PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

Quantum computing with controlled-NOT and few qubits

D. Bruss, A. Ekert, S. F. Huelga, J.-W. Pan and A. Zeilinger

Phil. Trans. R. Soc. Lond. A 1997 **355**, 2259-2266
doi: 10.1098/rsta.1997.0124

Quantum computing with controlled-NOT and few qubits

By D. Bruss[1]†, A. Ekert[1], S. F. Huelga[1,3], J.-W. Pan[2] and A. Zeilinger[2]

[1]*Clarendon Laboratory, Department of Physics, University of Oxford, Parks Road, Oxford OX1 3PU, UK*

[2]*Institut für Experimentalphysik, Universität Innsbruck, Technikerstraße 25, A-6020 Innsbruck, Austria*

[3]*Departamento de Fisica, Universidad de Oviedo, 33007 Oviedo, Spain*

We describe simple quantum networks which allow us to prepare, manipulate and measure quantum entanglement of few qubits.

1. Introduction

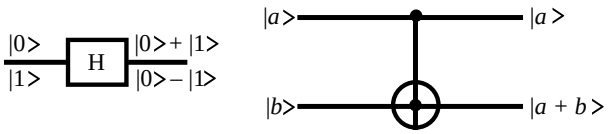
The phenomenon of quantum entanglement, a remarkable feature of quantum theory, was first noticed by Schrödinger (1935) and since then it has baffled generations of physicists. About a decade ago, Deutsch (1985) showed how quantum entanglement in principle allows new types of information processing and thus introduced the concepts of quantum computation and quantum networks. All known methods of quantum computation are applications of entanglement.

Recent progress in quantum complexity theory indicates that the computational power of quantum computers exceeds that of Turing machines, hence the experimental realization of such processes is a most interesting issue (Shor 1994; Ekert & Jozsa 1996). Unfortunately, at the present time it is not clear whether it will be practicable to build physical devices which can perform coherent quantum computations. This notwithstanding, the theoretical study of quantum physics from the point of view of computational complexity may at least be expected to shed new light on the foundations of quantum theory. On the experimental side, the current challenge is not to build a full quantum computer right away but rather to move from the experiments in which we merely observe quantum interference and entanglement to experiments in which we can *control* these quantum phenomena.

In this paper we describe how, with simple quantum logic gates and a handful of qubits, we can control and manipulate quantum entanglement. Here, and in the following, a *qubit* means a generic two-state quantum system with a chosen 'computational basis' $\{|0\rangle, |1\rangle\}$ (e.g. two-level atom, spin-$\frac{1}{2}$ particle, etc.) and a *quantum logic gate* is an elementary device which performs a fixed unitary operation on selected qubits in a fixed period of time (Barenco *et al.* 1995*b*). Single-qubit quantum logic

† Present address: Institute for Scientific Interchange Foundation, Villa Gualino, Viale Settimio Severo 65, I-10133 Torino, Italy.

Phil. Trans. R. Soc. Lond. A (1997) **355**, 2259–2266
Printed in Great Britain



The Hadamard gate Quantum Controlled-NOT

Figure 1. Graphical representations of **H** and the quantum controlled-NOT gates. Here, $a + b$ denotes addition modulo 2.

gates are rather trivial and can be implemented, for example, by exciting selected atomic transitions with laser pulses of controllable frequency, intensity and duration.

We will frequently use a simple gate **H** which prepares equally weighted superpositions of the two basis states $|0\rangle$ and $|1\rangle$:

$$|0\rangle \rightarrow (1/\sqrt{2})(|0\rangle + |1\rangle), \tag{1.1}$$

$$|1\rangle \rightarrow (1/\sqrt{2})(|0\rangle - |1\rangle). \tag{1.2}$$

Non-trivial quantum logic gates, operating on two or more qubits, require a *conditional quantum dynamics*, in which one subsystem undergoes a coherent evolution that depends on the quantum state of another subsystem. The unitary evolution operator for the combined system has the form

$$U = |0\rangle\langle 0| \otimes U_0 + |1\rangle\langle 1| \otimes U_1 + \cdots + |k\rangle\langle k| \otimes U_k, \tag{1.3}$$

where the projectors refer to quantum states of the *control* subsystem and the unitary operations U_i are performed on the *target* subsystem. The conditional dynamics are much more difficult to implement; however, first experimental steps towards implementation of quantum control gates have already been reported.

