r-Universal reversible logic gates

2004 J. Phys. A: Math. Gen. 37 5815

(http://iopscience.iop.org/0305-4470/37/22/008)

INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND GENERAL

J. Phys. A: Math. Gen. **37** (2004) 5815–5824 PII: S0305-4470(04)73937-2

r-Universal reversible logic gates

A De Vos[1] **and L Storme**[2]

[1] Imec v.z.w., Vakgroep Elektronika and Informatiesystemen, Universiteit Gent, Sint Pietersnieuwstraat 41, B-9000 Gent, Belgium
[2] Vakgroep Zuivere Wiskunde and Computeralgebra, Universiteit Gent, Krijgslaan 281, B-9000 Gent, Belgium

Received 19 December 2003
Published 18 May 2004
Online at stacks.iop.org/JPhysA/37/5815
DOI: 10.1088/0305-4470/37/22/008

Abstract

Reversible logic plays a fundamental role both in ultra-low power electronics and in quantum computing. It is therefore important to know which reversible logic gates can be used as building block for the reversible implementation of an arbitrary boolean function and which cannot.

PACS numbers: 02.10.Ab, 02.20.−a, 03.67.Lx, 84.30.Bv

1. Introduction

Reversible logic plays a fundamental role both in lossless computing [1–8] and in quantum computing [9–13]. Reversible logic circuits exclusively make use of reversible logic gates. Such gates have an equal number of binary inputs and binary outputs. This number is called the width w of the gate. Table 1 gives two examples of the truth table of a reversible gate of width 3. We see that the $2^w = 8$ output rows are a permutation of the 2^w input rows. This fact guarantees that it is possible to calculate backwards. Hence the gate is reversible.

Let $r(w)$ denote the number of different reversible gates of width w:

$$r(w) = (2^w)!.$$

Some of them are universal. We use here the following definition of universality:

Definition 1. *A gate is* universal *if and only if any boolean function* $f(X_1, X_2, \ldots, X_n)$ *can be synthesized by a loop-free combinatorial network built from a finite number of such gates, using each signal* $X_1, X_2, \ldots, X_n$ *at most once as input signal and using an arbitrary finite number of times the constant input signals 0 and 1.*

The definition tacitly assumes that a single variable of the circuit can address several gates. In other words, fan-out is allowed. In reversible circuits, however, fan-outs are not allowed. Therefore we need the notion of r-universality, as introduced by Kerntopf [14] in his so-called definition 7:

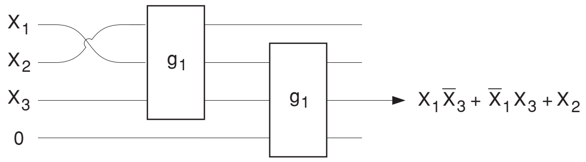

Figure 1. Synthesis of a boolean function by an r-universal reversible gate.

Table 1. Truth tables of two specific reversible gates g_1 and g_2.

(*a*) Reversible gate g_1		(*b*) Reversible gate g_2	
$A_1\ A_2\ A_3$	$P_1\ P_2\ P_3$	$A_1\ A_2\ A_3$	$P_1\ P_2\ P_3$
0 0 0	0 0 0	0 0 0	0 0 0
0 0 1	0 0 1	0 0 1	0 1 0
0 1 0	0 1 0	0 1 0	0 0 1
0 1 1	1 0 0	0 1 1	0 1 1
1 0 0	0 1 1	1 0 0	1 0 0
1 0 1	1 0 1	1 0 1	1 1 0
1 1 0	1 1 0	1 1 0	1 0 1
1 1 1	1 1 1	1 1 1	1 1 1

Definition 2. *A reversible gate is* r-universal *if and only if any boolean function $f(X_1, X_2, \ldots, X_n)$ can be synthesized by a loop-free and fan-out-free combinatorial network built from a finite number of such gates, using each signal $X_1, X_2, \ldots, X_n$ at most once as input signal and using an arbitrary finite number of times the constant input signals 0 and 1.*

An example of an r-universal gate is the gate g_1 of table 1(*a*). Figure 1 shows, e.g., the implementation of the function $f(X_1, X_2, X_3) = X_1\overline{X_3} + \overline{X_1}X_3 + X_2$ (where $\overline{X}$ is a short-hand notation for `NOT` X) by means of two such gates, using each one of the boolean variables X_1, X_2 and X_3 once as input and using the boolean constant 0 as an additional fourth input. Note that not all reversible gates are r-universal. For example, the same function $f(X_1, X_2, X_3)$ cannot be realized with the help of gate g_2, whose truth table is given in table 1(*b*). The reason why table 1(*a*) is r-universal and table 1(*b*) is not will become clear in section 4.

