Serdica J. Computing **2** (2008), 249–266

Serdica
Journal of Computing

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

ESSENTIAL ARITY GAP OF BOOLEAN FUNCTIONS

Slavcho Shtrakov

Abstract. In this paper we investigate the Boolean functions with maximum essential arity gap. Additionally we propose a simpler proof of an important theorem proved by M. Couceiro and E. Lehtonen in [3]. They use Zhegalkin's polynomials as normal forms for Boolean functions and describe the functions with essential arity gap equals 2. We use to instead Full Conjunctive Normal Forms of these polynomials which allows us to simplify the proofs and to obtain several combinatorial results concerning the Boolean functions with a given arity gap. The Full Conjunctive Normal Forms are also sum of conjunctions , in which all variables occur.

1. Introduction. Essential variables of functions have been studied by several authors [1, 2, 4]. In this paper we consider the problem of simplification of functions by identification of variables. This problem is discussed in the work of O. Lupanov, Yu. Breitbart, A. Salomaa, M. Couceiro, E. Lehtonen, etc., for Boolean functions and by K. Chimev for arbitrary discrete functions. Similar

ACM Computing Classification System (1998): G.2.0.
Key words: essential variable, identification minor, essential arity gap.

problems for terms and universal algebra are studied by the author and K. Denecke [7]. Essential input variables for tree automata are discussed in [6]. The problems concerning essential arity gap of functions are discussed in [3]. Here we study and count the Boolean functions which have maximum arity gap. Note that if a function f has greater essential arity gap than the essential arity gap of another function g, then f has a simpler automaton realization than g. This fact is of a great importance in theoretical and applied computer science and modeling.

2. Essential variables in Boolean functions.

Let $B = \{0, 1\}$ be the set (ring) of the residua modulo 2. An *n-ary Boolean function (operation)* is a mapping $f : B^n \to B$ for some natural number n, called *arity* of f. The set of all such functions is denoted by P_2^n.

A variable x_i is called *essential* in f, or f *essentially depends* on x_i, if there exist values $a_1, \ldots, a_n, b \in B$, such that

$$f(a_1, \ldots, a_{i-1}, a_i, a_{i+1}, \ldots, a_n) \neq f(a_1, \ldots, a_{i-1}, b, a_{i+1}, \ldots, a_n).$$

The set of essential variables in a function f is denoted by $Ess(f)$ and the number of essential variables in f is denoted by $ess(f) = |Ess(f)|$. The variables from $X = \{x_1, \ldots, x_n\}$ which are not essential in $f \in P_2^n$ are called *fictive* and the set of fictive variables in f is denoted by $Fic(f)$.

Let x_i and x_j be essential variables in f. We say that the function g is obtained from $f \in P_2^n$ by *identification of a variable x_i with x_j*, if

$$g(x_1, \ldots, x_n) = f(x_1, \ldots, x_{i-1}, x_j, x_{i+1}, \ldots, x_n) = f(x_i = x_j).$$

Briefly, when g is obtained from f, by identification of the variable x_i with x_j, we will write $g = f_{i \leftarrow j}$ and g is called *the identification minor of f*. The set of all identification minors of f will be denoted by $Min(f)$.

For completeness of our consideration we allow to be obtained identification minors when x_i or x_j are not essential in f, also. Thus if x_i does not occur in f, then we define $f_{i \leftarrow j} := f$.

Clearly, $ess(f_{i \leftarrow j}) \leq ess(f)$, because $x_i \notin Ess(f_{i \leftarrow j})$, even though it may be essential in f.

For a function $f \in P_2^n$ the *essential arity gap* (shortly *arity gap*) of f is defined as follows

$$gap(f) := ess(f) - \max_{g \in Min(f)} ess(g).$$

It is not difficult to see that the functions with huge gap are simpler for realization by switching circuits and functional schemas in theoretical and applied computer science.

Let us denote by G_p^m the set of all functions in P_2^n which essentially depend on m variables and have gap equals to p i.e. $G_p^m = \{f \in P_2^n \mid ess(f) = m \ \& \ gap(f) = p\}$, with $m \leq n$.

An upper bound of $gap(f)$ for Boolean functions is found by K. Chimev, A. Salomaa and O. Lupanov [2, 4, 5]. It is shown that $gap(f) \leq 2$, when $f \in P_2^n, \ n \geq 2$.

This result is generalized for arbitrary finite valued functions in [3]. It is proved that $gap(f) \leq k$ for all $f \in P_k^n$, $n \geq k$.

Let $m \in N$, $0 \leq m \leq 2^n - 1$ be an integer. It is well known that for every $n \in N$, there is a unique finite sequence $(\alpha_1, \ldots, \alpha_n) \in B^n$ such that

$$m = \alpha_1 2^{n-1} + \alpha_2 2^{n-2} + \ldots + \alpha_n. \tag{1}$$

The equation (1) is known as the presentation of m in binary positional numerical system. One briefly writes $m = \overline{\alpha_1 \alpha_2 \ldots \alpha_n}$ instead of (1)for short.

For a variable x and $\alpha \in B$, we define the following important function:

$$x^\alpha = \begin{cases} 1 & \text{if} \quad x = \alpha \\ 0 & \text{if} \quad x \neq \alpha. \end{cases}$$

This function is used in many investigation, concerning the applications of discrete functions in computer science [2].

There are many normal forms for representation of functions from P_2^n. In this paper we will use the *Full Conjunctive Normal Form (FCNF)* for studying the essential arity gap of functions. This normal form is based on the table representation of Boolean functions.

The next two theorems are in the basis of the Theory of Boolean functions, and they are well known.

Theorem 2.1. *Each function $f \in P_2^n$ can be uniquely represented in FCNF as follows*

$$f(x_1, \ldots, x_n) = a_0.x_1^0 \ldots x_n^0 \oplus \ldots a_m.x_1^{\alpha_1} \ldots x_n^{\alpha_n} \oplus \ldots a_{2^n-1}.x_1^1 \ldots x_n^1 \tag{2}$$

where $m = \overline{\alpha_1 \ldots \alpha_n}$, $a_m \in B$ and "$\oplus$", and "." are the operations addition and multiplication modulo 2 in the ring B.

Theorem 2.2. *A variable x_i is fictive in the function $f \in P_2^n$, if and only if*

$$f(x_1, \ldots, x_n) =$$

$$= x_i^0.f_1(x_1,\dots,x_{i-1},x_{i+1},\dots,x_n) \;\oplus\; x_i^1.f_2(x_1,\dots,x_{i-1},x_{i+1},\dots,x_n),$$

with $f_1 = f_2$ *and* $x_i \notin Ess(f_j)$*, where* $f_j \in P_2^{n-1}$*, for* $j = 1, 2$.

The next lemmas characterize the relation between the identification minors of Boolean functions.

Lemma 2.1. *Let* $f, g \in P_2^n$ *be two Boolean functions represented by their FCNF as follows*

$$f = \bigoplus_{m=0}^{2^{n-1}-1} a_m.x_1^{\alpha_1}\dots x_n^{\alpha_n} \quad \textit{and} \quad g = \bigoplus_{m=0}^{2^{n-1}-1} b_m.x_1^{\alpha_1}\dots x_n^{\alpha_n},$$

where $m = \overline{\alpha_1\dots\alpha_n}$*. If* $f_{i\leftarrow j} = g_{i\leftarrow j}$ *and* $\alpha_i = \alpha_j$ *for some* $i,\ j$ *with* $1 \le j < i \le n$*, then* $a_m = b_m$.

