Journal of Universal Computer Science, vol. 10, no. 9 (2004), 1294-1301
submitted: 19/1/04, accepted: 3/8/04, appeared: 28/9/04 © J.UCS

On the Decomposition of Boolean Functions via Boolean Equations

Sergiu Rudeanu
(Faculty of Mathematics and Computer Science
The University of Bucharest, Str. Academiei 14, Bucharest, Romania
Email: `rud@funinf.cs.unibuc.ro`)

Abstract: We propose an alternative solution to the problems solved in [1]. Our aim is to advocate the efficiency of algebraic methods for the solution of the Boolean equations which occur in the decomposition of Boolean functions.

Key Words: Boolean function, Boolean decomposition, Boolean equation
Category: F.4, G.2

1 Introduction

The application of Boolean equations in various fields such as logic, logical design, biology, grammars, graph theory, chemistry, law, medicine, operations research or spectroscopy, is well known. Boolean equations occur either directly or as a tool in the problem of decomposing a Boolean function. This problem is very important in the design of logic circuits. See e.g. [2], [3], [6], [8] and the literature cited therein.

Although the algebraic theory of Boolean equations is much developed and has powerful results [6], [8], most researchers interested in Boolean equations use tabular methods. In a series of papers [4], [5], [7], [9], among which [4], [7] refer to the decomposition of Boolean functions, we advocated the efficiency of algebraic methods by solving algebraically the Boolean equations solved by others using tabular methods. In the present article we do the same thing with respect to the paper [1].

In order to state the problem studied in [1], we first settle a matter of terminolgy. By a *Boolean function* of n variables over an arbitrary Boolean algebra $(B; \vee, \cdot, ', 0, 1)$ we mean a function $\varphi : B^n \longrightarrow B$ which can be constructed from variables and constants by superpositions of the basic operations $\vee, \cdot, '$, while a function $f : \{0,1\}^n \longrightarrow \{0,1\}$ will be termed a *truth function* or *switching function*. According to a well-known theorem, every truth function is Boolean. Although nowadays the unique term *Boolean function* seems to prevail, we prefer to make the distinction between the general and the particular case, as was the use in the fifties. In particular, by a *Boolean (truth) equation* we mean an equation expressed in terms of Boolean (truth) functions.

The decomposition of switching functions is an important concept which has been studied since the beginning of switching theory. According to Bibilo [1], it can be given the following formulation (in our terminology). Suppose $f : \{0,1\}^n \overset{\circ}{\longrightarrow} \{0,1\}$ is a *partially defined truth function*, that is, f is defined on a (proper or improper) subset of $\{0,1\}^n$, and let X be the set of its arguments. A *decomposition* of f is an identity of the form

$$f(X) \preceq g(h^1_{11}(Y^1), \ldots, h^1_{1p_1}(Y^1), \ldots, h^k_{k1}(Y^k), \ldots, h^k_{kp_k}(Y^k), Z) \ , \tag{1}$$

where $g, h^1_{11}, \ldots, h^k_{kp_k}$ are truth functions, $Y^1, \ldots, K^k, Z$ are (not necessarily disjoint) sets of arguments covering X, and $\varphi(X) \preceq \psi(X)$ means that φ is a restriction of ψ. The sets $Y^1, \ldots, Y^k, Z$ being given, two types of problem are considered: I) determine $g, h^1_{11}, \ldots, h^k_{kp_k}$ which satisfy (1) (possibly which optimize the decomposition (1) according to a certain criterion), and II) given g, find $h^1_{11}, \ldots, h^k_{kp_k}$ such that (1) holds. The problem is expressed in graph-theoretical terms and this intermediate problem is further reduced to the solution of a system of truth equations. A few concrete examples are worked out which illustrate the technique devised by the author.

On the other hand, there is a direct approach which transforms a functional Boolean equation into a system of ordinary Boolean equations; it has numerous applications [6], [8], in particular to the decomposition of Boolean functions. In the sequel we advocate the advantages of this technique by applying it to the concrete problems solved in [1]. We begin by recalling the prerequisites we are going to use; for details see e.g. [6] or [8].