Let $u(w)$ be the number of r-universal reversible gates of width w. Storme *et al* [15] mention that

$$r(3) - u(3) = 1344$$

whereas, according to Kerntopf [14], we have

$$r(4) - u(4) \leqslant 552\,960.$$

Because of $r(3) = 8!$ and $r(4) = 16!$, the two results can be rewritten as

$$u(3) = 38\,976$$

$$20\,922\,789\,335\,040 \leqslant u(4) < 20\,922\,789\,888\,000.$$

The purpose of the present paper is twofold:

- to give a precise value for $u(4)$ and
- to give an analytical expression for $u(w)$, for arbitrary w.

2. Definitions

We remind the reader that any boolean function can be written as a Reed–Muller expansion, i.e. as a XOR of piterms:

$$\begin{aligned} f(A_1, A_2, \ldots, A_w) \\ &= \overbrace{1} \oplus \overbrace{A_1} \oplus \overbrace{A_2} \oplus \cdots \oplus \overbrace{A_w} \oplus \overbrace{A_1 A_2} \oplus \overbrace{A_1 A_3} \oplus \cdots \\ &\oplus \overbrace{A_{w-1} A_w} \oplus \overbrace{A_1 A_2 A_3} \oplus \cdots \oplus \overbrace{A_1 A_2 \ldots A_w} \end{aligned}$$

where $\oplus$ denotes the XOR operation. The overbrace has the following meaning: for any piterm X, the notation $\overbrace{X}$ denotes either X or 0. In other words $\overbrace{X}$ means the piterm X is either present or not. As an example, the function $f(X_1, X_2, X_3)$, written as an OR of ANDs (i.e. $X_1\overline{X_3} + \overline{X_1}X_3 + X_2$) in the previous section, can be written as $f(X_1, X_2, X_3) = X_1 \oplus X_2 \oplus X_3 \oplus X_1X_2 \oplus X_2X_3$.

Definition 3. *A* function $f(A_1, A_2, \ldots, A_n)$ *is* selective *if and only if it equals either some* A_j *or some* $\overline{A_j}$*:*

$$f(A_1, A_2, \ldots, A_n) = \overbrace{1} \oplus A_j$$

where j *obeys* $1 \leqslant j \leqslant n$.

There exist, of course, $2n$ different selective functions of n arguments.

Definition 4. *A* function $f(A_1, A_2, \ldots, A_n)$ *is* linear *if and only if its Reed–Muller expansion contains no terms with two or more letters:*

$$f(A_1, A_2, \ldots, A_n) = \overbrace{1} \oplus \overbrace{A_1} \oplus \overbrace{A_2} \oplus \cdots \oplus \overbrace{A_n}. \tag{1}$$

The reader will easily verify that there exist 2^{n+1} different linear functions of n arguments.

Definition 5. *A* function $f(A_1, A_2, \ldots, A_n)$ *is* monotonic *(or monotone) if and only if its value increases along each climbing path from* $(A_1, A_2, \ldots, A_n) = (0, 0, \ldots, 0)$ *to* $(A_1, A_2, \ldots, A_n) = (1, 1, \ldots, 1)$: $f(A'_1, A'_2, \ldots, A'_n) \geqslant f(A''_1, A''_2, \ldots, A''_n)$ *as soon as* $A'_i \geqslant A''_i$ *for all i satisfying* $1 \leqslant i \leqslant n$.

See also the first part of the appendix. There exists no closed formula for the number of monotonic functions. The subject is a research field in itself [16–18].

With the above three classes of functions, we now construct four classes of reversible gates:

Definition 6. *A* reversible gate *of width* w *is an* exchanger *if and only if each of its* w *functions* $P_i(A_1, A_2, \ldots, A_w)$ *equals some* A_j, *where* j *obeys* $1 \leqslant j \leqslant w$.

The exchangers form a well-known subgroup [15, 19] of the group of reversible gates.