P r o o f. Without loss of generality we will prove the lemma for $i = 2$ and $j = 1$. Since $f_{2\leftarrow 1} = g_{2\leftarrow 1}$ we have

$$f(x_1, x_1, x_3, \dots, x_n) = g(x_1, x_1, x_3, \dots, x_n).$$

Hence

$$a_m = f(\alpha_1, \alpha_1, \alpha_3, \dots, \alpha_n) = g(\alpha_1, \alpha_1, \alpha_3, \dots, \alpha_n) = b_m.$$

$\square$

Lemma 2.2. *Let* $f, g \in P_2^n$*, be two functions, depending essentially on* n*,* $n \ge 3$ *variables. If* $f_{i\leftarrow j} = g_{i\leftarrow j}$ *for all* i, j*,* $1 \le j < i \le n$*, then* $f = g$.

P r o o f. Let f and g be functions represented by their FCNF as in Lemma 2.1. Let $m = \alpha_1.2^{n-1} + \alpha_2.2^{n-2} + \dots + \alpha_n$ be an arbitrary integer from $\{0, 1, \dots, 2^n - 1\}$. Since $n \ge 3$ there exist two natural numbers $i,\ j$ with $1 \le j < i \le n$ and $\alpha_i = \alpha_j$. From Lemma 2.1 we obtain

$$a_m = f(\alpha_1, \alpha_2, \dots, \alpha_n) = g(\alpha_1, \alpha_2, \dots, \alpha_n) = b_m.$$

Consequently, we have $f = g$. $\square$

Example 2.1. *Let us consider the Boolean functions* $f = x_1^0x_2^0 \oplus x_1^1x_2^0$ *and* $g = x_1^0x_2^0 \oplus x_1^0x_2^1$*. It is easy to see that for all* i, j*,* $1 \le j < i \le n$ *we have* $f_{i\leftarrow j} = g_{i\leftarrow j} = x_1^0$*, but* $f \ne g$*. This example shows that* $n \ge 3$ *is an essential condition in Lemma* 2.2.

3. Essential Arity Gap of Boolean Functions. For Boolean functions $\neg(x)$ denotes the unary operation negation, i.e.

$$\neg x = x^0 = \begin{cases} 1 & \text{if} \quad x = 0 \\ 0 & \text{if} \quad x \neq 0. \end{cases}$$

Proposition 3.1. *For each Boolean function f the following sentences are held:*

(i) $gap(f(x_1, \ldots, x_n)) = gap(f(\neg x_1, \ldots, \neg x_n))$;

(ii) $gap(f(x_1, \ldots, x_n)) = gap(\neg(f(x_1, \ldots, x_n)))$;

(iii) $gap(f(x_1, \ldots, x_n)) = gap(f(x_{\pi(1)}, \ldots, x_{\pi(n)}))$, *where* $\pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$ *is a permutation of the set* $\{1, \ldots, n\}$;

(iv) $ess(f_{i\leftarrow j}) = ess(f_{j\leftarrow i})$ *for all* $i, j,\ 1 \leq j < i \leq n$.

Note that the last two assertions *(iii)* and *(iv)* are valid in the more general case of k-valued functions.

For any natural number $n, n \geq 2$ we define the following two sets:

$$Od_2^n := \{\alpha_1\alpha_2 \ldots \alpha_n \in \{0, 1\}^n \mid \alpha_1 \oplus \alpha_2 \oplus \ldots \oplus \alpha_n = 1\}$$

and

$$Ev_2^n := \{\alpha_1\alpha_2 \ldots \alpha_n \in \{0, 1\}^n \mid \alpha_1 \oplus \alpha_2 \oplus \ldots \oplus \alpha_n = 0\}.$$

Clearly, $\alpha_1\alpha_2 \ldots \alpha_n \in Od_2^n$ if and only if the number of 1's in $\alpha_1\alpha_2 \ldots \alpha_n$ is odd, and $\alpha_1\alpha_2 \ldots \alpha_n \in Ev_2^n$ when this number is even.

Proposition 3.2. *For any n, $n \geq 4$, if*

$$f = \bigoplus_{\alpha_1 \ldots \alpha_n \in Od_2^n} x_1^{\alpha_1} \ldots x_n^{\alpha_n} \quad \text{or} \quad f = \bigoplus_{\alpha_1 \ldots \alpha_n \in Ev_2^n} x_1^{\alpha_1} \ldots x_n^{\alpha_n},$$

then $f \in G_2^n$.

Proof. Without loss of generality let us assume that $f = \bigoplus_{\alpha_1 \ldots \alpha_n \in Od_2^n} x_1^{\alpha_1} \ldots x_n^{\alpha_n}$. We have to show that $ess(f_{i\leftarrow j}) \leq n - 2$ for all $i, j,\ 1 \leq j < i \leq n$. Without loss of generality, again we will assume $i = 2$ and $j = 1$. Then we have

$$f_{2\leftarrow 1} = \bigoplus_{\alpha_1, \alpha_3, \ldots \alpha_n \in Od_2^{n-1}} x_1^{\alpha_1} x_3^{\alpha_3} \ldots x_n^{\alpha_n} =$$

$$= x_1^0 . \left[\bigoplus_{\alpha_3, \ldots \alpha_n \in Od_2^{n-2}} x_3^{\alpha_3} \ldots x_n^{\alpha_n} \right] \oplus x_1^1 . \left[\bigoplus_{\alpha_3, \ldots \alpha_n \in Od_2^{n-2}} x_3^{\alpha_3} \ldots x_n^{\alpha_n} \right] =$$

$$= \bigoplus_{\alpha_3,\ldots\alpha_n \in Od_2^{n-2}} x_3^{\alpha_3} \ldots x_n^{\alpha_n}.$$

The result is the same when $\alpha_1 \ldots \alpha_n \in Ev_2^n$. $\square$

We are going to describe the set G_2^n for $n = 2, 3, 4$. The results for $n = 4$ can be easily extended in the more general case of $n \geq 4$.

