COLLOQUIUM MATHEMATICUM

XIV WARSZAWA—WROCŁAW 1966

ON THE NUMBER OF INDEPENDENT ELEMENTS IN FINITE ABSTRACT ALGEBRAS HAVING A BINARY OPERATION *

BY

J. PŁONKA (WROCŁAW)

The following questions have been asked by Marczewski [2]: 1° how large can be the number of independent elements (in the sense of [1]) in an n-element abstract algebra with a binary operation and, conversely, 2° how small can be the cardinality of an algebra having a binary operation in which there exist n independent elements? In order to discuss these problems we consider the following classes of algebras in which there exists a binary algebraic operation f depending on both its variables: the class $\mathcal{K}_c$ of all such algebras with algebraic constants, the class $\mathcal{K}^s$ of all such algebras without constants, with symmetrical f, and the class $\mathcal{K}^u$ of all such algebras without constants, with unsymmetrical f.

For the classes $\mathcal{K}_c$, $\mathcal{K}^s$ and $\mathcal{K}^u$ Section 2 of this paper contains the complete answer to the second problem (which turns out to be easier than the first one) and Section 3, based on the preceding one, answers to the first. A certain result of S. Fajtlowicz concerning the class $\mathcal{K}^u$ (Theorem 12) has permited to finish the investigation of the first problem for that class.

The author is indebted to Professor E. Marczewski and Docent J. Mycielski for valuable suggestions and comments.

1. At first we shall prove a theorem which will be useful in the following considerations and which is also of some interest in itself.

THEOREM 1. *Let $\mathfrak{A}$ be an algebra, without algebraic constants, having a binary algebraic operation $f(x, y)$ which depends on both variables and is symmetrical, i. e. $f(x, y) = f(y, x)$. Then for every $n = 3, 4, \ldots$ there exists an algebraic operation of n variables depending on each one* (1).

---

* The main results of this paper were announced in [4] and presented to the Conference on General Algebra, held in Warsaw, September 7-11, 1965.

(1) Some generalization of Theorem 1 has been published by Marczewski [3].

The proof will be preceded by several definitions and lemmas. We shall write $f(x, y) = xy$ and we shall call *products* all algebraic operations generated by the operation xy. Every product, even xy, will be written in parantheses (e. g. instead xy we shall write (xy)). By the *n-th complete product* we shall mean the operation P_n of 2^n variables defined recursively as follows:

$$P_1(x_1, x_2) = (x_1 x_2),$$
$$P_{n+1}(x_1, \ldots, x_{2^{n+1}}) = \big(P_n(x_1, \ldots, x_{2^n}) P_n(x_{2^n+1}, \ldots, x_{2^{n+1}})\big).$$

LEMMA 1. *Let P_n be a complete product. Suppose $i \neq j$ are natural numbers not greater than 2^n. Then there exists a permutation φ of the set $1, 2, \ldots, 2^n$ such that $\varphi(i) = j$, $\varphi(j) = i$ and $P_n(x_1, \ldots, x_{2^n}) = P_n(x_{\varphi(1)}, \ldots$ $\ldots, x_{\varphi(2^n)})$.*

Proof. It is enough to apply a suitable number of times the commutativity of (xy).

LEMMA 2. *Let $F(x_1, \ldots, x_n)$ be a product of different variables $x_1, \ldots, x_n$. Then there exist indices $i_1, \ldots, i_k$ and complete products $F_{i_j}(x_{i_j}, y_1^{(i_j)}, \ldots, y_{s_{i_j}}^{(i_j)})$ such that after substituting x_{i_j} in F by these complete products we obtain a complete product.*

For example, the product $((x_1 x_2) x_3)$ can be completed to a complete product by substituting x_3 by $(x_3 x_4)$. The proof is obvious.

LEMMA 3. *If there are no constants in $\mathfrak{A}$, then every complete product depends on all its variables.*

Proof. Let $s(x_1, \ldots, x_{2^n})$ be a complete product, and suppose it does not depend on x_k. It depends on some variables $x_{i_1}, \ldots, x_{i_p}$ $(p < 2^n)$, because otherwise it would be a constant. So we can write

$$s(x_1, \ldots, x_{2^n}) = h(x_{i_1}, \ldots, x_{i_p}),$$

where h is some algebraic operation of algebra $\mathfrak{A}$ depending on each of its variables. Let us assume that e. g. $k < i_1$. Let us denote by φ the permutation given by Lemma 1 which changes the variables x_k and x_{i_1} on their places. We have

$$s(x_1, \ldots, x_{2^n})$$
$$= s(x_{\varphi(1)}, \ldots, x_{\varphi(k-1)}, x_{i_1}, x_{\varphi(k+1)}, \ldots, x_{\varphi(i_1-1)}, x_k, x_{\varphi(i_1+1)}, \ldots, x_{\varphi(2^n)}).$$