Definition 7. *A* reversible gate *of width* w *is* selective *if and only if each of its* w *functions* $P_i(A_1, A_2, \ldots, A_w)$ *is selective.*

Table 2(*a*) gives an example: the gate with functions $P_1 = A_1$, $P_2 = \overline{A_3}$ and $P_3 = A_2$. The selective gates form a subgroup [15, 19] of the group of reversible gates, as well as a

Table 2. Truth tables of three special reversible gates: a selective reversible gate, a linear reversible gate and a monotonic reversible gate.

(*a*) Selective reversible gate		(*b*) Linear reversible gate		(*c*) Monotonic reversible gate	
$A_1A_2A_3$	$P_1P_2P_3$	$A_1A_2A_3$	$P_1P_2P_3$	$A_1A_2A_3$	$P_1P_2P_3$
0 0 0	0 1 0	0 0 0	0 1 0	0 0 0	0 0 0
0 0 1	0 0 0	0 0 1	0 0 0	0 0 1	1 0 0
0 1 0	0 1 1	0 1 0	0 1 1	0 1 0	0 0 1
0 1 1	0 0 1	0 1 1	0 0 1	0 1 1	1 0 1
1 0 0	1 1 0	1 0 0	1 1 1	1 0 0	0 1 0
1 0 1	1 0 0	1 0 1	1 0 1	1 0 1	1 1 0
1 1 0	1 1 1	1 1 0	1 1 0	1 1 0	0 1 1
1 1 1	1 0 1	1 1 1	1 0 0	1 1 1	1 1 1

supergroup of the group of exchangers. They can be built by cascading inverters (or NOT gates) and exchangers. They correspond precisely to the gates described by Kerntopf [14] as ‘np-equivalent to the identity gate’.

Definition 8. *A* reversible gate *of width w is* linear *if and only if each of its w functions $P_i(A_1, A_2, \ldots, A_w)$ is linear.*

Table 2(*b*) gives an example: the gate with functions $P_1 = A_1$, $P_2 = 1 \oplus A_3$ and $P_3 = A_1 \oplus A_2$. Because each linear function of linear functions is itself a linear function, each cascade of linear reversible gates is itself a linear reversible gate. Therefore, the linear reversible gates form a subgroup of the group of reversible gates.

Definition 9. *A* reversible gate *of width w is* monotonic *if and only if each of its w functions $P_i(A_1, A_2, \ldots, A_w)$ is monotonic.*

Table 2(*c*) gives an example. Because each monotonic function of monotonic functions is itself a monotonic function, the monotonic reversible gates form a subgroup of the group of reversible gates.

We can now mention Kerntopf’s three theorems [14]. The first one basically recalls a theorem published both by Glushkov [20] (and called theorem 5 in chapter II of Glushkov’s book) and by Mukhopadhyay [21] (and called theorem 3.3 in Mukhopadhyay’s paper). It is related to conventional (i.e. not necessarily reversible) logic circuits:

Kerntopf’s theorem 1. *A logic gate is universal if and only if it is neither linear nor monotonic.*

The interdiction of fan-outs in reversible circuits can be circumvented by using a reversible gate with the so-called duplicating property and applying at least one constant input to that gate. Figure 2 illustrates the duplication property of gate g_1 of table 1(*a*). In a conventional combinatorial circuit, the fan-out of figure 2(*a*) is allowed. In a reversible circuit, it has to be replaced by a reversible gate, such as in figure 2(*b*), where we apply two constant inputs to gate g_1.

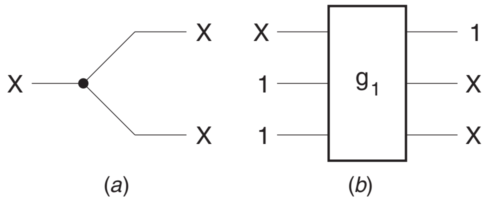

Figure 2. Duplicating a boolean variable X: (a) by conventional fan-out and (b) by a reversible gate.

Kerntopf proves the following theorem on reversible logic gates:

Kerntopf's theorem 2. *A reversible logic gate has duplicating property if and only if it is not selective.*

Combining his first two theorems, he finally comes to the following theorem on reversible logic circuits:

Kerntopf's theorem 3. *A reversible logic gate is r-universal if and only if it is neither selective nor linear nor monotonic.*

As r-universality is a stronger property than universality, it is no surprise that the third theorem gives more conditions than the first one.