Theorem 3.1. *Let $f \in P_2^2$. Then $f \in G_2^2$ if and only if*

$$f = a_0.(x_1^0 x_2^0 \ \oplus \ x_1^1 x_2^1) \oplus a_1.x_1^0 x_2^1 \oplus a_2.x_1^1 x_2^0, \quad \textit{with } a_1 \neq a_0 \quad \textit{or} \quad a_2 \neq a_0.$$

P r o o f. Let $f = a_0.x_1^0 x_2^0 \oplus a_1.x_1^0 x_2^1 \oplus a_2.x_1^1 x_2^0 \oplus a_3.x_1^1 x_2^1$. The variables x_1 and x_2 are essential in f if and only if $(a_0, a_1) \neq (a_2, a_3)$ and $(a_0, a_2) \neq (a_1, a_3)$. Consider the identification minor $h := f_{2\leftarrow 1} = a_0.x_1^0 \oplus a_3.x_1^1$ of f. We need $ess(h) = 0$ and from Theorem 2.2 it follows $a_0 = a_3$. If we suppose that $a_1 = a_2 = a_0$, then $f(x_1, x_2) = a_0$, which contradicts $ess(f) = 2$. $\square$

Corollary 3.1. *There are 6 functions in G_2^2, i.e. $|G_2^2| = 6$.*

P r o o f. Let $a_0 \in \{0, 1\}$. For a_1 and a_2 there are 3 possible choices which satisfy Theorem 3.1. The cases $a_1 = a_2 = a_0 = 0$ and $a_1 = a_2 = a_0 = 1$ are both impossible because then $ess(f) < 2$, since Theorem 2.2. $\square$

Corollary 3.2. *If $f = a_0.x_1^0 x_2^0 \oplus a_1.x_1^0 x_2^1 \oplus a_2.x_1^1 x_2^0 \oplus a_3.x_1^1 x_2^1 \in P_2^2$ then $ess(f_{2\leftarrow 1}) = 0$ if and only if $a_0 = a_3$.*

The next step is to describe the functions which essentially depend on 3 variables and have an essential arity gap equal to 2.

Theorem 3.2. *Let f be a Boolean function of three variables. Then $f \in G_2^3$ if and only if it can be represented in one of the following special forms:*

$$f = x_3^{\alpha}(x_1^0 x_2^1 \ \oplus \ x_1^1 x_2^0) \ \oplus \ x_1^{\beta} x_2^{\beta}, \tag{3}$$

or

$$f = x_3^{\alpha}(x_1^0 x_2^0 \ \oplus \ x_1^1 x_2^1) \ \oplus \ x_3^{\neg(\alpha)}(x_1^0 x_2^1 \ \oplus \ x_1^1 x_2^0), \tag{4}$$

where $\alpha, \beta \in \{0, 1\}$.

P r o o f. Note that the presentation of f in (4) is symmetric with respect to the variables, but in (3) f is not symmetric with respect to the variables x_1

and x_3. So, the theorem asserts that $f \in G_2^3$ if and only if f can be represented in one of the forms (3) or (4), after a suitable permutation of the variables.

"$\Leftarrow$": Clearly, x_1, x_2 and x_3 are essential variables in the functions of the right sides of (3) and (4). To see that $f \in G_2^3$ it is enough to do an immediate check. Thus for the function f in (3) we have $f_{2\leftarrow 1} = x_1^\beta$,

$$f_{3\leftarrow 1} = \begin{cases} x_1^\beta & \text{if} \quad \beta = \alpha \\ x_2^\beta & \text{if} \quad \beta \neq \alpha \end{cases} \quad \text{and} \quad f_{3\leftarrow 2} = \begin{cases} x_2^\beta & \text{if} \quad \beta = \alpha \\ x_1^\beta & \text{if} \quad \beta \neq \alpha. \end{cases}$$

The functions f as in (4) are in G_2^3 because $x_i, x_j \notin Ess(f_{i\leftarrow j})$ for all $i, j,\ 1 \leq j < i \leq 3$.

"$\Rightarrow$": Assume that $f \in G_2^3$. Let the FCNF of f is written as follows:

$$\begin{aligned} f = x_3^0(a_0.x_1^0x_2^0 \;\oplus\; a_1.x_1^0x_2^1 \;\oplus\; a_2.x_1^1x_2^0 \;\oplus\; a_3.x_1^1x_2^1) \;\oplus \\ \oplus x_3^1(a_4.x_1^0x_2^0 \;\oplus a_5.x_1^0x_2^1 \;\oplus a_6.x_1^1x_2^0 \;\oplus a_7.x_1^1x_2^1) = \\ = x_3^0.g(x_1, x_2) \;\oplus\; x_3^1.h(x_1, x_2). \end{aligned}$$

A. Suppose that $x_1 \in Ess(g_{2\leftarrow 1})$ or $x_1 \in Ess(h_{2\leftarrow 1})$. Then $x_1 \in Ess(f_{2\leftarrow 1})$ because $f_{2\leftarrow 1}(x_3 = 0) = g_{2\leftarrow 1}$ and $f_{2\leftarrow 1}(x_3 = 1) = h_{2\leftarrow 1}$. Hence $f \in G_2^3$ implies $x_3 \notin Ess(f_{2\leftarrow 1})$ i.e $g_{2\leftarrow 1} = h_{2\leftarrow 1}$. Consequently, $a_0 = a_4$ and $a_3 = a_7$. Then we obtain

$$u = f_{3\leftarrow 1} = a_0.x_1^0x_2^0 \;\oplus\; a_1.x_1^0x_2^1 \;\oplus\; a_6.x_1^1x_2^0 \;\oplus\; a_7.x_1^1x_2^1,$$

and

$$v = f_{3\leftarrow 2} = a_0.x_1^0x_2^0 \;\oplus\; a_2.x_1^1x_2^0 \;\oplus\; a_5.x_1^0x_2^1 \;\oplus\; a_7.x_1^1x_2^1.$$

There are the following cases:

A.a. $x_1 \notin Ess(u)$. Hence $a_0 = a_6$ and $a_1 = a_7$.

A.a.1. If we suppose that $x_1 \notin Ess(v)$, then $a_0 = a_2$ and $a_5 = a_7$ implies (according to Theorem 2.2) that $x_1, x_3 \notin Ess(f)$ and $f \notin G_2^3$.

A.a.2. If $x_2 \notin Ess(v)$, then $a_0 = a_5$ and $a_2 = a_7$. Note that if $a_0 = a_7$, then f has to be a constant. Hence $a_7 = \neg(a_0)$. Then we obtain

$$\begin{aligned} f = a_0.\big[x_1^0x_2^0x_3^0 \;\oplus\; x_1^0x_2^0x_3^1 \;\oplus\; x_1^0x_2^1x_3^1 \;\oplus\; x_1^1x_2^0x_3^1\big] \;\oplus \\ \oplus\; \neg(a_0).\big[x_1^0x_2^1x_3^0 \;\oplus x_1^1x_2^0x_3^0 \;\oplus x_1^1x_2^1x_3^0 \;\oplus x_1^1x_2^1x_3^1\big] = \\ = a_0\big[x_3^1(x_1^0x_2^1 \;\oplus\; x_1^1x_2^0) \;\oplus\; x_1^0x_2^0\big] \;\oplus\; \neg(a_0)\big[x_3^0(x_1^0x_2^1 \;\oplus\; x_1^1x_2^0) \;\oplus\; x_1^1x_2^1\big] \in G_2^3. \end{aligned}$$

Clearly, f is presented as in (3).

A.b. $x_2 \notin Ess(u)$. Hence $a_0 = a_1$ and $a_6 = a_7$.

A.b.1. If we suppose that $x_2 \notin Ess(v)$, then $a_0 = a_5$ and $a_2 = a_7$ implies (according to Theorem 2.2) that $x_2, x_3 \notin Ess(f)$ and $f \notin G_2^3$.