But the last equality is an identity, and so we can also write

$$s(x_{\varphi(1)}, \ldots, x_{\varphi(k-1)}, x_{i_1}, x_{\varphi(k+1)}, \ldots, x_{\varphi(i_1-1)}, x_k, x_{\varphi(i_1+1)}, \ldots, x_{\varphi(2^n)})$$
$$= h(x_k, x_{\varphi(i_2)}, \ldots, x_{\varphi(i_p)}).$$

Hence

$$s(x_1, \ldots, x_{2^n}) = h(x_k, x_{\varphi(i_2)}, \ldots, x_{\varphi(i_p)}),$$

where on the right side of the last formula the variable x_{i_1} does not appear. Consequently, the complete product $s(x_1, \ldots, x_{2^n})$ does not depend on x_{i_1} which contradicts our assumption.

LEMMA 4. *If in algebra $\mathfrak{A}$ there are no constants, then every product in which all variables are different depends on all its variables.*

To prove this, let us assume that the product $f(x_1, \ldots, x_n)$ does not depend on the variable x_k where $1 \leqslant k \leqslant n$. Then

$$f(x_1, \ldots, x_n) = h(x_{i_1}, \ldots, x_{i_p}),$$

where $k \neq i_j$ for $j = 1, \ldots, p$, and h is an algebraic operation depending on p variables ($p < n$). Let us complete the product f according to Lemma 2 to a complete product putting respective products on both sides of the last equation. We get

$$s = h',$$

where the variable x_k appears on the left side, and does not appear on the right side. Consequently, the complete product does not depend on x_k in contradiction to Lemma 3.

Our theorem is an immediate corollary of Lemma 4. The proof of Theorem 1 would be much simpler if we assumed associativity of $f(x, y)$ for the operation from this theorem, which was not done.

2. For every abstract algebra $\mathfrak{A} = (A; F)$ we shall denote by $\alpha(\mathfrak{A})$ the number of elements of A, and by $\iota(\mathfrak{A})$ the greatest possible number of independent elements in $\mathfrak{A}$ (see [1] and [2]). In the sequel we shall say shortly "an independent set" instead of "a set of independent elements". E. Marczewski and S. Świerczkowski have proved (see [2]) that

$$(1) \qquad |A| \geqslant |C(I)| = \sum_{j=0}^{n} \binom{n}{j} \omega_j,$$

where I is an independent subset of $\mathfrak{A}$ having n elements, $C(I)$ denotes the subalgebra of $\mathfrak{A}$ generated by I, and ω_j is the number of different algebraic operations of j variables depending on each its variable. Obviously, the ω_j are non-negative integers, and $\omega_1 \geqslant 1$ because $f(x) = x$ is an algebraic operation depending on x.

Let $\mathscr{K}$ be a given class of algebras, and let n be a natural number. We define the function $p(n, \mathscr{K}) = \min \alpha(\mathfrak{A})$, where this minimum is taken over all algebras $\mathfrak{A}$ from the class $\mathscr{K}$ for which $\iota(\mathfrak{A}) = n$. If there is no such algebra in $\mathscr{K}$, we put $p(n, \mathscr{K}) = 0$.

From now on we shall consider only such algebras $\mathfrak{A}$ which have at least one binary algebraic operation f depending on both variables and we shall use the symbols $\mathscr{K}_c$, $\mathscr{K}^s$ and $\mathscr{K}^u$ defined in the introduction.

THEOREM 2. *For* $n>1$ *we have*

$$p(n, \mathscr{K}_c) = \frac{n(n+1)}{2}+1. \tag{2}$$

Proof. By (1) and in view of suppositions on class $\mathscr{K}_c$ we have

$$p(n, \mathscr{K}_c) \geqslant n+\binom{n}{2}+1 = \frac{n(n+1)}{2}+1.$$

Formula (2) will be proved if we show that for each $n>1$ there exists an algebra $\mathfrak{C}_0$ belonging to the class $\mathscr{K}_c$ for which $\iota(\mathfrak{C}_0) = n$ and $\alpha(\mathfrak{C}_0) = \frac{1}{2}n(n+1)+1$. Let us take an arbitrary set P with $|P| = \frac{1}{2}n(n+1)+1$, and divide it into three disjoint sets: I ($|I| = n$), W $\left(|W| = \binom{n}{2}\right)$ and $C = \{c\}$. In the set P we define the operation $f(x, y)$ as follows: if $a, b \in I$ and $a \neq b$, then $f(a, b) = f(b, a)$ and $f(a, b)$ arbitrary in W, and if $\langle a, b\rangle \neq \langle a_1, b_1\rangle$, then $f(a, b) \neq f(a_1, b_1)$. Otherwise $f(x, y) = c$. It is easy to see that this algebra satisfies all required postulates.

