Zbornik radova Prirodno-matematičkog fakulteta—Univerzitet u Novom Sadu, knjiga 10 (1980)
Review of Research Faculty of Science — University of Novi Sad, Volume 10 (1980)

ON THE CLASS OF CONSTANT-PRESERVING BOOLEAN FUNCTIONS OVER THE FINITE BOOLEAN ALGEBRAS

Ratko Tošić
Prirodno-matematički fakultet. Institut za matematiku.
21 000 Novi Sad, ul. dr Ilije Đuričića 4, Jugoslavija.

1. Before proceeding to a consideration of our subject we would like to give a short survey of our instruments.

First we shall give the following definitions (see [1]).

DEFINITION 1. *The Boolean functions of n variables (BFn) over the Boolean algebra* $\langle B, \vee, \cdot, ', 0, 1\rangle$ *are determined by the following rules:*

0) *For every* $a \in B$, *the constant function* $f_a : B^n \to B$ *defined by*

$$(1.1) \qquad (\forall x_1, \ldots, x_n \in B)\ f_a(x_1, \ldots, x_n) = a$$

is a BFn.

1) *For every* $i = 1, 2, \ldots, n$, *the projection function* $e_i : B^n \to B$ *defined by*

$$(1.2) \qquad (\forall x_1, \ldots, x_n \in B)\ e_i(x_1, \ldots, x_n) = x_i$$

is a BFn.

2) *If* $f, g : B^n \to B$ *are BFn, then the functions* $f \vee g$, fg, $f' : B^n \to B$ *defined by*

$$(1.3) \qquad (\forall x_1, \ldots, x_n \in B)\ (f \vee g)(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) \vee g(x_1, \ldots, x_n)$$

$$(1.4) \qquad (\forall x_1, \ldots, x_n \in B)\ (fg)(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) \cdot g(x_1, \ldots, x_n)$$

$$(1.5) \qquad (\forall x_1, \ldots, x_n \in B)\ f'(x_1, \ldots, x_n) = (f(x_1, \ldots, x_n))'$$

are BFn.

3) *Any BFn is obtained by applying rules* 0), 1) *and* 2) *a finite number of times.*

DEFINITION 2. *The simple Boolean functions of n variables* (SBFn) *over the Boolean algebra* $\langle B, \vee, \cdot, ', 0, 1\rangle$ *are determined by the following rules:*

1') *For every* $i = 1, 2, \ldots, n$, *the projection function* (1.2) *is an* SBFn.

2') *If* $f, g : B^n \to B$ *are* SBFn, *then functions* (1.3), (1.4), *and* (1.5) *are SBFn.*

3') *Any* SBFn *is obtained by applying rules* 1') *and* 2') *a finite number of times.*

DEFINITION 3. *Let $B_2=\{0, 1\}$ be the two-element Boolean algebra. For every natural number n, every function $f: B_2^n \to B_2$ is called a truth function.*

A suitable model for the investigation of some properties of Boolean functions over finite Boolean algebras is just the B-modul defined in [2]. For this reason we do not deal in this paper with an abstract Boolean algebra but with its isomorphic representation — the B-modul.

DEFINITION 4. *Let there be given a set $B_2=\{0, 1\}$. Let us call each element of the Cartesian power B_2^q the q-dimensional B-vector (or briefly vector) over B_2 and denote it by the symbol $a=(a^1, \dots, a^q)$, where $a^k \in B_2$ for $k=1, 2, \dots, q$. Elements a^k are called coordinates of the B-vector. We shall call the set B_2^q of all q--dimensional B-vectors the q-dimensional B-modul over B_2. The B-vector $a=(a^1, \dots, a^q)$ is equal to the B-vector $b=(b^1, \dots, b^q)$ just when $a^k=b^k$ for all $k=1, 2, \dots, q$. By $a \vee b$ we denote the disjunction of vectors a and b i.e. vector $c=(c^1, \dots, c^q)$ where $c^k=a^k \vee b^k$, for the coordinates holding: $0\vee 0=0$, $0 \vee 1=1\vee 0=1\vee 1=1$.* By *$a \cdot b$ we denote the conjunction of vectors a and b i.e. vector $d=(d^1, \dots, d^q)$, where $d^k=a^k \cdot b^k$, for the coordinates holding $0\cdot 0=0\cdot 1=1\cdot 0=0$, $1\cdot 1=1$. Vector $1=(1, \dots, 1)$ is called a unit vector, vector $0=(0, \dots, 0)$ a zero vector. Vector a' is called a complement of vector a, if it holds $a\vee a'=1$, $a\cdot a'=0$. In fact, for $a=(a^1, \dots, a^q)$, $a'=((a^1)', \dots, (a^q)')$, for the coordinates holding: $0'=1$, $1'=0$.*

