On the symmetry of logic

1995 J. Phys. A: Math. Gen. 28 5623

(http://iopscience.iop.org/0305-4470/28/19/016)

J. Phys. A: Math. Gen. **28** (1995) 5623–5631. Printed in the UK

On the symmetry of logic

Martin R Rayner† and Douglas J Newman
Department of Physics, University of Southampton, Highfield, Southampton, SO17 1BJ, UK

Received 30 March 1995

Abstract. Embedding logical operations in non-dissipative physical processes requires the use of reversible logic. Following Feynman's approach, the sixteen distinct truth tables of classical logic are shown to be contained in the 8! reversible logic operations covered by the symmetric group S_8, which permute the eight values of three logical variables. Small subgroups of S_8 are shown to cover, respectively, reversible logic, reversible switching and reversible arithmetic. A new universal primitive is found which generates a covering group of reversible logic. It is shown that the octahedral group in four dimensions covers both reversible logic and switching and, hence, that the orthogonal group O(4) provides a covering group for quantum gates.

1. Introduction

Computers are based on *logical* operations, such as AND and OR, which act upon Boolean, or logical, variables which take the value one ($\equiv true$) or zero ($\equiv false$). These operations are frequently expressed in terms of *truth tables* which determine the value of one output variable in relation to the values of two input variables. There are just sixteen distinct truth tables of this type. We shall refer to the physical realizations of truth tables as *gates*. Connections between gates, which transmit the values of logical variables, will be referred to as *wires*. It is usual to describe computer architecture in terms of a series of connected gates which are supposed to operate sequentially. Such a computer has a definite number of *input* and *output* wires.

Gates which emulate truth tables are not reversible; they lose one bit of information per operation. Thermodynamically, this corresponds to a loss of at least $kT \ln 2$ in heat energy in each operation (Landauer [1], Feynman [2]). As Feynman points out, such quantities of energy are trivial compared with the actual amounts of energy dissipated in even the most miniaturized solid-state logic gates. Nevertheless, an important principle is involved, for it shows that a network of conventional logic gates cannot be embedded in a *lossless* dynamical process, whether this be described in terms of classical or quantum mechanics.

It has frequently been pointed out, e.g. by Bennett [3], Feynman [2], Benioff [4–6], Peres [7], Fredkin and Toffoli [8], that it is possible to design a lossless dynamical computer using the operations of *reversible logic*, in which no information is lost and no heat is dissipated during each operation. Such computers have an equal number of input and output wires. The operations of reversible logic can be expressed as *permutations* of the possible values of sets of logical variables. While ordinary digital logic is clearly appropriate for problems in which a single numerical or logical result, such as an average, is required, reversible logic

† In memoriam: this work is based on a final year project report by the first author, who subsequently died in a climbing accident on Ben Nevis in February 1995.

0305-4470/95/195623+09$19.50

is more appropriate for parallel information processing and the simulation of dynamical systems.

An N-input *reversible computer* permutes the set of all the 2^N possible values of its input logical variables to provide its 2^N possible outputs. While such a process can be envisaged as taking place in a single time step it can, in practice, be carried out sequentially in several time steps by combining operations in subsystems of the reversible computer. In order to be embedded in a lossless dynamical process, each of these subsystems must also *operate reversibly*.

The 'standard problem' of classical digital logic is to find a way of expressing an arbitrary logical function of N variables as a sequence of operations, each of which can be carried by a single logical gate, with two inputs and one output. In the case of reversible logic, the standard problem is to find a systematic method of reducing a specified operation, acting upon N variables, to a succession of operations acting upon $n \ll N$ subsystem variables at a time.

There is a considerable literature [2, 4–8] on the relationship between the truth-table formulation of classical logic and the reversible operations into which it can be embedded. The basic result, on which both the existing literature and the following discussion are based, is that *permutations of the values of at least three logical variables are required to express all of the 16 possible truth tables of classical logic.* Hence, in terms of the above notation, the minimum value of n is three; each reversible gate has three input and three output wires. The permutation operators (which characterize gates) act on the components of eight-dimensional vectors, formed from the outer product of three two-dimensional vectors. Each of these two-dimensional vectors expresses the truth value of a single logical variable in the form $[1, 0] \equiv true$, or $[0, 1] \equiv false$. It follows that the eight-dimensional vectors are all in a *standard form*, in which seven elements are zero and the remaining element is unity. The position of the unit element specifies the simultaneous truth values of all three logical variables.

