COLLOQUIUM MATHEMATICUM

VOL. XV 1966 FASC. 2

EXCHANGE OF INDEPENDENT SETS IN ABSTRACT ALGEBRAS (III)

BY

JERZY PŁONKA (WROCŁAW)

Introduction. In the present paper we are concerned with the condition of exchange of independent sets (EIS) studied in [1] and [6]. It has been proved that EIS is fulfilled in many algebras, e.g. in Boolean algebras, Marczewski's v^*-algebras, Abelian groups (see [1]), semi-lattices and algebras having at most six elements (see [6]). This condition, however, is not satisfied in all algebras. There is a group having 729 elements and an algebra having 7 elements, which do not satisfy EIS (see [1], [6]) and 729 and 7 are the minimal numbers for which this is possible. So far, however, counterexamples contained algebraic constants. In the present paper I give: (1) an example of an algebra without algebraic constants which has 12 elements and does not satisfy EIS and a proof that 12 is the minimal number for which this is possible; (2) a proof that EIS is satisfied in all distributive lattices.

In this paper we will use the following abbreviations: *constants* and *operations* for algebraic constants and algebraic operations; *essentially n-ary operations* for n-ary operations depending on all variables.

1. EIS in algebras without constants having at most 11 elements.

Let $\mathfrak{A}$ be an arbitrary algebra. We say that *the condition of exchange of independent sets* (EIS) *is satisfied in* $\mathfrak{A}$ if for arbitrary subsets P, Q, R of this algebra the conditions

(a) $P \cap Q = \emptyset$,

(b) $P \cup Q$ is an independent set,

(c) R is an independent set,

(d) Q generates R

imply the condition

(e) $P \cup R$ is an independent set.

Let $a(\mathfrak{A})$ denote the power of an algebra $\mathfrak{A}$.

THEOREM 1. (i) *For every number* $a \geqslant 12$ *there exists a semigroup* $\mathfrak{P}$ *without constants which does not satisfy EIS, for which* $a(\mathfrak{P}) = a$.

(ii) *If* $a(\mathfrak{A}) < 12$ *and there are no constants in* $\mathfrak{A}$, *then* $\mathfrak{A}$ *satisfies EIS.*

Proof of (i). $\mathfrak{P}$ has the form $\mathfrak{P} = (A \cup B \cup C; \cdot)$, where

$$A = \{a, b, c\},$$
$$B = \{\langle a, b\rangle, \langle a, c\rangle, \langle b, c\rangle, \langle b, a\rangle, \langle c, a\rangle, \langle c, b\rangle\},$$
$$C = \{\langle a, a\rangle, \langle b, b\rangle, \langle c, c\rangle, d_1, d_2, \ldots, d_n\} \quad (n \geqslant 0)$$

and the operation $\cdot$ is defined as follows:

if $x, y \in A$, then $x \cdot y = \langle x, y\rangle$;
if $x \in A, y \in B \cup C$, then $x \cdot y = \langle x, x\rangle$;
if $\langle u, v\rangle \in B$, then $\langle u, v\rangle \cdot z = \langle u, u\rangle$;
if $x \in C$, then $x \cdot y = x$.

It is easily seen that the only non-trivial operations of this algebra are $x \cdot y$ and $x \cdot x$, and, consequently, there are no constants in $\mathfrak{P}$.

Let $P = \{c\}$, $Q = \{a, b\}$, $R = \{\langle a, b\rangle\}$. We see that conditions (a)-(d) are fulfilled, but condition (e) is not, as

$$\langle a, b\rangle \cdot c = \langle a, b\rangle \cdot \langle a, b\rangle = \langle a, a\rangle,$$

though the identity $x \cdot y = x \cdot x$ does not hold.

Proposition (i) is thus proved. The proof of (ii) will be preceded by a lemma.

LEMMA. *If an algebra* $\mathfrak{A}$ *is finite and the conditions* (a)-(d) *are satisfied for some subsets* P, Q, R, *the set* R *being generated by the set* Q *only by means of unary operations, then the condition* (e) *is satisfied.*

Proof of Lemma. Let elements of the sets P, Q, R be denoted by letters p, q, r with indices, respectively. We can assume that the set R is generated by Q by means of unary operations $h_i(x)$ $(i \in I)$. Because of (c) there are no constants among operations h_i. In part 3° of the proof of theorem 2 of [6] it has been proved that if $b = h(a)$ and both sets $\{a\}$ and $\{b\}$ are independent, then either the algebra is infinite or there exists an index k such that the k-th iteration of the function $h(x)$ is a trivial operation, i.e. $h^k(x) = x$.