A Boolean function $\varphi : B^n \longrightarrow B$ satisfies the *Boole expansion*

$$\varphi(x_1, \ldots, x_n) = \bigvee\nolimits_{\alpha_1, \ldots, \alpha_n \in \{0,1\}} \varphi(\alpha_1, \ldots, \alpha_n) x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} \ , \tag{2}$$

where $\bigvee$ denotes iterated disjunction $\vee$ and x^α is defined by $x^1 = x$ and $x^0 = x'$; the 2^n coefficients $\varphi(\alpha_1, \ldots, \alpha_n)$ are called the *discriminants* of the function φ (cf. Whitehead (1898)). The expansion (2) implies the Müller-Löwenheim *verification theorem*, which states that a Boolean function is completely determined by its discriminants and, more generally, an equality between Boolean functions holds identically if and only if it is satisfied for all possible values 0–1 given to the variables. So, the solution of a functional Boolean equation amounts to the solution of a system of Boolean equations in thediscriminants of the unknown functions.

Recall also that a system of equations of the form $\varphi_j = 1$ $(j = 1, \ldots, m)$ is equivalent to the single equation $\varphi_1 \cdot \ldots \cdot \varphi_m = 1$. The Boolean equation in one unknown

$$\varphi(x) \equiv \varphi(1)x \vee \varphi(0)x' = 1 \tag{3.1}$$

has solutions if and only if

$$\varphi(1) \vee \varphi(0) = 1 \ , \tag{4.1}$$

in which case the solutions are given by the inequalities

$$\varphi'(0) \leq x \leq \varphi(1) \ . \tag{5.1}$$

This is the base for the *method of successive elimination of variables*. For instance, in the case $n = 2$ it runs as follows. The equation

$$\Phi(x, y) \equiv \Phi(1, 1)xy \vee \Phi(1, 0)xy' \vee \Phi(0, 1)x'y \vee \Phi(0, 0)x'y' = 1 \tag{3.2}$$

is written in the form

$$(\Phi(1, 1)x \vee \Phi(0, 1)x')y \vee (\Phi(1, 0)x \vee \Phi(0, 0)x')y' = 1 \ ,$$

whose consistency condition with respect to y is

$$(\Phi(1,1) \vee \Phi(1,0))x \vee (\Phi(0,1) \vee \Phi(0,0))x' = 1 \; ,$$

which we solve as an equation in x: we obtain the consistency condition

$$\Phi(1,1) \vee \Phi(1,0) \vee \Phi(0,1) \vee \Phi(0,0) = 1 \; , \tag{4.2}$$

which is also the consistency condition for the original equation (3.2), while the solutions are described by the system of recurrent inequalities

$$\Phi'(0,1)\Phi'(0,0) \leq x \leq \Phi(1,1) \vee \Phi(1,0) \; , \tag{5.2.1}$$

$$\Phi'(1,0)x \vee \Phi'(0,0)x' \leq y \leq \Phi(1,1)x \vee \Phi(0,1)x' \; . \tag{5.2.2}$$

2 Examples

We can apply the technique described above because condition (1) means that the equality

$$f(X) = g(h^1_{11}(Y^1), \ldots, h^1_{1p_1}(Y^1), \ldots, h^k_{k1}(Y^k), \ldots, h^k_{kp_k}(Y^k), Z) \tag{6}$$

holds for all those $X \in \{0,1\}^n$ for which $f(X)$ is defined.

All the examples given in [1] refer to the function f of four variables defined in Table 1 below.

x_1	x_2	x_3	x_4	f
0	0	0	0	1
0	0	0	1	1
1	0	0	0	1
1	0	0	1	1
1	1	0	1	1
1	1	1	1	1
0	0	1	0	0
1	1	0	0	0
0	1	1	1	0

Table 1

The instance of problem I (cf. Introduction) solved in [1] is $k = 2$, $Y^1 = \{x_1, x_2\}$, $Y^2 = \{x_2, x_3, x_4\}$, $Z = \emptyset$. In the following we solve the case $k = 2$, $Y^1 = \{x_2, x_3\}$, $Y^2 = \{x_1, x_2, x_4\}$, $Z = \emptyset$, which seems to have the same degree of difficulty, but which will facilitate the study of the other examples given in [1].

