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α and β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$.

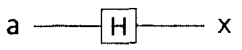
The quantum exclusive-or (XOR) gate is denoted as



where the *inputs* are a and b and the *outputs* are x and y. This gate sends $|00\rangle$ to $|00\rangle$, $|01\rangle$ to $|01\rangle$, $|10\rangle$ to $|11\rangle$ and $|11\rangle$ to $|10\rangle$. In other words, *provided the inputs at* a *and* b *are in basis states,* the output state at x is the same as the input state at a, and the output state at y is the exclusive-or of the two input states at a and b. This is also known as the controlled-not gate because the state carried by the *control* wire "ax" is not disturbed whereas the state carried by the *target* wire "by" is flipped if and only if the state on the control wire

was $|1\rangle$. Note that the classical interpretation given above no longer holds if the input qubits are not in basis states: it is possible for the output state on the control wire (at x) to be different from its input state (at a). Moreover, the joint state of the output qubits can be entangled even if the input qubits were not, and vice versa.

The Walsh–Hadamard gate is denoted as



and sends $|0\rangle$ to $(|0\rangle + |1\rangle)/\sqrt{2}$ and $|1\rangle$ to $(|0\rangle - |1\rangle)/\sqrt{2}$.

In terms of unitary matrices, the operations are

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

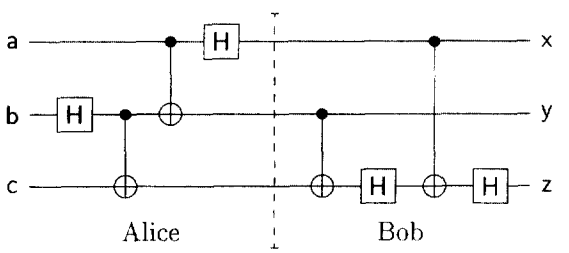
and

$$\mathsf{XOR} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

where $\alpha|0\rangle + \beta|1\rangle$ and $\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$ are represented by the transpose of vectors (α, β) and $(\alpha, \beta, \gamma, \delta)$, respectively.

4. The teleportation circuit

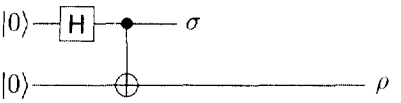
Consider the following quantum circuit. Please disregard the dashed line for the moment.



Let $|\psi\rangle$ be an arbitrary one-qubit state. Consider what happens if you feed $|\psi 00\rangle$ in this circuit, that is if you set upper input a to $|\psi\rangle$ and both other inputs b and c to $|0\rangle$. It is a straightforward exercise to verify that state $|\psi\rangle$ will be transferred to the lower output z, whereas both other outputs x and y will come out in state $|\phi\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. In other words, the output will be $|\phi\phi\psi\rangle$. If the two upper outputs are measured in the standard basis ($|0\rangle$ versus $|1\rangle$), two random classical bits will be obtained in addition to the quantum state $|\psi\rangle$ on the lower output.

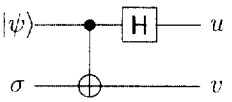
Now, we consider how the system evolves if the first two qubits are measured (in the standard basis) at the point where the dashed line occurs. This measurement results in two random classical bits u and v, which, being classical, are necessarily unentangled with the third qubit. These two classical bits can be thought of as basis quantum states $|u\rangle$ and $|v\rangle$, respectively, and the remaining gates of the circuit (after the dashed line) can be performed with states $|u\rangle$ and $|v\rangle$ for the first two qubits. It turns out that, *since the first two qubits only participate in the rest of the computation as the control bits of controlled-not gates,* measuring them at the point of the dashed line does not affect the final outcome of the computation. This phenomenon was previously exploited by Griffiths and Niu [21], who noted that, for any controlled-U gate (where U is any one-qubit unitary transformation), if the *control* qubit is to be measured in the standard basis then the measurement may be performed either before or after the gate is executed, without making any difference to the final outcome. Thus, we have that the outcome of the circuit is unaffected if the first two qubits are measured (in the standard basis) before the dashed line, rather than at the end of the computation.

To turn this circuit into a quantum teleportation device, we need the ability to store qubits. Assume Alice prepares two qubits in state $|0\rangle$ and pushes them through the first two gates of the circuit.



She keeps the upper qubit σ in quantum memory and gives the other, ρ, to Bob. (We do not denote these qubits by kets because they are not individual pure states: together they are in state $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$.) At some later time, Alice

receives a mystery qubit in unknown state $|\psi\rangle$. In order to teleport this qubit to Bob, she releases σ from her quantum memory and pushes it together with the mystery qubit through the next two gates of the circuit. She measures both output wires to turn them into classical bits u and v. (Note that an irreversible measurement is *not* a requirement here [16], in which case the teleportation procedure may in principle be reversed [27].)



To complete teleportation, Alice has to communicate u and v to Bob by way of a classical communication channel. Upon reception of the signal, Bob creates quantum states $|u\rangle$ and $|v\rangle$ from the classical information received from Alice, he releases the qubit ρ he had kept in quantum memory, and he pushes all three qubits into his part of the circuit (on the right of the dashed line). At this point, teleportation is complete as Bob's output Z is in state $|\psi\rangle$.

Note that this process works equally well if Alice's mystery qubit is not in a pure state, as originally pointed out in [4]. In particular, Alice can teleport to Bob entanglement with an arbitrary auxiliary system, possibly outside both Alice's and Bob's laboratories. Also, such a scheme can be used to teleport an arbitrarily large quantum state by mapping it into some possibly entangled n-qubit state and then independently teleporting each qubit – linearity guarantees that the complete state is successfully teleported.