A.b.2. If $x_1 \notin Ess(v)$, then $a_0 = a_2$ and $a_5 = a_7$. Again, if $a_0 = a_7$, then f has to be a constant. Hence $a_7 = \neg(a_0)$. Then we obtain

$$f = a_0.\big[x_1^0x_2^0x_3^0 \ \oplus \ x_1^0x_2^0x_3^1 \ \oplus \ x_1^0x_2^1x_3^0 \ \oplus \ x_1^1x_2^0x_3^0\big] \oplus$$

$$\oplus \ \neg(a_0).\big[x_1^0x_2^1x_3^1 \ \oplus x_1^1x_2^0x_3^1 \ \oplus x_1^1x_2^1x_3^0 \ \oplus x_1^1x_2^1x_3^1\big] =$$

$$= a_0\big[x_3^0(x_1^0x_2^1 \ \oplus \ x_1^1x_2^0) \ \oplus \ x_1^0x_2^0\big] \ \oplus \ \neg(a_0)\big[x_3^1(x_1^0x_2^1 \ \oplus \ x_1^1x_2^0) \ \oplus \ x_1^1x_2^1\big] \in G_2^3.$$

Clearly, f is presented as in (3).

B. Let us suppose that $x_1 \notin Ess(g_{2\leftarrow 1})$ and $x_1 \notin Ess(h_{2\leftarrow 1})$. Then we have $g \in G_2^2$ and $h \in G_2^2$. From Theorem 3.1 it follows that

$$g(x_1, x_2) = a_0.(x_1^0x_2^0 \ \oplus \ x_1^1x_2^1) \ \oplus \ a_1.x_1^0x_2^1 \ \oplus \ a_2.x_1^1x_2^0,$$

and

$$h(x_1, x_2) = a_4.(x_1^0x_2^0 \ \oplus \ x_1^1x_2^1) \ \oplus \ a_5.x_1^0x_2^1 \ \oplus \ a_6.x_1^1x_2^0.$$

Then we obtain

$$u = f_{3\leftarrow 1} = a_0.x_1^0x_2^0 \ \oplus \ a_1.x_1^0x_2^1 \ \oplus \ a_6.x_1^1x_2^0 \ \oplus \ a_4.x_1^1x_2^1,$$

and

$$v = f_{3\leftarrow 2} = a_0.x_1^0x_2^0 \ \oplus \ a_2.x_1^1x_2^0 \ \oplus \ a_5.x_1^0x_2^1 \ \oplus \ a_4.x_1^1x_2^1.$$

B.a. $x_1 \notin Ess(u)$. Hence $a_0 = a_6$ and $a_1 = a_4$.

B.a.1. If $x_1 \notin Ess(v)$, then $a_0 = a_2$ and $a_4 = a_5$. Note that if $a_0 = a_4$, then f has to be a constant. Hence $a_4 = \neg(a_0)$. Then we obtain

$$f = a_0.\big[x_1^0x_2^0x_3^0 \ \oplus \ x_1^1x_2^0x_3^0 \ \oplus \ x_1^1x_2^0x_3^1 \ \oplus \ x_1^1x_2^1x_3^0\big] \oplus$$

$$\oplus \ \neg(a_0).\big[x_1^0x_2^0x_3^1 \ \oplus x_1^0x_2^1x_3^0 \ \oplus x_1^0x_2^1x_3^1 \ \oplus x_1^1x_2^1x_3^1\big] =$$

$$= a_0\big[x_1^1(x_2^0x_3^1 \ \oplus \ x_2^1x_3^0) \ \oplus \ x_2^0x_3^0\big] \ \oplus \ \neg(a_0)\big[x_1^0(x_2^0x_3^1 \ \oplus \ x_2^1x_3^0) \ \oplus \ x_2^1x_3^1\big] \in G_2^3.$$

Clearly, f is presented as in (3).

B.a.2. If $x_2 \notin Ess(v)$, then $a_0 = a_5$ and $a_2 = a_4$. Again, if $a_0 = a_4$, then f has to be a constant. Hence $a_4 = \neg(a_0)$. Then we obtain

$$f = a_0.\big[x_1^0x_2^0x_3^0 \;\oplus\; x_1^0x_2^1x_3^1 \;\oplus\; x_1^1x_2^0x_3^1 \;\oplus\; x_1^1x_2^1x_3^0\big] \oplus$$

$$\oplus\ \neg(a_0).\big[x_1^0x_2^0x_3^1 \;\oplus x_1^0x_2^1x_3^0 \;\oplus x_1^1x_2^0x_3^0 \;\oplus x_1^1x_2^1x_3^1\big] =$$

$$= a_0\big[x_3^0(x_1^0x_2^0 \;\oplus\; x_1^1x_2^1) \;\oplus\; x_3^1(x_1^1x_2^0 \;\oplus\; x_1^0x_2^1)\big] \oplus$$

$$\oplus\ \neg(a_0)\big[x_3^1(x_1^0x_2^0 \;\oplus\; x_1^1x_2^1) \;\oplus\; x_3^0(x_1^1x_2^0 \;\oplus\; x_1^0x_2^1)\big] \in G_2^3.$$

Clearly, f is presented as in (4).

B.b. $x_2 \notin Ess(u)$. Hence $a_0 = a_1$ and $a_6 = a_4$.

B.b.1. If we suppose that $x_1 \notin Ess(v)$, then $a_0 = a_2$ and $a_4 = a_5$ implies (according Theorem 2.2) that $x_1, x_2 \notin Ess(f)$ and $f \notin G_2^3$.

B.b.2. If $x_2 \notin Ess(v)$, then $a_0 = a_5$ and $a_2 = a_4$. Again, if $a_0 = a_4$, then f has to be a constant. Hence $a_4 = \neg(a_0)$. Then we obtain

$$f = a_0.\big[x_1^0x_2^0x_3^0 \;\oplus\; x_1^0x_2^1x_3^0 \;\oplus\; x_1^0x_2^1x_3^1 \;\oplus\; x_1^1x_2^1x_3^0\big] \oplus$$

$$\oplus\ \neg(a_0).\big[x_1^0x_2^0x_3^1 \;\oplus x_1^1x_2^0x_3^0 \;\oplus x_1^1x_2^0x_3^1 \;\oplus x_1^1x_2^1x_3^1\big] =$$

$$= a_0\big[x_2^1(x_1^0x_3^1 \;\oplus\; x_1^1x_3^0) \;\oplus\; x_1^0x_3^0\big] \;\oplus\; \neg(a_0)\big[x_2^0(x_1^0x_3^1 \;\oplus\; x_1^1x_3^0) \;\oplus\; x_1^1x_3^1\big] \in G_2^3.$$

Clearly, f is presented as in (3). □

Corollary 3.3. *Let $f \in P_2^3$. Then $ess(f_{i\leftarrow j}) \le 1$ for all $i, j,\ 1 \le j < i \le 3$ if and only if*

$$\begin{aligned} f \;\;=\;\; & x_3^\alpha(x_1^0x_2^0 \;\oplus\; x_1^1x_2^1) \;\oplus\; a_1.x_1^0x_2^1x_3^0 \;\oplus\; a_2.x_1^1x_2^0x_3^0 \;\oplus \\ & \oplus\ \neg(a_2).x_1^0x_2^1x_3^1 \;\oplus\; \neg(a_1).x_1^1x_2^0x_3^1, \end{aligned}$$

where $\alpha, a_1, a_2 \in \{0, 1\}$.