The physical realization of reversible operations on three logical variables will be called *reversible gates.* The operation of reversible gates can be expressed in the form of 8×8 *permutation matrices* which, by their construction, keep the eight-dimensional vectors in standard form. It is convenient to represent permutation operators in standard cyclic notation, using the labels $0, 1, \ldots, 7$ to denote the eight distinct basis vectors according to their binary value. For example, the label $3 \equiv 110$ denotes $[0, 0, 0, 1, 0, 0, 0, 0]$. Note that, for easy comparison with the literature, we have written these numbers in the reverse of the usual binary digital order.

Most discussions of reversible gates have centred on their relationship with reversible (i.e. energy conserving) dynamics. In particular, Feynman [2], Benioff [4–6] and Peres [7] have investigated methods of constructing Hamiltonians which describe the time evolution of the logical states of reversible computers. This paper is concerned with the *group theoretical* properties of reversible logic gates, especially in relation to the characterization of reversible computer architecture. It also provides a new group theoretical characterization of quantum gates (Deutsch [9]).

2. Logical primitives and logical groups

Denote the two input variables of a logic gate by a and b and its output variable by c. Writing the four possible values of the logical variables ab in the *standard order* {00, 10, 01, 11} it is possible to express truth tables in terms of the four corresponding values of c. For example, AND is characterized by the values {0001} and OR by {0111}. It will be convenient, in

the following, to characterize the truth tables of the 16 distinct logical functions either by such sets of four binary digits, or by the decimal equivalents of their binary values. Hence, AND $\equiv \{0001\} \equiv \{1\}$ and OR $\equiv \{0111\} \equiv \{7\}$. It is well known that either NAND $\equiv \{1110\} \equiv \{14\}$ or NOR $\equiv \{1000\} \equiv \{8\}$ provide *universal* primitives for classical logic in the sense that gates of just one of these types alone can be combined to produce any logical function. This is significant in relation to the design of hardware for digital circuits.

Analogous universal primitives have been sought for reversible logic. Feynman [2] determined a set of *three* universal primitives which, for a particular choice of arguments, can be expressed in cyclic form as follows.

(i)

$$\mathrm{NOT}(a) \equiv (01)(23)(45)(67)$$

which has the effect of replacing the Boolean variable a by $1 - a$ and leaves b and c unchanged;

(ii)

$$\mathrm{CONTROL}(b) - \mathrm{NOT}(a) \equiv (23)(67)$$

which replaces a by $1 - a$ if $b = 1$, and leaves a unchanged if $b = 0$;

(iii)

$$\mathrm{CONTROL}(c) - \mathrm{CONTROL}(b) - \mathrm{NOT}(a) \equiv (67)$$

which replaces a by $1 - a$ if both $c = 1$ and $b = 1$, and otherwise leaves a unchanged.

Gate (iii) has been proposed as providing a *single* universal primitive by Toffoli [10] on the grounds that, as it contains the truth table for NOR ($a' = b$ NOR c), it can certainly be used to construct all other truth tables. It turns out, however, that this gate, even when combined with wire switching, does not generate all of the 16 truth tables of classical logic without the introduction of additional logical inputs. It is not, therefore, a *universal generator* of reversible logic in the sense used in this paper.

The first result of this paper is derived in the appendix: Feynman's [2] three primitives, taken together with the 'switching' permutations which interchange the variables a, b and c, generate all the elements of the symmetric group S_8. In this sense (i), (ii) and (iii) taken together generate classical logic. We therefore identify S_8 as a *covering group* of reversible logic. Multiplication of elements in S_8 corresponds to the combination of two reversible gates in sequence to form another gate. It is interesting to note that all of the elements in S_8 can be constructed using *only two generators*, i.e. the eight-fold cycle (01234567) and the interchange (67). However, the use of these generators to obtain any particular element of S_8 may require the construction of a very complicated product.

Fredkin and Toffoli [8] have studied the effect of adding the additional constraint that reversible operations should be *bit conserving*, in the sense that only operations that permute the logical triples within either or both of the two sets $[1 = 100, 2 = 010, 4 = 001]$ or $[3 = 110, 5 = 101, 6 = 011]$ are allowed. This, as they demonstrate in their paper, is of particular interest in relation to setting up simple mechanical realizations of reversible logic. Fredkin and Toffoli [8] were able to show that the single primitive 'Fredkin' gate represented by the permutation (12), when taken together with arbitrary wire permutations, is sufficient to generate all possible logical and arithmetical relationships. This is achieved, however, at the expense of using very complicated interconnections between several gates, involving the introduction of more than three logical input variables, to produce all 16 truth tables of classical logic. Hence, for similar reasons to the Toffoli gate, the Fredkin gate does not provide a universal generator of reversible logic.

