COLLOQUIUM MATHEMATICUM

VOL. XV 1966 FASC. 2

ON FUNCTIONALLY UNIFORM SYMMETRICAL ALGEBRAS

BY

JERZY PŁONKA (WROCŁAW)

Introduction. In the present paper so-called functionally uniform symmetrical algebras are considered. The idea of treating such algebras has arisen in connection with a problem given by E. Marczewski which consists in the estimation of the number of independent elements in binary algebras (see [2]). In section 4 of the present paper we prove that a certain functionally uniform algebra is the only extremal algebra for those estimations in case of binary algebras with constants. The existence of only four functionally uniform symmetrical algebras has been proved in section 1, representation theorems and other properties are given in sections 2 and 3.

1. Definition and simplest properties. Let $\mathfrak{A} = (X; g)$ be an abstract algebra with one fundamental operation $g(x_1, \ldots, x_n)$ which is *symmetrical*, i.e. invariant under every permutation of the variables. We shall call $\mathfrak{A}$ a *functionally uniform symmetrical algebra*, or shortly FUS-algebra, if every algebraic operation has one of the following forms:

(a_1) $f(x_1, \ldots, x_m) = c$ with some $c \in X$,

(a_2) $f(x_1, \ldots, x_m) = x_i$ with some $i \in \{1, 2, \ldots, m\}$,

(a_3) $f(x_1, \ldots, x_m) = g(x_{i_1}, \ldots, x_{i_n})$ $(1 \leqslant i_j \leqslant m$ for $j = 1, 2, \ldots, n)$.

THEOREM 1. *If in an algebra $\mathfrak{A}$ there is a symmetrical n-ary operation g such that every algebraic $(2n-1)$-ary operation f has one of the forms (a_1), (a_2) or (a_3), then g satisfies one of the following conditions:*

(b_1) *g is unary and $g(g(x)) = g(x)$,*

(b_2) *g is unary and $g(g(x)) = x$,*

(b_3) *$g(g(x_1, \ldots, x_n), x_{n+1}, \ldots, x_{2n+1}) = c$ with some $c \in X$ (in the case $n = 1$ this shall be understood as $g(g(x)) = c$),*

(b_4) *$g(g(x_1, \ldots, x_n), x_{n+1}, \ldots, x_{2n-1}) = g(x_{n+1}, \ldots, x_{2n-1}, x_j)$ with some $j \in \{n+1, n+2, \ldots, 2n-1\}$.*

Proof. Note at first that g either is constant or depends on all its variables. In the first case it satisfies (b_3), so we may assume that g depends

on all variables. Consider first the case $n = 1$. From (a_1), (a_2), (a_3) it follows that $f(x) = g(g(x))$ is either trivial or constant or equal to $g(x)$, and so one of the equalities (b_1), (b_2), (b_3) holds.

Now let $n > 1$. The operation $g(g(x_1, \ldots, x_n), x_{n+1}, \ldots, x_{2n-1})$ depends evidently on all or none of the variables $x_1, \ldots, x_n$, because g is symmetrical. Similarly, it depends on all or none of the variables $x_{n+1}, \ldots, x_{2n-1}$ if $n \neq 2$. If follows that for $n \neq 2$ this operation cannot have the form (a_1) or (a_2), hence, it must have the form (a_3).

Now let $n = 2$. If $g(g(x_1, x_2), x_3) = x_3$, then

$$g(g(x_1, x_2), g(x_3, x_4)) = g(x_3, x_4),$$

$$g(g(x_3, x_4), g(x_1, x_2)) = g(x_1, x_2),$$

but the left-hand sides of the last equalities are equal, and it follows that g is constant, contrary to our assumption. Consequently, in the case $n = 2$ the operation $g(g(x_1, \ldots, x_n), x_{n+1}, \ldots, x_{2n-1})$ must have the form (a_3). Hence we have

(b_5) $g(g(x_1, \ldots, x_n), x_{n+1}, \ldots, x_{2n-1}) = g(x_{i_1}, \ldots, x_{i_n})$ with $1 \leqslant i_j \leqslant 2n-1$.