In practice, Bob need not use the quantum circuit shown right of the dashed line at all. Instead, he may choose classically one of four possible unitary transformations to apply to the qubit he had kept in quantum memory, depending on the two classical bits he receives from Alice. (This would be more in tune with the original teleportation proposal [4].) This explains the earlier claim that quantum teleportation can be achieved at the cost of only two quantum exclusive-ors: those of Alice. Nevertheless, the unitary version of Bob's process given here may be more appealing than choosing classically among four courses of action if teleportation is used inside a quantum computer.

Acknowledgements

We gratefully acknowledge the Institute for Theoretical Physics, University of California at Santa Barbara, where the final t's were crossed. Gilles Brassard is grateful to Asher Peres for his continued encouragements.

References

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

[2] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, J.A. Smolin, Experimental quantum cryptography, J. Cryptology 5 (1992) 3–28.

[3] C.H. Bennett, G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984, pp. 175–179.

[4] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W.K. Wootters, Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels, Phys. Rev. Lett. 70 (13) (1993) 1895–1899.

[5] C.H. Bennett, G. Brassard, A.K. Ekert, Quantum cryptography, Sci. Am. (October 1992) 50–57.

[6] C.H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J.A. Smolin, W.K. Wootters, Purification of noisy entanglement and faithful teleportation via noisy channels, Phys. Rev. Lett. 76 (5) (1996) 722–725.

[7] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, W.K. Wootters, Mixed-state entanglement and quantum error correction, Phys. Rev. A 54 (5) (1996) 3824–3851.

[8] D. Boschi, S. Branca, F. De Martini, L. Hardy, S. Popescu, Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein–Podolsky–Rosen channels, Phys. Rev. Lett. 80 (6) (1998) 1121–1125.

[9] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter and A. Zeilinger, Experimental quantum teleportation, Nature 390 (6660) (1997) 575–579.

[10] M. Boyer, G. Brassard, P. Høyer, A. Tapp, Tight bounds on quantum searching, Fortschritte Der Physik, to appear.

[11] G. Brassard, A quantum jump in computer science, in: Jan van Leeuwen (Ed.), Computer Science Today Lecture Notes in Computer Science, vol. 1000, Springer, Berlin, 1995, pp. 1–14.

[12] G. Brassard, The impending demise of RSA?, RSA Laboratories CryptoBytes 1 (1) (1995) 1–4.

[13] G. Brassard, New trends in quantum computing, in: Proceedings of 13th Annual Symposium on Theoretical Aspects of Computer Science, Springer Berlin, 1996, pp. 3–10.
[14] G. Brassard, Searching a quantum phone book, Science 275 (1997) 627–628.
[15] G. Brassard, C. Crépeau, Cryptology column – 25 years of quantum cryptography, Sigact News 27 (3) (1996) 13–24.
[16] S.L. Braunstein, Quantum teleportation without irreversible detection, Phys. Rev. A 53 (3) (1996) 1900–1902.
[17] A.R. Calderbank, P.W. Shor, Good quantum error-correcting codes exist, Phys. Rev. A 54 (2) (1996) 1098–1105.
[18] D. Deutsch, Quantum theory, the Church–Turing principle and the universal quantum computer, Proc. Roy. Soc. London A400 (1985) 97–117.
[19] A. Einstein, B. Podolsky, N. Rosen, Can quantum-mechanical description of physical reality be considered complete?, Phys. Rev. 47 (1935) 777–780.
[20] R.P. Feynman, Quantum mechanical computers, Optics News, 1985; Reprinted in: Foundations Phys. 16 (1986) 507–531.
[21] R.B. Griffiths, C.-S. Niu, Semiclassical Fourier transform for quantum computation, Phys. Rev. Lett. 76 (17) (1996) 3228–3231.
[22] L.K. Grover, Quantum mechanics helps in searching for a needle in a haystack, Phys. Rev. Lett. 79 (2) (1997) 325–328.
[23] R.J. Hughes, G.G. Luther, G.L. Morgan, C.G. Peterson, C. Simmons, Quantum cryptography over underground optical fibers, Advances in Cryptology: Crypto'96 Proceedings, Springer, Berlin, 1996, pp. 329–342.
[24] International Business Machines, Stand by: I'll teleport you some goulash, advertisement in Scientific American (North American Edition), February 1996, 0–1 (sic).
[25] C. Marand, P.D. Townsend, Quantum key distribution over distances as long as 30 km, Opt. Lett. 20 (1995) 1695–1697.
[26] A. Muller, H. Zbinden, N. Gisin, Underwater quantum coding, Nature 378 (1995) 449.
[27] M.T. Nielsen, C.M. Caves, Reversible quantum operations and their application to teleportation, Phys. Rev. A 55 (4) (1997) 2547–2556.
[28] P.W. Shor, Scheme for reducing decoherence in quantum memory, Phys. Rev. A 52 (4) (1995) 2493–2496.
[29] P.W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Comp. 26 (5) (1997) 1484–1509.
[30] A.M. Steane, Error correcting codes in quantum theory, Phys. Rev. Lett. 77 (5) (1996) 793–797.
[31] H. Zbinden, N. Gisin, B. Huttner, A. Muller, W. Tittel, Practical aspects of quantum cryptographic key distribution, J. Cryptology, to appear.