On two numerical costants associated with finite algebras

by S. ŚWIERCZKOWSKI (Glasgow, Gran Bretagna)

Summary. - *Certain ι_* elements of an abstract algebra are called independent if every equation satisfied by these elements is identically true in the algebra* [2]. *For finite algebras we have: Given an integer $\iota_* > 3$, every ι_* elements are independent if every operation of ι_* variables is trivial, i. e. if it is identically equal to one of the variables (Th. 1). If $\iota_* \leq 3$, then there exists an algebra in which every ι_* elements are independent but not every operation of ι_* variables is trivial; moreover if $\iota_* = 3$, then n is the number of elements of such an algebra if $n = 2$ or 4 (mod 6) and $n > 3$ (Th. 2).*

1. INTRODUCTION. - In his study [2] of certain numerical constants associated with a finite algebra $\mathfrak{A}$, E. MARCZEWSKI introduced the following two

ι_* - the greatest integer such that every set composed of ι_* elements of $\mathfrak{A}$ is a subset of independent elements,

τ — the greatest integer such that every algebraic operation in $\mathfrak{A}$ of τ variables is trivial.

There are no trivial operations of 0 variables but the range of values of τ is extended to 0 and -1 as follows: If there are non-trivial operations of one variable in $\mathfrak{A}$, then we put $\tau = 0$ provided there are no algebraic constants (constant operations) in $\mathfrak{A}$ and we put $\tau = -1$ if there are such constants. It is shown in [2] (see property *(vii)*) that always, in a non-trivial finite algebra $\mathfrak{A}$,

$$(*) \qquad \iota_* = \tau \quad \text{or} \quad \iota_* - 1 = \tau$$

(ι_* is ranging through the values 0, 1, 2, ...). The purpose of this note is to discuss the type of algebra for which either of these two equalities holds. We introduce two kinds of independence in $\mathfrak{A}$, called "trivial,, and "non-trivial,, and we prove some theorems concerning these. From Theorem 1 we deduce that in a finite algebra $\mathfrak{A}$, $\iota_* - 1 = \tau$ can hold only if $\iota_* = 0, 1, 2$ or 3. Theorems 2 and 3 deal with algebras of this kind.

We adopt the notation and basic definitions given in the first section of [2].

2. **Two kinds of independence.** - Let $\mathfrak{A}$ be an arbitrary algebra and let $A^{(l)}$ denote the class of algebraic operations of l variables in $\mathfrak{A}$. If, for some $l \geq 1$, $A^{(l)}$ contains only the trivial operations (identity operations) of l variables, then it is clear that every l elements of $\mathfrak{A}$ are independent.

Such independence we shall call *trivial.* If, on the other hand there is a non-trivial operation in $A^{(l)}$ and certain l elements of $\mathfrak{A}$ are independent, then we shall call them *non-trivially independent.* We extend our definition to the case $l = 0$ calling the empty set trivially independent if and only if there are no algebraic constants in $\mathfrak{A}$. We shall frequently use the following property of trivial independence,

Lemma 1. - *If l elements of $\mathfrak{A}$ are independent, then this independence is trivial if and only if these elements form a subalgebra of $\mathfrak{A}$.*

The set $\{a_1, \ldots, a_l\}$ is a subalgebra of $\mathfrak{A}$ if and only if, for every f in $A^{(l)}$, we have $f(a_1, \ldots, a_l) \in \{a_1, \ldots, a_l\}$. The latter condition means that $A^{(l)}$ contains no other operations except the trivial ones, because $f(a_1, \ldots, a_l) = a_i$ implies, by the independence of $a_1, \ldots, a_l$ that $f(x_1, \ldots, x_l) = x_i$ holds identically in $\mathfrak{A}$; i. e. f is trivial. In case $l = 0$, the lemma follows from the fact that the empty set is a subalgebra if and only if there are no algebraical constants.

From now on we assume that $\mathfrak{A}$ is a finite algebra which has at least two elements. We deduce from (*) the following

Lemma 2. - *If the algebra $\mathfrak{A}$ is non-trivial, then every ι_* elements of $\mathfrak{A}$ are trivially independent if and only if $\iota_* = \tau$.*
Another consequence of (*) is. Lemma 3 below. To deduce Lemma 3 note that $q \leq \tau$ implies that every q elements are trivially independent. This implication is always true if $\tau = 0$ or if $q > 0$, but in the case $\tau > 0, q = 0$ one has to assume that the algebra has at teast two elements.