THEOREM 3. *For* $n>1$ *there is*

$$p(n, \mathscr{K}^s) = 2^n-1. \tag{3}$$

Proof. Formula (3) follows at once from Theorem 1 and from the following theorem of Marczewski [2]: If $\iota(\mathfrak{A}) = n > 1$ and for each j ($j = 2, 3, \ldots$) there exists in the algebra $\mathfrak{A}$ a j-ary operation depending on each variable, then $\alpha(\mathfrak{A}) \geqslant 2^n-1$, where the algebra of non-void sets with the addition of sets as the fundamental operation is the algebra realising the equality.

THEOREM 4. *For* $n>1$ *holds*

$$p(n, \mathscr{K}^u) = n^2. \tag{4}$$

Proof. From (1) and from the definition of class $\mathscr{K}^u$ it follows that

$$p(n, \mathscr{K}^u) \geqslant n+2\binom{n}{2} = n+2\frac{n(n-1)}{2} = n^2.$$

Let us consider the 2-dimensional diagonal algebra (see [4] and [5])

$$\mathfrak{D}_{n,n} = (I\times I; \circ),$$

where $|I| = n$ and the fundamental operation $\circ$ is defined by the formula

$$\langle a, b\rangle \circ \langle c, d\rangle = \langle a, d\rangle.$$

The algebra $\mathfrak{D}_{n,n}$ is an algebra of the class $\mathscr{K}^u$ in which $\alpha = n^2$ and $\iota = n$ (see Theorem 2 of [4]).

Theorem is thus proved.

The following theorem has been proved in [5]:

(*) *If $g(x,y)$ is an algebraic operation in $\mathfrak{A}$ depending on both variables and if all algebraic m-ary operations for $m \leqslant 2$ and the operations $g(g(x,y),z)$ and $g(x,g(y,z))$ are of the form $g(x_{i_1}, x_{i_2})$ with suitable i_1, i_2, then the operation $g(x,y)$ is a diagonal multiplication (i. e. it satisfies the postulates 1°, 2° and 3° as given before).*

From (*) follows

THEOREM 5. *If $\mathfrak{A}$ is an algebra from the class $\mathscr{K}^u$, $a(\mathfrak{A}) = n^2$, $\iota(\mathfrak{A}) = n > 2$, then the operation f appearing in the definition of $\mathscr{K}^u$ is a diagonal multiplication.*

Proof. In fact, from (1) and the last formula it follows that every algebraic operation $g \in A^{(j)}$ $(j \leqslant 3)$ must be trivial or it must have the form $f(x_i, x_j)$, and so the assumptions of (*) are verified.

Let us observe that in the case $n = 2$ Theorem 5 is not true any longer. Let $\mathfrak{B} = (a,b,c,d;\, h(x,y))$, where $h(a,b) = c$, $h(b,a) = d$ and $h(x,y) = x$ in all remaining cases. Evidently the set (a,b) is independent, $\mathfrak{B}$ belongs to $\mathscr{K}^u$ but nevertheless $h(x,y)$ is not a diagonal multiplication. In fact, $\mathfrak{B}$ has no constants, because for every algebraic operation $f(x_1, \ldots, x_n)$ of $\mathfrak{B}$ one has $f(x,x,\ldots,x) = x$; moreover, there are no non-trivial operations of one variable, and the only operations of two variables, which depend on both variables, are $h(x,y)$ and $h(y,x)$.

We shall now compute the values of $p(n, \mathscr{K}_c)$, $p(n, \mathscr{K}^s)$, $p(n, \mathscr{K}^u)$ in the case $n = 1$.

LEMMA 5. *Every algebra from the classes considered has at least two elements.*

This is obvious, as in a set of one element it is impossible to define an operation depending on two variables.