So, the decomposition (6) becomes

$$f(x_1, x_2, x_3, x_4) = g(h_1(x_2, x_3), h_2(x_1, x_2, x_4)) \tag{7}$$

for the vectors (x_1, x_2, x_3, x_4) depicted in Table 1.

We use the Boole expansions of the unknown functions g, h_1, h_2:

$$g(x, y) = axy \vee bxy' \vee cx'y \vee dx'y' \; , \tag{8}$$

$$h_1(x_2, x_3) = px_2x_3 \vee qx_2x_3' \vee rx_2'x_3 \vee sx_2'x_3' \; , \tag{9}$$

(10)
$$h_2(x_1,x_2,x_4) = Ax_1x_2x_4 \vee Bx_1x_2x_4' \vee Cx_1'x_2x_4 \vee Dx_1'x_2x_4' \vee \\ \vee Ex_1x_2'x_4 \vee Fx_1x_2'x_4' \vee Gx_1'x_2'x_4 \vee Hx_1'x_2'x_4' \ .$$

In the sequel we assume that the function f is given in Table 1, while g, h_1 and h_2 are of the form (8), (9) and (10), respectively.

Proposition 1. *The function f is decomposed in the form*

(11)
$$f(x_1,x_2,x_3,x_4) \preceq g(h_1(x_2,x_3),h_2(x_1,x_2,x_4))$$

if and only if

(12)
$$a(bc' \vee b'c) \vee a'b'c' \leq d \leq a(b' \vee c') \vee a'bc \vee b'c' \ ,$$

(13.1)
$$cd \vee c'd' \leq p \leq ab' \vee a'b \ ,$$

(13.2)
$$(a \vee b' \vee c \vee d')(a' \vee b \vee c' \vee d)p \vee (cd \vee c'd')p' \leq q \leq \\ \leq (ab' \vee a'b)p \vee (a'bc'd \vee ab'cd')p' \ ,$$

(14.1)
$$(a' \vee c)(b' \vee d) \leq r \leq a'c \vee b'd \ ,$$

(14.2)
$$(a \vee c')(b \vee d') \vee r' \leq s \leq (ac' \vee bd')r' \ ,$$

(15.1)
$$b'(p \vee q) \vee d'(p \vee q') \leq A \leq (ap \vee cp')(aq \vee cq') \ ,$$

(15.2)
$$bq \vee dq' \leq B \leq a'q \vee c'q' \ ,$$

(15.3)
$$bp \vee dp' \leq C \leq a'p \vee c'p' \ ,$$

(15.4)
$$b's \vee d's' \leq E \leq as \vee cs' \ ,$$

(15.5)
$$b's \vee d's' \leq F \leq as \vee cs' \ ,$$

(15.6)
$$b's \vee d's' \leq G \leq as \vee cs' \ ,$$

(15.7)
$$br \vee dr' \vee b's \vee d's' \leq H \leq (as \vee cs')(a'r \vee c'r') \ ,$$

while a, b, c, D remain arbitrary.

Comment. Formulas (12)–(15), via (8)–(10), provide a recursive construction of the set of solutions to the functional equation (11).