In view of the assumption of the Lemma such an index k_i exists for every function h_i.

Now we shall show that every element of the set R is generated by at most one element of the set Q, and every element of the set Q generates at most one element of the set R. Indeed, if $r = h_1(q_1) = h_2(q_2)$, then $h_1(x) = h_2(y) = c$, which is impossible, since R, being independent, does not contain constants. If, however, $r_1 = h_1(q)$, $r_2 = h_2(q)$, then

$q = h_1^{k_1-1}(r_1) = h_2^{k_2-1}(r_2)$, whence, because of the independence of R, $h_1^{k_1-1}(x) = h_2^{k_2-1}(y) =$ constant, contrary to the independence of the set Q.

Let now two operations f and g be equal for certain arguments of the set $P \cup R$. We thus have the equality

$$f(p_1, \dots, p_m, r_1, \dots, r_n) = g(p_1, \dots, p_m, r_1, \dots, r_n).$$

For every r_i there exists exactly one element q_i generating r_i, and, in view of independence of the set Q, there is exactly one operation h_i such that $r_i = h_i(q_i)$. Hence

$$f\big(p_1, \dots, p_m, h_1(q_1), \dots, h_n(q_n)\big) = g\big(p_1, \dots, p_m, h_1(q_1), \dots, h_n(q_n)\big).$$

But the set $P \cup R$ is independent. Consequently

$$f\big(x_1, \dots, x_m, h_1(y_1), \dots, h_n(y_n)\big) = g\big(x_1, \dots, x_m, h_1(y_1), \dots, h_n(y_n)\big).$$

Putting $y_i = h_i^{k_i-1}(z_i)$ in the last equality, we obtain

$$f(x_1, \dots, x_m, z_1, \dots, z_n) = g(x_1, \dots, x_m, z_1, \dots, z_n).$$

Thus the functions f and g are identical, and since they have been chosen arbitrarily, the set $P \cup R$ is independent, q.e.d.

Remark. The supposition of the Lemma that $\mathfrak{A}$ is finite is essential. In fact, let $\mathfrak{A} = (\{m\sqrt{n}\colon m = 1, 2, \dots, n = 1, 2, 3, 5\};\ h_0, h_1, h_2, \dots)$, where h_i with $i > 0$ are unary operations defined by $h_i(x) = ix$ and h_0 is a binary operation defined by

$$h_0(x, y) = \begin{cases} \sqrt{3} & \text{if } \quad x = 1 \text{ and } y = \sqrt{2}, \\ \sqrt{5} & \text{if } \quad x = \sqrt{2} \text{ and } y = 1, \\ x & \text{in all other cases.} \end{cases}$$

We set $P = \{1\}$, $Q = \{\sqrt{2}\}$, $R = \{2\sqrt{2}\}$. It is easy to check that conditions (a)-(d) are satisfied (e.g. the independence of $P \cup Q$ follows from the fact that the only operations of at most two variables depending on each variable are $h_i(x)$ with $i > 0$ and $h_i\big(h_0(x, y)\big)$ with $i > 0$, these operations are one-to-one and their ranges are disjoint). Yet (e) is not true, since $h_0(1, 2\sqrt{2}) = 1$ whereas $h_0(1, \sqrt{2}) \neq 1$.

Proof of (ii). Let R be generated by the set Q by means of operations h_i $(i \in I)$. We can assume that each h_i depends on all of its variables. Elements of the sets P, Q, R will be denoted by p, q, r, respectively. If condition (e) does not hold, then there exist two different operations $f(x_1, \dots, x_m)$ and $g(x_1, \dots, x_n)$, each being dependent on all its variables, which satisfy the formula

$$(1) \qquad f(p_1, \dots, p_{m_1}, r_1, \dots, r_{m_2}) = g(p_1', \dots, p_{n_1}', r_1', \dots, r_{n_2}'),$$

where $m_1+m_2 = m$, $n_1+n_2 = n$ and all arguments of each of the functions f and g are different, whereas a certain p_i may be equal to a certain p'_j, and a certain r_i may be equal to a certain r'_j.