It is easy to show (see [2]) that each Boolean algebra having 2^q elements is isomorphic with q-dimensional B-modul B_2^q. We define a further operation:

DEFINITION 5. *The operation of multiplying of a vector $a \in B_2^q$ by element $\alpha \in B_2$ is given by the rule:*

$$\alpha \cdot a = a \cdot \alpha = \begin{cases} 0 \text{ when } \alpha=0 \\ a \text{ when } \alpha=1. \end{cases} \tag{1.6}$$

Now it is possible to introduce in B_2^q a concept of a linear combination:

DEFINITION 6. *A vector $c \in B_2^q$ is a linear combination of the vectors $a_j \in B_2^q$, $j=1, 2, \dots, s$ iff there exist $\alpha_j \in B_2$, such that*

$$c=\alpha_1 \cdot a_1 \vee \alpha_2 \cdot a_2 \vee \dots \vee \alpha_s \cdot a_s = \vee_{j=1}^{s} \alpha_j \cdot a_j \tag{1.7}$$

Vectors $\Delta_1=(1, 0, \dots, 0)$, $\Delta_2=(0, 1, 0, \dots, 0), \dots, \Delta_q=(0, \dots, 0, 1)$ are called base vectors of the B-modul B_2^q. In fact, they are atoms of the Boolean algebra $\langle B_2^q, \vee, \cdot, ', 0, 1\rangle$.

In what follows, we consider only Boolean functions over a finite Boolean algebra B_2^q having 2^q elements, instead of B_2^q we write simply B.

An arbitrary element of B can be represented in the form

$$a=\vee_{k=1}^{q} \Delta_k a^k \tag{1.8}$$

where

$$a^k=\begin{cases} 1 \text{ when } a \geqslant \Delta_k \\ 0 \text{ otherwise} \end{cases} \tag{1.9}$$

The following relations hold:

$$a \vee b = \vee_{k=1}^{q} \Delta_k (a^k \vee b^k) \tag{1.10}$$

$$a \cdot b = \vee_{k=1}^{q} \Delta_k (a^k \cdot b^k) \tag{1.11}$$

$$a' = \vee_{k=1}^{q} \Delta_k (a^k)'. \tag{1.12}$$

LEMMA 1.1. *For $a, b \in B$, $a \leqslant b$ iff $a^k \leqslant b^k$ for all $k=1, 2, \ldots, q$.*

Proof. $a \leqslant b \Leftrightarrow a \vee b = b$

$$\Leftrightarrow \vee_{k=1}^{q} \Delta_k (a^k \vee b^k) = \vee_{k=1}^{q} \Delta_k b^k$$

$$\Leftrightarrow a^k \vee b^k = b^k \text{ for all } k=1, 2, \ldots, q$$

$$\Leftrightarrow a^k \leqslant b^k \text{ for all } k=1, 2, \ldots, q.$$

LEMMA 1.2. *For any Boolean function $f: B^n \to B$ holds*

$$f(X) = \vee_{k=1}^{q} \Delta_k f^k (X^k) \tag{1.13}$$

where $f^k: B_2^n \to B_2$ $(k=1, 2, \ldots, q)$ is a truth function such that, for all $X \in B^n$

$$f^k (X^k) = \begin{cases} 1 & \text{when } f(X) \geqslant \Delta_k \\ 0 & \text{otherwise.} \end{cases} \tag{1.14}$$

Proof. Follows from (1.8), (1.10), (1.11) and (1.12).

According to (1.13), every BFn can be represented as an oı dered q-tuple of truth functions $f^k: B_2^n \to B_2$ $(k=1, 2, \ldots, q)$, f^k being the k-th component of BFn $f: B^n \to B$.