Proof. Taking into account (8)–(10), we write down the relation

$$g(h_1(x_2,x_3),h_2(x_1,x_2,x_4)) = f(x_1,x_2,x_3,x_4)$$

for the 9 vectors (x_1,x_2,x_3,x_4) in Table 1:

(16.1)
$$(as \vee cs')H \vee (bs \vee ds')H' = 1 \ ,$$

(16.2)
$$(as \vee cs')G \vee (bs \vee ds')G' = 1 \ ,$$

(16.3)
$$(as \vee cs')F \vee (bs \vee ds')F' = 1 \ ,$$

$$(as \vee cs')E \vee (bs \vee ds')E' = 1 \, , \tag{16.4}$$

$$(aq \vee cq')A \vee (bq \vee dq')A' = 1 \, , \tag{16.5}$$

$$(ap \vee cp')A \vee (bp \vee dp')A' = 1 \, , \tag{16.6}$$

$$(ar \vee cr')H \vee (br \vee dr')H' = 0 \, , \tag{16.7}$$

$$(aq \vee cq')B \vee (bq \vee dq')B' = 0 \, , \tag{16.8}$$

$$(ap \vee cp')C \vee (bp \vee dp')C' = 0 \, , \tag{16.9}$$

and we have to solve the system of Boolean equations (16).

The subsystem (16.5), (16.6) is equivalent to the single equation

$$(ap \vee cp')(aq \vee cq')A \vee (bp \vee dp')(bq \vee dq')A' = 1 \, , \tag{17}$$

obtained by multiplication. Then we transform the equations (16.7)–(16.9) by complementation:

$$(a'r \vee c'r')H \vee (b'r \vee d'r')H' = 1 \, , \tag{16.7'}$$

$$(a'q \vee c'q')B \vee (b'q \vee d'q')B' = 1 \, , \tag{18}$$

$$(a'p \vee c'p')C \vee (b'p \vee d'p')C' = 1 \, , \tag{19}$$

and finally we reduce (16.1) and (16.7′) to the single equation

$$(as \vee cs')(a'r \vee c'r')H \vee (bs \vee ds')(b'r \vee d'r')H' = 1 \, . \tag{20}$$

Thus, the original system (16) has been transformed into the equivalent system (17), (18), (19), (16.4), (16.3), (16.2), (20). We can solve these equations separately as equations in a single unknown, namely A, B, C, E, F, G and H, respectively. The solutions of the form (5.1) are (15.1)–(15.7), while the corresponding consistency conditions (14.1) are

$$(ap \vee cp')(aq \vee cq') \vee (bp \vee dp')(bq \vee dq') = 1 \, , \tag{21.1}$$

$$(a' \vee b')q \vee (c' \vee d')q' = 1 \, , \tag{21.2}$$

$$(a' \vee b')p \vee (c' \vee d')p' = 1 \, , \tag{21.3}$$

$$(a \vee b)s \vee (c \vee d)s' = 1 \, , \tag{21.4}$$

$$(as \vee cs')(a'r \vee c'r') \vee (bs \vee ds')(b'r \vee d'r') = 1 \, , \tag{21.5}$$

and it remains to solve the system (21). We can solve separately the subsystem (21.1), (21.2), (21.3) with respect to the unknowns p, q and the subsystem (21.4), (21.5) with respect to the unknowns r, s.

We write (21.1) in the form

$$(a \vee b)pq \vee (ac \vee bd)pq' \vee (ac \vee bd)p'q \vee (c \vee d)p'q' = 1 \, ;$$

this equation and (21.2) are equivalent to the single equation

$$(ab' \vee a'b)pq \vee (ac \vee bd)(a' \vee b')p'q \vee (ac \vee bd)(c' \vee d')pq'$$
$$\vee(cd' \vee c'd)p'q' = 1 \ ,$$

while this equation and (21.3) are equivalent to the equation

$$(ab' \vee a'b)pq \vee (a'bd \vee ab'c)(c' \vee d')pq' \vee (bc'd \vee acd')(a' \vee b')p'q$$
$$\vee(cd' \vee c'd)p'q' = 1 \ ,$$

so that the system (21.1), (21.2), (21.3) is equivalent to the single equation

$$(ab' \vee a'b)pq \vee (a'bc'd \vee ab'cd')pq' \vee (a'bc'd \vee ab'cd')p'q$$
$$\vee(cd' \vee a'd)p'q' = 1 \ .$$