The simplest non-trivial operation of this sort is the *quantum controlled-NOT*, a gate operating on two qubits, for which $U_0 = \mathbf{1}$ and $U_1 = |0\rangle\langle 1| + |1\rangle\langle 0|$. In the computational basis, the value of the target qubit is negated iff the control qubit has logical value 1, the logical value of the control qubit does not change. This is described in the following equations, in which the first ket represents the control bit and the second ket represents the target bit:

$$|0\rangle|0\rangle \rightarrow |0\rangle|0\rangle, \tag{1.4}$$

$$|0\rangle|1\rangle \rightarrow |0\rangle|1\rangle, \tag{1.5}$$

$$|1\rangle|0\rangle \rightarrow |1\rangle|1\rangle, \tag{1.6}$$

$$|1\rangle|1\rangle \rightarrow |1\rangle|0\rangle. \tag{1.7}$$

It is very convenient to use graphical representations of quantum logic gates. Figure 1 shows diagrams of a single-qubit gate **H**, also known as the Hadamard gate, and the quantum controlled-NOT.

The quantum controlled-NOT gate has a variety of interesting properties and applications and in the following we will describe some of them.

2. Quantum measurements

The quantum controlled-NOT gate transforms superpositions into entanglements

$$(\alpha|0\rangle + \beta|1\rangle)|0\rangle \leftrightarrow \alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle. \tag{2.1}$$

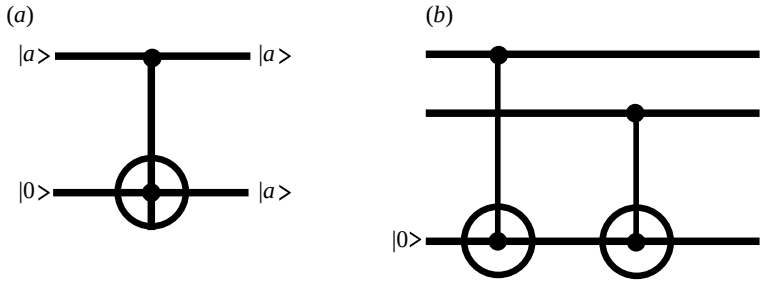


Figure 2. (*a*) Quantum controlled-NOT effecting a quantum 'non-demolition' measurement. (*b*) Quantum 'non-demolition' projection on two orthogonal subspaces spanned by $\{|01\rangle, |10\rangle\}$ and $\{|00\rangle, |11\rangle\}$.

Thus it acts as a *measurement gate* because if the target qubit is initially in state $|0\rangle$, then this qubit, together with the gate, amount to an apparatus that performs a perfectly accurate non-perturbing (quantum non-demolition) measurement (von Neumann 1932; Braginsky *et al.* 1977) of an observable pertaining to the control qubit whose eigenvectors coincide with $|0\rangle$ and $|1\rangle$. Clearly, any other single-qubit observable with eigenvectors $|u\rangle$ and $|v\rangle$ can be measured in the same way by applying to the control qubit a compensating single-qubit operation which maps $|u\rangle \rightarrow |0\rangle$ and $|v\rangle \rightarrow |1\rangle$, followed by the controlled-NOT.

For two or more qubits, networks composed of the controlled-NOT gates can effect 'quantum non-demolition' projections on selected subspaces. Consider, for example, the four-dimensional Hilbert space of two qubits spanned by the four basis vectors $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ and a projection on the subspace spanned by the vectors $\{|01\rangle, |10\rangle\}$. The projection can be 'constructed' out of two controlled-NOT gates as shown in figure 2*b*, followed by the measurement performed on the third, auxiliary, qubit which acts as a probe.

