

ANNALES ACADEMIAE SCIENTIARUM FENNICAE

Series A

I. MATHEMATICA

339

ON ESSENTIAL VARIABLES
OF FUNCTIONS, ESPECIALLY IN THE
ALGEBRA OF LOGIC

BY

ARTO SALOMAA

HELSINKI 1963
SUOMALAINEN TIEDEAKATEMIA

<https://doi.org/10.5186/aasfm.1964.339>

Communicated 13 September 1963 by P. J. MYRBERG and K. INKERI

KESKUSKIRJAPAINO
HELSINKI 1963

On essential variables of functions, especially in the algebra of logic

Current research in the theory of finite automata and deterministic operators has led to problems concerning essential variables of functions in the algebra of logic. In the present paper we give some results in this direction. As it turns out, many of the proofs remain valid for arbitrary functions.

SOLOVJEV, [2], has considered the problem how many essential variables are preserved if a constant value is assigned for some variable. He has proved two theorems, one of which has been established also by LUPANOV, [1, pp. 95—97]. All these proofs make use of some intrinsic properties of functions in the algebra of logic. By an argument of a more general character, we prove two theorems which are extensions of SOLOVJEV's theorems for arbitrary functions. This is done in section 1.

In section 2, we discuss the problem how the number of essential variables is reduced if some variables are identified. We prove two theorems. One of them (theorem 3) deals with arbitrary functions. In the other (theorem 4) we show that in the algebra of logic, for any function f of n essential variables, there is a function of at least $n-2$ essential variables which is obtained from f by identifying some of its variables.

Section 3 deals with the distribution of values of functions, all of whose variables are essential. We prove a theorem which strengthens the well-known »fundamental lemma» of JABLONSKIĀ, [3, pp. 68—70].

1. Let $\mathfrak{F}_{M_1, \dots, M_n}^N$ denote the set of functions mapping the Cartesian product $M_1 \times \dots \times M_n$ of non-empty sets M_i , $i = 1, \dots, n$, into a non-empty set N . Assume M'_i is a non-empty subset of M_i , $i = 1, \dots, n$. Then, for any function

$$f(x_1, \dots, x_n) \in \mathfrak{F}_{M_1, \dots, M_n}^N,$$

we denote by $f(M'_1, \dots, M'_n)$ the set of values assumed by $f(x_1, \dots, x_n)$ when, for $i = 1, \dots, n$, the variable x_i is restricted to the set M'_i . A function $f(x_1, \dots, x_j, \dots, x_n)$ depends essentially on the variable x_j (or x_j is an essential variable of this function) if there are sets M'_i , $i = 1, \dots, n$, such that

$$f(M'_1, \dots, M'_j, \dots, M'_n)$$

contains at least two elements and every M'_i , $i \neq j$, contains only one element.

Theorem 1. *Let the function $f(x_1, \dots, x_n) \in \mathfrak{F}_{M_1, \dots, M_n}^N$ depend essentially on all of its n variables, $n \geq 2$. Then there is an index j and an element $c \in M_j$ such that the function*

$$f(x_1, \dots, x_{j-1}, c, x_{j+1}, \dots, x_n)$$

depends essentially on all of its $n - 1$ variables.

Proof. For $n = 2$, the assertion follows by the definition of essential variables. (In fact, we may choose $j = 1$ or $j = 2$.) We, therefore, assume that $n > 2$.

Because f depends essentially on the variable x_1 , we have

$$f(a_1, a_2, \dots, a_n) \neq f(a'_1, a_2, \dots, a_n),$$

for some $a'_1 \in M_1$, and $a_i \in M_i$, $i = 1, \dots, n$. Hence, the function $f(x_1, a_2, \dots, a_n)$ depends essentially on the variable x_1 . I.e., we have replaced $n - 1$ variables of f by constants (elements of the sets M_i) in such a way that f depends essentially on the remaining variable.