Marczewski proved in [3] the inequality

$$a(\mathfrak{A}) \geqslant |C(I)| = \sum_{j=0}^{n} \binom{n}{j} \omega_j, \tag{2}$$

where I is an independent subset of $\mathfrak{A}$, $|I| = n$, ω_j is the number of essentially j-ary operations, $C(I)$ is the subalgebra generated by I.

In view of the Lemma it suffices to consider the cases when among the operations h_i there occur operations of two or more variables. We take the notation $T = P \cup Q$ and consider two cases.

1° Let one of operations h_i be essentially n-ary, with $n \geqslant 3$. Hence $|Q| \geqslant n$, $|T| \geqslant n+1$. If $n \geqslant 5$, then, because of (2),

$$a(\mathfrak{A}) \geqslant \binom{n+1}{n} + n+1 \geqslant 12,$$

which contradicts $a(\mathfrak{A}) < 12$. Let then n be equal to 3 or 4. If $|T| \geqslant n+2$, then, because of (2),

$$a(\mathfrak{A}) \geqslant \binom{n+2}{n} + n+2 \geqslant 12.$$

Thus let $|T| = n+1$. Then $|P| = 1$ and $|Q| = n$. From (2) it follows that $\mathfrak{A}$ has no essentially m-ary operations with $1 \leqslant m \leqslant n$, distinct from n-ary operations h_i, except the identity operation. This also implies that h_i is symmetrical, i.e. no new operation is obtained by permuting its arguments. Hence $R = \{h_i(q_1, \ldots, q_n)\}$ and $|P \cup R| = 2$. But there are no non-trivial unary or binary operations and (e) follows.

2° Let one of the operations h_i be essentially binary; let us denote it by $\cdot$. If $|T| > 3$ and the operation $\cdot$ were symmetrical then, by Theorem 3 of [5], this algebra would have at least 2^n-1 elements, and if this operation were not symmetrical, then, by Theorem 4 of [5], the algebra would have at least n^2 elements. Both numbers are obviously greater than 11. Thus let $|T| = 3$ and $|P| = 1$. Then $|Q| = 2$ and T consists of the elements p, q_1, q_2. If the operation $\cdot$ is not symmetrical, then the algebra $\mathfrak{A}$ has at least 9 elements. If $a(\mathfrak{A}) = 9$, then by Theorem 5 of [5] all operations of at most three variables will be such as in a diagonal algebra (see Theorem 5 of [5]). Since in this case the set R may contain only at most three elements $p, q_1 \cdot q_2, q_2 \cdot q_1$, so, if EIS were not satisfied, it would be not satisfied within a diagonal algebra. This would contradict a theorem that EIS is satisfied in diagonal algebras (see [6]). Theorem 11 of [5] states that 10- and 11-element algebras with a three-element independent set and a non-symmetrical essentially binary operation $\cdot$ do not exist. Thus the operation $\cdot$ must be symmetrical. From Theorem 1 of [5] it follows that, because of the lack of constants, there exists an essentially ternary operation $(x\cdot y)\cdot z$. The algebra has thus the elements

$$p, \quad q_1, \quad q_2, \quad q_1\cdot q_2, \quad p\cdot q_1, \quad p\cdot q_2, \quad (q_1\cdot q_2)\cdot p.$$

If there were no other essentially unary or binary operations in $\mathfrak{A}$ besides operation $\cdot$ and the trivial operation, then we had $R = \{q_1\cdot q_2\}$ and the condition EIS would be satisfied. Indeed, each of the operations f and g in (1) has then to be either trivial or the operation $\cdot$. However, neither $p\cdot(q_1\cdot q_2) = p$, nor $p\cdot(q_1\cdot q_2) = q_1\cdot q_2$ can occur, since in view of the independence of T, this would yield $x\cdot(y\cdot z) = x$, $x\cdot(y\cdot z) = y\cdot z$. But this is impossible, because the operation $x\cdot(y\cdot z)$ is an operation of three variables.