Much more interesting projections are those which involve projecting on entangled states. Networks of the quantum controlled-NOT gates can both prepare highly entangled quantum states and project on them by applying the same controlled-NOT operations but in reversed order. For example, the network shown in figure 3*a* prepares two qubits in one of the four maximally entangled Bell states and the reversed quantum network can be used to implement the so-called *Bell measurement* (Barenco *et al.* 1995*a*) on the two qubits by disentangling the Bell states

$$|0\rangle|0\rangle \rightarrow (1/\sqrt{2})(|0\rangle|0\rangle + |1\rangle|1\rangle), \tag{2.2}$$

$$|1\rangle|0\rangle \rightarrow (1/\sqrt{2})(|0\rangle|0\rangle - |1\rangle|1\rangle), \tag{2.3}$$

$$|0\rangle|1\rangle \rightarrow (1/\sqrt{2})(|0\rangle|1\rangle + |1\rangle|0\rangle), \tag{2.4}$$

$$|1\rangle|1\rangle \rightarrow (1/\sqrt{2})(|0\rangle|1\rangle - |1\rangle|0\rangle). \tag{2.5}$$

In this way, the Bell measurement is reduced to two single-particle measurements. The method can be easily extended to a three-qubit case. Figure 3*b* shows how to prepare eight maximally entangled three-particle states, known as the Greenberger–Horne–Zeilinger (GHZ) states (Greenberger *et al.* 1989, 1990; see also Mermin 1990). Reversing the preparation procedure we obtain the unitary transformation which reduces the GHZ measurement to the three single-particle measurements.

We can write this in the following compact form, where a and b can each take the values 0 and 1 and $\bar{a}$ and $\bar{b}$ denote NOT-a and NOT-b, respectively:

$$|0\rangle|a\rangle|b\rangle \leftrightarrow (1/\sqrt{2})(|0\rangle|a\rangle|b\rangle + |1\rangle|\bar{a}\rangle|\bar{b}\rangle), \tag{2.6}$$

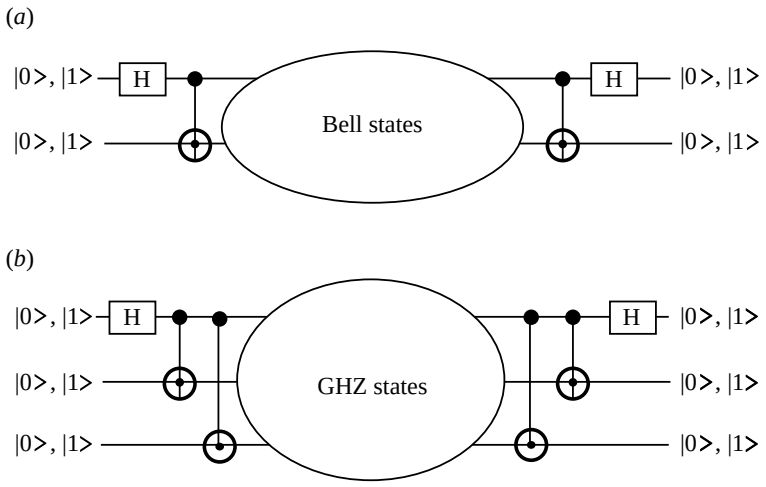


Figure 3. (*a*) The Bell measurement: the gates on the left-hand side allow us to generate the four Bell states from the four possible different inputs. Reversing the order of the gates (right-hand side of the diagram) corresponds to a Bell measurement. (*b*) GHZ measurement: the same as in (*a*) for the eight GHZ states.

$$|1\rangle|a\rangle|b\rangle \leftrightarrow (1/\sqrt{2})(|0\rangle|a\rangle|b\rangle - |1\rangle|\bar{a}\rangle|\bar{b}\rangle). \tag{2.7}$$

Let us also mention that the GHZ measurement provides an interesting possibility of labeling the GHZ states via the corresponding binary output. The three output bits then have the following meanings.

(i) The first output bit tells us whether the number of $|0'\rangle$s in the GHZ state, written in the conjugate basis (this is given by $|0'\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$ and $|1'\rangle = (1/\sqrt{2})(|0\rangle - |1\rangle)$), is even or odd. If the first output bit is $|0\rangle$, there is an odd number of $|0'\rangle$s in the conjugate basis, otherwise an even number.

(ii) The second output bit indicates whether the first two bits in the GHZ superposition are the same or different. If the second output bit is $|0\rangle$, they are the same.

(iii) The third output bit provides the same information with respect to the first and third bit of the GHZ superposition.

We hope to elaborate on this in a forthcoming paper.

The Bell measurement is essential for quantum dense coding (Bennett & Wiesner 1992) and for quantum teleportation (Bennett *et al.* 1993); the GHZ measurement allows to generalize the two- to the three-particle case. In general, *'any measurement on any number of qubits can be implemented using only single-qubit operations and the quantum controlled-NOT gates'*.