3. Calculations

In this section, we evaluate the number of different selective reversible gates, the number of different linear reversible gates and the number of different monotonic reversible gates.

The number $l(w)$ of linear reversible gates of width w can be counted as follows:

- For the first linear function, i.e. $P_1(A_1, A_2, \dots, A_w)$, all linear functions are eligible, with two exceptions: the constant function 0 and the constant function 1. Therefore we count
$$2^{w+1} - 2 = 2(2^w - 1).$$
- For the second linear function, i.e. $P_2(A_1, A_2, \dots, A_w)$, all linear functions are eligible, except the functions 0, 1, P_1 and $\overline{P_1}$. Therefore we count
$$2^{w+1} - 4 = 2^2(2^{w-1} - 1).$$
- For the third linear function, i.e. $P_3(A_1, A_2, \dots, A_w)$, all linear functions are eligible, except the functions 0, 1, P_1, $\overline{P_1}$, P_2, $\overline{P_2}$, $P_1 \oplus P_2$ and $\overline{P_1 \oplus P_2}$. Therefore we count
$$2^{w+1} - 8 = 2^3(2^{w-2} - 1).$$
- And finally for the ith linear function, i.e. $P_i(A_1, A_2, \dots, A_w)$, we count
$$2^{w+1} - 2\left(1 + C_{i-1}^1 + C_{i-1}^2 + \cdots + C_{i-1}^{i-1}\right) = 2^{w+1} - 2(1+1)^{i-1} = 2^i(2^{w-i+1} - 1)$$
eligible functions.

Thus the total amount of allowed combinations is
$$\begin{aligned} l(w) &= 2(2^w - 1) \times 2^2(2^{w-1} - 1) \times 2^3(2^{w-2} - 1) \times \cdots \times 2^w(2 - 1) \\ &= 2^{1+2+3+\cdots+w}(2-1)(2^2-1)(2^3-1)\cdots(2^w-1) \\ &= 2^{(w+1)w/2}\prod_{i=1}^{w}(2^i - 1). \end{aligned}$$

Table 3. The number of different reversible gates, the number of different linear reversible gates, the number of different selective reversible gates, the number of different monotonic reversible gates and the number of different conservative reversible gates, as a function of the gate width w.

w	$r(w) = 2^w!$	$l(w)$	$s(w) = 2^w w!$	$m(w) = w!$	$c(w)$
1	2	2	2	1	1
2	24	24	8	2	2
3	40 320	1 344	48	6	36
4	20 922 789 888 000	322 560	384	24	414 720

This result is in accordance with the formulae published by Shende *et al* [22, 23]: it is the product of $\prod_{i=1}^{w}(2^w - 2^{i-1})$, the number of 'C-constructible gates' (i.e. the number of gates generated by wiring CONTROLLED NOTs), and 2^w, the number of 'N-constructible gates' (i.e. the number of gates generated by wiring NOTs). The number $\prod_{i=1}^{w}(2^w - 2^{i-1})$ also appears in projective geometry, as the order $|GL(w, 2)|$ of the general linear group [24] of bijective linear transformations of the w-dimensional vector space over the Galois field $GF(2)$. It is the number of linear $w \times w$ matrices with matrix elements 0 and 1 and with unitary determinant. The additional factor 2^w accounts for the number of translations in affine geometry. It is the number of $w \times 1$ vectors with vector components 0 and 1. The product $2^w|GL(w, 2)|$ is the order of the affine linear group $AGL(w, 2)$. Table 3 gives numerical values of $l(w)$, for the cases $1 \leqslant w \leqslant 4$.

The number $s(w)$ of selective reversible gates of width w is well known and amounts to $2^w w!$. We note that all these selective reversible gates are linear and thus are included in $l(w)$.

The number $m(w)$ of monotonic reversible gates of width w is counted in the appendix. It turns out that the only monotonic reversible gates which exist are the $w!$ exchangers, and therefore are linear. Thus all monotonic reversible gates are also included in the set of linear reversible gates.

4. Conclusion

Kerntopf's theorem 3 together with the calculation in the previous section leads to a new theorem:

Theorem. *A reversible gate is r-universal if and only if it is not linear.*

The reader will easily verify that linear gates are not universal, for the simple reason that any circuit built from linear gates can only synthesize linear functions, thus explaining the 'only-if'. The 'if' part of the theorem is less self-evident: it needs

- Kerntopf's theorem 3,
- the fact that each selective reversible gate is linear and
- the proof in the appendix that each monotonic reversible logic gate is an exchanger and hence is linear.

