МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2001
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2001
Proceedings of Thirtieth Spring Conference of
the Union of Bulgarian Mathematicians
Borovets, April 8–11, 2001

ON SOME PROPERTIES OF VARIABLES IN REED-MULLER DECOMPOSITIONS

Ivo Yordanov Damyanov

The Theory of Essential Variables is an important field of Theoretical Computer Science, that have been intensively developed during the last years. The concept of essential variables and separable sets of variables has been also introduced for terms in Universal algebra by K. Denecke and Sl. Shtrakov [2]. In this paper we consider another classification of Boolean functions variables and we study their behavior in accordance with the work of Breitbart [3], Lupanov [4] and Chimev [1]. Analogous theorems are proved.

1. Introduction. For the Boolean functions we will consider the following three decompositions [5]:

$$\begin{array}{lll} & f = xf_1 \oplus f_2 & \text{positive Davio (positive polarity)} \\ (1) & f = x(f_1 \oplus f_2) \oplus f_2 = xf_1 \oplus \overline{x}f_2 & \text{Shannon decomposition} \\ & f = xf_1 \oplus f_1 \oplus f_2 = \overline{x}f_1 \oplus f_2 & \text{negative Davio (negative polarity)} \end{array}$$

Positive and negative Davio are also known as Reed-Muller expansions.

Many properties of variables and sets of variables, such as essentiality and separability, are introduced using Shannon decomposition [1].

The function $f(x_1, \dots, x_n)$ can be decomposed with respect to (w.r.t.) variable x_i using Shannon expansion such as:

$$f(x_1, \dots, x_n) = \overline{x}_i f_1 \oplus x_i f_2. \tag{2}$$

Here $f_1 := f(x_i = 0)$ and $f_2 := f(x_i = 1)$ are functions of $n-1$ variables (the functions which are obtained by substituting x_i by two possible constants) and usually they are called *subfunctions* of $f(x_1, \dots, x_n)$.

As other types of subfunctions will also be introduced, let us call this kind of subfunctions *sh-subfunctions* (*Shannon's subfunctions*). Shannon's subfunctions will be denoted by $f^{sh}(x_i = \text{const})$.

Let us fix the positive polarity of the Reed-Muller decomposition and consider the decomposition formula $xf_1 \oplus f_2$. The definitions and results that we will obtain can be easily transformed to the negative Davio.

The function $f(x_1, \dots, x_n)$ can be decomposed w.r.t. variable x_i as follows:

$$f(x_1, \dots, x_n) = x_i f_1 \oplus f_2. \tag{3}$$

Here f_1 and f_2 are functions of $n-1$ variables and we will call them *rm-subfunctions* of $f(x_1, \dots, x_n)$, or *Reed-Muller's subfunctions* and will denote them by $f^{rm}(x_i = \text{const})$.

Let

$$(4) \qquad f^{rm}(x_i = c_i) = \begin{cases} f_2, \text{ if } c_i = 0 \\ f_1, \text{ if } c_i = 1 \end{cases} .$$

If $g = f^{rm}(x_{i_1} = \text{const}, \ldots, x_{i_k} = \text{const})$, where $M = \{x_{i_1}, \ldots, x_{i_k}\}$ then we will use the denotation $g \prec_{rm}^{M} f$.

Definition 1. *Let f be a Boolean function and its Shannon decomposition w.r.t. variable x_i be $f = \overline{x}_i f_1 \oplus x_i f_2$. The variable x_i is called* fictive (sh-fictive) for $f(x_1, \ldots, x_n)$ *iff $f_1 = f_2$ and* essential (sh-essential) *iff $f_1 \neq f_2$.*

The set of all essential variables for $f(x_1, \ldots, x_n)$, in the case of Shannon decomposition, will be denoted by $shEss(f)$. The set of all functions that depend sh-essentially exactly on n variables will be denoted by $F^{sh}(n)$.

It is clear that if we get a function and all its variables are sh-fictive then this function is *constant.*

In the case of Reed-Muller decomposition by analogy with the definition of sh-fictive variables we can define rm-fictive variables.

Definition 2. *Let f be a Boolean function and its Reed-Muller decomposition w.r.t. variable x_i is determined by the equation $f = x_i f_1 \oplus f_2$. The variable x_i is called* rm-fictive (quasi fictive) *iff $f_1 = f_2$. The variable x_i is* rm-essential for $f(x_1, \ldots, x_n)$ *iff $f_1 \neq f_2$.*

If a function has "many" quasi-fictive variables we may expect that the function is "more" simple. Note that rm-fictivity depends on the polarity of the decomposition formulae, i.e. a variable can be rm-fictive when using positive polarity, but the same variable is rm-essential w.r.t. the alternative polarity.

For our next considerations we fix and use only positive polarity.