Since

$$(a'bc'd \vee ab'cd')'(cd' \vee c'd)' = (a \vee b' \vee c \vee d')(a' \vee b \vee c' \vee d)(cd \vee c'd')$$
$$= (a \vee b' \vee c \vee d')(cd \vee c'd') = cd \vee c'd' \ ,$$

formulas (5.2.1) and (5.2.2), which describe the solutions, become (13.1) and (13.2), respectively, while the consistency conditions (4.2) reduce to

$$ab' \vee a'b \vee cd' \vee c'd = 1 \ . \tag{22.1}$$

Now we write (21.5) in the form

$$(a'c \vee b'd)rs' \vee (ac' \vee bd')r's = 1 \tag{21.5$'$}$$

and observe that this equation implies (21.4). So the subsystem (21.4), (21.5) is equivalent to the single equation (21.5′), whose solutions of the form (5.2.1), (5.2.2) are precisely (14.1), (14.2), provided the consistency condition

$$a'c \vee ac' \vee b'd \vee bd' = 1 \tag{22.2}$$

is fulfilled.

Finally it remains to solve the system (22). We obtain by multiplication

$$ab'c' \vee a'bc \vee ab'd \vee a'bd' \vee a'cd' \vee bcd' \vee ac'd \vee b'c'd = 1 \ ,$$

or equivalently,

$$(a'bc \vee ab' \vee ac' \vee b'c')d \vee (ab'c' \vee a'b \vee a'c \vee bc)d' = 1$$

and since

$$(ab'c' \vee a'(b \vee c) \vee bc)' = (a(b \vee c) \vee a'b'c')(b' \vee c') = a(bc' \vee b'c) \vee a'b'c' \ ,$$

the solutions of the last equation are given by formula (12), while the consistency condition is fulfilled:

$$ab' \vee ac' \vee b'c' \vee a'b \vee a'c \vee bc = (ab' \vee a'b \vee a' \vee b)c \vee (ab' \vee a \vee b' \vee a'b)c' = c \vee c' = 1 \ .$$

□

In the sequel we resume the examples of type II (cf. Introduction) given in [1], that is, those with prescribed function g.

Proposition 2. *The function f is decomposed in the form*

$$f(x_1, x_2, x_3, x_4) \preceq h_1(x_2, x_3) + h_2(x_1, x_2, x_4) \tag{23}$$

if and only if the functions h_1 and h_2 are of the form

$$h_1(x_2, x_3) = px_2 + (r + x_3')x_2' \ , \tag{24}$$

$$h_2(x_1, x_2, x_4) = px_2(x_1 + x_4) + p'x_1x_2x_4 + Dx_1'x_2x_4' + rx_2' \ . \tag{25}$$

Proof. The decomposition (23) is of the form (11) with $g(x, y) = x + y$, that is, $a = d = 0$ and $b = c = 1$. These values satisfy condition (12), hence decompositions (23) do exist. We obtain all of them by introducing the above values into (13), (14) and (15). Since $cd \vee c'd' = (a' \vee c)(b' \vee d) = 0$ and $ab' \vee a'b = a'c \vee b'd = 1$, it follows from (13.1) and (14.1) that p and r remain arbitrary, while (13.2) yields $p \leq q \leq p$, that is, $p = q$, and similarly, $s = r'$, $A = p'$, $B = p$, $C = p$, $E = F = G = r$, $H = r$. Thus formulas (9) and (10) yield

$$h_1(x_1, x_2) = px_2 \vee (rx_3 \vee r'x_3')x_2' \ ,$$
$$\begin{aligned} h_2(x_1, x_2, x_4) &= p'x_1x_2x_4 \vee px_1x_2x_4' \vee px_1'x_2x_4 \vee Dx_1'x_2x_4' \vee rx_2' \\ &= p'x_1x_2x_4 \vee px_2(x_1x_4' \vee x_1'x_4) \vee Dx_1'x_2x_4' \vee rx_2' \ , \end{aligned}$$