LEMMA 6. *In the class $\mathscr{K}^u$ there are no 2-element algebras.*

In fact, if such an algebra existed, we could denote its elements by a, b. Because in the considered algebra there are no constants, and the operation $f(x,y)$ from the definition of the class $\mathscr{K}^u$ is not symmetrical, only four combinations can hold:

1. $f(a,b) = a,\quad f(b,a) = b,\quad f(a,a) = a,\quad f(b,b) = b,$
2. $f(a,b) = a,\quad f(b,a) = b,\quad f(a,a) = b,\quad f(b,b) = a,$
3. $f(a,b) = b,\quad f(b,a) = a,\quad f(a,a) = a,\quad f(b,b) = a,$
4. $f(a,b) = b,\quad f(b,a) = a,\quad f(a,a) = b,\quad f(b,b) = a.$

In the cases 1 and 4 the function f does not, however, depend on the second variable, and in remaining cases it does not depend on the first variable, in contradiction to the definition of the class $\mathscr{K}^u$.

THEOREM 6. *There is*

$$p(1, \mathcal{K}_c) = 2, \tag{5}$$

$$p(1, \mathcal{K}^s) = 2, \tag{6}$$

$$p(1, \mathcal{K}^u) = 3. \tag{7}$$

Proof. Formula (5) follows from Lemma 5 and from the existence of the algebra $\mathfrak{C}_1 = (\{a, b\}; f(x, y), b)$, where b is constant, and

$$f(a, b) = f(b, a) = b, \quad f(x, x) = x. \tag{8}$$

Formula (6) follows from Lemma 5 and from the existence of the algebra $\mathfrak{S}_1 = (a, b; f(x, y))$, where

$$f(a, b) = f(b, a) = b \quad \text{and} \quad f(x, x) = x. \tag{9}$$

Formula (7) follows from Lemmas 5 and 6 and from the existence of the algebra $\mathfrak{U}_1 = (a, b, c; f(x, y))$, where

$$\begin{gathered} f(x, y) = x \quad \text{if} \quad x \neq y, \\ f(a, a) = b, \quad f(b, b) = c, \quad f(c, c) = a. \end{gathered} \tag{10}$$

Our theorem is thus proved.

Theorems 2, 3, 4 and 6 give all values of the function p for the classes $\mathcal{K}_c$, $\mathcal{K}^s$ and $\mathcal{K}^u$. In particular, we have

n	1	2	3	4	5
$p(n, \mathcal{K}_c)$	2	4	7	11	16
$p(n, \mathcal{K}^s)$	2	3	7	15	31
$p(n, \mathcal{K}^u)$	3	4	9	16	25

Let us notice that for $n \geqslant 5$ we have always $p(n, \mathcal{K}_c) < p(n, \mathcal{K}^u) < p(n, \mathcal{K}^s)$.

3. Let $\mathcal{K}$ be a class of algebras, and n a natural number. We define the function $q(n, \mathcal{K})$ as follows:

$$q(n, \mathcal{K}) = \max \iota(\mathfrak{A}), \tag{11}$$

where this maximum is taken over all algebras $\mathfrak{A} \in \mathcal{K}$ having n elements. If such an algebra does not exist we put $q(n, \mathcal{K}) = -1$.

THEOREM 7. *For* $n \geqslant 4$ *there is*

$$q(n, \mathcal{K}_c) = \left[\frac{-1 + \sqrt{1 + 8(n-1)}}{2}\right], \tag{12}$$

where $[x]$ *denotes the integral part of* x.

Proof. From Theorem 2 it follows that

$$q(n, \mathcal{K}_c) \leqslant \left[\frac{-1+\sqrt{1+8(n-1)}}{2}\right].$$

The algebra $\mathfrak{C}$ of the class $\mathcal{K}_c$ satisfying formulas

$$\alpha(\mathfrak{C}) = n, \quad \iota(\mathfrak{C}) = \left[\frac{-1+\sqrt{1+8(n-1)}}{2}\right] = q,$$

is constructed in the manner that we divide an arbitrary set P with n elements into four disjoint sets: I ($|I| = q$), W $\left(|W| = \binom{q}{2}\right)$, $C = \{c\}$ (where c is a distinguished element) and $R = P\setminus(I \cup W \cup C)$. In the set P we define the operation $f(x, y)$ as follows: if $a, b \in I$ and $a \neq b$, then $f(a, b) = f(b, a)$ and $f(a, b) \in W$, and if $\langle a, b\rangle \neq \langle a_1, b_1\rangle$, then $f(a, b) \neq f(a_1, b_1)$.