Proof. This Corollary summarizes all cases considered in Theorem 3.2. For instance if $\alpha = 1$, $a_1 = 0$ and $a_2 = 0$ we obtain

$$f = x_3^1(x_1^0x_2^0 \;\oplus\; x_1^1x_2^1) \;\oplus\; x_1^0x_2^1x_3^1 \;\oplus\; x_1^1x_2^0x_3^1 \;= x_3^1.$$

This is the case **B.b.1**. □

Corollary 3.4. $|G_2^3| = 10$.

P r o o f. As we have noted the functions f in the form (4) are symmetric with respect to their variables. Hence there are exactly two such functions, obtained for $\alpha = 1$ and $\alpha = 0$. These functions are realized in the case **B.a.2.**

Let us consider the functions f in the form (3) with $\alpha = \beta$. Then we have

$$f = x_1^0 x_2^1 x_3^\alpha \ \oplus\ x_1^1 x_2^0 x_3^\alpha \ \oplus\ x_1^\alpha x_2^\alpha x_3^0 \ \oplus\ x_1^\alpha x_2^\alpha x_3^1.$$

It is easy to check that in both cases $\alpha = 1$ and $\alpha = 0$ the function f is symmetric. Hence there exist exactly two functions from P_2^2 in the form (3) with $\alpha = \beta$. These two functions are realized in the case **A.b.2.**

Finally, let us consider the functions in the form

$$f = x_3^\alpha (x_1^0 x_2^1 \ \oplus\ x_1^1 x_2^0) \ \oplus\ x_1^{\neg\alpha} x_2^{\neg\alpha}. \tag{5}$$

Since $f(\alpha, \beta, \neg(\alpha)) = 0$ and $f(\neg(\alpha), \beta, \alpha) = 1$ for all $\beta \in \{0, 1\}$ it follows that f is not symmetric with respect to x_1 and x_3. Furthermore, it is clear that f is symmetric with respect to x_1 and x_2. Hence there are exactly six functions from P_2^3 in the form (5). When $\alpha = 1$ we obtain three function by three permutations of the variables and the same number of functions for $\alpha = 0$. These functions are realized in the cases: **A.a.2.**, **B.a.1.** and **B.b.2.** $\Box$

Lemma 3.1. *Let $f = x_4^0.g(x_1, x_2, x_3) \oplus x_4^1.h(x_1, x_2, x_3) \in P_2^4$. If $f \in G_2^4$, then $ess(g_{i\leftarrow j}) < 2$ and $ess(h_{i\leftarrow j}) < 2$ for all $i, j,\ 1 \le i < j \le 3$.*

P r o o f. Let us suppose that the lemma is false. Without loss of generality let us assume $ess(g_{2\leftarrow 1}) \ge 2$. If $f \in G_2^4$, then $x_4 \notin Ess(f_{2\leftarrow 1})$ because

$$f_{2\leftarrow 1} = x_4^0.g_{2\leftarrow 1} \oplus x_4^1.h_{2\leftarrow 1} \ \text{ and } \ f_{2\leftarrow 1}(x_4 = 0) = g_{2\leftarrow 1}.$$

From Theorem 2.2 it follows that $g_{2\leftarrow 1} = h_{2\leftarrow 1}$. Let us set

$$g := \bigoplus_{m=0}^{7} a_m^{(0)}.x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} \ \text{ and } \ h := \bigoplus_{m=0}^{7} a_m^{(1)}.x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3},$$

where $m = \overline{\alpha_1 \alpha_2 \alpha_3}$, and

$$t := a_0^{(0)}.x_1^0 x_2^0 x_3^0 \ \oplus\ a_1^{(0)}.x_1^0 x_2^0 x_3^1 \ \oplus\ a_6^{(0)}.x_1^1 x_2^1 x_3^0 \ \oplus\ a_7^{(0)}.x_1^1 x_2^1 x_3^1.$$

Then from $g_{2\leftarrow 1} = h_{2\leftarrow 1}$, we obtain

$$g := t(x_1, x_2, x_3) \oplus \left(\bigoplus_{\alpha_1 \ne \alpha_2} a_m^{(0)}.x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} \right) \ \text{ and}$$

$$h := t(x_1, x_2, x_3) \oplus \left(\bigoplus_{\alpha_1 \neq \alpha_2} a_m^{(1)}.x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} \right).$$

Note that

$$f_{2\leftarrow 1} = t_{2\leftarrow 1} = g_{2\leftarrow 1} = h_{2\leftarrow 1}.$$

If $ess(g_{2\leftarrow 1}) > 2$, then from $f_{2\leftarrow 1}(x_4 = 0) = g_{2\leftarrow 1}$ it follows that $f \notin G_2^4$. Hence $ess(g_{2\leftarrow 1}) = 2$. Thus we have $\{x_1, x_3\} = Ess(g_{2\leftarrow 1})$. This implies

$$(a_0^{(0)}, a_6^{(0)}) \neq (a_1^{(0)}, a_7^{(0)}) \text{ and } (a_0^{(0)}, a_1^{(0)}) \neq (a_6^{(0)}, a_7^{(0)}). \tag{6}$$

From $x_4 \in Ess(f)$ it follows that there are three numbers $\alpha_1, \alpha_2, \alpha_3 \in \{0, 1\}$ such that $a_m^{(0)} \neq a_m^{(1)}$ where $m = \overline{\alpha_1 \alpha_2 \alpha_3}$. Then $\alpha_1 \neq \alpha_2$. Hence we have $\alpha_1 = \alpha_3$ or $\alpha_2 = \alpha_3$.

Let us assume $\alpha_1 = \alpha_3$. Then the identification minor $u = f_{3\leftarrow 1}$ can be written as follows

$$u = a_0^{(0)}.x_1^0 x_2^0 \oplus a_7^{(0)}.x_1^1 x_2^1 \oplus x_4^0(a_2^{(0)}.x_1^0 x_2^1 \oplus a_5^{(0)}.x_1^1 x_2^0) \oplus x_4^1(a_2^{(1)}.x_1^0 x_2^1 \oplus a_5^{(1)}.x_1^1 x_2^0).$$

Without loss of generality let us assume that $a_2^{(0)} \neq a_2^{(1)}$, i.e. $m = \overline{010} = 2$. (An alternative opportunity is $m = 5$.) Then we have $a_2^{(0)} \neq 0$ or $a_2^{(1)} \neq 0$. Again, without loss of generality let us assume $a_2^{(0)} = 1$ and $a_2^{(1)} = 0$. Then $u(x_1 = \alpha_1, x_2 = \alpha_2) = a_2^{(0)}.x_4^0 \ \oplus \ a_2^{(1)}.x_4^1$. Hence $x_4 \in Ess(u)$.

