COLLOQUIUM MATHEMATICUM

VOL. XXXVI 1976 FASC. 2

EXCHANGE PROPERTY AND t-INDEPENDENCE

BY

K. GOLEMA-HARTMAN (WROCŁAW)

The subject of this paper is the property of exchange of independent sets (EIS) in some classes of algebras. The property has been introduced by Marczewski (see, e.g., [2]) and has been considered in [2], [5], [6] and in some other papers devoted to such classes as groups, Boolean algebras, distributive lattices and diagonal algebras. In Section 1 we prove that the full idempotent reduct of an abelian group has the EIS property (Theorem 1). In Lemma 1 a general condition appears which can be applied to an arbitrary algebra. This is studied in Section 2 by comparing it with common notions of independence, both for quite general algebras and for some special classes. We also give to it a more suggestive form (Theorem 2).

Results contained in this paper were announced in [1].

The author is indebted to Professor J. Płonka for guidance and suggestions.

0. $\mathfrak{A} = (A; \boldsymbol{F})$ means that $\mathfrak{A}$ is an algebra, A — the set of its elements, and $\boldsymbol{F}$ — the set of its fundamental operations. If $\boldsymbol{F}$ is finite, $\boldsymbol{F} = \{f_1, \ldots, f_n\}$, then we write also $\mathfrak{A} = (A; f_1, \ldots, f_n)$. By $\boldsymbol{A}(\boldsymbol{F})$ we denote the set of all algebraic operations of $\mathfrak{A}$. For any subset $Y \subset A$, $C(Y)$ will mean the *algebraic closure* of Y, i.e. the smallest subalgebra of $\mathfrak{A}$ containing Y. A set $I \subset A$ is called *algebraically independent* (or, briefly, *independent*) in $\mathfrak{A}$ if, for any $a_1, \ldots, a_n \in I$ and any two operations $f, g \in \boldsymbol{A}(\boldsymbol{F})$, the equality $f(a_1, \ldots, a_n) = g(a_1, \ldots, a_n)$ implies $f = g$ (see [4]). A set $I \subset A$ is called *C-independent* if, for any $a \in I$, $a \notin C(I \setminus \{a\})$ (cf. [2]). An algebra $\mathfrak{B} = (A; \boldsymbol{G})$ is said to be a *reduct* of $\mathfrak{A}$ if $\boldsymbol{G} \subset \boldsymbol{A}(\boldsymbol{F})$. An algebraic operation $f(x_1, \ldots, x_n)$ is called *idempotent* if $f(x, \ldots, x) = x$ holds identically. The *full idempotent reduct* $\varrho(\mathfrak{A})$ of $\mathfrak{A}$ is the algebra $(A; \boldsymbol{I})$, where $\boldsymbol{I}$ is the set of all idempotent operations in $\mathfrak{A}$.

An algebra $\mathfrak{A}$ is said to have the *exchange property* (EIS, [2]) if, for any subsets $P, Q, R \subset A$, the conditions

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

(ii) both $P \cup Q$ and R are algebraically independent,

(iii) $R \subset C(Q)$

imply independence of $P \cup R$.

1. Let $\mathfrak{G} = (G; \cdot, ^{-1})$ be an abelian group. The *exponent* of $\mathfrak{G}$, $\exp\mathfrak{G}$, is the least positive integer m for which $x^m = 1$ $(x \in G)$. If there is no such number, then we write $\exp\mathfrak{G} = \infty$, and the congruence $k \equiv 1 (\mathrm{mod}\ \infty)$ will mean equality. We set $x^0 = 1$. Clearly, every n-ary operation in an abelian group can be represented as $x_1^{k_1} \cdot \ldots \cdot x_n^{k_n}$, where k_i are integers, and we shall use such representations in the sequel. An operation is *idempotent* in $\mathfrak{G}$ if $x^{k_1+\cdots+k_n} = x$ for each $x \in G$, and this means that $k_1 + \ldots + k_n \equiv 1 (\mathrm{mod}\, m)$. Independence of a set in $\mathfrak{G}$ is not equivalent to its independence in the full idempotent reduct $\varrho(\mathfrak{G})$. Evidently, independence of a set in $\mathfrak{G}$ implies its independence in $\varrho(\mathfrak{G})$, but the converse does not hold. Here is an example.

Let $\mathfrak{G}$ be the abelian group with exponent 2 and with two generators a and b. It has 4 elements: $a, b, ab, 1$. The set $E = \{a, b, ab\}$ is not algebraically independent in $\mathfrak{G}$, but it is independent in $\varrho(\mathfrak{G})$. In fact, the only idempotent operations in $\mathfrak{G}$ of at most three variables are the trivial ones and the operation $x_1x_2x_3$, but if f and g are any two of them, we have $f(x_1, x_2, x_3) \neq g(x_1, x_2, x_3)$ whenever x_i are different elements of E.