We shall now make the following hypothesis of induction: we have replaced $n - k$ variables of f , $1 \leq k < n - 1$, by constants b_i in such a way that f depends essentially on the remaining k variables. By a suitable renumbering of the variables, we may assume that they are the first k variables, i.e. the function

$$f_1(x_1, \dots, x_k) = f(x_1, \dots, x_k, b_{k+1}, \dots, b_n)$$

depends essentially on all of its k variables.

Let l , $k + 1 \leq l \leq n$, be the number defined as follows: for some elements $c_i \in M_i$, $k + 1 \leq i \leq l$,

$$(1) \quad f(x_1, \dots, x_k, c_{k+1}, \dots, c_{l-1}, c_l, b_{l+1}, \dots, b_n) \neq f_1(x_1, \dots, x_k)$$

whereas, for all elements $y_i \in M_i$, $k + 1 \leq i \leq l - 1$,

$$(2) \quad f(x_1, \dots, x_k, y_{k+1}, \dots, y_{l-1}, b_l, \dots, b_n) = f_1(x_1, \dots, x_k).$$

Such a number l exists because, otherwise, f would depend essentially on the variables x_1, \dots, x_k only. The function

$$(3) \quad f_2(x_1, \dots, x_k, x_l) = f(x_1, \dots, x_k, c_{k+1}, \dots, c_{l-1}, x_l, b_{l+1}, \dots, b_n)$$

depends essentially on all of its $k + 1$ variables. In fact, by (2) and (1),

$$f_2(x_1, \dots, x_k, b_l) = f_1(x_1, \dots, x_k)$$

and

$$f_2(x_1, \dots, x_k, c_l) \neq f_1(x_1, \dots, x_k).$$

Hence, (3) defines a function of $k + 1$ essential variables which is obtained by replacing $n - (k + 1)$ variables of f by constants. The proof of theorem 1 is completed by induction.

Theorem 1 implies that it is always possible to replace $n - 2$ variables of f by constants in such a way that the resulting function depends essentially on both of the remaining variables. The following theorem gives a stronger result.

Theorem 2. *Let $f(x_1, \dots, x_n)$ be as in the preceding theorem. Then for any $\mu, 1 \leq \mu \leq n$, there is a $\nu \neq \mu$ and $n - 2$ constants such that if the variables of f distinct from x_μ and x_ν are replaced by these constants then the resulting function depends essentially on both of its variables.*

Proof. Without loss of generality, we let $\mu = 1$ because we may, if necessary, transpose the indices μ and 1. As in the proof of the preceding theorem, we first determine constants $a_i, i = 2, \dots, n$, such that the function

$$f_1(x_1) = f(x_1, a_2, \dots, a_n)$$

depends essentially on x_1 . We define $l, 2 \leq l \leq n$, to be the number such that, for some elements $c_i \in M_i, 2 \leq i \leq l$,

$$(4) \quad f(x_1, c_2, \dots, c_l, a_{l+1}, \dots, a_n) \neq f_1(x_1)$$

whereas, for all elements $y_i \in M_i, 2 \leq i \leq l - 1$,

$$(5) \quad f(x_1, y_2, \dots, y_{l-1}, a_l, \dots, a_n) = f_1(x_1).$$

Then it is a consequence of (4) and (5) that the function

$$f_2(x_1, x_l) = f(x_1, c_2, \dots, c_{l-1}, x_l, a_{l+1}, \dots, a_n)$$

satisfies the requirements of the theorem, i.e. we may choose $\nu = l$. Thus, theorem 2 follows.

It is obvious that if we choose *two* arbitrary variables x_μ and x_ν , then we do not always find $n - 2$ constants such that when the variables of f distinct from x_μ and x_ν are replaced by these constants then the resulting function depends essentially on both x_μ and x_ν . Even the weaker *statement obtained from theorem 2 by changing the order of quantification of μ and ν* is false. This is shown in [2]. We give the following more general counterexample.

