COLLOQUIUM MATHEMATICUM

VOL. XXV 1972 FASC. 1

ON THE NUMBER OF POLYNOMIALS OF A UNIVERSAL ALGEBRA IV

BY

J. PŁONKA (WROCŁAW)

Let $\mathfrak{A}$ be an algebra. By $p_n(\mathfrak{A})$ we denote the number of essentially n-ary polynomials in $\mathfrak{A}$ (i.e., polynomials depending on each variable) different from the trivial operation $e_1^{(1)}(x) = x$. We say (see [1]) that a sequence $a_0, a_1, \ldots$ of non-negative integers is *representable* if there exists an algebra $\mathfrak{A}$ such that $p_n(\mathfrak{A}) = a_n$ for $n = 0, 1, \ldots$ There are sequences non-representable, e.g., $0, 0, 1, 0, 0, \ldots$, because if in an algebra $\mathfrak{A}$ without constant algebraic operations there exists a binary symmetrical operation, then, by Theorem 1 in [4], $p_n(\mathfrak{A}) \geqslant 1$ for $n = 3, 4, \ldots$ If $a_0 > 0$, then the sequence is representable (see [1]). Thus the examination of representable sequences splits into two cases: $p_0 = 0, p_1 = 0$, and $p_0 = 0, p_1 > 0$. Concerning the first case some results can be found in [5]. In this paper we study the second case. In [1] it was proved that any sequence $0, a_1, a_2, \ldots$, in which $a_n > 0$ for $n \geqslant 1$, is representable.

Our result is: if the sequence $0, a_1, a_2, \ldots$, in which $a_m = 0$ for some odd m exceeding 2, is representable, then n divides a_n for each $n > 0$. Moreover, if $a_1 > 0$, then this divisibility gives necessary and sufficient condition for representability. For $n = 3$ this theorem was proved in [2] by using another methods. By the way we obtained Theorem 1 which seems to be interesting for itself and is a generalisation of Theorem 1 in [3]. If $f(x_1, \ldots, x_n)$ is an n-ary operation, we denote by $S(f)$ the group of symmetry of f, i.e., the group of permutations σ of variables of f which do not change the value of f:

$$\sigma \in S(f) \text{ iff } f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

We say that $S(f)$ is *movable* if for any index $i \in \{1, \ldots, n\}$ there exists $\sigma \in S(f)$ such that $\sigma(i) \neq i$. We denote $f^0(x) = x, f^{k+1}(x) = f(f^k(x), \ldots, f^k(x))$

LEMMA 1. *If in an algebra $\mathfrak{A}$, n does not divide p_n for some $n \geqslant 2$, then there exists in $\mathfrak{A}$ an essentially n-ary polynomial $f(x_1, \ldots, x_n)$ such that $S(f)$ is movable.*

Proof. Assume to the contrary, that for any essentially n-ary polynomial $g(x_1, \ldots, x_n)$, there exists a fixed variable, say x_1, such that every permutation moving x_1 from its place changes the value of g. Then putting x_i $(i = 1, \ldots, n)$ on the first place, we would get $n \cdot k$ different operations for any g, and thus k would divide $(n-1)!$, a contradiction.

LEMMA 2. *If $f(x_1, \ldots, x_n)$, where $n \geqslant 3$, is a polynomial in $\mathfrak{A}$ such that $S(f)$ is movable, and $g(x_1, \ldots, x_s)$ is a polynomial in $\mathfrak{A}$ such that for some $i \in \{1, \ldots, s\}$ the polynomial $g(x_1, \ldots, x_{i-1} f^k(x_i), x_{i+1}, \ldots, x_s)$ $(k \geqslant 1)$ is essentially s-ary, then either*