The following lemma will be needed to prove Theorem 1.

LEMMA 1. *A set J is not independent in $\varrho(\mathfrak{G})$ if and only if the following conditon holds:*

there exist elements $a_1, \ldots, a_n \in J$ such that, for some $i \in [1, n]$,

$$a_i = a_1^{k_1} \cdot \ldots \cdot a_n^{k_n}, \tag{1}$$

where $x_1^{k_1} \cdot \ldots \cdot x_n^{k_n}$ is an idempotent operation and $k_i \not\equiv 1$ (mod m), $m = \exp\mathfrak{G}$ $(m \leqslant \infty)$.

Proof. Assume that J is not independent in $\varrho(\mathfrak{G})$. Then there are two different idempotent operations $x_1^{k_1} \cdot \ldots \cdot x_n^{k_n}$ and $x_1^{l_1} \cdot \ldots \cdot x_n^{l_n}$ and some elements $a_1, \ldots, a_n \in J$ such that

$$a_1^{k_1} \cdot \ldots \cdot a_n^{k_n} = a_1^{l_1} \cdot \ldots \cdot a_n^{l_n}. \tag{2}$$

Since the two operations are different, there exists an i such that $k_i \not\equiv l_i$ (mod$\,m$). Multiplying (2) by $a_1^{-k_1} \cdot \ldots \cdot a_i^{-k_i+1} \cdot \ldots \cdot a_n^{-k_n}$ we get

$$a_i = a_1^{l_1-k_1} \cdot \ldots \cdot a_i^{l_i-k_i+1} \cdot \ldots \cdot a_n^{l_n-k_n}.$$

The operation $f = x_1^{l_1-k_1} \cdot \ldots \cdot x_i^{l_i-k_i+1} \cdot \ldots \cdot x_n^{l_n-k_n}$ is idempotent and $l_i - k_i + 1 \not\equiv 1$ (mod$\,m$).

Conversely, let (1) be satisfied. The equality $x_i = x_1^{k_1} \cdot \ldots \cdot x_n^{k_n}$ does not hold identically in $\mathfrak{G}$. In fact, if it did, then choosing, for each $j \neq i$,

$x_j = 1$ (the neutral element), we would have $x_i^{k_i-1} = 1$ for every value of x_i, contrary to the assumption $\exp\mathfrak{E} = m$.

The above argument also shows that the operation $x_1^{k_1}\cdot \ldots \cdot x_n^{k_n}$ is not trivial.

THEOREM 1. *The full idempotent reduct of an abelian group has the exchange property.*

Proof. Let P, Q and R satisfy (i)-(iii). Assume that the set $P\cup R$ is not independent. By Lemma 1 it contains elements $a_1, \ldots, a_n$ such that, for some i, (1) holds with $k_i \not\equiv 1 \pmod m$. Let $i = 1$, for convenience. So we have

$$(3) \qquad a_1 = a_1^{k_1}\cdot \ldots \cdot a_n^{k_n}, \qquad k_1 \not\equiv 1 \pmod m.$$

We consider separately two cases: $a_1 \in P$ and $a_1 \in R$.

In the first case, let $a_2, \ldots, a_l \in P$, and $a_{l+1}, \ldots, a_n \in R$. For $a_j \in R$ we have

$$(4) \qquad a_j = f_j(q_1^{(j)}, \ldots, q_{p_j}^{(j)}),$$

where f_j is an idempotent operation and $q_k^{(j)} \in Q$ $(l+1 \leqslant j \leqslant n,\ 1 \leqslant k \leqslant p_j)$. Taking into account (4), from (3) we get

$$a_1 = a_1^{k_1}\cdot \ldots \cdot a_l^{k_l}\cdot f_{l+1}^{k_{l+1}}(q_1^{(l+1)}, \ldots, q_{p_{l+1}}^{(l+1)})\cdot \ldots \cdot f_n^{k_n}(q_1^{(n)}, \ldots, q_{p_n}^{(n)}),$$

but, in view of Lemma 1, this contradicts the independence of $P\cup Q$.