Suppose first that, for some j, $i_j \leqslant n$ and the operation on the left-hand side of (b_5) depends on x_{i_j}. Then every index $1, \ldots, n$ must occur among the $i_1, \ldots, i_n$ and so we have

$$g(g(x_1, \ldots, x_n), x_{n+1}, \ldots, x_{2n-1}) = g(x_1, \ldots, x_n),$$

whence

$$g(g(x_1, \ldots, x_n), g(y_1, \ldots, y_n), x_{n+2}, \ldots, x_{2n-1}) = g(x_1, \ldots, x_n)$$

and similarly

$$g(g(y_1, \ldots, y_n), g(x_1, \ldots, x_n), x_{n+2}, \ldots, x_{2n-1}) = g(y_1, \ldots, y_n),$$

but the left-hand sides of the last two equalities are equal in view of the symmetry of g, and so g must be constant, contrary to our assumption.

If the operation on the left-hand side of (b_5) is constant, then (b_3) is true. If not, then it must depend on some x_{i_j} with $i_j \geqslant n+1$. But now every index $n+1, \ldots, 2n-1$ must occur among the $i_1, \ldots, i_n$, and no index $\leqslant n$ can occur there as otherwise all variables $x_{i_1}, \ldots, x_{i_n}$ would be different, and so the operation in (b_5) would depend on all of them. But it cannot depend on a variable x_j with $j \leqslant n$ as we just proved. Consequently, exactly one of the indices $n+1, \ldots, 2n-1$ must occur twice. This proves (b_4) and so the theorem is proved.

2. Representation theorems. Now we prove theorems concerning the representation of FUS-algebras.

At first observe that if f is a retraction of a set X onto its subset Y, i.e. the identity on Y, then the algebra (X, f) is a FUS-algebra satisfying (b_1), and every FUS-algebra satisfying (b_1) can be obtained in this way. Similarly, if f is an arbitrary involution acting on a set X, i.e. $ff(x) = x$, then the algebra (X, f) is a FUS-algebra satisfying (b_2), and every FUS-algebra satisfying equality (b_2) can be obtained in this way.

It remains thus to prove representation theorems for FUS-algebras satisfying (b_3) or (b_4).

THEOREM II. *If in a FUS-algebra* (b_3) *holds, then this algebra has the form* $(A \cup C; g)$, *where* A *and* C *are disjoint sets,* C *contains a distinguished element* 0, *and there exists a function* f *defined on the set of all* n*-tuples of elements of* A *with values in* C (n *is the number of arguments of* g) *such that the operation* g *is defined as follows: if at least one of elements* $a_1, \ldots, a_n$ *belongs to* C, *then* $g(a_1, \ldots, a_n) = 0$, *and if not, then* $g(a_1, \ldots, a_n) = f(a_1, \ldots, a_n)$.

Proof. Suppose (X, g) is a FUS-algebra satisfying (b_3). At first we shall prove

(b_6) $g(c, x_2, \ldots, x_n) = c$.

Indeed, by (b_3),

$$g(c, x_2, \ldots, x_n) = g\big(g\big(g(x_1, \ldots, x_n), x_{n+1}, \ldots, x_{2n-1}\big), x_2, \ldots, x_n\big) = c.$$

Let now C be the set of all $a \in X$ such that $g(a, x_2, \ldots, x_n) = c$.

In view of (b_6), C is non-empty. It is easy to see that every element of the form $g(a_1, \ldots, a_n)$ belongs to C. Let A be the complement of C, and let $f(a_1, \ldots, a_n) = g(a_1, \ldots, a_n)$. From the symmetry of g and from (b_3) it follows that the algebra has the form described in the theorem.

THEOREM III. *If in a FUS-algebra* (b_4) *holds, then this algebra has the form* $(A \cup C; g)$, *where* A *and* C *are disjoint sets,* C *contains a distinguished element* 0 *and there exists a function* f *defined on the class of all subsets of* A *having at most* n *elements with values in* C *such that* $f(\emptyset) = 0$ *and* $g(a_1, \ldots, a_n) = f(\{a_1, \ldots, a_n\} \cap A)$.

At first we need some lemmas. We shall not repeat in them the assumption that the algebra is a FUS-algebra satisfying (b_4).

LEMMA 1. *If* $1 \leqslant i \leqslant n$, *then* $g(x_1, \ldots, x_{n-1}, x_i) = g(x_1, \ldots, x_{n-1}, x_j)$.