As two examples, we recall the gates g_1 and g_2 of table 1. Gate g_1 is r-universal, as it is not linear. To demonstrate its nonlinearity, it suffices to remark that the function $P_1(A_1, A_2, A_3) = A_1A_2 \oplus A_2A_3 \oplus A_3A_1$ is nonlinear. In contrast, gate g_2 is linear, as all three functions $P_1(A_1, A_2, A_3)$, $P_2(A_1, A_2, A_3)$ and $P_3(A_1, A_2, A_3)$ are linear. Indeed, we have $P_1 = A_1$, $P_2 = A_3$ and $P_3 = A_2$.

Table 4. The number of different reversible gates and the number of different r-universal reversible gates, as a function of the gate width w.

w	$r(w)$	$u(w)$	$\frac{u(w)}{r(w)}$ (in %)
1	2	0	0
2	24	0	0
3	40 320	38 976	96.7
4	20 922 789 888 000	20 922 789 565 440	99.999 998 5

From the above theorem, together with the calculations in the previous section, the following theorem is obtained:

Theorem. *The number of r-universal reversible gates is given by*

$$u(w) = r(w) - l(w) = (2^w)! - 2^{(w+1)w/2} \prod_{i=1}^{w} (2^i - 1).$$

Table 4 gives the values of $u(w)$ for $1 \leqslant w \leqslant 4$. It is clear that the fraction $u(w)/r(w)$ increases rapidly from 0 to unity, for w increasing from 2 to infinity. Thus, in accordance with Kerntopf [14], we can conclude that (for $w \geqslant 4$) 'almost all' reversible gates are r-universal.

Appendix. Monotonic reversible gates

We consider a logic gate with w binary inputs A_i and w binary outputs P_i. We use the different values of the input $(A_1, A_2, \ldots, A_w)$ as the coordinates of a hypercube. We can represent a truth table by giving each corner of the hypercube a label $(P_1, P_2, \ldots, P_w)$. If the truth table is reversible, all 2^w labels are different.

We call a climbing path, a path that travels from point $(0, 0, \ldots, 0)$ to point $(1, 1, \ldots, 1)$ by consecutive steps that each increases a single coordinate A_i from 0 to 1. Such path necessarily contains w steps, each one an edge of the hypercube. As

- for the first step there are w possible choices,
- for the second step there are $w - 1$ possible choices,
- and for the jth step there are $w - j + 1$ possible choices,

there are $w!$ different climbing paths.

If the truth table is reversible, then, at each step of a climbing path, at least one of the numbers $P_1, P_2, \ldots, P_w$ must change. Such change can only be from 0 to 1, if the functions $P_1(A_1, A_2, \ldots, A_w)$, $P_2(A_1, A_2, \ldots, A_w)$, etc are all monotonic. Because there are only w steps, this means that at each step exactly one of the numbers $P_1, P_2, \ldots, P_w$ must increase from 0 to 1. Now, we call the 'weight' of a vector $(X_1, X_2, \ldots, X_w)$ the number of ones in the vector. Note that all corners $(A_1, A_2, \ldots, A_w)$ with the same weight p lie in a same hyperplane $A_1 + A_2 + \cdots + A_w = p$, perpendicular to the vector $(1, 1, \ldots, 1)$. The above reasoning demonstrates that, along a climbing path of a monotonic reversible gate, not only the weight of $(A_1, A_2, \ldots, A_w)$ increases in unitary steps from 0 to w, but also the weight of $(P_1, P_2, \ldots, P_w)$. We can conclude that in each corner, the weight of $(P_1, P_2, \ldots, P_w)$ equals the weight of $(A_1, A_2, \ldots, A_w)$. In other words, monotonic reversible gates conserve weight. Thus all monotonic reversible gates are conservative reversible gates. The opposite, however,