Consider the set

$$(6) \quad \mathfrak{F}_{M_1, \dots, M_4}^N$$

where each of the sets M_1, \dots, M_4, N contains at least two elements. Choose two elements, denoted by 0 and 1, from each of the sets M_1, \dots, M_4, N and denote by $\bar{x}^{(i)}$ some fixed function in $\mathfrak{F}_{M_i}^N, i = 1, \dots, 4$,

which interchanges the elements 0 and 1. We now define by the following equations a function f belonging to the set (6):

$$\begin{aligned} f(x_1, 0, 0, x_4) &= x_1, \\ f(x_1, 0, 1, x_4) &= x_4, \\ f(x_1, 1, 0, x_4) &= \bar{x}_4^{(4)}, \\ f(x_1, 1, 1, x_4) &= \bar{x}_1^{(1)}, \\ f(0, x_2, x_3, 0) &= x_2, \\ f(0, x_2, x_3, 1) &= x_3, \\ f(1, x_2, x_3, 0) &= \bar{x}_3^{(3)}, \\ f(1, x_2, x_3, 1) &= \bar{x}_2^{(2)}, \\ f(x_1, x_2, x_3, x_4) &= x_1, \text{ otherwise.} \end{aligned}$$

It is easy to check that no contradiction arises in this definition, i.e. there is no argument for which f has been defined twice. Furthermore, f depends essentially on all of its four variables. But, for any constants a and b , both $f(x_1, a, b, x_4)$ and $f(a, x_2, x_3, b)$ depend essentially on one variable only. It is not possible to construct a 3-place function which would provide a similar counter-example.

We note, finally, that the converse of theorem 2 holds, whereas the converse of theorem 1 is false.

2. We denote

$$\mathfrak{F}_A = \bigcup_{n=1}^{\infty} \mathfrak{F}_{A, \dots, A}^A$$

n copies

where A is a set containing at least two elements. Following [3], we also denote $\mathfrak{F}_A = \mathfrak{P}_k$ if A is a finite set of cardinality k . The set \mathfrak{P}_2 is termed the set of functions in the *algebra of logic*.

Any function, obtained from a given function $f(x_1, \dots, x_n) \in \mathfrak{F}_A$ by identifying some of its variables, is called a *diagonalization* of f . In this section, we consider the problem whether essential variables are preserved in diagonalizations. If n is less than or equal to the cardinality of A (denoted by $\text{card}(A)$), we may choose n distinct elements $a_1, \dots, a_n \in A$ and define a function f as follows:

$$\begin{aligned} f(a_1, \dots, a_n) &= a_1, \\ f(x_1, \dots, x_n) &= a_2, \text{ otherwise.} \end{aligned}$$

Clearly, f depends essentially on all of its n variables. But all diagonalizations of f are constants ($= a_2$). Hence, we have the following

Theorem 3. *For any $n \leq \text{card}(A)$, there is an n -place function $f \in \mathfrak{F}_A$ such that all variables of f are essential and every diagonalization of f is a constant.*

Theorem 3 shows that, in general, essential variables can be preserved in diagonalizations only in the case that $n > \text{card}(A)$. We shall now consider functions in the algebra of logic. It is well-known that every function in the algebra of logic can be uniquely expressed as a polynomial modulo 2. All variables appearing in this polynomial representation are essential.

A linear polynomial of n variables possesses diagonalizations of at most $n - 2$ variables. Similarly, the polynomial $x_1x_2 + x_2x_3 + x_3x_1$ does not possess diagonalizations of two variables. Hence, given a function f of n essential variables in the algebra of logic, one can not always find a diagonalization of f which possesses $n - 1$ essential variables. However, as shown in our next theorem, a diagonalization of $n - 2$ essential variables can always be found.