On the other hand we have

$$u_1 = u(x_4 = 0) = a_0^{(0)}.x_1^0 x_2^0 \ \oplus \ a_7^{(0)}.x_1^1 x_2^1 \ \oplus \ x_1^0 x_2^1 \ \oplus \ a_5^{(0)}.x_1^1 x_2^0 \ \text{ and}$$

$$u_2 = u(x_4 = 1) = a_0^{(0)}.x_1^0 x_2^0 \ \oplus \ a_7^{(0)}.x_1^1 x_2^1 \ \oplus \ a_5^{(1)}.x_1^1 x_2^0.$$

Thus we have:
If $a_0^{(0)} = a_7^{(0)} = 0$ or $a_0^{(0)} = a_7^{(0)} = 1$, then $Ess(u_1) = \{x_1, x_2\}$.

Let $a_0^{(0)} \neq a_7^{(0)}$. Then according to (6) we can assume without loss of generality that $a_0^{(0)} = 1$ and $a_7^{(0)} = 0$. Now, we have:
If $a_5^{(0)} = 1$ or $a_5^{(1)} = 0$, then $Ess(u_1) = \{x_1, x_2\}$ or $Ess(u_2) = \{x_1, x_2\}$.

Finally, if $a_0^{(0)} = 1$, $a_7^{(0)} = 0$, $a_5^{(0)} = 0$ and $a_5^{(1)} = 1$ we have $u_1(x_1, x_2) = x_1^0$ and $u_2(x_1, x_2) = x_2^0$.

So, we have shown that $Ess(u) = \{x_1, x_2, x_4\}$. Hence $f \notin G_2^4$, which is a contradiction.

By symmetry, we obtain the same contradiction when $\alpha_2 = \alpha_3$ and we have to use the identification minor $v = f_{3\leftarrow 2}$ instead of $u = f_{3\leftarrow 1}$. $\square$

Lemma 3.2. *Let* $f = x_4^0.g(x_1, x_2, x_3) \oplus x_4^1.h(x_1, x_2, x_3) \in P_2^4$. *If* $f \in G_2^4$, *then* $ess(g) = ess(h) = 3$.

P r o o f. Let us suppose that $x_3 \notin Ess(g)$ and $f \in G_2^4$.

Let g and h are represented as follows

$$g := \bigoplus_{m=0}^{7} a_m.x_1^{\alpha_1}x_2^{\alpha_2}x_3^{\alpha_3} \quad \text{and} \quad h := \bigoplus_{m=0}^{7} b_m.x_1^{\alpha_1}x_2^{\alpha_2}x_3^{\alpha_3},$$

where $m = \overline{\alpha_1\alpha_2\alpha_3} = \alpha_1.2^2 + \alpha_2.2 + \alpha_3$. Since $x_3 \notin Ess(g)$, we obtain

$$(a_0, a_2, a_4, a_6) = (a_1, a_3, a_5, a_7). \tag{7}$$

On the other hand $x_3 \notin Ess(g)$ implies $x_3 \in Ess(h)$. Hence, we have

$$(b_0, b_2, b_4, b_6) \neq (b_1, b_3, b_5, b_7). \tag{8}$$

Without loss of generality let us assume that $b_0 = 1$ and $b_1 = 0$. Consequently,

$$u = f_{2\leftarrow 1} = x_4^0(a_0x_1^0 \ \oplus \ a_6x_1^1) \ \oplus \ x_4^1(x_1^0x_3^0 \ \oplus \ b_6.x_1^1x_3^0 \ \oplus \ b_7x_1^1x_3^1).$$

From $u(x_1 = 0, x_4 = 1) = x_3^0$ it follows that $x_3 \in Ess(u)$. If $a_0 = 1$, then $u(x_1 = 0, x_3 = 1) = x_4^0$ and if $a_0 = 0$, then $u(x_1 = 0, x_3 = 0) = x_4^1$. Hence $x_4 \in Ess(u)$. The proof will be complete if we show that $x_1 \in Ess(u)$. Suppose the opposite, i.e., $x_1 \notin Ess(u)$. From Theorem 2.2 it follows that $a_0 = a_6$, $b_6 = 1$ and $b_7 = 0$. Then we have

$$v = f_{3\leftarrow 1} = x_4^0[a_0.(x_1^0x_2^0 \ \oplus \ x_1^1x_2^1) \ \oplus \ a_2.x_1^0x_2^1 \ \oplus \ a_4.x_1^1x_2^0] \ \oplus$$
$$\oplus \ x_4^1[x_1^0x_2^0 \ \oplus \ b_2.x_1^0x_2^1 \ \oplus \ b_5.x_1^1x_2^0].$$

If $a_0 = 1$, then $v(x_1 = 1, x_2 = 1) = x_4^0$ and if $a_0 = 0$, then $v(x_1 = 0, x_2 = 0) = x_4^1$. Hence $x_4 \in Ess(v)$. On the other side it is clear that $v(x_4 = 1) := x_1^0x_2^0 \oplus b_2.x_1^0x_2^1 \oplus b_5.x_1^1x_2^0$ is not a constant. Assume that $x_2 \in Ess(v)$. Suppose that $x_1 \notin Ess(v)$. Hence $a_0 = a_2 = a_4$, $b_5 = 1$ and $b_2 = 0$. Thus we obtain

$$w = f_{3\leftarrow 2} = a_0.x_4^0 \ \oplus \ x_4^1(x_1^0x_2^0 \ \oplus \ b_3.x_1^0x_2^1 \ \oplus \ b_4x_1^1x_2^0).$$

Clearly $x_4 \in Ess(w)$. On the other hand it is clear that $w(x_4 = 1) := x_1^0x_2^0 \oplus b_3.x_1^0x_2^1 \oplus b_4.x_1^1x_2^0$ is not a constant. Assume that $x_2 \in Ess(w)$. Suppose that $x_1 \notin Ess(w)$. Hence $b_3 = 0$ and $b_4 = 1$. Thus finally, we obtain

$$f = a_0.x_4^0 \ \oplus \ x_4^1(x_1^0x_2^0x_3^0 \ \oplus \ x_1^1x_2^0x_3^0 \ \oplus \ x_1^1x_2^0x_3^1 \ \oplus \ x_1^1x_2^1x_3^0).$$

The contradiction is $f \notin G_2^4$ because $f_{4\leftarrow 2} = a_0.x_2^0 \ \oplus \ x_1^1 x_2^1 x_3^0$.

By analogy we conclude that $f \notin G_2^4$ for all other cases generated by (7) and (8), which is a contradiction. $\square$

Theorem 3.3. *Let $f \in P_2^4$. Then $f \in G_2^4$ if and only if $f = x_4^0.g(x_1, x_2, x_3) \oplus x_4^1.h(x_1, x_2, x_3)$, with*

$$g = x_3^{\alpha}(x_1^0 x_2^0 \ \oplus \ x_1^1 x_2^1) \ \oplus \ x_3^{\neg(\alpha)}(x_1^0 x_2^1 \ \oplus \ x_1^1 x_2^0), \tag{9}$$

and

$$h = x_3^{\neg(\alpha)}(x_1^0 x_2^0 \ \oplus \ x_1^1 x_2^1) \ \oplus \ x_3^{\alpha}(x_1^0 x_2^1 \ \oplus \ x_1^1 x_2^0), \tag{10}$$

for some α, $\alpha \in \{0, 1\}$.