This article is concerned with finding answers to four related questions.

(1) What is the *minimal covering group* of reversible logic?

(2) Is there a *single* universal generator of reversible logic?

(3) What are the *minimal covering groups* of wire switching and arithmetic?

(4) Are group theoretical considerations relevant to the characterization of quantum gates?

3. Minimal covering groups of reversible logic

Our starting point is the characterization of reversible logic by the 8! elements in S_8 which covers all the distinct permutations a', b', c' of the eight possible triplets a, b, c of the logical variables. The simplest way to embed truth tables in these transformations is to regard a and b as logical input variables and c as a *control* variable. The variable c is assigned the role of selecting sets of four output values from the upper or lower halves of the eight output values of one of a' or b' or c'. It can easily be verified that the constraint $c' = c$ is too strong for all 16 truth tables to be found in the values of a' or b'. With no constraints, each reversible operation produces six (possibly all different) truth tables corresponding to the values of a' or b' or c' for either $c = 0$ or $c = 1$.

Table 1. Permutations of the eight values of the three logical variables (a, b, c), corresponding to the four elements of the group $G_4(I)$. All sixteen distinct truth tables appear in the 24 columns of four values corresponding to the choices $c = 0$, $c = 1$ in the column headed E. The last two rows identify the truth tables appearing in the column above.

$G_4(I)$	E	$A = (07)$	$B = (34)$	$C = (07)(34)$
0	000	111	000	111
1	100	100	100	100
2	010	010	010	010
3	110	110	001	001
4	001	001	110	110
5	101	101	101	101
6	011	011	011	011
7	111	000	111	000
$c = 0$	10, 12, 0	11, 13, 1	2, 4, 8	3, 5, 9
$c = 1$	10, 12, 15	2, 4, 7	11, 13, 14	3, 5, 6

Given that the original array, corresponding to the identity, defines four distinct truth tables, the smallest possible covering group would contain just two elements in addition to the identity. Each of the elements of this group would be required to produce six distinct truth tables, giving the required total of 16. Such a group, which would necessarily have a single generator and, hence, just one primitive, has not been found. We have, nevertheless, found two distinct groups of order four which reproduce all 16 truth tables, as is demonstrated in tables 1, 2 and 3. These groups provide alternative *minimal covering groups of reversible logic*. In terms of permutations they are given by

$$G_4(I) = [E, (07), (34), (07)(34)] = [E, (07)] \otimes [E, (34)]$$

and

$$G_4(II) = [E, (0374), (0473), (07)(34)]$$

where E denotes the identity operation. The generators of $G_4(I)$ are the permutations (07) and (34). $G_4(II)$ is a four element *cyclic* covering group of reversible logic. This group

Table 2. Permutations of the eight values of the three logical variables (a, b, c), corresponding to the four elements of the group $G_4(II)$. All sixteen distinct truth tables appear in the 24 columns of four values corresponding to the choices $c = 0$, $c = 1$ in the column headed E.

$G_4(II)$	E	$A = (0374)$	$B = (0473)$	$C = (07)(34)$
0	000	001	110	111
1	100	100	100	100
2	010	010	010	010
3	110	000	111	001
4	001	111	000	110
5	101	101	101	101
6	011	011	011	011
7	111	110	001	000

Table 3. Appearance of the truth tables, designated $\{n\}$, in the groups of reversible logic operations $G_4(I)$ and $G_4(II)$. $c = 0$ corresponds to the rows 0–3, and $c = 1$ to rows 4–7 in tables 1 and 2. All truth tables appear either once or twice. Subscripts a, b, c indicate which column corresponds to the indicated truth table.