Theorem 4. *For any function in the algebra of logic possessing $n (\geq 2)$ essential variables, there is a diagonalization possessing at least $n - 2$ essential variables.*

Given an arbitrary function in the algebra of logic, we denote by \mathfrak{p} the polynomial representing it. We shall first prove the following

Lemma. *If \mathfrak{p} contains a conjunction of rank ≥ 3 then, for some i and j ,*

$$(7) \quad \mathfrak{p} = x_i x_j \mathfrak{a}_1 + x_i \mathfrak{a}_2 + x_j \mathfrak{a}_3 + \mathfrak{a}_4$$

where either \mathfrak{a}_1 contains a term which is both in \mathfrak{a}_2 and \mathfrak{a}_3 or \mathfrak{a}_1 contains a term which is neither in \mathfrak{a}_2 nor in \mathfrak{a}_3 .¹

Proof. We choose from \mathfrak{p} a conjunction \mathfrak{b} such that \mathfrak{p} contains no conjunction of a rank higher than the rank of \mathfrak{b} . By renumbering the variables, we may assume

$$\mathfrak{b} = x_1 x_2 \dots x_k$$

where $k \geq 3$. Consider the following conjunctions:

$$\mathfrak{b}_1 = x_1 x_2 x_4 \dots x_k,$$

$$\mathfrak{b}_2 = x_1 x_3 x_4 \dots x_k,$$

$$\mathfrak{b}_3 = x_2 x_3 x_4 \dots x_k.$$

If at least two of them, say \mathfrak{b}_1 and \mathfrak{b}_2 , are contained in \mathfrak{p} , then we choose $i = 2$ and $j = 3$ and obtain an equation (7) where the first alternative for \mathfrak{a}_1 is satisfied. If at least two of them, say \mathfrak{b}_2 and \mathfrak{b}_3 , are

¹ The notion of rank is defined in [3, p. 22]. No superfluous terms (subject to cancellation) are allowed on the right side of the equation (7) which is the expansion of \mathfrak{p} in the variables x_i and x_j .

missing from \mathfrak{p} , then we choose $i = 1$ and $j = 2$ and obtain an equation (7) where the second alternative for \mathfrak{a}_1 is satisfied. This proves our lemma.

Proof of the main theorem. The assertion is trivial for $n = 2$. We assume the assertion holds for $n < m$ (≥ 3). Let \mathfrak{p} be the polynomial representing an arbitrary given function of m essential variables. We separate two cases.

Case 1. \mathfrak{p} contains at least one conjunction of rank ≥ 3 . We choose variables x_i and x_j as in the lemma and write \mathfrak{p} in the form (7). Next, we define polynomials c_1, \dots, c_7 as follows:

c_1 consists of terms common to $\mathfrak{a}_1, \mathfrak{a}_2$ and \mathfrak{a}_3 .

$c_i, i = 2, 3$, consists of those terms common to \mathfrak{a}_1 and \mathfrak{a}_i which are not in c_1 .

c_4 consists of those terms common to \mathfrak{a}_2 and \mathfrak{a}_3 which are not in c_1 .

$c_{4+i}, i = 1, 2, 3$, consists of the remaining terms in \mathfrak{a}_i .

Hence,

$$(8) \quad \mathfrak{p} = x_i x_j (c_1 + c_2 + c_3 + c_5) + x_i (c_1 + c_2 + c_4 + c_6) + x_j (c_1 + c_3 + c_4 + c_7) + \mathfrak{a}_4.$$

According to the choice of x_i and x_j ,

$$(9) \quad c_1 + c_5 \neq 0.$$

We now form a diagonalization \mathfrak{p}' by identifying x_i and x_j . Clearly,

$$\mathfrak{p}' = x_i (c_1 + c_5 + c_6 + c_7) + \mathfrak{a}_4.$$

We denote

$$c' = c_2 + c_3 + c_4$$

and refer to the variables which appear in c' but do not appear elsewhere in \mathfrak{p} as ζ -variables. If r is the number of ζ -variables then, by the choice of the polynomials c_i , \mathfrak{p}' possesses $m - (r + 1)$ essential variables. Hence, if $r = 0$ or $r = 1$ we obtain the required diagonalization by identifying x_i and x_j .

We, therefore, assume that $r \geq 2$. (Clearly, $r \leq m - 2$.) Our inductive assumption implies that we may identify some ζ -variables in such a way that, after the identification, the resulting polynomial contains at least $r - 2$ ζ -variables. (In this identification, some variables other than ζ -variables may vanish from c' .) This identification gives the required diagonalization because no variables other than ζ -variables vanish from \mathfrak{p} . In particular, by (8) and (9), x_i and x_j are preserved.