This follows from the fact that the quantum controlled-NOT gate, together with relatively trivial single-qubit operations, forms an adequate set of quantum gates, i.e. the set from which any unitary operation may be built (Barenco *et al.* 1995*b*). Thus if we want to measure observable A pertaining to n qubits, we construct a compensating unitary transformation U which maps 2^n states of the form $|a_1\rangle|a_2\rangle \ldots |a_n\rangle$, where $a_i = 0, 1$, into the eigenstates of A. This allows both to prepare the eigenstates of A, which in general can be highly entangled, and to reduce the measurement described by A to n simple, single-qubit measurements. (Note: the statement is also

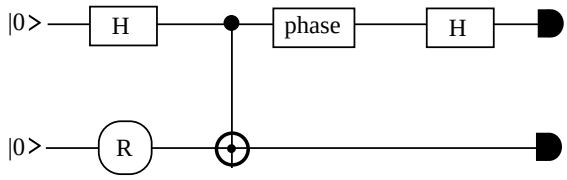


Figure 4. C-NOT simulating decoherence and destroying single-particle interference. The combined effect of a continuous rotation of the second qubit followed by an ideal C-NOT operation is equivalent to the incomplete C-NOT gate analysed in the text.

true for non-orthogonal, POVM measurements because all non-orthogonal measurements are implemented as regular, von Neumann-type measurements on extended systems (Peres 1993).)

At this stage one may get the impression that the quantum controlled-NOT gate is a very special gate. It is not. In fact, almost any non-trivial gate operating on two qubits is universal (Deutsch *et al.* 1995; see also Lloyd 1995).

3. Manipulation of quantum entanglement

Quantum entanglement can be held responsible for destroying single-particle interference. Consider, for example, the network shown in figure 4.

Here, we first prepare the control qubit in a superposition of $|0\rangle$ and $|1\rangle$ and then we entangle it with the target qubit via the controlled-NOT gate. Let us assume that the controlled-NOT gate does not completely flop the target qubit, i.e. instead of $|0\rangle \rightarrow |1\rangle$ and $|1\rangle \rightarrow |0\rangle$, it performs

$$|0\rangle \rightarrow \alpha|0\rangle + \beta|1\rangle, \quad |1\rangle \rightarrow \beta|0\rangle - \alpha|1\rangle, \tag{3.1}$$

where α and β are taken to be real. Here, β parametrizes the degree of entanglement: $\beta = 1$, $\alpha = 0$ corresponds to the controlled-NOT gate, i.e. complete entanglement. (Performing a continuous rotation on the second qubit before a perfect controlled-NOT gate leads to a result which is equivalent to this 'incomplete' controlled-NOT gate.)

Thus the state at the output of the network can be written as

$$\tfrac{1}{2}[((1+\alpha e^{i\phi})|0\rangle + (1-\alpha e^{i\phi})|1\rangle)|0\rangle + \beta e^{i\phi}(|0\rangle - |1\rangle)|1\rangle]. \tag{3.2}$$

The probability of observing 0 or 1 on the control qubit at the output oscillates with ϕ, e.g. if α is chosen to be real, then

$$P_0(\phi) = \tfrac{1}{2}(1 + \alpha\cos\phi). \tag{3.3}$$

The single-particle interference pattern is washed out by an increasing entanglement with the auxiliary qubit. The reduced density operator of the control qubit right before the second gate **H** is given by $\frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1| + \alpha e^{-i\phi}|0\rangle\langle 1| + \alpha e^{i\phi}|1\rangle\langle 0|)$. The entanglement with the auxiliary qubit can be quantified by $1 - |\alpha|^2$. When the entanglement increases, i.e. $|\alpha|$ decreases, so does the modulus of the off-diagonal elements which effectively leads to decoherence of the control qubit. This simple network can be viewed either as simulating decoherence of the control qubit by a tunable entanglement with the target qubit, or as an illustration of the trade-off between the single-particle interference and the two-particle interference due to the entanglement, or as an illustration of the back-action of the measuring apparatus which performs the 'QND' measurement of the bit values but messes up the phase, and this is why the single-particle interference disappears.