P r o o f. "$\Leftarrow''$: The proof in this direction is given in Proposition 3.2.

"$\Rightarrow$": Suppose that some of the equations (9) or (10) are not satisfied. From Lemma 3.1 and Lemma 3.2 there are two possible cases:

A.

$$g = x_3^{\alpha}(x_1^0 x_2^1 \ \oplus \ x_1^1 x_2^0) \ \oplus \ x_1^{\beta} x_2^{\beta},$$

and

$$h = x_3^{\gamma}(x_1^0 x_2^0 \ \oplus \ x_1^1 x_2^1) \ \oplus \ x_3^{\neg(\gamma)}(x_1^0 x_2^1 \ \oplus \ x_1^1 x_2^0).$$

Then we have the following identification minor of f:

$$u = f_{4\leftarrow 1} = x_1^0 x_2^1 x_3^{\alpha} \ \oplus \ \neg(\beta).x_1^0 x_2^0 \ \oplus \ x_1^1 x_2^1 x_3^{\gamma} \ \oplus \ x_1^1 x_2^0 x_3^{\neg(\alpha)}.$$

Since $u(x_1 = 0) = x_2^1 x_3^{\alpha} \ \oplus \ \neg(\beta).x_2^0$ it follows that $\{x_2, x_3\} \subseteq Ess(u)$. We will show that $x_1 \in Ess(u)$, also.

Let $\beta = 0$. If $\gamma = \alpha$, then we have $u(x_2 = 0, x_3 = \gamma) = x_1^0$, and if $\gamma \neq \alpha$, then we have $u(x_2 = 1, x_3 = \gamma) = x_1^1$.

Let $\beta = 1$. If $\gamma = \alpha$, then $u(x_2 = 0, x_3 = \neg(\gamma)) = x_1^1$, and if $\gamma \neq \alpha$, then we have $u(x_2 = 1, x_3 = \gamma) = x_1^1$.

Hence $x_1 \in Ess(u)$ and $f \notin G_2^4$ in the case **A.**

B.

$$g = x_3^{\alpha}(x_1^0 x_2^1 \ \oplus \ x_1^1 x_2^0) \ \oplus \ x_1^{\beta} x_2^{\beta},$$

and

$$h = x_3^{\gamma}(x_1^0 x_2^1 \ \oplus \ x_1^1 x_2^0) \ \oplus \ x_1^{\delta} x_2^{\delta}.$$

Since $x_4 \in Ess(f)$ it follows that $g \neq h$.

Let us also consider the identification minor u of f :

$$u = f_{4\leftarrow 1} = x_1^0 x_2^1 x_3^\alpha \ \oplus\ \neg(\beta).x_1^0 x_2^0 \ \oplus\ x_1^1 x_2^0 x_3^\gamma \ \oplus\ \delta.x_1^1 x_2^1.$$

Since $u(x_1 = 0) = x_2^1 x_3^\alpha \oplus \neg(\beta).x_2^0$ it follows that $\{x_2, x_3\} \subseteq Ess(u)$. We will prove that $x_1 \in Ess(u)$, also.

Let $\beta = \delta = 0$. Then $u(x_2 = 1, x_3 = \alpha) = x_1^0$;
Let $\beta = \delta = 1$. Then $u(x_2 = 0, x_3 = \gamma) = x_1^1$;
Let $\beta = 1$ and $\delta = 0$. Then $u(x_2 = 0, x_3 = \gamma) = x_1^1$;
Let $\beta = 0$ and $\delta = 1$. Then $u(x_2 = 1, x_3 = \neg(\alpha)) = x_1^1$.

Hence $x_1 \in Ess(u)$ and $f \notin G_2^4$ in the case **B.**, also. This is a contradiction. $\square$

Remark 1. Note that g and h have to be two special functions from G_2^3, represented by the equation (4) of Theorem 3.2. Such functions can be obtained in the cases of the same theorem **B.a.2** and **B.b.2**, only.

Corollary 3.5. *Let $f \in P_2^4$. Then $f \in G_2^4$ if and only if $f = x_4^0.g(x_1, x_2, x_3) \oplus x_4^1.h(x_1, x_2, x_3)$, with*

$$g = x_3^\alpha (x_1^0 x_2^0 \ \oplus\ x_1^1 x_2^1) \ \oplus\ x_3^{\neg(\alpha)} (x_1^0 x_2^1 \ \oplus\ x_1^1 x_2^0),$$

and $h = \neg(g(x_1, x_2, x_3))$.

Corollary 3.6. *Let $f \in P_2^4$. Then $f \in G_2^4$ if and only if*

$$f = a_0. \left(\bigoplus_{\alpha_1\alpha_2\alpha_3\alpha_4 \in Od_2^4} x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} x_4^{\alpha_4} \right) \oplus \neg(a_0). \left(\bigoplus_{\alpha_1\alpha_2\alpha_3\alpha_4 \in Ev_2^4} x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} x_4^{\alpha_4} \right).$$

Corollary 3.7. *If $f \in G_2^4$ then $x_j \notin Ess(f_{i\leftarrow j})$ for all $i, j \in \{1, 2, 3, 4\}$ $i \neq j$.*

Proof. The three corollaries above can be proved by immediate checking of both functions from G_2^4, obtained in Theorem 3.3. $\square$

Theorem 3.4. *A Boolean function $f \in P_2^n$, depending on n essential variables with $n \geq 4$, has essential arity gap 2 if and only if*

$$f = \bigoplus_{\alpha_1\ldots\alpha_n \in Od_2^n} x_1^{\alpha_1} \ldots x_n^{\alpha_n} \quad \text{or} \quad f = \bigoplus_{\alpha_1\ldots\alpha_n \in Ev_2^n} x_1^{\alpha_1} \ldots x_n^{\alpha_n}.$$

Proof. "$\Leftarrow$": In this direction the proof is done by Proposition 3.2.

"$\Rightarrow$": We will proceed by induction on n. If $n = 4$ the theorem is true because of Theorem 3.3. Suppose that if $4 \leq n \leq l$ and $f \in G_2^n$, then

$$f = \bigoplus_{\alpha_1 \ldots \alpha_n \in Od_2^n} x_1^{\alpha_1} \ldots x_n^{\alpha_n} \quad \text{or} \quad f = \bigoplus_{\alpha_1 \ldots \alpha_n \in Ev_2^n} x_1^{\alpha_1} \ldots x_n^{\alpha_n}.$$

Let $f \in G_2^{l+1}$. Hence f can be presented as follows

$$f = x_{l+1}^0.g(x_1, \ldots, x_l) \oplus x_{l+1}^1.h(x_1, \ldots, x_l).$$

In the same way as in Lemma 3.1 and Lemma 3.2 it can be proved that $g, h \in G_2^l$. By the inductive supposition g and h are functions of the forms

$$\bigoplus_{\gamma_1 \ldots \gamma_l \in Od_2^l} x_1^{\gamma_1} \ldots x_l^{\gamma_l} \quad \text{or} \quad \bigoplus_{\gamma_1 \ldots \gamma_l \in Ev_2^l} x_1^{\gamma_1} \ldots x_l^{\gamma_l},$$

with $g \neq h$. Note that g and h are not constants because $ess(f) = n \geq 4$. Hence $Ess(g_{i\leftarrow j}) = Ess(h_{i\leftarrow j})$ for $i, j \in \{1, \ldots, l\}$ and $i \neq j$. Assume that

$$g = \bigoplus_{\gamma_1 \ldots \gamma_l \in Od_2^l} x_1^{\gamma_1} \ldots x_l^{\gamma_l} \quad \text{and} \quad h = \bigoplus_{\delta_1 \ldots \delta_l \in Ev_2^l} x_1^{\delta_1} \ldots x_l^{\delta_l}.$$