In the second case, if $a_1 \in R$, let $a_2, \ldots, a_r \in R$ and $a_{r+1}, \ldots, a_n \in P$. Taking into account (4), from (3) for $j \in [2, r]$ we get

$$f_1(q_1^{(1)}, \ldots, q_{p_1}^{(1)}) = f_1^{k_1}(q_1^{(1)}, \ldots, q_{p_1}^{(1)})\cdot \ldots \cdot f_r^{k_r}(q_1^{(r)}, \ldots, q_{p_r}^{(r)})\cdot a_{r+1}^{k_{r+1}}\cdot \ldots \cdot a_n^{k_n}.$$

Since $P\cup Q$ is independent in $\varrho(\mathfrak{E})$ by assumption, the equality

$$f_1(x_1^{(1)}, \ldots, x_{p_1}^{(1)}) = f_1^{k_1}(x_1^{(1)}, \ldots, x_{p_1}^{(1)})\cdot \ldots \cdot f_r^{k_r}(x_1^{(r)}, \ldots, x_{p_r}^{(r)})\cdot x_{r+1}^{k_{r+1}}\cdot \ldots \cdot x_n^{k_n}$$

holds identically in $\varrho(\mathfrak{E})$, and so in $\mathfrak{E}$. Putting here 1 for every variable except for some x_t, where $t \in [r+1, n]$, we find $x_t^{k_t} = 1$, and so $k_t \equiv 0 \pmod m$ for all $t > r$. Hence we may drop in (3) the last $n-r$ factors, thus getting $a_1 = a_1^{k_1}\cdot \ldots \cdot a_r^{k_r}$, so R is not independent by Lemma 1, contrary to the assumption.

Lemma 1 implies

LEMMA 1′. *A set I is algebraically independent in the full idempotent reduct of an abelian group if and only if, for any distinct elements $a_1, \ldots, a_n$ of I and every non-trivial operation $x_1^{k_1}\cdot \ldots \cdot x_n^{k_n}$ we have*

$$a_1^{k_1}\cdot \ldots \cdot a_n^{k_n} \neq a_i \quad \textit{for all } i \in [1, n].$$

The condition appearing in Lemma 1′ can be put in the following abstract form:

2. Definition. Given an algebra $\mathfrak{A} = (A; F)$, a set $I \subset A$ is called *t-independent* if, for any distinct elements $a_1, \ldots, a_n \in I$ and any non-trivial operation $f(x_1, \ldots, x_n)$, we have

$$f(a_1, \ldots, a_n) \neq a_i \quad (i = 1, \ldots, n).$$

Remark 1. *Any t-independent set is C-independent.*

Indeed, if a set I is not C-independent, then it contains an element a_1 which can be expressed by means of some other elements $a_1 = f(a_2, \ldots, a_n)$, where f is a non-trivial operation. Assuming

$$g(x_1, \ldots, x_n) = f(x_2, \ldots, x_n),$$

we have $a_1 = g(a_1, \ldots, a_n)$; hence I is not t-independent.

Remark 2. *Algebraic independence implies t-independence.*

To show this, assume that I is not t-independent. Then there exist a non-trivial operation $f(x_1, \ldots, x_n)$, distinct elements $a_1, \ldots, a_n \in I$ and an index i such that $f(a_1, \ldots, a_n) = a_i$. These elements satisfy the equation $x_i = f(x_1, \ldots, x_n)$, which is not identically fulfilled. Hence I is not algebraically independent.

In the full idempotent reduct of an abelian group, t-independence coincides with algebraic independence (this is the statement of Lemma 1′), but it does not coincide with C-independence which is shown by

Example 1. Let $\mathfrak{E}$ be an abelian group with exponent 6 and with two generators a and b. The set $\{a^3, b^3\}$ is C-independent in $\mathfrak{E}$, and so in $\varrho(\mathfrak{E})$. Nevertheless, it is not t-independent (hence it is not algebraically independent) in $\varrho(\mathfrak{E})$, since $a^3 = (a^3)^3 \cdot (b^3)^4$ and the operation x^3y^4 is not trivial.

There exist algebras in which t-independence is different from algebraic independence. Here we have an example:

Example 2. In the semilattice with elements a, b, c, d, in which a, b, c are incomparable and $ab = ac = bc = d$, the set $\{a, b, c\}$ is not algebraically independent, since, e.g., $ab = ac$ although $x_1 \cdot x_2 = x_1 \cdot x_3$ does not hold identically. However, this set is t-independent, since the value of any non-trivial algebraic operation on its elements is d.

Theorem 2. *A set I is t-independent if and only if, for any system $a_1, \ldots, a_n \in I$ and any non-trivial operation $f(x_1, \ldots, x_n)$, we have*

$$f(a_1, \ldots, a_n) \notin I.$$

Proof. It is obvious that the above condition implies t-independence. Conversely, if $f(a_1, \ldots, a_n) \in I$ for a non-trivial f and some $a_1, \ldots, a_n \in I$, I would be not C-independent, and so not t-independent.