Figure 5

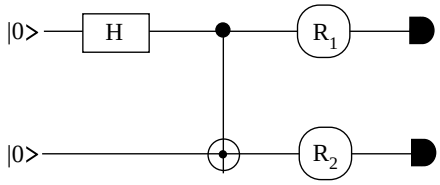


Figure 6

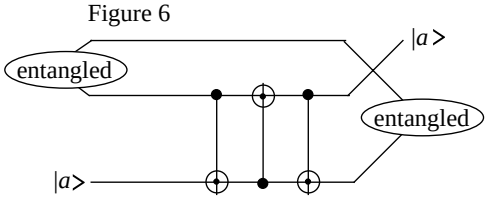


Figure 5. Testing Bell's inequalities with a tunable source of entanglement. The measurements are supposed to be instantaneous which ensures the spacelike separation of detection events.
Figure 6. Transferring quantum entanglement from A and B to A and C.

In addition, the fact that we can have a 'tunable' source of correlated particles offers an interesting possibility for new tests of the Bell inequality (Bell 1964).

For that, the previous arrangement has to be modified to the one sketched in figure 5, where the additional rotations play the role of the polarization analysers in conventional tests (Selleri 1988; Mandel 1995). Using state-selective detectors, such a set-up may allow us to test the CHSH form of the Bell inequality (Clauser *et al.* 1969). Note that as the degree of correlation is tunable, ranging from totally uncorrelated to maximally entangled particles, it would be possible to monitor the transition between the classically allowed and the non-local quantum correlation domain.

Quantum entanglement can be regarded as a precious resource, e.g. for secure communication and for computation, so it is important to be able to transfer it from one pair of qubits to another and to regenerate it if necessary.

Suppose we have three qubits A, B, and C; A and B are entangled and C is in some quantum state of its own, not necessarily pure, but we assume that C is entangled neither with A nor with B. If we cascade three quantum controlled-NOT gates and apply them to qubits B and C so that the first gate takes qubit B as the control and qubit C as the target, the second gate takes C as the control and B as the target, and the third gate repeats the action of the first gate, then we effectively transfer the entanglement from A and B to A and C, and qubit B acquires the initial state of C. We have thus swapped the qubits B and C. The corresponding network is shown in figure 6 (see Barenco *et al.* (1995*a*) for state transfer and Zukowski *et al.* (1993) for entanglement swapping).

While transferring quantum entanglement between qubits, we may want to improve the degree of entanglement of one partially entangled pair of qubits by transferring some entanglement from another partially entangled pair of qubits. If pair A and B contains more quantum entanglement than pair C and D, then in order to boost the entanglement of C and D we can just swap the entanglement between the pairs by extending the transfer procedure described above; we simply apply the three cascaded controlled-NOT gates to qubits A and C, and to B and D. But what if qubits A and B contain not more entanglement than C and D? It turns out that in some cases one can still improve the entanglement of C and D by adopting the entanglement purification (Bennett *et al.* 1993) or the quantum privacy amplification procedure (Deutsch *et al.* 1996).

Maximally entangled states have several interesting invariant properties under single qubit unitary operations. Some of them are now being studied in connection with the new, rapidly developing area of quantum error correction (Shor 1995; Ekert & Macchiavello 1996; Steane 1996).

4. Concluding remarks

In this paper we have described several quantum measurements and entanglement manipulations in terms of quantum networks. This 'higher-level description' is very useful—it allows us to view more complex experiments as networks of quantum logic gates. Such a 'reductionist' approach also helps to design new experiments.

While discussing what can be achieved with two or three qubits and few quantum controlled-NOT gates, we have generalized the Bell measurement to three or more qubits (e.g. the GHZ measurement) and we have suggested a simple transfer of quantum entanglement between three qubits.

We hope that the entanglement manipulation of this kind will soon become a standard experimental technique and will lead to implementing more sophisticated quantum data processing.

This work was supported in part by the European TMR Research Network ERP-4061PL95-1412, Hewlett-Packard, Elsag–Bailey and The Royal Society, London. S.F.H. acknowledges support from DGICYT project no. PB-95-0594 (Spain).

References

Barenco, A., Deutsch, D., Ekert, A. & Jozsa, R. 1995*a* Conditional quantum dynamics and logic gates. *Phys. Rev. Lett.* **74**, 4083.