It is easy to show that a BFn $f: B^n \to B$ is simple iff $f^1 = f^2 = \ldots = f^q$, and in that case the analytic expression of that SBFn is identical to the analytic expression of any of its components.

2. Now, we shall use the componentwise treatment in oreder to prove some properties of BFn.

DEFINITION 7. *We say that* BFn $f: B^n = B$ *preserves a constant* $a \in B$ *iff* $f(a, a, \ldots, a) = a$.

Constant-preserving Boolean functions are of special importance in the switching theory.

LEMMA 2.1. *BFn $f: B^n \to B$ preserves a constant $a \in B$ iff, for all $k=1, 2, \ldots, q$, the truth function $f^k: B_2^n \to B_2$ preserves the constan $a^k \in B_2$.*

Proof. Let $f(a, a, \ldots, a) = a$ for some $a \in B$. Then

$$\vee_{k=1}^{q} \Delta_k f^k (a^k, a^k, \ldots, a^k) = \vee_{k=1}^{q} \Delta_k a^k,$$

hence

$$f^k (a^k, a^k, \ldots, a^k) = a^k, \text{ for all } k=1, 2, \ldots, q.$$

Conversely, if for all $k=1, 2, \ldots, q$,

$$f^k(a^k, a^k, \ldots, a^k)=a^k, \text{ then } f(a, a, \ldots, a)=$$
$$=\vee_{k=1}^{q} \Delta_k f^k(a^k, a^k, \ldots, a^k)=\vee_{k=1}^{q} \Delta_k a^k=a.$$

Now, the following theorems about the constant-preserving Boolean functions can be proved:

THEOREM 2.1. *Let BFn $f: B^n \to B$ satisfy the condition*

$$f(0, 0, \ldots, 0) \leqslant f(1, 1, \ldots, 1). \tag{2.1}$$

Then $f(c, c, \ldots, c)=c$ *iff*

$$f(0, 0, \ldots, 0) \leqslant c \leqslant f(1, 1, \ldots, 1). \tag{2.2}$$

Proof. Let $(f(0, 0, \ldots, 0 \leqslant c \leqslant f(1, 1, \ldots, 1)$, then for all $k=1, 2, \ldots, q$,

$$f^k(0, 0, \ldots, 0) \leqslant c^k \leqslant f^k(1, 1, \ldots, 1). \tag{2.2^k}$$

Now, there are three possibilities:

(A) $f^k(0, 0, \ldots, 0)=0$ (A′)
$f^k(1, 1, \ldots, 1)=0$ (A″)

In that case $c^k=0$, and by (A′): $f^k(c^k, c^k, \ldots, c^k)=c^k$.

(B) $f^k(0, 0, \ldots, 0)=1$ (B′)
$f^k(1, 1, \ldots, 1)=1$ (B″)

In that case $c^k=1$ and by (B″): $f^k(c^k, c^k, \ldots, c^k)=c^k$.

(C) $f^k(0, 0, \ldots, 0)=0$ (C′)
$f^k(1, 1, \ldots, 1)=1$ (C″)

In that case, there are two possibilities:

(i) $c^k=0$, hence by (C′): $f^k(c^k, c^k, \ldots, c^k)=c^k$

(ii) $c^k=1$, hence by (C″): $f^k(c^k, c^k, \ldots, c^k)=c^k$.

In any case, $f^k(c^k, c^k, \ldots, c^k)=c^k$, for all $k=1, 2, \ldots, q$; from Lemma 2.1, it follows: $f(c, c, \ldots, c)=c$.

Conversely, let $f(c, c, \ldots, c)=c$, for some $c \in B$. Then

$$f^k(c^k, c^k, \ldots, c^k)=c^k \text{ for all } k=1, 2, \ldots, q. \tag{2.3^k}$$

On the other hand, from (2.1) follows

$$f^k(0, 0, \ldots, 0) \leqslant f^k(1, 1, \ldots, 1) \text{ for all } k=1, 2, \ldots, q. \tag{2.1^k}$$

From (2.3^k) and (2.1^k) follows:

$$f^k(0, 0, \ldots, 0) \leqslant c^k \leqslant f^k(1, 1, \ldots, 1) \text{ for all } k=1, 2, \ldots, q, \tag{2.2^k}$$

hence (2.2) follows.