Thus it is enough to prove that there exists no such operation distinct from $\cdot$ and the trivial operations. Suppose on the contrary that $g(x)$ is such a non-trivial essentially unary operation of $\mathfrak{A}$. Because of (2) and the inequality $a(\mathfrak{A}) < 12$ it had to be one such operation. But then the operation $g(x\cdot y)$ would be a new essentially binary operation. Indeed, let $d = q_1\cdot q_2$. The operation $g(x\cdot y)$ is symmetrical and essentially binary. If $g(x\cdot y) = x\cdot y$, then, putting $x = q_1, y = q_2$, we would obtain $g(d) = d$, contrary to the independence of the set R and the non-triviality of g. In this case the algebra would have two different essentially binary operations and a non-trivial essentially unary operation, whence, by virtue of (2), it would have more than 11 elements. If there existed in $\mathfrak{A}$ another essentially binary operation, let us denote it by $+$; then in view of the former considerations it should be symmetrical too. From (2) and the inequality $a(\mathfrak{A}) < 12$ it follows that no other essentially unary or binary operations exist in $\mathfrak{A}$. Thus the operations $+$ and $\cdot$ must be idempotent. From Theorem 1 of [5] it follows then that there exist essentially ternary operations

$$f_1(x, y, z) = (x+y)+z, \qquad f_2(x, y, z) = (x\cdot y)\cdot z.$$

Let $f_3(x, y, z) = (x+y)\cdot z$. We shall prove that the operation f_3 is essentially ternary, and that the operations f_1, f_2, f_3 are all different. Indeed, the operation f_3 may be completed to a quasi-symmetric one by putting $z = u+v$ (see Marczewski [4]). Thus if the operation f_3 did not depend on some of the variables x, y, z, then a quasi-symmetrical operation $(x+y)\cdot(u+v)$ would not depend on some of its variables, which would contradict a theorem of Marczewski (see [4]).

Neither $f_1 = f_2$ nor $f_1 = f_3$ can be true, because each of them would imply the identity of the operations $+$ and $\cdot$ (by putting $x = y$).

If $f_2 = f_3$, i.e. $(x\cdot y)\cdot z = (x+y)\cdot z$, then replacing z by $x+y$ and then by $x\cdot y$ we get $(x\cdot y)\cdot(x+y) = (x+y)\cdot(x+y) = x+y$, $(x\cdot y)\cdot(x\cdot y)$

$= (x+y)\cdot(x\cdot y)$, i.e. $x\cdot y = (x+y)\cdot(x\cdot y)$, whence $x+y = x\cdot y$, thus a contradiction again. In such a case there exist in $\mathfrak{A}$ two essentially binary operations $\cdot$ and $+$ and three essentially ternary operations f_1, f_2 and f_3. Hence, considering (2), we obtain a contradiction with the inequality $a(\mathfrak{A}) < 12$. Since all cases have been considered the proof is complete.

2. EIS in distributive lattices. A distributive lattice is an algebra $(X; +, \cdot)$, where each of the operations $+$ and $\cdot$ is idempotent, symmetrical, associative and distributive with respect to the other operation, and we have the formula $x\cdot(x+y) = x$. Marczewski showed in [2] that a subset $J = \{a_1, \ldots, a_n\}$ of a distributive lattice is dependent if and only if

(1) $$a_{i_1}\cdot\ldots\cdot a_{i_k} \leqslant a_{i_{k+1}}+\ldots+a_{i_{k+l}} \quad \text{for some } i_j\in\{1, \ldots, n\},$$

where $k+l\leqslant n$ and $a_{i_j}\neq a_{i_{j'}}$ for $j\neq j'$.

THEOREM 2. *Condition EIS is satisfied in distributive lattices.*

Proof. Because of the distributivity of multiplication with respect to addition, every algebraic operation of a distributive lattice has the form

$$f(x_1, \ldots, x_n) = w_1+w_2+\ldots+w_k, \quad \text{where} \quad w_s = x_{i_1}\cdot x_{i_2}\cdot\ldots\cdot x_{i_{k_s}},$$
$$s = 1, 2, \ldots, k, \quad i_j\in\{1, 2, \ldots, n\}, \quad i_j < i_{j'}. \text{ for } j < j'.$$

Let us assume that conditions (a)-(d) (§ 1) are satisfied. Because of the finite character of independence, it suffices to consider the case, where each of the sets P, Q, R is finite. The elements of those sets will be denoted by p, q, r, respectively. If the condition (e) were not fulfilled, formula (1) could be written in the form

(2) $$p_1\cdot\ldots\cdot p_m\cdot r_1\cdot\ldots\cdot r_n \leqslant p_{m+1}+\ldots+p_{m+s}+r_{n+1}+\ldots+r_{n+t}.$$

In the presence of condition (d) and because of the form of algebraic operations in a distributive lattice we can write