In all other cases $f(x, y) = c$. It is easy to verify that this algebra satisfies the required conditions.

THEOREM 8. *For $n \geqslant 3$ there is*

$$q(n, \mathcal{K}^s) = \left[\frac{\log(n+1)}{\log 2}\right]. \tag{13}$$

Proof. From Theorem 3 it follows that

$$q(n, \mathcal{K}^s) \leqslant \left[\frac{\log(n+1)}{\log 2}\right].$$

We shall construct an algebra

$$\mathfrak{S} = (A; f(x, y)), \quad |A| = n, \quad \iota(\mathfrak{S}) = \left[\frac{\log(n+1)}{\log 2}\right] = q.$$

Let $A = W \cup V$, where W is a set of all non empty subsets of a q-element set I and $V = \{J_1, J_2, \ldots, J_{n-2^q+1}\}$. We suppose that $I \subset J_1 \subset J_2 \ldots \subset J_{n-2^q+1}$, and that those sets are distinct. Put $f(x, y) = x \cup y$ for $x, y \in A$.

It is easy to verify that the set $\{\{p\}: p \in I\}$ is independent and that the algebra $\mathfrak{S}$ satisfies all required conditions.

Let us compute remaining values of the function $q(n, \mathcal{K}_c)$ and $q(n, \mathcal{K}^s)$.

THEOREM 9. *There is*

$$q(3, \mathcal{K}_c) = 1, \tag{14}$$

$$q(2, \mathcal{K}_c) = 1, \tag{15}$$

$$q(1, \mathcal{K}_c) = -1, \tag{16}$$

$$q(2, \mathcal{K}^s) = 1, \tag{17}$$

$$q(1, \mathcal{K}^s) = -1. \tag{18}$$

Proof. From (1) it follows that each of these values must be smaller than 2. Formula (14) follows from the existence of the algebra $\mathfrak{C}_3 = (\{a, b, c\}; c, f(x, y))$, where c is an algebraic constant, $f(x, x) = x$, $f(a, b) = f(b, a) = b$, $f(a, c) = f(c, a) = f(b, c) = f(c, b) = c$.

Formula (15) follows from the existence of the algebra $\mathfrak{C}_1$ (see Theorem 6). Formulas (16) an (18) follow from Lemma 5. Formula (17) follows from the existence of algebra $\mathfrak{S}_1$ (see Theorem 6).

THEOREM 10. *For $m \geqslant 3$ there does not exist an algebra $\mathfrak{A} = (A; F)$ without constants with a binary operation f, depending on both arguments and non-commutative, in which*

$$|A| = m^2+k, \tag{19}$$

where $m = \iota(\mathfrak{A})$ and $0 < k < m$.

Proof. Let us assume that such algebra exists. From formulas (19) and (1) it follows that in view of $m > 3$ the assumptions of (*) are satisfied and thus f is a diagonal multiplication.

But the algebra $\mathfrak{A}$ cannot be a diagonal algebra, because for the 2-dimensional proper diagonal algebra $\mathfrak{D}$ formula (19) cannot hold, as we have

(+) $a(\mathfrak{D}) = n_1 n_2$, where n_1 and n_2 are positive integers $n_i > 1$, $\iota(\mathfrak{D}) = \min(n_1, n_2)$ (see [5], Theorem 3).

Let us now consider the diagonal algebra $\mathfrak{D}' = (A; f)$. Of course, $\iota(\mathfrak{D}') \geqslant \iota(\mathfrak{A})$ and so

$$\iota(\mathfrak{D}') = \iota(\mathfrak{A}), \tag{20}$$

because if $\iota(\mathfrak{A}) < \iota(\mathfrak{D}') = m+p$, then in view of (+) we should have

$$|\mathfrak{D}'| \geqslant (m+p)^2 > m^2+k = a(\mathfrak{A}) = a(\mathfrak{D}').$$

Formulas (20) and (19) also give contradiction, because (19) cannot hold for diagonal algebra.

Hence our theorem is proved.

We shall now compute values of the function $q(n, \mathscr{K}^u)$ for $n \leqslant 12$.

LEMMA 7. *For $n \geqslant 4$ we have $q(n, \mathscr{K}^u) \geqslant 2$.*

For the proof we construct the algebra $\mathfrak{U}_n = (a_1, \ldots, a_n; f(x, y))$, where $f(a_1, a_2) = a_3$, $f(a_2, a_1) = a_4$ and otherwise $f(x, y) = x$. It is easy to verify that the set $\{a_1, a_2\}$ is independent and $\mathfrak{U}_n$ belongs to the class $\mathscr{K}^u$.