THEOREM 2.2. *A necessary nad sufficient condition for a BFn $f:B^n \to B$ to be preserving at least one constant is*

$$(2.1) \qquad f(0, 0, \dots, 0) \leqslant f(1, 1, \dots, 1).$$

Proof. Sufficiency follows from Theorem 2.1.

To prove the necessity, suppose that for some $c \in B$, $f(c, c, \dots, c) = c$ holds, Then, Lemma 2.1 implies

$$(2.3^k) \qquad f^k(c^k, c^k, \dots, c^k) = c^k \text{ for all } k = 1, 2, \dots, q$$

Now, we consider two possibilities:

(i) $c^k = 0$, hence, according to (2.3^k), it follows: $f^k(0, 0, \dots, 0) = 0$ which, independently of the value of $f^k(1, 1, \dots, 1)$, implies

$$(2.2^k) \qquad f^k(0, 0, \dots, 0) \leqslant c^k \leqslant f^k(1, 1, \dots, 1).$$

(ii) $c^k = 1$, hence, according to (2.3^k), it follows: $f^k(1, 1, \dots, 1) = 1$ which, independently of the value of $f^k(0, 0, \dots, 0)$, implies (2.2^k).

In any case, (2.2^k) holds for all $k = 1, 2, \dots, q$ and from Lemma 1.1 we have that (2.2) holds, which implies (2.1).

Besides (2.1), there are two other possibilities:
$f(0, 0, \dots, 0)$ and $f(1, 1, \dots, 1)$ to be noncomparable and
$f(0, 0, \dots, 0) \geqslant f(1, 1, \dots, 1)$. The latter case is considered in the following theorem.

THEOREM 2.3. *For every Boolean function $f:B^n \to B$, the following two conditions are equivalent:*

$$(2.4) \qquad f(0, 0, \dots, 0) \geqslant f(1, 1, \dots, 1)$$

$$(2.5) \qquad f(c, c, \dots, c) = f(1, 1, \dots, 1) \vee c' f(0, 0, \dots, 0) \text{ for all } c \in B.$$

Proof. Let (2.4) be true. Then, from Lemma 1.1, we have:

$$(2.4^k) \qquad f^k(0, 0, \dots, 0) \geqslant f^k(1, ,1 \dots, 1) \text{ for all } k = 1, 2, \dots, q$$

Now, the relation

$$(2.5^k) \qquad f^k(c^k, c^k, \dots, c^k) = f^k(1, 1, \dots, 1) \vee (c^k)' f^k(0, 0, \dots, 0)$$

is true for all $k = 1, 2, \dots, q$, because for $c^k = 0$ it becomes: $f^k(0, 0, \dots, 0) = f^k(1, 1, \dots, 1) \vee f^k(0, 0, \dots, 0)$, which is equivalent to (2.4^k) and for $c^k = 1$ we obtain an identity. So, (2.5) is true.

Conversely, let (2.5) be true, for all $c \in B$. Taking $c = 0$, we obtain: $f(0, 0, \dots, 0) = f(1, 1, \dots, 1) \vee f(0, 0, \dots, 0)$ which is equivalent to (2.4).

REMARK. It is easy to see that

$$\langle [f(1,1,\ldots,1), f(0,0,\ldots,0)], \vee, \cdot, ', f(1,1,\ldots,1), f(0,0,\ldots,0)\rangle$$

is a Boolean algebra, where $f: B^n \to B$ is any BFn satisfying (2.4), and for any $c \in [f(1,1,\ldots,1), f(0,0,\ldots,0)]$:
$c' = f(c,c,\ldots,c)$; however $[f(1,1,\ldots,1), f(0,0,\ldots,0)]$ is not a subalgebra of $\langle B, \vee, 0, ', 0, 1\rangle$.

3. It is worth pointing out some consequences of the previous theorems, concerning the numbers of constant-preserving functions over the finite Boolean algebra having 2^q elements.

COROLLARY 1. A Boolean function $f: B^n \to B$ preserves all constants (i. e. $f(a,a,\ldots,a)=a$ for all $a \in B$ iff it preserves the constants 0 and 1 (i. e iff $f(0,0,\ldots,0)=0$ and $f(1,1,\ldots,1)=1$.