Lemma 3. - *If every l elements of $\mathfrak{A}$ are independent and $l \geq 1$ (i. e. $l \leq \iota_*$), then every $l - 1$ elements are trivially independent (i. e. $l - 1 \leq \tau$).*
From this lemma we deduce easily

Lemma 4. - *If every l elements of $\mathfrak{A}$ are non-trivially independent, then $l = \iota_*$.*
If $l > 3$, then Lemma 3 can be improved as follows.

Theorem 1. - *If $l > 3$ and every l elements of $\mathfrak{A}$ are independent, then this independence is trivial.*

Suppose that every l elements of $\mathfrak{A}$ are independent and $l > 3$. Let $a_1, \ldots, a_l$ be any l elements of $\mathfrak{A}$ and let $\mathfrak{A}_0$ be the subalgebra of $\mathfrak{A}$ which they generate. Clearly every l elements of $\mathfrak{A}_0$ are independent in $\mathfrak{A}_0$.

Thus, by Theorem 1 of [3] (p. 749) $\mathfrak{A}_0$ is also generated by any l of its elements. Since $l > 3$, we can apply Theorem 2 of [4]. We conclude that $\mathfrak{A}_0 = \{a_1, \ldots, a_l\}$, which means, by Lemma 1, that $a_1, \ldots, a_l$ are trivially independent.

From the above theorem and from Lemma 2 we deduce the

COROLLARY. - *If the algebra* $\mathfrak{A}$ *is non-trivial and* $\iota_* > 3$, *then* $\iota_* = \tau$.

If $\iota_* = 0, 1, 2$ or 3, then we may have $\iota_* - 1 = \tau$; we discuss the corresponding algebras in the next section.

3. - Non-trivial independence and Steiner's systems.

From Theorem 1, Lemmas 2 and 4 and (*) we obtain without difficulty

THEOREM 2. - *If* $\mathfrak{A}$ *is an algebra in which every* l *elements are non-trivially independent, then* $l = 0, 1, 2,$ *or* 3, $\iota_* = l$, *and* $\iota_* - 1 = \tau$. *Conversely, if* $\mathfrak{A}$ *is an algebra for which* $\iota_* - 1 = \tau$ *holds, then every* ι_* *elements of* $\mathfrak{A}$ *are non-trivially independent.*

Given $l = 0, 1, 2$ or 3, the question arises whether, for every integer $n > 1$, there exists an algebra $\mathfrak{A}_l$ which has n elements such that every l elements of $\mathfrak{A}_l$ are non-trivially independent. The answer is positive if $l = 0$ or 1; it is enough to take $\mathfrak{A}_0 = (\{1, 2, \ldots, n\}; f)$, where $f(x) = 1$ for every x, and $\mathfrak{A}_1 = (\{1, 2, \ldots, n\}: g)$, where $g(x) = x + 1 \pmod{n}$. If $l = 2$ or 3, then the answer to the above question is negative; the admissible values for the number of elements of $\mathfrak{A}_l$ are described below in terms of Steiner's systems.

Given a set A of n elements, we denote by $S(l, m, n)$ a system (family) of subsets of A (sometimes called Steiner's system, see [5]) having m elements each such that every subset of A having l elements is contained in exactly one set of the system $S(l, m, n)$. A list of known Steiner's systems is given by E. Witt in [5].

THEOREM 3. - *Let* $l = 2$ *or* 3. *Then* n *is the number of elements of an algebra in which every* l *elements are non-trivially independent if and only if there exists a Steiner's system* $S(l, m, n)$ *such that*

a) *m is a power of a prime number and $m > 2$ in the case when $l = 2$,*

b) *$m = 4$ in the case when $l = 3$.*

Suppose first that $\mathfrak{A}$ is an algebra which has n elements and every l elements of $\mathfrak{A}$ are non-trivially independent. Then the subalgebras of $\mathfrak{A}$

which have l generators are isomorphic to each other, hence they all have the same number of elements, say m. It is clear that the family of all these subalgebras forms an $S(l, m, n)$ system. Moreover each of these subalgebras is independently generated by any l of its elements (see proof of Theorem 1). It follows that $m = 4$ if $l = 3$ (by Theorem 4 in [4]) and that m is a power of a prime if $l = 2$ (by Theorem 6 in [4]). If $l = 2$, then $m > 2$ since, by Lemma 1, $\mathfrak{A}$ cannot contain a subalgebra of 2 elements.