In the sequel we shall write for simplicity (as in § 1) xy instead of $f(x, y)$, and call this operation *multiplication*. We shall say that the multiplication xy is *trivial* if it depends on one variable only, i. e. if for all x, y we have $xy = x$ or for all x, y we have $xy = y$. We shall say that xy is *idempotent multiplication* if $xx = x$ for all x. All algebras considered are from $\mathscr{K}^u$.

LEMMA 8. *An idempotent multiplication, satisfying one of the identities* $(xy)z = z(xy)$, $(xy)z = z(yx)$, *is commutative.*

Proof. Identify x and y.

LEMMA 9. *If there are no non-trivial unary algebraic operations in* A, *and the multiplication is non-trivial and non-commutative, then the equality* $x_1(x_2x_3) = x_ix_j$ *for all* x_k *and for fixed* i, j *implies* $i = 1, j = 2$ *or* 3.

Proof. As every unary operation is trivial, and xy is non-trivial, it follows that $i \neq j$ and obviously $\{i, j\} \subset \{1, 2, 3\}$. There remain the cases

$$(21) \qquad x_1(x_2x_3) = x_2x_3, \qquad\qquad (22) \qquad x_1(x_2x_3) = x_3x_2,$$

$$(23) \qquad x_1(x_2x_3) = x_2x_1, \qquad\qquad (24) \qquad x_1(x_2x_3) = x_3x_1,$$

$$(25) \qquad x_1(x_2x_3) = x_1x_2, \qquad\qquad (26) \qquad x_1(x_2x_3) = x_1x_3.$$

If we identify in the cases (22), (23) and (24) the variables x_2 and x_3, we see that the multiplication is either trivial or commutative against our assumption.

LEMMA 10. *If* xy *is idempotent,* $(xy)z = (yx)z$ *and* $x(yz) = xy$ *hold for all* x, y, z, *then* xy *is trivial.*

Proof. We have

$$\begin{aligned}
\big((xy)z\big)u &= \big((yx)z\big)u, \\
\big((xy)z\big)u &= \big(z(xy)\big)u = (zx)u, \\
\big((xy)z\big)u &= \big(z(yx)\big)u = (zy)u,
\end{aligned}$$

whence $(zx)u = (zy)u$. By putting here $z = x$ we obtain $xu = (xy)u$. Thus $xy = (xz)y = (zx)y = zy$, and finally, by putting $x = y$, we get $x = zx$.

LEMMA 11. *If* xy *is idempotent,* $(xy)z = (yx)z$ *and* $x(yz) = xz$ *hold for all* x, y, z, *then* xy *is diagonal.*

Proof. We have

$$\begin{aligned}
\big((xy)z\big)u &= \big((yx)z\big)u, \\
\big((xy)z\big)u &= \big(z(xy)\big)u = (zy)u, \\
\big((yx)z\big)u &= \big(z(yx)\big)u = (zx)u.
\end{aligned}$$

Thus $(zy)u = (zx)u$ and by putting $z = y$ we get $zu = (zx)u$.

LEMMA 12. *If* xy *is idempotent,* $(xy)z$ *and* $z(xy) = z(yx)$ *hold for all* x, y, z, *then* $xy = yx$ *for all* x, y.

Proof. Put $z = yx$ in the first formula, and $z = xy$ in the second.

LEMMA 13. *If* xy *is idempotent,* $(xy)z = (zy)x$ *and* $x(yz) = xy$ *hold for all* x, y, z, *then* xy *is trivial.*

Proof. We have

$$u\big((xy)z\big) = u\big((zy)\big)x,$$
$$u\big((xy)z\big) = u(xy) = ux,$$
$$u\big((zy)x\big) = u(zy) = uz,$$

and therefore $ux = uz$ nad $x = xz$.

LEMMA 14. *If xy is idempotent, $(xy)z = (zy)x$ and $x(yz) = xy$ hold for all x, y, z, then xy is trivial.*

Proof. We have

$$u\big((xy)z\big) = u\big((zx)y\big),$$
$$u\big((xy)z\big) = u(xy) = ux,$$
$$u\big((zx)y\big) = u(zx) = uz.$$

Thus $ux = uz$, $u = uz$.

LEMMA 15. *If xy is idempotent, $(xy)z = (xz)y$ and $x(yz) = xz$ hold for all x, y, z, then xy is trivial.*

Proof. We have $uy = u\big((xz)y\big) = u\big((xy)z\big) = uz$, thus $u = uz$.