	$G_4(I)$	$G_4(II)$
{0}	$E_c(c=0)$	$E_c(c=0)$
{1}	$A_c(c=0)$	$A_c(c=0)$
{2}	$A_a(c=1), B_a(c=0)$	$A_a(c=0), B_a(c=1)$
{3}	$C_a(c=0), C_a(c=1)$	$C_a(c=0), C_a(c=1)$
{4}	$A_a(c=1), B_a(c=0)$	$A_a(c=0), B_a(c=1)$
{5}	$C_b(c=0), C_b(c=1)$	$C_b(c=0), C_b(c=1)$
{6}	$C_c(c=1)$	$C_c(c=1)$
{7}	$A_c(c=1)$	$A_c(c=1)$
{8}	$B_c(c=0)$	$B_c(c=0)$
{9}	$C_c(c=0)$	$C_c(c=0)$
{10}	$E_a(c=0), E_a(c=1)$	$E_a(c=0), E_a(c=1)$
{11}	$A_a(c=0), B_a(c=1)$	$A_a(c=1), B_a(c=0)$
{12}	$E_b(c=0), E_b(c=1)$	$E_b(c=0), E_b(c=1)$
{13}	$A_b(c=0), B_b(c=1)$	$A_b(c=1), B_b(c=0)$
{14}	$B_c(c=1)$	$B_c(c=1)$
{15}	$E_c(c=1)$	$E_c(c=1)$

can be generated with either (0374) or (0473), either of which, therefore, provides a *single universal generator of reversible logic.*

Several groups of order six have been found which embed all sixteen truth tables. Examples are

$$G_6(I) = \{E, (07)(12), (07)(14), (07)(24), (124), (142)\}$$
$$G_6(II) = \{E, (07)(35), (07)(36), (07)(56), (365), (356)\}$$

and

$$G_6(III) = \{E, (236), (263)\} \otimes \{E, (07)\}.$$

Each of these groups clearly requires a minimum of two generators.

4. Switching

In addition to the logical operations, it is necessary to be able to interchange, or switch, the relative positions of the input and output wires which interconnect the reversible gates; this corresponds to interchanging the variables a, b, c. Most authors [2, 4–6] have considered only *feed-through gates* which have separate input and output lines. In this case switching can be achieved simply by interchanging the wiring which connects the different gates, so there is little point in considering its implementation by the gates themselves. However, in the construction of array processors it is natural to use *sequential response gates* where the outputs appear, in the next time step, on the same three wires as the inputs. In this case it is appropriate to implement wire interchanges as an internal function of the gates.

Including the identity, there are *six switching operations* which can be represented as permuting the three inputs a, b, c, or as acting upon the eight logical variables $0, \ldots, 7$. They form the group

$$\begin{aligned} G_6(SW) &= [E, (ab), (ac), (bc), (abc), (acb)] \\ &= [E, (12)(56), (14)(36), (24)(35), (124)(365), (142)(356)]. \end{aligned}$$

This group requires a minimum of two generators; for example, the wire interchange operations (12)(56) and (24)(35). It is, of course, a subgroup of S_8; taken together with Feynman's three primitives, in the appendix it is shown to generate S_8. This choice of five generators has the advantage that it allows the construction of all logical and switching operations using relatively simple combinations.

We now seek to find the minimal covering group of reversible logic that also contains the switching group $G_6(SW)$ as a subgroup. Simply combining the permutations of $G_6(SW)$ with those of $G_4(I)$ or $G_4(II)$ can be shown to generate groups with 96 elements. This is because the operation (34) does not commute with the generator (24)(35) of $G_6(SW)$. Note, however, that the group G_{96} formed by combining $G_4(II)$ with $G_6(SW)$ requires only three generators, namely (12)(56), (14)(36) and (0374).

We have also discovered two 36 element covering groups of reversible logic *and* switching. These are

$$\begin{aligned} G_{36}(I) &= [\{E, (124), (142)\} \otimes \{E, (356), (365)\}, \{(12), (24), (14)\} \otimes \{(35), (36), (56)\}] \\ &\quad \otimes [E, (07)] \\ &= [S_3(1, 2, 4) \otimes S_3(3, 5, 6)]_{EVEN} \otimes [E, (07)] \end{aligned}$$

where $S_3(i, j, k)$ denotes the symmetric group based on permutations of i, j, k and

$$G_{36}(II) = G_6(I) \otimes G_6(II)$$

where $G_6(I)$ and $G_6(II)$ are as defined above. A systematic search has not revealed any covering groups which have a smaller number of elements. We therefore assert that these are *minimal* covering groups of reversible logic and switching. Both $G_{36}(I)$ and $G_{36}(II)$ have four generators. For $G_{36}(I)$ these are (07), (24)(35), (14)(36) and (14)(35). The generators of $G_{36}(II)$ comprise the four products of the generators of $G_6(I)$ and $G_6(II)$.