COROLLARY 2. A Boolean function $f: B^n \to B$ preserves exactly one constant $a \in B$ iff $f(0,0,\ldots,0)=a$ and $f(1,1,\ldots,1)=a$.

COROLLARY 3. For any Boolean function $f: B^n \to B$, the following two conditions are equivalent:

(i) $f(a,a,\ldots,a) \neq a$ for all $a \in B$

(ii) $f(0,0,\ldots,0) \not\leq f(1,1,\ldots,1)$.

COROLLARY 4. For any Boolean function $f: B^n \to B$, the following two conditions are equivalent:

(i) $f(a,a,\ldots,a)=a'$ for all $a \in B$

(ii) $f(0,0,\ldots,0)=1$ and $f(1,1,\ldots,1)=0$.

COROLLARY 5. Let $\langle B, \vee, 0, ', 0, 1\rangle$ be a finite Boolean algebra having 2^q elements. Then, the number of Boolean functions $f: B^n \to B$ preserving at least one constant is $3^q \cdot 2^{q(2^n-2)}$; the number of BFn not preserving any constant is $2^{q(2^n-2)}(2^{2q}-3^q)$; the number of BFn preserving all constants of a given interval and only them is $2^{q(2^n-2)}$ (it is worth remarking that this number is independent of the interval); the number of BFn preserving exactly 2^m constants $(0 \leq m \leq q)$ is $\binom{q}{m} \cdot 2^{q(2^n-1)-m}$.

COROLLARY 6. Any simple Boolean function $f: B^n \to B$ belongs to one and only one of the following four classes:

K_{00} — the class of SBFn preserving only constant 0;

K_{01} — the class of SBFn preserving all constants;

K_{10} — the class of SBFn not preserving any constant;

K_{11} — the class of functions preserving only constant 1.

A SBFn belongs to the class K_{ij} $(i, j \in \{0, 1\})$ iff $f(0,0,\ldots 0)=i$ and $f(1,1,\ldots,1)=j$.

Any of the class K_{ij} contains exactly 2^{2^n-2} functions.

REFERENCES

[1] S. Rudeanu, *Boolean functions and equations*, North-Holland, 1974.

[2] J. Metelka, *Vektorielles Modell der endlichen Booleschen Algebren*, Acta Universitatis Palackianea Olomucensis, 1966.

O KLASI BULOVIH FUNKCIJA KOJE ČUVAJU KONSTANTE NAD KONAČNIM BULOVIM ALGEBRAMA

Ratko Tošić

REZIME

U radu se ispituje klasa Bulovih funkcija od n promenljivih (BFn) koje čuvaju konstante nad konačnim Bulovim algebrama. Za BFn $f:B^n\to B$ kažemo da čuva konstantu a akko $f(a, a, \ldots, a)=a$.

Dokazana su sledeća tvrđenja:

TEOREMA 2.1. *Neka BFn zadovoljava uslov*

(2.1) $f(0, 0, \ldots, 0)\leq f(1, 1, \ldots, 1)$.

Tada je $f(c, c, \ldots, c)=c$ *akko*

(2.2) $f(0, 0, \ldots, 0)\leq c\leq f(1, 1, \ldots, 1)$.

TEOREMA 2.2. *Potreban i dovoljan uslov da BFn* $f:B^n\to B$ *čuva barem jednu konstantu je*

(2.1) $f(0, 0, \ldots, 0)\leq f(1, 1, \ldots, 1)$.

TEOREMA 2.3. *Za svaku BFn* $f:B^n\to B$, *sledeća dva tvrđenja su ekvivalentna*:

(2.4) $f(0, 0, \ldots, 0)\geq f(1, 1, \ldots, 1)$

(2.5) $f(c, c, \ldots, c)=f(1, 1, \ldots, 1)\vee c'f(0, 0, \ldots, 0)$ za svaki $c\in B$.

Izveden je niz posledica koje se odnose na broj BFn koje čuvaju konstante nekog intervala i broj BFn koje čuvaju određen broj konstanti. Izvršena je klasifikacija prostih BFn na četiri klase iste kardinalnosti.