LEMMA 16. *If xy is idempotent, $(xy)z = (yz)x$ and $x(yz) = xz$ hold for all x, y, z, then xy is trivual.*

Proof. We have $ux = u\big((yz)x\big) = u\big((xy)z\big) = uz$. Thus $u = uz$.

THEOREM 11.

$$q(1, \mathscr{K}^u) = -1, \tag{27}$$
$$q(2, \mathscr{K}^u) = -1, \tag{28}$$
$$q(3, \mathscr{K}^u) = 1, \tag{29}$$
$$q(4, \mathscr{K}^u) = \ldots = q(8, \mathscr{K}^u) = 2, \tag{30}$$
$$q(9, \mathscr{K}^u) = 3, \tag{31}$$
$$q(10, \mathscr{K}^u) = 2, \tag{32}$$
$$q(11, \mathscr{K}^u) = 2, \tag{33}$$
$$q(12, \mathscr{K}^u) = 3. \tag{34}$$

Proof. From (1) follows $q(n, \mathscr{K}^u) \leqslant \sqrt{n}$. Now (27) follows from Lemma 5, (28) from Lemma 6, (29) from the existence of the algebra $\mathfrak{A}_1$ constructed in the proof of Theorem 6. Moreover, (30) follows from Lemma 7, (31) from the existence of the diagonal algebra $\mathfrak{D}_{3,3}$ and (34) from the existence of the diagonal algebra $\mathfrak{D}_{3,4}$. To prove (32) and (33) it suffices by Lemma 7 to show that

(I) There exists no algebra $\mathfrak{A}$ in $\mathscr{K}^u$ such that $\alpha(\mathfrak{A}) = 10$, $\iota(\mathfrak{A}) = 3$ and

(II) There exists no algebra $\mathfrak{A}$ in $\mathscr{K}^u$ such that $\alpha(\mathfrak{A}) = 11$, $\iota(\mathfrak{A}) = 3$.

Proof of (I). Suppose that such an algebra exists. Then there exists in it an algebraic binary operation $f(x, y)$, which we shall denote by xy, that depends on both variables and is not commutative. Let $\{a, b, c\}$ be an independent subset of this algebra. The remaining elements of our algebra are thus ab, ba, ac, ca, bc, cb and a tenth element, say, d. We prove first that one of the following formulas must hold:

(a) $$(ab)c = d$$
or
(b) $$c(ab) = d.$$

Suppose this is not the case, then xy must be idempotent, and there are no other binary operations depending on both variables, as otherwise the algebra would have more elements. Hence the application of (*) shows that the algebra is diagonal. But there is no diagonal algebra with 10 elements and an independent triple (see (+)).

Obviously, (a) and (b) could not hold simultaneously as it would contradict the independence of (a, b, c) in view of Lemma 8.

Suppose now that (a) holds. Then $(ba)c = d$, and $c(ab) = ca$ or $c(ab) = cb$ (see Lemma 9). The first possibility contradicts Lemma 9, and the second contradicts Lemma 11. In the case (b) the proof is similar.

Proof of (II). Suppose that there exists an algebra $\mathfrak{A} = (X, \boldsymbol{F})$ in $\mathscr{K}^u$, such that $\alpha(\mathfrak{A}) = 11$, and $\iota(\mathfrak{A}) = 3$.

Let $\{a, b, c\}$ be an independent triple in $\mathfrak{A}$ and let $xy = f(x, y)$ be a non-commutative binary algebraic operation depending in both variables.

X consists of the following elements: a, b, c, ab, ba, ac, ca, bc, cb, d, e. At first observe that either $(ab)c = d$, $(ab)c = e$, $c(ab) = d$, or $c(ab) = e$, because otherwise an argument analogous to the argument used in the proof of (I) would show that the algebra in question is diagonal, which is impossible by (+).

Suppose then that $(ab)c = d$ (the case $(ab)c = e$ can be dealt with in exactly the same way). By Lemma 9 we must distinguish between two following cases only: 1° $(ba)c = d$ and 2° $(ba)c = e$.

In the case 1° we have $(ab)c = (ba)c = d$. By Lemma 8 we have also $c(ab) \neq d$, and, by Lemma 10 and 11, $c(ab) \neq d$, $c(ab) \neq e$ (otherwise $c(ab) = ca$ and $c(ab) = cb$).