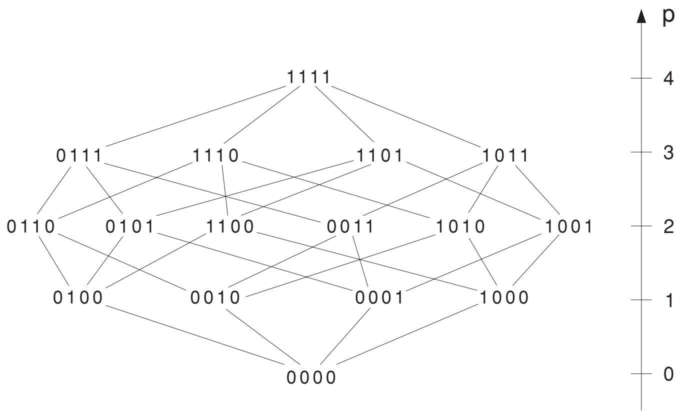

Figure 3. Four-dimensional hypercube with labels representing a monotonic reversible gate of width 4.

is not true. Conservative gates have been studied by Saso and Kinoshita [25]; conservative reversible gates have been studied by Fredkin and Toffoli [26] and by Cattaneo *et al* [27]. There exist $c(w) = C_w^0!C_w^1!C_w^2!\dots C_w^w!$ different conservative reversible gates. Table 3 gives the explicit values for w up to 4. The majority is not monotonic.

We first remark that each corner of the hypercube (with weight p) is connected by edges to its w neighbours, of which p have weight $p-1$ and $w-p$ have weight $p+1$. We now construct a monotonic reversible gate, by applying labels $(P_1, P_2, \dots, P_w)$ in hyperplanes of ever increasing weight:

- For $p = 0$, there is no freedom: we have to attach the label $(P_1, P_2, \dots, P_w) = (0, 0, \dots, 0)$ to the corner $(A_1, A_2, \dots, A_w) = (0, 0, \dots, 0)$.
- For $p = 1$, we can distribute the w labels $(1, 0, 0, \dots, 0), (0, 1, 0, 0, \dots, 0), \dots, (0, 0, \dots, 0, 1)$ freely among the w corners. This yields $w!$ possibilities.
- For $p = 2$, there is again no freedom: as each corner of weight 2 is connected (by means of two edges) to two corners of weight 1, its label is determined by the two labels downstream.
- For arbitrary p (with $2 \leqslant p \leqslant w$), there is again no freedom: as each corner of weight p is connected (by means of $p!$ different paths) to p different corners of weight 1, its label of weight p is completely determined by the p labels of weight 1.

See example in figure 3, with $w = 4$. We conclude that there are only $w!$ different monotonic reversible gates.

Now we remark that all exchangers are monotonic and that the number of different exchangers equals $w!$. As the number of exchangers equals the number of monotonic reversible gates, and as all exchangers are monotonic, this leads unavoidably to the conclusion that the only monotonic reversible gates that exist are the exchangers. Table 2(*c*) gives an example: this monotonic reversible gate indeed is an exchanger: $P_1 = A_3$, $P_2 = A_1$ and $P_3 = A_2$.

Figure 4 shows a Venn diagram of the set **R** of reversible gates with the important subsets: the set **L** of linear reversible gates, the set **S** of selective reversible gates, the set **M** of monotonic reversible gates (i.e. the set of exchangers) and finally the set **C** of conservative reversible gates. We distinguish two chains of subgroups:

$$\mathbf{M} \subset \mathbf{S} \subset \mathbf{L} \subset \mathbf{R} \qquad \text{and} \qquad \mathbf{M} \subset \mathbf{C} \subset \mathbf{R}.$$

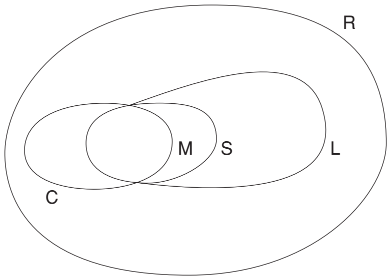

Figure 4. Venn diagram of the set of reversible gates, with its major subsets.

We finally remark the property

$$\mathbf{L} \cap \mathbf{C} = \mathbf{M}.$$

The latter property can be proved as follows. Conservation of zero weight at $(A_1, A_2, \ldots, A_w) = (0, 0, \ldots, 0)$ implies that $\overbrace{\;1\;}$ in formula (1) equals 0 for all w functions P_i. Permutation of $(1, 0, 0, \ldots, 0)$, $(0, 1, 0, 0, \ldots, 0), \ldots, (0, 0, \ldots, 0, 1)$ in the hyperplane $p = 1$ implies that among the resulting w values P_i there is one and only one 1. But the number of 1s in that hyperplane also equals the number of terms in the linear Reed–Muller expansion of the function P_i. Hence, the expansion contains only one term. Thus P_i equals some A_j. This fact applies to all i and therefore the gate is an exchanger.