Case 2. \mathfrak{p} contains only conjunctions of ranks 1 and 2. If \mathfrak{p} is linear we may identify any two variables. Otherwise, we choose some non-linear term, say $x_1 x_2$, and write

$$p = x_1x_2 + x_1(\delta_1 + \delta_2) + x_2(\delta_1 + \delta_3) + \delta_4$$

where $\delta_1, \delta_2, \delta_3$ are linear and δ_2 and δ_3 do not contain common terms. We separate three subcases.

Subcase 2a. δ_1 contains at least two variables which do not appear elsewhere in p . We may identify any two such variables.

Subcase 2b. Every variable of δ_1 appears also elsewhere in p . In this case, we identify x_1 and x_2 .

Subcase 2c. δ_1 contains exactly one variable, say x_3 , which does not appear elsewhere in p . We identify first x_1 and x_2 . If the resulting polynomial depends on the variable identified we have finished the proof. Otherwise, p is of one of the forms

$$p = x_1x_2 + x_1(x_3 + 1) + x_2x_3 + \delta_4$$

or

$$p = x_1x_2 + x_1x_3 + x_2(x_3 + 1) + \delta_4.$$

In the former case, we identify x_2 and x_3 . In the latter, x_1 and x_3 .

We have, thus, completed the induction. (In fact, the inductive assumption was not used in case 2.) This proves theorem 4.

The proof is easier in some special cases as, for instance, if p contains some conjunction of rank $\geq n - 3$. It is also easy to see that the statement analogous to theorem 2 is false for diagonalizations of functions in the algebra of logic. In fact, if we choose some variable x_μ it may happen that, for any other variable x_ν , the diagonalization obtained by identifying x_μ and x_ν is a constant.

3. JABLONSKII has proved in [3, pp. 68—70] the following

Fundamental lemma. *Let $f(x_1, \dots, x_n) \in \mathfrak{P}_k$ ($k \geq 3$) depend essentially on at least two variables and assume $l > 2$ values. Then there are sets G_i , $i = 1, \dots, n$, each containing at most two elements such that the set $f(G_1, \dots, G_n)$ contains at least three elements.*

This lemma is an efficient tool in establishing completeness criteria for sets of functions over a finite domain, and in some analogous problems. We shall now extend the lemma to arbitrary sets \mathfrak{F}_A where $\text{card}(A) \geq 3$. Furthermore, we strengthen it by constructing the sets G_i in such a way that an arbitrary preassigned value of the function f is included in the set $f(G_1, \dots, G_n)$.

Theorem 5. *Let $\text{card}(A) \geq 3$ and $f(x_1, \dots, x_n) \in \mathfrak{F}_A$ depend essentially on at least two variables and assume at least three values and let a be one of these values. Then there are sets $G_i \subset A$, $i = 1, \dots, n$, each consisting of at most two elements such that $f(G_1, \dots, G_n)$ contains at least three elements, one of which is a .*

Proof. We first choose elements $a_1, \dots, a_n \in A$ such that

$$f(a_1, \dots, a_n) = a.$$

Let U be the set of n -tuples (u_1, \dots, u_n) where, for $n - 1$ elements u_i , $u_i = a_i$ and the n^{th} element u_i is arbitrary $\in A$. Denote by $f(U)$ the set of values assumed by f when its argument is restricted to the elements of U . Clearly, $a \in f(U)$. We may assume that $f(U)$ contains an element $b \neq a$. For if all elements in U satisfy the equation

$$f(u_1, \dots, u_n) = a$$

then our original n -tuple (a_1, \dots, a_n) may be replaced by any element in U . Then, for every n -tuple in U , we form the set of n -tuples differing by at most one coordinate from the given n -tuple and, if necessary, continue the process. Because f does not assume the constant value a we obtain an element b as required. By a suitable renumbering of the variables, we may assume that

$$(10) \quad a = f(a_1, \dots, a_{n-1}, a_n) \neq f(a_1, \dots, a_{n-1}, b_n) = b.$$

In what follows, we separate cases and subcases.