Proof. Let us assume that $i < j$. If $i > j$ only typographical changes are needed.

From (b_4) it follows

$$g\big(g(y_1, \ldots, y_n), x_1, \ldots, x_{n-1}\big) = g(x_1, \ldots, x_{n-1}, x_j),$$

whence

$$g(x_1, \ldots, x_{n-1}, x_j) = g\big(g(y_1, \ldots, y_n), x_1, \ldots, x_{n-1}\big)$$

$$= g\big(g(y_1, \ldots, y_n), x_1, \ldots, x_{i-1}, x_j, x_{i+1}, \ldots, x_{j-1}, x_i, x_{j+1}, \ldots, x_{n-1}\big)$$

$$= g(x_1, \ldots, x_{i-1}, x_j, x_{i+1}, \ldots, x_{j-1}, x_i, x_{j+1}, \ldots, x_{n-1}, x_i)$$

$$= g(x_1, \ldots, x_{n-1}, x_i).$$

By repeated application of Lemma 1 we get

LEMMA 2. *Every non-constant and non-trivial algebraic operation can be written in the form*

$$g(x_1, \ldots, x_k, x_{j_1}, \ldots, x_{j_{n-k}}),$$

where $1 \leqslant j_i \leqslant k \leqslant n$, *and for arbitrary* m_i $(1 \leqslant m_i \leqslant k)$ *we have*

$$g(x_1, \ldots, x_k, x_{j_1}, \ldots, x_{j_{n-k}}) = g(x_1, \ldots, x_k, x_{m_1}, \ldots, x_{m_{n-k}}).$$

LEMMA 3. *For arbitrary* $x_1^1, \ldots, x_n^n$ *the following equality holds with some fixed* c:

$$g\big(g(x_1^1, \ldots, x_n^1), \ldots, g(x_1^n, \ldots, x_n^n)\big) = c.$$

Proof. By (b_4) and Lemma 2 we have

$$g\big(g(x_1^1, \ldots, x_n^1), \ldots, g(x_1^n, \ldots, x_n^n)\big) = g\big(g(x_1^1, \ldots, x_n^1), \ldots, g(x_1^{i-1}, \ldots, x_n^{i-1}),$$

$$g(x_1^{i+1}, \ldots, x_n^{i+1}), \ldots, g(x_1^n, \ldots, x_n^n), g(x_1^k, \ldots, x_n^k)\big),$$

where $i = 1, 2, \ldots, n$ and $k \neq i$. Consequently, the operation on the left-hand side of the last equality does not depend on any variable. Hence it is a constant.

We shall say that an element a is *reducible* if for arbitrary $x_1, \ldots, x_{n-1}$

$$g(a, x_1, \ldots, x_{n-1}) = g(x_1, \ldots, x_{n-1}, x_{n-1})$$

holds.

LEMMA 4. *The constant* c *appearing in Lemma* 3 *is reducible.*

Proof. By Lemma 2, Lemma 3 and (b_4)

$$g(c, x_1, \ldots, x_{n-1}) = g\big(g\big(g(x_1^1, \ldots, x_n^1), \ldots, g(x_1^n, \ldots, x_n^n)\big), x_1, \ldots, x_{n-1}\big)$$

$$= g(x_1, \ldots, x_{n-1}, x_k)$$

with arbitrary $k \in (1, \ldots, n-1)$, q.e.d.

LEMMA 5. *If $a_1, \ldots, a_n$ are reducible, then $g(a_1, \ldots, a_n) = c$.*

Proof. $g(a_1, \ldots, a_n) = g(a_2, \ldots, a_n, a_2) = g\big(g(x_1^1, \ldots, x_n^1), a_2, \ldots, a_n\big)$. In this way we replaced a_1 by $g(x_1^1, \ldots, x_n^1)$. In the same way we can replace a_i by $g(x_1^i, \ldots, x_n^i)$ and the Lemma follows by Lemma 3.

Proceeding similarly we obtain the following

LEMMA 6. *If $a_1, \ldots, a_p$ are reducible and $b_1, \ldots, b_r$ are not reducible, then*

$$g(a_1, \ldots, a_p, b_1, \ldots, b_r, a_{i_1}, \ldots, a_{i_s}, b_{j_1}, \ldots, b_{j_t}) = g(b_1, \ldots, b_r, b_{k_1}, \ldots, b_{k_{n-r}})$$

where $p+r+s+t = n, 1 \leqslant i_w \leqslant p, 1 \leqslant j_w \leqslant r$, and the $k_w - s$ can be taken arbitrarily from the set $\{1, 2, \ldots, r\}$.