5. Reversible arithmetic

In applications of classical logic to computer design it is usual to construct arithmetical gates as combinations of logical gates. This is usually done by first constructing *half-adders* in terms of logical gates. Two half-adders are then combined with a NOT gate to form a *full-adder*. Although a full-adder relates three input variables to two output variables

it cannot be embedded into any reversible gate. Half-adders combine two binary digits to provide both their binary *sum*, corresponding to the truth function {6} = {0110}, and a *carry* digit corresponding to {8} = {0001}. It can easily be verified that either of the operations (25)(36) and (236) contain both of these truth tables. Of these, (25)(36) is by far the most interesting as it contains the carry of the binary sums of all three input digits in the b' column and their sum digit in the a' column for $c = 0$ and in the c' column for $c = 1$ (see table 4). In other words it carries out the function of a *full-adder*, except that the first digit of the output can be in either of the two columns a' and c'.

Table 4. A reversible half-adder. In the case $c = 0$, a' is the first digit of the sum $a + b$ $(= a+b+c)$, and b' is the carry digit. In the case $c = 1$, c' is the first digit of the sum $a+b+c$ and b' (again) is the carry digit.

	E	(25)(36)
	abc	$a'b'c'$
0	000	000
1	100	100
2	010	101
3	110	011
4	001	001
5	101	010
6	011	110
7	111	111

None of the covering groups of reversible logic and switching that have already been discussed (apart from S_8 itself) contain operations that produce both {6} and {8} on single output wires. Nevertheless, the fact that the operations (25)(36) and (236) certainly appear in S_8 leads to the question as to whether a subgroup can be found which covers both logic and half-adders. A six element group which satisfies this criterion is

$$G_6(\mathrm{HA}) = \{E, (07)\} \otimes \{E, (236), (263)\}.$$

This group has two generators, i.e. (07) and (236). The smallest covering group which contains both logic and the half-adder (25)(36) is the eight element Abelian group with three generators

$$G_8(\mathrm{HA}) = \{E, (07)\} \otimes \{E, (25)\} \otimes \{E, (36)\}.$$

Because of the need to incorporate a carry operation which involves a feedback loop, arithmetic can only be properly expressed in terms of a time-ordered sequence of operations. Hence, a full analysis of reversible arithmetic requires the development of computer architectures involving feed-through gates operating in time-ordered sequences. We shall not pursue this topic further in the present work.

6. Embedding in continuous groups and the characterization of quantum gates

Baake *et al* [11] have shown that the 384 elements of the hyperoctahedral group (denoted W_4) can be expressed as permutations of the eight vertices of the four-dimensional generalization of the octahedron. The relationship between these vertices and the eight values of three logical variables is specified by the vertex labelling shown in table 5, where the e_i represent unit vectors in the four-dimensional domain. The operations of the group W_4 correspond to the 4! permutations of the rows of table 5, combined with the 2^4 interchanges

of the two elements in any given row. This group is clearly a subgroup of S_8, and has been shown [11] to be generated by just two elements which, in terms of the labelling of table 5, can be written as (02317546) and (01547623).

Table 5. Numbering of the eight vertices of the hyperoctahedron.

$e_1 : 0$	$-e_1 : 7$
$e_2 : 1$	$-e_2 : 6$
$e_3 : 2$	$-e_3 : 5$
$e_4 : 3$	$-e_4 : 4$

For a given subgroup of S_8 to be a subgroup of W_4, each of its elements must conform to the S_8 cycle structure of some element of W_4. The groups G_4(I), G_4(II), G_6(SW) and G_8(HA) satisfy this criterion. However, G_6(I), G_6(II), G_6(III) and G_6(HA) do not satisfy this criterion because they include elements of order three consisting of a single three-fold cycle of S_8, while all elements of order three of W_4 consist of a pair of three-fold cycles of S_8. Of the groups that do satisfy this criterion, it may be shown that, apart from G_8(HA), their generators are all included in W_4. The element (36) of G_8(HA) is not, however, an element of W_4. The survival of G_4(I), G_4(II), G_6(SW) as subgroups of W_4 implies that the *hyperoctahedral group* W_4 *is a covering group of both reversible logic and switching*. We have not carried out an exhaustive examination of the elements of W_4 to determine whether or not it contains any elements that provide reversible half-adder operations.