Case 1. There is an n -tuple (c_1, \dots, c_n) where $c_n = a_n$ or $c_n = b_n$ such that

$$f(c_1, \dots, c_n) \neq a, b.$$

Then, by (10), we may choose $G_i = \{a_i, c_i\}$, for $i = 1, \dots, n - 1$, and $G_n = \{a_n, b_n\}$.

Case 2. For all n -tuples (y_1, \dots, y_n) where $y_n = a_n$ or $y_n = b_n$,

$$f(y_1, \dots, y_n) = a \text{ or } f(y_1, \dots, y_n) = b.$$

Subcase 2a. All values assumed by f can not be represented in the form

$$(11) \quad f(a_1, \dots, a_{n-1}, x_n)$$

where x_n runs through the elements of A . This implies that there is a $d \in A$ such that, for some n -tuple (d_1, \dots, d_n) ,

$$f(d_1, \dots, d_n) = d$$

and, for every n -tuple $(a_1, \dots, a_{n-1}, x_n)$,

$$f(a_1, \dots, a_{n-1}, x_n) \neq d.$$

Hence, by (10), $d \neq a, b$. By the assumption of case 2, $d_n \neq a_n, b_n$.

Denote

$$e = f(a_1, \dots, a_{n-1}, d_n).$$

According to the definition of d , $e \neq d$.

If $e = a$ we choose $G_i = \{a_i, d_i\}$, for $i = 1, \dots, n-1$, and $G_n = \{b_n, d_n\}$,

If $e \neq a$ we choose $G_i = \{a_i, d_i\}$, for $i = 1, \dots, n$.

Subcase 2b. All values assumed by f can be represented in the form (11). Hence, there are at least three distinct values of the form (11).

There is an n -tuple (h_1, \dots, h_n) such that

$$(12) \quad h' = f(a_1, \dots, a_{n-1}, h_n) \neq f(h_1, \dots, h_{n-1}, h_n) = h$$

because, otherwise, f would depend essentially on the last variable only.

Suppose $a = h$ or $a = h'$. By the assumption of subcase 2b, there is an element $h'_n \in A$ such that

$$f(a_1, \dots, a_{n-1}, h'_n) \neq h, h'.$$

By (12), we may choose $G_i = \{a_i, h_i\}$, for $i = 1, \dots, n-1$, and $G_n = \{h_n, h'_n\}$.

Suppose $a \neq h, h'$. Then we may choose $G_i = \{a_i, h_i\}$, for $i = 1, \dots, n$.

Thus, we have completed the proof of theorem 5 in all cases.

In general, it is not possible to construct the sets G_i in such a way that two arbitrary preassigned values of the function f are included in the set $f(G_1, \dots, G_n)$. Thus, a further strengthening of the fundamental lemma in this direction is not possible. We shall finally mention a consequence of theorem 5 which can be proved by an easy induction. (Cf. the proof of consequence 1 in [3, p. 70].)

Theorem 6. *Let $\text{card}(A) \geq 3$ and $f(x_1, \dots, x_n) \in \mathfrak{F}_A$ depend essentially on at least two variables and assume at least $r+2$ values and let a_1, \dots, a_r be some of these values. Then there are sets $G_i \subset A$, $i = 1, \dots, n$, each consisting of at most $r+1$ elements such that $f(G_1, \dots, G_n)$ contains at least $r+2$ elements, including the elements a_1, \dots, a_r .*

References

- [1] Лупанов, О. Б.: Об одном классе схем из функциональных элементов. - Сб. «Проблемы кибернетики», 7 (1962), 61—114.
- [2] Соловьев, Н. А.: К вопросу о существенной зависимости функций алгебры логики. - Сб. «Проблемы кибернетики», 9 (1963), 333—335.
- [3] Яблонский, С. В.: Функциональные построения в k -значной логике. - Тр. Матем. инст. им. В. А. Стеклова, 51 (1958), 5—142.