The set of all rm-essential variables for $f(x_1, \ldots, x_n)$, will be denoted by $rmEss(f)$. The set of all functions which depend rm-essentially exactly on n variables will be denoted by $F^{rm}(n)$.

Example 1. Let $f = x_1 x_2 + x_1 + x_2 + 1$. The Reed-Muller decomposition of f w.r.t. x_1 is: $f = x_1(\overline{x}_2) + \overline{x}_2$. Hence $x_1 \notin rmEss(f)$. Analogously, Reed-Muller decomposition of f w.r.t. x_2 is $f = x_2(\overline{x}_1) + \overline{x}_1$, i.e. $x_2 \notin rmEss(f)$. So, $rmEss(f) = \emptyset$, but f is not constant. □

By analogy with the case of Shannon decomposition [1] we define rm-strongly essential variables and rm-separable sets as follows:

Definition 3. *If $f \in F^{rm}(n)$, $n \geq 1$ and $\emptyset \neq M \subseteq rmEss(f)$ then the variable $x \in M$ is called* rm-strongly essential for f w.r.t. M, *if there exists value c, such that $M \setminus \{x\} \subseteq rmEss(f^{rm}(x = c))$.*

If $f \in F^{rm}(n)$, $n \geq 1$ and $\emptyset \neq M \subseteq rmEss(f)$ then the set of all rm-strongly essential variables for f w.r.t. M will be denoted by $rmEss^*(f, M)$.

Definition 4. *If $f \in F^{rm}(n)$, $n \geq 1$ and $\emptyset \neq M_1 \subseteq rmEss(f)$, $M_2 \subseteq rmEss(f)$, $M_1 \cap M_2 = \emptyset$, then we say that* the set M_2 is rm-separable for f w.r.t. M_1, *if for the variables from M_1 there exist values such that when replacing them by Boolean constants, the new rm-subfunction g obtained from f satisfies $M_2 \subseteq rmEss(g)$. This will be denoted by $M_2 \in rmSep(f, M_1)$.*

Definition 5. *For the Boolean function f we say that* the set M ($M \subseteq rmEss(f)$) is rm-separable for f, *if M is rm-separable for f w.r.t. $rmEss(f) \setminus M$.*

2. Essentiality and Separability in Reed-Muller decompositions. Example 1 allows us to view rm-fictive variables in their difference with sh-fictive variables.

The essential variable is dual to the fictive one. Hence there are differences between rm-essential and sh-essential variables.

In this section we will show that the most important properties of the traditional (Shannon case) notions – essentiality, separability, etc. are preserved when going to Reed-Muller decomposition scheme.

It is obvious that:

$$\begin{array}{l} f^{rm}(x_i = 1) = f^{sh}(x_i = 0) + f^{sh}(x_i = 1) \text{ and} \\ f^{rm}(x_i = 0) = f^{sh}(x_i = 0). \end{array} \tag{5}$$

Lemma 2.1. *The variable x_i is rm-fictive iff $f^{sh}(x_i = 1) = 0$ for the Boolean function $f(x_1, \ldots, x_n)$.*

To prove next theorems we need the following lemmas.

Lemma 2.2. *Let x_i and x_j be two variables of Boolean function $f(x_1, \ldots, x_n)$. If $g = f^{rm}(x_i = \alpha_i)$ and $h = f^{rm}(x_j = \beta_j)$ for $\alpha_i, \beta_j \in \{0, 1\}$ then $g^{rm}(x_j = \beta_j) = h^{rm}(x_i = \alpha_i)$.*

Proof. (The proof is easy to be done by using (5) and considering three non-trivial cases: $\alpha_i = \beta_j = 0$, $\alpha_i = 0, \beta_j = 1$, $\alpha_i = \beta_j = 1$.) □

Lemma 2.3. *If x_i is rm-fictive for the Boolean function $f(x_1, \ldots, x_n)$, then x_i is rm-fictive for each rm-subfunction of f.*

Proof. By Lemma 2.1. if x_i is rm-fictive for the Boolean function $f(x_1, \ldots, x_n)$ it follows $f^{rm}(x_i = 0) = f^{rm}(x_i = 1) = f^{sh}(x_i = 0)$.

Let $g = f^{rm}(x_k = 0)$ for $k \neq i$, i.e. $g = f^{sh}(x_k = 0)$ and $h = f^{rm}(x_k = 1) = f^{sh}(x_k = 0) + f^{sh}(x_k = 1)$.

Now we will prove that x_i is rm-fictive for g and h. From (5) it follows that $g^{rm}(x_i = 0) = g^{sh}(x_i = 0)$ and $g^{rm}(x_i = 1) = g^{sh}(x_i = 0) + g^{sh}(x_i = 1)$.