Consequently

$$f = x_{l+1}^0.\Big(\bigoplus_{\gamma_1 \ldots \gamma_l \in Od_2^l} x_1^{\gamma_1} \ldots x_l^{\gamma_l}\Big) \oplus x_{l+1}^1.\Big(\bigoplus_{\delta_1 \ldots \delta_l \in Ev_2^l} x_1^{\delta_1} \ldots x_l^{\delta_l}\Big) =$$

$$= \bigoplus_{\alpha_1 \ldots \alpha_{l+1} \in Od_2^{l+1}} x_1^{\alpha_1} \ldots x_{l+1}^{\alpha_{l+1}}.$$

The case $g = h$ is impossible because $ess(f) = l + 1$, but the replacement of g and h will produce the function

$$f = \bigoplus_{\alpha_1 \ldots \alpha_l \in Ev_2^l} x_1^{\alpha_1} \ldots x_l^{\alpha_l},$$

which does not depend on x_{l+1}. $\square$

Corollary 3.8. *A Boolean function $f \in P_2^n$, which essentially depends on n variables with $n > 4$, has essential arity gap 2 if and only if*

$$f = x_n^0.g(x_1, \ldots, x_i, \ldots, x_{n-1}) \oplus x_n^1.g(x_1, \ldots, x_{i-1}, \neg(x_i), x_{i+1}, \ldots, x_{n-1}),$$

where $g \in G_2^{n-1}$ and $i \in \{1, \ldots, n-1\}$.

P r o o f. If

$$g = \bigoplus_{\gamma_1 \ldots \gamma_{n-1} \in Od_2^{n-1}} x_1^{\gamma_1} \ldots x_{n-1}^{\gamma_{n-1}} \quad \text{and} \quad h = \bigoplus_{\gamma_1 \ldots \gamma_{n-1} \in Od_2^{n-1}} x_1^{\gamma_1} \ldots x_{n-1}^{\gamma_{n-1}},$$

then $\neg(g) = h$ and $\neg(h) = g$ for all $l \geq 4$. On the other hand, for each $i \in \{1, \ldots, n-1\}$, we have

$$\neg(g) = \bigoplus_{\gamma_1 \ldots \gamma_{n-1} \in Od_2^{n-1}} x_1^{\gamma_1} \ldots x_{i-1}^{\gamma_{i-1}} \neg(x_i^{\gamma_i}) x_{i+1}^{\gamma_{i+1}} \ldots x_{n-1}^{\gamma_{n-1}}.$$

$\square$

Corollary 3.9. $|G_2^n| = 2$ *for each $n, n \geq 4$.*

One of the most important problems concerning the essential arity gap is to calculate the number of all functions from P_2^n, which depend essentially on at most n variables and which have the maximum gap, i.e., with gap equal to 2. The next theorem gives the answer of this problem. It summarizes the results obtained above in the paper.

Let us denote by H_n the set of all functions in P_2^n, which have gap equal to 2, i.e.,

$$H_n := \bigcup_{m=2}^{n} G_2^m \quad \text{and} \quad h_n := |H_n|.$$

Theorem 3.5. *The following combinatorial equations are held:*
(i) $h_2 = 6$;
(ii) $h_3 = 28$;
(iii) $h_n = 3.\binom{n}{2} + 5.\binom{n}{3} + 2^{n+1} - 2n - 2$, *when* $n \geq 4$;

P r o o f. (i) follows from Corollary 3.1 of Theorem 3.1;

(ii) Let $X_3 = \{x_1, x_2, x_3\}$. There are $6.\binom{3}{2}$ Boolean functions with essential arity gap equal to 2, which depend essentially on 2 variables from X_3, according to Corollary 3.1 of Theorem 3.1.

From Corollary 3.4 of Theorem 3.2 it follows that there are 10 Boolean functions with essential arity gap equal to 2, which depend essentially on all 3 variables from X_3. Hence $h_3 = 6.3 + 10 = 28$.

(iii) Let $X_n = \{x_1, \ldots, x_n\}$, $n \geq 4$. There are $6.\binom{n}{2}$ Boolean functions with essential arity gap equal to 2, which depend essentially on 2 variables from X_n, according to Corollary 3.1 of Theorem 3.1.

There are $10.\binom{n}{3}$ Boolean functions with essential arity gap equal to 2, which depend essentially on 3 variables from X_n, according to Corollary 3.4 of Theorem 3.2.

Finally, for each m, $3 < m \leq n$ there are $2.\binom{n}{m}$ Boolean functions with essential arity gap equal to 2, which depend essentially on m variables from X_n, according to Corollary 3.9 of Theorem 3.4.

Hence we have

$$h_n = 6.\binom{n}{2} + 10.\binom{n}{3} + 2.\left[\binom{n}{4} + \binom{n}{5} + \ldots + \binom{n}{n}\right] =$$

$$= 3.\binom{n}{2} + 5.\binom{n}{3} + 2^{n+1} - 2n - 2.$$

$\square$

REFERENCES

[1] Breitbart Yu. On the essential variables of functions in the algebra of logic. *Dokl. Acad. Sci. USSR*, **172**, No. 1 (1967), 9–10 (in Russian).

[2] Chimev K. Separable Sets of Arguments of Functions. MTA SzTAKI Tanulmányok, 180/1986, 173 pp.

[3] Couceiro M., E. Lehtonen. On the effect of variable identification on the essential arity of functions on finite sets. *Int. Journal of Foundations of Computer Science*, **18**, Issue 5, (October 2007), 975–986.

[4] Salomaa A. On Essential Variables of Functions, Especially in the Algebra of Logic. *Annales Academia Scientiarum Fennicae, Ser. A*, **333** (1963), 1–11.

[5] LUPANOV O. On a class schemas of functional elements. *Problemy Kibernetiki*, **9** (1963), 333–335 (in Russian).

[6] SHTRAKOV S. Tree Automata and Essential Input Variables. Contributions to General Algebra 13, Verlag Johannes Heyn, Klagenfurt, 2001, 309–320.

[7] SHTRAKOV S., K. DENECKE. Essential Variables and Separable Sets in Universal Algebra. *Taylor & Francis, Multiple-Valued Logic, An International Journal*, **8**, No. 2 (2002), 165–182.

Slavcho Shtrakov
Department of Computer Science
South-West University
2700 Blagoevgrad, Bulgaria
e-mail: `shtrakov@aix.swu.bg`
URL: `http://home.swu.bg/shtrakov`

Received September 25, 2008
Final Accepted October 15, 2008