Baake *et al* [11] have also shown that the hyperoctahedral group W_4 is a subgroup of the orthogonal group O(4). The identification of W_4 as a covering group of reversible logic and switching shows that O(4) is a *continuous group* that contains all these operations. Hence, O(4) is a covering group of the quantum logic gates that have been investigated by Deutsch [9] and DiVincenzo [12] and, given this fact, the latter group is identified as a covering group of quantum gates. This improves on the recent finding of DiVincenzo [12] that *two-bit gates are universal for quantum computation* which, in group theoretical terms, corresponds to saying that U(4) is a covering group of quantum gates. Given that O(4) is isomorphic to $SU(2) \otimes SU(2)$, we have the fact that *coordinated pairs of single bit gates are universal for quantum computation*. This way of expressing O(4) suggests that a physical realization of quantum computers could be obtained by using single spin systems coupled only by the action of the gates.

7. Conclusions

The characterization of reversible logic in terms of permutations [2, 10] has been shown to lead to the identification of S_8 as a covering group of reversible logic. In the course of an attempt to obtain a better insight into the underlying group theoretical structure of reversible logic, answers have been obtained for each of the four questions that were posed at the end of section 2.

(1) Two groups of order four, denoted G_4(I) and G_4(II), provide alternative *minimal covering groups* of reversible logic.

(2) The generator (0374) of G_4(II) is identified as a *universal generator* of reversible logic. The use of this generator as the primitive generator in serial reversible computers avoids the complicated wiring constructions that are necessary when using the Toffoli gate (67) and the Fredkin gate (12).

(3) The six element group, denoted G_6(SW), has been shown to cover all wire switching

operations. As is shown in table 4, it is possible to find a group of order two in which the element other than the identity, functions as a half-adder. A group with six elements and two generators, denoted $G_6(C)$, has been found which covers all logical operations as well as the half-adder.

(4) Both $G_4(II)$ and $G_6(SW)$ have been shown to be subgroups of the hyperoctahedral group W_4, which has a minimum of two generators. Given that the orthogonal group O(4) contains W_4 as a subgroup [11], O(4) has been identified as the covering group for quantum gates. We speculate that it is also the *minimal* covering group.

Several interesting questions have not been addressed. For example, nothing has been said about the relationship between the group theoretical characterization of gates and the architecture of complete reversible or quantum computers. The problem of programming reversible and quantum computers is also worth considering.

Acknowledgments

Both authors benefitted from helpful discussions with Ian George and Lee Harrison during the early stages of the development of this project. Very special thanks go to Professor R C King who has been unstinting with his help and advice to the second author (DJN) from the inception, right through to the completion of this work. The second author is also grateful to Dr S F King for his comments on the manuscript.

Appendix

Standard generators of the symmetric groups S_n are the cyclic elements (j, i) for all i not equal to some fixed j. In the case of S_8 it will be convenient to take $j = 7$ and $i = 0, \ldots, 6$. We show that these seven generators can be obtained from the reduced set of five, comprising of Feynman's three generators (01)(23)(45)(67), (23)(67) and (67), and the two generators of the wire switching group $G_6(SW)$, (12)(56) and (14)(36).

(a) (67) is one of Feynman's generators.

(b) (57) = (12)(56) (67) (12)(56).

(c) (37) = (14)(36) (67) (14)(36).

(d) (23) can be obtained as a product of Feynman's generators, i.e. (23) = (23)(67) (67), hence (27) = (23) (37) (23).

(e) (17) = (12)(56) (27) (12)(56).

(f) (01)(45) = (01)(23)(45)(67) (23)(67), so that (07) = (01)(45) (17) (01)(45).

(g) (47) = (14)(36) (17) (14)(36).

References

[1] Landauer R 1961 *IBM J. Res. Dev.* **5** 183
[2] Feynman R P 1986 *Found. Phys.* **16** 507
[3] Bennett C H 1973 *IBM J. Res. Dev.* **17** 525
[4] Benioff P 1980 *J. Stat. Phys.* **22** 563
[5] Benioff P 1982 *Phys. Rev. Lett.* **48** 1581
[6] Benioff P 1982 *J. Stat. Phys.* **29** 515
[7] Peres A 1985 *Phys. Rev.* A **32** 3266
[8] Fredkin E and Toffoli T 1982 *Int. J. Theor. Phys.* **21** 219
[9] Deutsch D 1988 *Proc. R. Soc.* A **425** 73
[10] Toffoli T 1981 *Math. Syst. Theory* **14** 13
[11] Baake M, Gemünden B and Oedingen R 1982 *J. Math. Phys.* **23** 944
[12] DiVincenzo D P 1995 *Phys. Rev.* A **51** 1015