Assume now that $l = 2$ or 3 and let m satisfy a) or b) respectively. Then there exists an algebra $\mathfrak{A}_0$ which has m elements. is independently generated by every l elements and is such that the class $\boldsymbol{F}$ of fundamental operations (see [2], section 1) of $\mathfrak{A}_0$ contains only operations of l variables. The existence of such an algebra follows from either Theorem 5 or Theorem 4 of [4].

To prove the sufficiency part of our theorem, assume that n is such that there exists a system $S(l, m, n)$, where $l = 2$ or 3 and m satisfies either a) or b). We consider a set A of n elements and a system $S(l, m, n)$ of subsets of A. For every set E belonging to $S(l, m, n)$ we fix an arbitrary one-to-one mapping φ_E of E onto the algebra $\mathfrak{A}_0$ defined above. Let $\boldsymbol{F}$ be the class of fundamental operations in $\mathfrak{A}_0$. Using the correspondence φ_E we define $\boldsymbol{F}$ on E so that E with the class of operations $\boldsymbol{F}$ becomes an algebra isomorphic to $\mathfrak{A}_0$; φ_E being the isomorphism. We observe now that, if in every set E belonging to $S(l, m, n)$ the class of operations $\boldsymbol{F}$ is introduced in this way, then $\boldsymbol{F}$ is defined on the whole of A. Indeed, this follows from the fact that all the operations in F are of l variables.

We define now $\mathfrak{A} = (A; \boldsymbol{F})$, and we shall prove that $\mathfrak{A}$ is the required algebra in which every l elements are non-trivially independent. We observe first that each set belonging to $S(l, m, n)$ forms a subalgebra of $\mathfrak{A}$ which is isomorphic to $\mathfrak{A}_0$. We assume that $a_1, \ldots, a_l$ are arbitrary l elements of $\mathfrak{A}$. We shall prove that they are independent. Suppose that there are operations f, g in $A^{(l)}$ such that

$$(**) \qquad f(a_1, \ldots, a_l) = g(a_1, \ldots, a_l).$$

Let E be the set in $S(l, m, n)$ which contains $a_1, \ldots, a_l$, and let $\mathfrak{A}_1 = (E; \boldsymbol{F})$. Since the algebra $\mathfrak{A}_1$ is isomorphic to $\mathfrak{A}_0$, every l elements of $\mathfrak{A}_1$ are independent in $\mathfrak{A}_1$; thus (**) implies $f = g$ in $\mathfrak{A}_1$. But since all sets belonging to $S(l, m, n)$ form subalgebras of $\mathfrak{A}$ isomorphic to $\mathfrak{A}_0$, hence to $\mathfrak{A}_1$, we conclude that f $= g$ holds in each of them, i. e. $f = g$ identically in $\mathfrak{A}$. This means that $a_1, \ldots, a_l$ are independent in $\mathfrak{A}$, and as they generate the subalgebra $\mathfrak{A}_1$ which has $m > l$ elements, it follows, by Lemma 1, that this independence is non-trivial.

COROLLARY. - *A natural integer $n > 3$ is the number of elements of an algebra in which every three elements are non-trivially independent if and only if*

$$n = 2 \text{ or } 4 \pmod 6). \tag{***}$$

This follows from Theorem 3, as, by a result of Haim Hanai [1], condition (***) is equivalent to the existence of a system $S(3, 4, n)$.

REFERENCES

[1] HAIM HANAI, *On quadruple systems*, Canad. J. Math, 12 (1960), 145-157

[2] E. MARCZEWSKI, *Nombre d'éléments indépendants et nombre d'éléments générateurs dans les algèbres abstraites finies*, Ann. Mat. Pura Appl., (4) 59 (1962), 1-10.

[3] S. ŚWIERCZKOWSKI, *On independent elements in finitely generated algebras*. Bull. Acad, Pol. Sc., Serie math. astr. phys. 6, (1958) 749-752.

[4] S. ŚWIERCZKOWSKI, *Algebras which are independently generated by every n elements*. Fund. Math. 49 (1960), 93-104.

[5] E. WITT, *Ueber Steinersche Systeme*, Abh. Math. Sem. Hamburg, 12 (1938), 265-275.