Barenco, A., Bennett, C. H., Cleve, R., DiVincenzo, D. P., Margolus, N., Shor, P., Sleator, T., Smolin, J. & Weinfurter, H. 1995*b* Elementary gates for quantum computation. *Phys. Rev.* A **52**, 3457–3467.

Bell, J. S. 1964 On the Einstein–Podolsky–Rosen paradox. *Physics* **1**, 195–200.

Bennett, C. H. & Wiesner, S. 1992 Communication via one- and two-particle operators on Einstein–Podolsky–Rosen states. *Phys. Rev. Lett.* **69**, 2881.

Bennett, C. H., Brassard, G., Popescu, S., Schumacher, B., Smolin, J. & Wootters, W. K. 1993 Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels. *Phys. Rev. Lett.* **76**, 722.

Braginsky V. B., Vorontsov, Yu. I. & Khalili, F. Ya. 1977 *Eksp. Theo. Fiz.* **73**, 1340. (Engl. transl. 1977 *Sov. Phys. JETP* **46**, 705.)

Clauser, J. F., Horne, M. A., Shimony, A. & Holt, R. A. 1969 *Phys. Rev. Lett.* **23**, 880.

Deutsch, D. 1985 Quantum theory, the Church–Turing principle and the universal quantum computer. *Proc. R. Soc. Lond.* A **400**, 97.

Deutsch, D., Barenco, A. & Ekert, A. 1995 Universality in quantum computation. *Proc. R. Soc. Lond.* A **449**, 669–677.

Deutsch, D., Ekert, A., Jozsa, R., Macchiavello, C., Popescu, S. & Sanpera, A. 1996 Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Phys. Rev. Lett.* **77**, 2818–2821.

Ekert, A. & Jozsa, R. 1996 Quantum computation and Shor's factoring algorithm. *Rev. Mod. Phys.* **68**, 733–753.

Ekert, A. & Macchiavello, C. 1996 Quantum error-correction for communication. *Phys. Rev. Lett.* **77**, 2585–2588.

Greenberger, D. M., Horne, M. & Zeilinger, A. 1989 Going beyond Bell's theorem. In *Bell's theorem, quantum theory, and conceptions of the universe* (ed. M. Kafatos), pp. 69–72. Dordrecht: Kluwer.

Greenberger, D. M., Horne, M., Shimony, A. & Zeilinger, A. 1990 Bell's theorem without inequalities. *Am. J. Phys.* **58**, 1131–1143.

Lloyd, S. 1995 Almost any quantum logic gate is universal. *Phys. Rev. Lett.* **75**, 346.

Mandel, L. 1995 Two-photon downconversion experiments. *Ann. NY Acad. Sci.* **755**, 1 (and references therein).

Mermin, N. D. 1990 Quantum mysteries revisited. *Am. J. Phys.* **58**, 8.

Peres, A. 1993 *Quantum theory: concepts and methods*. Dordrecht: Kluwer.

Schrödinger, E. 1935 Die gegenwärtige Situation in der Quantenmechanik. *Naturwissenschaften* **23**, 807–812. (Engl. transl. 1980 The present situation in quantum mechanics. *Proc. Am. Phil. Soc.* **124**, 323–338.)

Selleri, F. (ed.) 1988 *Quantum mechanics versus local realism*. New York: Plenum.

Shor, P. 1994 In *Proc. 35th Ann. Symp. on the Foundations of Computer Science* (ed. S. Goldwasser), p. 124. Los Alamitos, CA: IEEE Computer Society Press.

Shor, P. 1995 Scheme for reducing decoherence in quantum computer memory. *Phys. Rev.* A **52**, R2493.

Steane, A. 1996 Error correction codes in quantum theory. *Phys. Rev. Lett.* **77**, 793.

Vedral, V., Barenco, A. & Ekert, A. 1996 Quantum networks for elementary arithmetic operations. *Phys. Rev.* A **54**, 147–153.

von Neumann, J. 1932 *Mathematische Grundlagen der Quantenmechanik*. Springer. (Engl. transl. Beyer, E. T. 1955 *Mathematical foundations of quantum mechanics*. Princeton University Press.)

Zukowski, M., Zeilinger, A., Horne, M. & Ekert, A. 1993 'Event-ready detectors' Bell experiment via entanglement swapping. *Phys. Rev. Lett.* **71**, 4287–4290.