Proof of Theorem III. Let (X, g) be a FUS-algebra satisfying (b_4). Denote by C the set of all reducible elements of X, and let $A = X \setminus C$. The set C is not void because every element of the form $g(a_1, \ldots, a_n)$ is reducible by (b_4) and c is reducible by Lemma 4. If $R \subset A$ and R has at most n elements, say $a_1, \ldots, a_k$ $(k \leqslant n)$, then define $f(R) = g(a_1, \ldots, a_k, a_1, \ldots, a_l)$, and put $f(\emptyset) = c$. The Theorem is now a corollary of Lemmas 5 and 6.

3. Corollaries. The following results are easy consequences from the representation theorems.

(i) *A subset of a FUS-algebra is independent iff every of its subsets consisting of at most $2n$ elements is independent.*

This follows from the observation that every algebraic operation depends on at most n variables.

(ii) *A FUS-algebra (X, g) is free in the class determined by the equation satisfied by g iff*

(a) *in the case g satisfies (b_3) or (b_4), the function f is one-to-one and its range is $C \setminus \{c\}$,*

(b) *in the case g satisfies (b_1), every element in the image of the retraction is an image of exactly two elements,*

(c) *in the case g satisfies (b_2), the involution has no fixed points.*

Moreover, in all cases the set of free generators is unique.

LEMMA 7. *Let $\mathfrak{A}$ be a FUS-algebra satisfying (b_3) or (b_4). If for some $k < n$ an algebraic operation $h(x_1, \ldots, x_k)$ is equal to a constant d, then $d = c$ and every algebraic operation of not more than k variables is equal to c.*

Proof. $h(x_1, \ldots, x_k) = g(x_{i_1}, \ldots, x_{i_n})$. If (b_3) is satisfied, then put here $x_1 = g(x_1, \ldots, x_n)$ and use (b_3), and if (b_4) is satisfied then put $x_{i_j} = g(x_1^j, \ldots, x_n^j)$ for $j = 1, 2, \ldots, n$ and use Lemma 3.

(iii) *A FUS-algebra satisfying* (b_1) *has a basis iff either every element of the image of the retraction g is an image of exactly two elements of the algebra or g is the identity map.*

(iv) *A FUS-algebra satisfying* (b_2) *has a basis iff either the involution has no fixed points or is the identity map.*

(v) *A FUS-algebra satisfying* (b_3) *has a basis iff the function f maps the set of all n-tuples having at least $k+1$ different elements onto C, and is one-to-one on them.*

(vi) *A FUS-algebra satisfying* (b_4) *has a basis iff the function f maps the class of all subsets of A having at least $k+1$ elements onto C, and is one-to-one on them.*

In (iv) and (v) k is the number appearing in Lemma 7.

We shall say that *two FUS-algebras have the same type* (b_j) if both satisfy the same condition (b) with some $j = 1, 2, 3, 4$.

(vii) *The product of two FUS-algebras of the same type* (b_j) *is a* FUS*-algebra of the same type, and the set C of the product is the product of corresponding sets C of the factors. (In the cases $j = 1, 2$ we understand here by C the image of the algebra under g).*

(viii) *If D is a subset of a FUS-algebra, then the subalgebra generated by D has the form $D \cup D' \cup (c)$, where D' is the image of $D \cap A$ under f in the types* (b_3) *and* (b_4), *and D' is the image of D under g in the types* (b_1) *and* (b_2). *(In the last two cases there is no c.)*

(ix) *Every homomorphism of a FUS-algebra in a FUS-algebra of the same type maps c in c' and carries the image of f resp. g in the corresponding image.*

We prove this for the type (b_3). In other cases the reasoning is similar. Let h be a homomorphism. Then

$$h(c) = h\big(g\big(g(x_1, \ldots, x_n), x_{n+1}, \ldots, x_{2n-1}\big)\big)$$

$$= g\big(g\big(h(x_1), \ldots, h(x_n)\big), h(x_{n+1}), \ldots, h(x_{2n-1})\big) = c'.$$

If a is a reducible element of the algebra, then clearly the element $h(a)$ is also a reducible element of the corresponding algebra.