which coincide with (24) and (25), respectively. □

Proposition 3. *The unique decomposition of the form*

$$f(x_1, x_2, x_3, x_4) \preceq h_1(x_2, x_3) \vee h_2(x_1, x_4) \tag{26}$$

is

$$f(x_1, x_2, x_3, x_4) \preceq x_2'x_3' \vee x_1x_4 \ . \tag{27}$$

Proof. We are looking for a decomposition of the form (11) such that $g(x, y) = x \vee y$ and the function h_2 does not actually depend on x_2. This amounts to the following conditions on the solutions (12)–(15): $a = b = c = 1, d = 0$ and $A = E$, $B = F$, $C = G$, $D = H$.

The above values of a, b, c, d satisfy (12) and conditions (13)–(15) imply in turn $p = 0$, $q = 0$, $r = 0$, $s = 1$, $A = 1$, $B = 0$, $C = 0$, E : arbitrary, F : arbitrary, G : arbitrary, $H = 0$. So we can take $E = A = 1$, $F = B = 0$, $G = C = 0$, $H = D = 0$ and obtain $h_1(x_2, x_3) = x_2'x_3'$ and $h_2(x_1, x_4) = x_1x_4$. □

Proposition 4. *There is no decomposition of the form*

$$f(x_1, x_2, x_3, x_4) \preceq h_1(x_2, x_3)h_2(x_1, x_4) \ . \tag{28}$$

Proof. We are looking for solutions (12)–(15) satisfying $a = 1, b = c = d = 0$ and again $A = E$, $B = F$, $C = G$, $D = H$. From (13.1)–(14.2) we obtain in turn $p = 1$, $q = 1$, $r = 0$, $s = 1$, hence (15.2) yields $B = 0$, while (15.5) reduces to $F = 1$, therefore $B \neq F$. □

Remark. As we mentioned it, the example of type I (cf. Introduction) solved in [1] is in fact

$$f(x_1, x_2, x_3, x_4) \preceq g(h_1(x_2, x_3), h_2(x_1, x_4)) \ . \tag{29}$$

The reader is urged to solve this equation in a proposition similar to Proposition 1 and to obtain Propositions 3 and 4 as corollaries, in the same way as Proposition 2 was obtained from Proposition 1.

3 Conclusions

This paper, like [4], [7], [9], is a pleading for the direct algebraic approach to the decomposition of truth functions via truth equations. The versatility of this procedure is illustrated by the quick way in which Propositions 2-4 have been obtained from the general result in Proposition 1.

Acknowledgement

The author wishes to thank the three referees for their helpful remarks, which improved the presentation of this paper.

References

1. P.N.Bibilo: Decomposition of Boolean functions based on the solution of logic equations. I. II. (Russian). Izv. Akad. Nauk Teor. Sist. Upr. 2002, no.4, 53-64; no.5, 57-63.

2. F.M.Brown: Boolean Reasoning: The Logic of Boolean equations. Kluwer, Boston 1990. Second edition: Dover, Mineola 2003.

3. P.L.Hammer, S.Rudeanu: Boolean Methods in Operations Research and Related Areas. Springer-Verlag, Berlin 1968. French translation: Dunod, Paris 1970.

4. S.Rudeanu: On Tohma's decomposition of logical functions. IEEE Trans. Electronic Computers EC-14 (1965), 929-931.

5. S.Rudeanu: An algebraic approach to Boolean equations. IEEE Trans. Computers C-23 (1974), 206-207.

6. S.Rudeanu: Boolean Functions and Equations. North-Holland, Amsterdam/London 1974. Japanese translation: Kogaku Tosho, Tokyo 1984.

7. S.Rudeanu: Square roots and functional decompositions of Boolean functions. IEEE Trans. Computers C-25 (1976), 528-532.

8. S.Rudeanu: Lattice Functions and Equations. Springer-Verlag, London 2001.

9. S.Rudeanu: Algebraic methods versus map methods of solving Boolean equations. Intern. J. Computer Math. 80(2003), 815-817.