By Lemma 2.1. we have $g^{sh}(x_i = 1) = 0$. Consequently $g^{rm}(x_i = 0) = g^{rm}(x_i = 1)$, i.e. x_i is rm-fictive for g ($g \prec_{rm} f$).

For h we have $h = f^{rm}(x_k = 1) = f^{sh}(x_k = 0) + f^{sh}(x_k = 1) = g + f^{sh}(x_k = 1)$.

Let us set $t = f^{sh}(x_k = 1)$. In a similar way as above we obtain that x_i is rm-fictive for t and by Lemma 2.1. follows that x_i is rm-fictive for h. □

Lemma 2.4. *If $f \in F^{rm}(n)$, $g \prec_{rm} f$ and $M \in rmSep(g)$ then $M \in rmSep(f)$.*

In the Shannon case, many researchers have paid efforts to obtain lower bounds of the number of strongly essential variables. O.B. Lupanov [4] in 1962 proved that each Boolean function f with $|shEss(f)| \geq 2$ has at least one sh-strongly essential variable. N.A. Solovi'ev in 1963 gave another proof of this result. A. Salomaa in 1963 generalized proof for arbitrary discrete function. J. Breitbart [3] in 1967 proved that there are at least two strongly essential variables for each Boolean function. K. Chimev [1] generalized this result for arbitrary discrete function.

Theorem 2.5. *If $f \in F^{rm}(n)$, $n \geq 2$ and $M_1 \in rmSep(f, M_2)$, $M_2 \neq \emptyset$, then there exists at least one variable from M_2 which is rm-strongly essential for f with respect to $M_1 \cup M_2$.*

Proof. The proof will be done by induction on the cardinality of the set M_2. For $|M_2| = 1$, the proof of the theorem is obvious. Let us assume that the theorem is true for $1 \leq |M_2| \leq l$. We will prove the theorem for the case $|M_2| = l + 1$.

Let $|M_2| = l + 1 \geq 2$. Let us assume that $M_1 = \{x_1, \dots, x_m\}$ and $M_2 = \{x_{m+1}, \dots, x_{m+l+1}\}$, where $m + l + 1 \leq n$.

Let $c_{m+1}, \dots, c_{m+l+1}$ be such values of $x_{m+1}, \dots, x_{m+l+1}$, that $\{x_1, \dots, x_m\} \subset rmEss(f_1)$, where $f_1 = f^{rm}(x_{m+1} = c_{m+1}, \dots, x_{m+l+1} = c_{m+l+1})$.

If $f_2 = f^{rm}(x_{m+1} = c_{m+1})$, then $\{x_1, \dots, x_m\} \subset rmEss(f_2)$, which follows from Lemma 2.3., because of $\{x_1, \dots, x_m\} \subset rmEss(f_1)$ and $f_1 \prec_{rm} f_2$.

If $\{x_{m+2}, \dots, x_{m+l+1}\} \subset rmEss(f_2)$, then x_{m+1} will be rm-strongly essential for f with respect to $M_1 \cup M_2$ and the theorem is proved in this case.

Let us consider the case when there exist variables x_j, $j \in \{m+2, \dots, m+l+1\}$, such that $x_j \notin rmEss(f_2)$, i.e. for each value α_j of x_j $f_2 = x_j f_{21} + f_{22} = \overline{x}_j f_{21}$

Let us assume that there exist variables x_k, $1 \leq k \leq m$ such that $x_k \in rmEss(f_2)$ and $x_k \notin rmEss(f_2(x_j = \alpha_j))$. Then from (3) and the definition of rm-fictive variables follows that $f_2^{rm}(x_j = \alpha_j) = \overline{x}_k f_2^{rm}(x_j = \alpha_j, x_k = \alpha_k)$, and $f_2 = x_j f_{21} + f_{22} = \overline{x}_j f_{21} = \overline{x}_j f_2^{rm}(x_j = \alpha_j) = \overline{x}_j \overline{x}_k f_2^{rm}(x_j = \alpha_j, x_k = \alpha_k) = = \overline{x}_k \overline{x}_j f_2^{rm}(x_j = \alpha_j, x_k = \alpha_k) = \overline{x}_k f_2^{rm}(x_k = \alpha_k)$, which is a contradiction to the assumption that $x_k \in rmEss(f_2)$. Consequently it follows that $M_1 \subset rmEss(f_2(x_j = \alpha_j))$. Let now c'_j be such value of x_j that $x_{m+1} \in rmEss(f_3)$, where $f_3 = f^{rm}(x_j = c'_j)$. From $M_1 \subset rmEss(f_2)$ and $x_j \notin rmEss(f_2)$ it follows $M_1 \subset rmEss(f_2(x_j = c'_j))$. But $f_2(x_j = c'_j) \prec_{rm} f_3$, from which follows that

$$(6) \qquad M_1 \subset rmEss(f_3).$$

Let $M_3 = M_2 \backslash rmEss(f_3)$. As $x_j \in M_2$ and x_j - rm-fictive for f_3 implies that $M_3 \neq \emptyset$. There follows that $1 \leq |R_3| \leq l$.