Theorem 2 enables us to compare the notion of algebraic independence and that of t-independence. Namely, if a set I is algebraically independent, then the value of any non-trivial algebraic operation on I is outside I and, moreover, the values which such an operation assumes on different systems of elements of I are different (this can be easily proved) whereas for t-independence the latter property does not always hold.

We now turn to t-independence in semilattices and Boolean algebras.

THEOREM 3. *Given a semilattice* $\mathfrak{S} = (S; +)$ *with more than* 1 *element, a set* $J \subset S$ *is t-independent if and only if it contains no pair of comparable elements.*

Proof. If $a, b \in J$ and $a \leqslant b$, then $a+b = b$, hence J is not t-independent. Conversely, if J is not t-independent, then there exist a non-trivial operation $x_1 + x_2 + \ldots + x_n$ $(n > 1)$ and a system of elements $a_1, \ldots, a_n \in J$ such that, for some i, $a_i = a_1 + \ldots + a_n$. For any $j \neq i$ we thus have

$$a_i \geqslant a_1 + \ldots + a_{i-1} + a_{i+1} + \ldots + a_n \geqslant a_j.$$

THEOREM 4. *In Boolean algebras, algebraic independence and t-independence coincide.*

Proof. We have but to prove that t-independence implies algebraic independence. Marczewski has shown [3] that a subset J of a Boolean algebra is not algebraically independent if and only if there exist an atom $x_1^{\delta_1} \cdot \ldots \cdot x_n^{\delta_n}$ $(\delta_i = 0$ or 1, $x^1 = x$, $x^0 = x')$ and a system of elements $a_1, \ldots, a_n \in J$ such that

$$a_1^{\delta_1} \cdot \ldots \cdot a_n^{\delta_n} = 0. \tag{5}$$

Assume that J is not algebraically independent. So it satisfies the above condition. If $1 \in J$, then, since $1 = 1 + 1'$ and the operation $f(x) = x + x'$ is non-trivial, J is not t-independent. We have the same conclusion in the case $0 \in J$, in view of $0 = 0 \cdot 0'$, the operation $f(x) = x \cdot x'$ being non-trivial. If $0, 1 \notin J$, then there are at least two factors on the left-hand side of (5). Let us consider two cases.

1. For some i, we have $\delta_i = 0$. Assume this holds for $i = 1$. Then (5) implies

$$a_1 + a_1' \cdot a_2^{\delta_2} \cdot \ldots \cdot a_n^{\delta_n} = a_1.$$

By distributivity we have

$$(a_1 + a_1')(a_1 + a_2^{\delta_2} \cdot \ldots \cdot a_n^{\delta_n}) = a_1,$$

and so

$$a_1 + a_2^{\delta_2} \cdot \ldots \cdot a_n^{\delta_n} = a_1.$$

Since the operation $x_1 + x_2^{\delta_2} \cdot \ldots \cdot x_n^{\delta_n}$ is non-trivial, this implies that J is not t-independent.

2. $\delta_i = 1$ for all $i \in [1, n]$. Then, if we pass in (5) to the complements, we get $a_1' + a_2' + \ldots + a_n' = 1$, and so

$$a_1(a_1' + a_2' + \ldots + a_n') = a_1$$

or else

$$a_1 \cdot a_1' + a_1(a_2' + \ldots + a_n') = a_1.$$

Hence $a_1(a_2' + \ldots + a_n') = a_1$. Since the operation $x_1(x_2' + \ldots + x_n')$ is non-trivial, J is not t-independent.

REFERENCES

[1] K. Golema-Hartman, *Idempotent reducts of abelian groups and minimal algebras*, Bulletin de l'Académie Polonaise des Sciences, Série des sciences mathématiques, astronomiques et physiques, 21 (1973), p. 809-812.

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

[3] E. Marczewski, *Independence in algebras of sets and Boolean algebras*, Fundamenta Mathematicae 48 (1960), p. 135-145.

[4] — *Independence and homomorphisms in abstract algebras*, ibidem 50 (1961), p. 45-61.

[5] J. Płonka, *Exchange of independent sets in abstract algebras (II)*, Colloquium Mathematicum 14 (1966), p. 217-224.

[6] — *Exchange of independent sets in abstract algebras (III)*, ibidem 15 (1966), p. 173-180.

TECHNICAL UNIVERSITY, WROCŁAW

Reçu par la Rédaction le 3. 4. 1975