4. Number of independent elements. Let us denote by $\alpha(\mathfrak{A})$ the number of elements of the algebra $\mathfrak{A}$, and by $\iota(\mathfrak{A})$ the maximal cardinality of an independent [1] subset of $\mathfrak{A}$. In [2] was investigated the function $p(n, \boldsymbol{K}_c)$ defined as

$$\min\{\alpha(\mathfrak{A}) \colon \mathfrak{A} \in \boldsymbol{K}_c, \iota(\mathfrak{A}) = n\},$$

[1] in the sense of Marczewski [1].

where K_c is the class of binary algebras having constants with an operation depending on exactly two variables. It was proved that $p(n, K_c) = \lfloor n(n+1)/2 \rfloor + 1$ and the minimal value was obtained for an algebra with a fundamental operation $g(x, y) = xy$ subject to conditions: $(xy)z = c$, $xy = yx$, $xx = c$. It is clear that this is a FUS-algebra. Now we prove

THEOREM IV. *If* $\mathfrak{A} \in K_c$, $\iota(\mathfrak{A}) = n > 2$, *and* $a(\mathfrak{A}) = \lfloor n(n+1)/2 \rfloor + 1$, *then the binary operation* xy *in* $\mathfrak{A}$ *satisfies* $(xy)z = c$, $xy = yx$, $xx = c$.

Proof. Let I be the largest independent subset of $\mathfrak{A}$. Thus I has n elements. Let CI be the subalgebra of $\mathfrak{A}$ generated by I. It contains the constant c, all elements from I, and $\binom{n}{2}$ products of elements of I. Hence it must coincide with $\mathfrak{A}$. Consequently, every non-constant and non-trivial algebraic operation of at most n variables must satisfy $f(x_1, \ldots, \ldots, x_m) = x_i x_j$ with suitable i, j. Moreover, $xy = yx$ because otherwise CI would have more elements than $\mathfrak{A}$. Consequently, the assumptions of Theorem I are satisfied, whence $(xy)z = c$ or $(xy)z = zz$. The operation xx must be either trivial or constant as otherwise the algebra would have more elements. It cannot be trivial as then $(xy)z = z$, and thus $uv = (xy)(uv) = (uv)(xy) = xy$ for arbitrary x, y, u, v; a contradiction. Hence $xx = c$, and so $(xy)z = c$, and the Theorem is proved.

In the case $\iota(\mathfrak{A}) = 2$ this theorem fails to be true as the example of the group $C_2 \times C_2$ shows.

In the case $n > 3$ one obtains a stronger result, namely

THEOREM V. *If* $a(\mathfrak{A}) = \lfloor n(n+1)/2 \rfloor + 1$, $\iota(\mathfrak{A}) = n > 3$ *and there exists a binary algebraic operation* xy *depending on both variables, then there is a unique algebraic constant* c *in the algebra and, moreover,* $(xy)z = c$, $xy = yx$ *and* $xx = c$ *holds.*

Proof. If the algebra does not contain any constants, then from Theorems 3 and 4 of [2] follows that the algebra contains at least $\min(n^2, 2^n - 1)$ elements, and so more than $\lfloor n(n+1)/2 \rfloor + 1$. But if $\mathfrak{A}$ has constants then we can apply Theorem IV to get the desired result.

In the case $n = 3$ there is a unique counterexample: the algebra of non-empty subsets of $(0, 1, 2)$ with set-theoretical addition as the fundamental operation.

Let $\mathfrak{A}_0 = (X; c, \cdot)$ be the free algebra with n free generators in the class defined by the equations

$$x(yz) = c, \quad xy = yx, \quad xx = c.$$

From a result of Urbanik (see [3], Theorem 15.1) follows that every algebra satisfying the assumptions of Theorem IV or V may be written in the form $(Y; \cdot)$. It is to see that $(Y; \cdot)$ is isomorphic to $\mathfrak{A}_0$.

REFERENCES

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

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

[3] K. Urbanik, *On some numerical constants associated with abstract algebras*, Fundamenta Mathematicae (in print).

Reçu par la Rédaction le 6. 6. 1965