Thus $c(ab) = e$ and $c(ba) = e$, as the equality $c(ba) = d$ contradicts Lemma 8, and if $c(ba) \neq d$, $c(ba) \neq e$, then we would have contradiction with Lemma 9.

But the system $(ab)c = (ba)c$, $c(ab) = c(ba)$ is incompatible by Lemma 12.

Now consider the case 2°, where $(ab)c = d$ and $(ba)c = e$. By Lemmas 8 and 9 we must also have $c(ab) = ca$ or $c(ab) = cb$. In the first case $(cb)a$

$= d$ or $(cb)a = e$, which contradicts the Lemma 13 or, resp., Lemma 14, and in the second case we have $(ac)b = d$ or $(ac)b = e$ in contradiction with Lemma 15 or, resp., with Lemma 16.

In the remaining cases the proof is similar.

From Theorem 11 it follows that Theorem 10 is true for the case $n = 3$ as well.

The following theorem is given by S. Fajtlowicz:

THEOREM 12. *For* $n = m^2+k$ ($m \geqslant 2$, $n \geqslant 6$) *there exists an algebra* $\mathfrak{A} \in \mathscr{K}^u$ *in which* $a(\mathfrak{A}) = n$, $\iota(\mathfrak{A}) = m$.

Proof. Let us consider an infinite set A and an m-element subset B of it ($m \geqslant 2$). We define a binary operation in the Cartesian product $B \times A$ as follows:

$$\langle x, y\rangle \cdot \langle u, v\rangle = \langle x, u\rangle.$$

It is easy to verify that every subset C of $B\times A$ containing $B\times B$ is a subalgebra of the algebra $\mathfrak{A}^* = \langle B\times A; \cdot\rangle$. Let $\mathfrak{A}$ denote an algebra $\langle C; \cdot\rangle$. The operation $\cdot$ satisfies the equalities

$$(x\cdot y)\cdot z = xz, \qquad x\cdot(y\cdot z) = xy, \qquad (xy)(uv) = xu.$$

Hence we have in the algebra $\mathfrak{A}$ only three non-trivial operations depending on each variable, i. e. $x\cdot y$, $y\cdot x$, x^2.

Since $m \geqslant 2$, all these operations are different and none of them is constant.

Let $p \in A\setminus B$, $B\times(B \cup \{p\}) \subset C$ and $|C| = m^2+k$. The set $B\times\{p\}$ is independent on account of the form of the algebraic operations in $\mathfrak{A}$. Moreover, as $\iota(\mathfrak{A}) \leqslant m$ (see Theorem 4 of this paper), then we have $\iota(\mathfrak{A}) = m$.

Theorems 7, 8, 9, 11 and 12 give the full description of the function q for the classes $\mathscr{K}_c$, $\mathscr{K}^s$ and $\mathscr{K}^u$:

n	1	2	3	4	5
$q(n, \mathscr{K}_c)$	-1	1	1	2	2
$q(n, \mathscr{K}^s)$	-1	1	2	2	2
$q(n, \mathscr{K}^u)$	-1	-1	1	2	2

$$q(n, \mathscr{K}_c) = \left[\tfrac{1}{2}(-1+\sqrt{1+8(n-1)}\right] \quad \text{for} \quad n \geqslant 4,$$

$$q(n, \mathscr{K}^s) = \left[\frac{\log(n+1)}{\log 2}\right] \quad \text{for} \quad n \geqslant 3,$$

and

$$q(n, \mathscr{K}^u) = \begin{cases} m & \text{for} \quad k = 0, \\ m-1 & \text{for} \quad 0 < k < m, \\ m & \text{for} \quad m \leqslant k < 2m, \end{cases}$$

where $5 \neq n = m^2+k$ nad $m \geqslant 2$.

It is interesting that the function $q(n, \mathscr{K}^u)$ is not monotone.

REFERENCES

[1] E. Marczewski, *Independence and homomorphisms in abstract algebras* Fundamenta Mathematicae 50 (1961), p. 45-61.

[2] — *The number of independent elements in abstract algebras with unary and binary operations*, Bulletin de l'Académie Polonaise des Sciences, Série des sc. math., astr. et phys., 12 (1964), p. 723-727.

[3] — *Remarks on symmetrical and quasi-symmetrical operations*, ibidem 12 (1964), p. 735-737.

[4] J. Płonka, *Diagonal algebras and algebraic independence*, ibidem 12 (1964), p. 729-734.

[5] — *Diagonal algebras*, Fundamenta Mathematicae (in print).

Reçu par la Rédaction le 1. 3. 1965