(3) $$r_i = \sum_{j=1}^{n_i} w_j,$$

where w_j is a product of certain elements q_μ of the set Q. But the sums and products of expressions such as the right-hand side of formula (3) have the same form again. Hence, substituting the right-hand sides of (3) for the r_i's in (2) and multiplying expressions within parantheses obtained in this way on the left-hand side of (2) we get the formula

(4) $$p_1\cdot\ldots\cdot p_m\cdot(w_1+w_2+\ldots+w_k) \leqslant p_{m+1}+\ldots+p_{m+s}+w_{k+1}+\ldots+w_{k+l}.$$

If the elements r_i did not occur on the right-hand side of (2), then replacing the sum of elements w_i occurring in parantheses on the left-hand side of (4) by the product of all w_i and considering (1) we would obtain a contradiction with the independence of the set $P\cup Q$. Similarly, if the elements r_i did not occur on the left-hand side of (2), then replacing each w_i occurring on the right-hand side of (4) by the sum of elements of the set Q occurring in (4) we would obtain a similar contradiction. Thus the elements w_i must occur on the right- and left-hands sides of (4).

If for every $i \leqslant k$ we had

$$w_i \leqslant w_j \text{ for some } j > k, \tag{5}$$

then it would be easily seen that $r_1\cdot\ldots\cdot r_n \leqslant r_{n+1}+\ldots+r_{n+t}$, contrary to the independence of the set R. Thus there exists such an $i \leqslant k$ for which (5) does not hold. Let $i = 1$. Thus in every product w_j for $j > k$ there exists an element, say q_{i_j}, which does not occur in w_1.

If

$$p_1\cdot\ldots\cdot p_m\cdot w_1 \leqslant p_{m+1}+p_{m+s}+w_{k+1}+\ldots+w_{k+l}, \tag{6}$$

then also

$$p_1\cdot\ldots\cdot p_m\cdot w_1 \leqslant p_{m+1}+\ldots+p_{m+s}+q_{i_{k+1}}+q_{i_{k+l}},$$

where elements occurring in the product on the left-hand side would be different from elements occurring on the right-hand side, contrary to the independence of the set $P \cup Q$. Formula (4) can be rewritten in the form

$$p_1\cdot\ldots\cdot p_m\cdot w_1+p_1\cdot\ldots\cdot p_m\cdot w_2+\ldots+p_1\cdot\ldots\cdot p_m\cdot w_k$$
$$\leqslant p_{m+1}+\ldots+p_{m+s}+w_{k+1}+\ldots+w_{k+l}.$$

But the last condition cannot be satisfied, since formula (6) does not hold. Thus formula (4) does not hold and formula (2) is not satisfied either. This proves the independence of the set $P \cup R$.

REFERENCES

[1] A. Hulanicki, E. Marczewski and J. Mycielski, *Exchange of independent sets in abstract algebras (I)*, Colloquium Mathematicum 14 (1966), p. 203-215.

[2] E. Marczewski, *Concerning independence in lattices*, ibidem 10 (1963), p. 21-23.

[3] — *Number of independent elements in abstract algebras with unary and binary operations*, Bulletin de l'Académie Polonaise des Sciences, Série des sciences mathématiques, astronomiques et physiques, 12 (1964), p. 723-727.

[4] — *Remarks on symmetrical and quasi-symmetrical operations*, ibidem, p. 735-737.

[5] J. Płonka, *On the number of independent elements in finite abstract algebras having a binary operation*, Colloquium Mathematicum 14 (1966), p. 189-201.

[6] — *Exchange of independent sets in abstract algebras (II)*, ibidem 14 (1966), p. 217-224.

INSTITUTE OF MATHEMATICS OF THE POLISH ACADEMY OF SCIENCES

Reçu par la Rédaction le 22. 7. 1965

Added in proof. Professor Bjarni Jónsson, in a letter of June 17, 1966, to Professor Edward Marczewski pointed out that the EIS-property is closely connected with the amalgamation property, as studied by B. Jónsson (*Universal relational systems*, Mathematica Scandinavica 4 (1956), p. 193-208, *Sublattices of a free lattice*, Canadian Journal of Mathematics 13 (1961), p. 256-264, and *Extensions of relational structures*, The Theory of Models, Proceedings of the 1963 International Symposium at Berkeley, Amsterdam 1965, p. 146-157). By means of Jónsson's results the EIS-property can be obtained for Abelian groups, Boolean algebras and distributive lattices.