From (6) follows that there exist such values for the variables from M_3 that after replacing them, the variables from M_1 remain rm-essential. For example it is enough to put, instead of x_j the constant c'_j, and for all of the other variables in M_3 (if there exist any) - arbitrary values. Then we receive the function f_3. This means that $M_1 \cup (M_2 \backslash M_3) \in rmSep(f, M_3)$, and it brings us to step 2 in our proof - the inductive assumption. □

Corollary 2.6. *If $f \in F^{rm}(n)$, $n \geq 2$ and $M \in rmSep(f)$, where $M \subset rmEss(f)$ $(M \neq rmEss(f))$, then there exists at least one variable $x_t \in rmEss(f) \setminus M$ such that $M \cup \{x_t\} \in rmSep(f)$.*

Proof. Let $rmEss(f) = \{x_1, \dots, x_n\}$ and $M = \{x_1, \dots, x_m\}$, $m \leq n$.

Let us at suppose first that $n = m + 1$. Then $M \cup \{x_n\} = rmEss(f) \in rmSep(f)$.

Second, let $m + 1 < n$. Consider the set $M_1 = \{x_{m+1}, \dots, x_n\}$. From Theorem 2.5. there exists $x_{j_1} \in M_1$ such that $M \cup M_2 \in rmSep(f_1)$, where $M_2 = M_1 \setminus \{x_{j_1}\}$ and $f_1 = f^{rm}(x_{j_1} = \alpha_{j_1})$ for some $\alpha_{j_1} \in \{0, 1\}$.

If we apply Theorem 2.5. for M, M_2 and f_1 we will obtain set M_3 and rm-subfunction f_2 of f_1 such that $M \cup M_3 \in rmSep(f_2)$ and $M_3 = M_2 \setminus \{x_{j_2}\}$.

Clearly this process can be continued until we obtain set M_{n-m} and rm-subfunction

f_{n-m-1} of f_{n-m-2} such that

$$M_{n-m} = \{x_{j_{n-m-1}}\} \text{ and } M \cup \{x_{j_{n-m-1}}\} \in rmSep(f_{n-m-1}).$$

Lemma 2.4. implies $M \cup \{x_{j_{n-m-1}}\} \in rmSep(f)$. □

Corollary 2.7. *If $f \in F^{rm}(n)$, $n \geq 2$ and g is rm-subfunction of f with respect to M $(M \neq \emptyset)$, then there exist rm-functions f_i, $(i = 1, \ldots, m$ where $m = |M|)$ of f that*

$$g \prec_{rm} f_1 \prec_{rm} f_2 \prec_{rm} \cdots \prec_{rm} f_m = f \tag{7}$$

and for each $i = 1, \ldots, m$, the function f_i depends rm-essentially on exactly i variables which belong to M.

Acknowledgements. The author is grateful to Sl. Shtrakov, K. Denecke and P. Pandeliev for their interest in reading an earlier version of this paper and for their constructive discussions.

REFERENCES

[1] K. Chimev. Separable sets of arguments of functions. MzTAKI Tanulmanyok, Budapest, 1986.

[2] K. Denecke, Sl. Shtrakov. Essential variables and Separable sets in Universal algebra. *MVL journal*, preprint, 1998.

[3] J. Breitbart. Essential Variables of Boolean Functions. *Dokl. Acad Nauk SSSR*, **172**, (1967), 9–10 (in Russian).

[4] O. Lupanov. On a class of schemes of functional elements. *Problems of cybernetics*, **7**, (1962), 61–114 (in Russian).

[5] J. Denev. On a Generalization of the Subfunction Concept. *Mathematics and Mathematical Education*, **4**, (1975), 98–104 (in Bulgarian).

Ivo Damyanov
Department of Computer Sciences
South-West University "Neofit Rilski"
2700 Blagoevgrad, Bulgaria
e-mail: Ivo.Damianov@mail.csm.swu.bg

ВЪРХУ НЯКОИ СВОЙСТВА НА ПРОМЕНЛИВИТЕ ПРИ РИЙД-МЮЛЕРОВА ДЕКОМПОЗИЦИЯ

Иво Йорданов Дамянов

Теорията на съществените променливи е важна част от теоретичната информатика, която интензивно се развива през последните години. Концепцията за съществените променливи и отделимите множества от променливи е въведена също и за термите в Универсалната алгебра от К. Денеке и Сл. Щраков [2]. В тази статия ние разглеждаме една нова класификация на променливите на булевите функции и изучаваме тяхното поведение в съзвучие с работите на Брейтбарт [3], Лупанов [4] и Чимев [1]. Доказани са аналогични теореми.