References

[1] Landauer R 1961 Irreversibility and heat generation in the computational process *IBM J. Res. Dev.* **5** 183–91
[2] Keyes R and Landauer R 1970 Minimal energy dissipation in logic *IBM J. Res. Dev.* **14** 153–57
[3] Bennett C 1973 Logical reversibility of computation *IBM J Res. Dev.* **17** 525–32
[4] Bennett C and Landauer R 1985 The fundamental physical limits of computation *Sci. Am.* **253** 38–46
[5] De Vos A 1996 Introduction to r-MOS systems *Proc. 4th Workshop on Physics and Computation (Boston, Nov. 1996)* pp 92–6
[6] De Vos A 1997 Towards reversible digital computers *Proc. European Conference on Circuit Theory and Design (Budapest, Sept. 1997)* pp 923–31
[7] De Vos A 1999 Reversible computing *Prog. Quantum Electron.* **23** 1–49
[8] De Vos A 2003 Lossless computing *Proc. IEEE Workshop on Signal Processing (Poznań, Oct. 2003)* pp 7–14
[9] Feynman R 1985 Quantum mechanical computers *Opt. News* **11** 11–20
[10] Feynman R 1996 *Feynman Lectures on Computation* ed A Hey and R Allen (Reading, MA: Addison-Wesley)
[11] Barenco A, Bennett C, Cleve R, Di Vincenzo D, Margolus N, Shor P, Sleator T, Smolin J and Weinfurter H 1995 Elementary gates for quantum computation *Phys. Rev.* A **52** 3457–67
[12] Beckman D, Chari A, Devabhaktuni S and Preskill J 1996 Efficient networks for quantum factoring *Phys. Rev.* A **54** 1034–63
[13] Bettelli S, Calarco T and Serafini L 2003 Towards an architecture for quantum programming *Eur. Phys. J.* D **25** 181–200
[14] Kerntopf P 2002 On universality of binary reversible logic gates *Proc. 5th Workshop on Boolean Problems (Freiberg, Sept. 2002)* pp 47–52
[15] Storme L, De Vos A and Jacobs G 1999 Group theoretical aspects of reversible logic gates *J. Universal Comput. Sci.* **5** 307–21
[16] Hansel G 1966 Sur le nombre des fonctions booléennes monotones de *n* variables *Comptes Rendues de l'Académie des Sciences de Paris* **262** 1088–90
[17] Kleitman D 1969 On Dedekind's problem: the number of monotone boolean functions *Proc. Am. Math. Soc.* **21** 677–82
[18] Fidytek R, Mostowski A, Somla R and Szepietowski A 2001 Algorithms counting monotone Boolean functions *Inform. Proc. Lett.* **79** 203–9

[19] De Vos A, Raa B and Storme L 2002 Generating the group of reversible logic gates *J. Phys. A: Math. Gen.* **35** 7063–78

[20] Glushkov V 1966 *Introduction to cybernetics* (New York: Academic) pp 39–66

[21] Mukhopadhyay A 1971 Complete sets of logic primitives *Recent Developments in Switching Theory* ed A Mukhopadhyay (New York: Academic) pp 1–26

[22] Shende V, Prasad A, Markov I and Hayes J 2002 Synthesis of optimal reversible logic circuits *Proc. Int. Workshop on Logic and Synthesis (New Orleans, June 2002)* pp 125–30

[23] Shende V, Prasad A, Markov I and Hayes J 2003 Synthesis of reversible logic circuits *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.* **22** 710–22

[24] Hirschfeld J W P 1998 *Projective Geometries Over Finite Fields* (Oxford: Oxford University Press) pp 41–2

[25] Sasao T and Kinoshita K 1979 Conservative logic elements and their universality *IEEE Trans. Comput.* **28** 682–85

[26] Fredkin E and Toffoli T 1982 Conservative logic *Int. J. Theor. Phys.* **21** 219–53

[27] Cattaneo G, Leporati A and Leporini R 2002 Fredkin gates for finite-valued reversible and conservative logics *J. Phys. A: Math. Gen.* **35** 9755–85