(a) *there exists in $\mathfrak{A}$ an essentially $(s+2)$-ary operation being of one of the forms:*

$$(1) \quad g\big(x_1, \ldots, x_{i-1}, f\big(f^{k-1}(x), f^{k-1}(y), f^{k-1}(z), \ldots, f^{k-1}(z)\big), x_{i+1}, \ldots, x_s\big),$$

$$(2) \quad g\big(x_1, \ldots, x_{i-1}, f\big(f^{k-1}(x), \ldots, f^{k-1}(x), f^{k-1}(y), f^{k-1}(z), \ldots, f^{k-1}(z)\big), x_{i+1}, \ldots, x_s\big),$$

or

(b) *there exists in $(\mathfrak{A})$ an essentially $(s+1)$-ary operation which is of the form*

$$(3) \quad g\big(x_1, \ldots, x_{i-1}, f\big(f^{k-1}(x), f^{k-1}(y), \ldots, f^{k-1}(y)\big), x_{i+1}, \ldots, x_s\big),$$

where x and y can be interchanged without changing its value of it.

Proof. Consider operations

$$g_r = g\big(x_1, \ldots, x_{i-1}, f\big(f^{k-1}(y), \ldots, f^{k-1}(y), f^{k-1}(x), f^{k-1}(y), \ldots, f^{k-1}(y)\big), x_{i+1}, \ldots, x_s\big),$$

where $f^{k-1}(x)$ stands in the r-th place in f. Each g_r depends on variables $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_s$ and on at least one of variables x, y, for otherwise, identifying x and y, we would get a contradiction.

Suppose first that no g_r is $(s+1)$-ary. Then each g_r depends only either on x or on y. If g_r depends on x and does not depend on y, then we can assume $r = 1$ and so we have

$$g_1 = g\big(x_1, \ldots, x_{i-1}, f\big(f^{k-1}(x), f^{k-1}(y), \ldots, f^{k-1}(y)\big), x_{i+1}, \ldots, x_s\big) = g\big(x_1, \ldots, x_{i-1}, f\big(f^{k-1}(x), \ldots, f^{k-1}(x)\big), x_{i+1} \ldots, x_s\big).$$

Since f is movable, there exists $r' \neq 1$ such that $g_{r'}$ has the same property. We can assume $r' = 2$. Then, as can be checked by putting $z = x$ or $z = y$, operation (1) is $(s+2)$-ary. If no g_r depends on x, consider operations

$$g^{(t)} = g\big(x_1, \ldots, x_{i-1}, f\big(\underbrace{f^{k-1}(x), \ldots, f^{k-1}(x)}_{t \text{ times}}, f^{k-1}(y), \ldots, f^{k-1}(y)\big), x_{i+1}, \ldots, x_s\big).$$

Observe that $g^{(1)}$ depends on y and $g^{(n-1)}$ depends on x. Thus there exists t_0 such that $g^{(t_0)}$ depends on y and $g^{(t_0+1)}$ depends on x. It is easy to show that operation (2) in which $f^{k-1}(y)$ appears, for some t_0, in the (t_0+1)-th place, depends on $s+2$ variables.

If g_r is $(s+1)$-ary, then we can assume $r=1$. But f is movable and therefore there exists r' such that $g_{r'}$ is also $(s+1)$-ary. We can assume $r'=2$. Consider operation of the form (1). If it depends on z, we are ready. If it is not, then

$$g\big(x_1,\dots,x_{i-1},f\big(f^{k-1}(x),f^{k-1}(x),f^{k-1}(z),\dots,f^{k-1}(z)\big),x_{i+1},\dots,x_s\big)$$
$$=g\big(x_1,\dots,x_{i-1}\cdot f\big(f^{k-1}(x),\dots,f^{k-1}(x)\big),x_{i+1},\dots,x_s\big).$$

If there exists $r\notin\{1,2\}$ such that g_r is $(s+1)$-ary, we can assume $r=3$. Then, by (4), it is easy to check that operation of the form (2), where $f^{k-1}(x)$ appears two times, is essentially $(s+2)$-ary. If no g_r $(r>2)$ is essentially $(s+1)$-ary, then x and y commute in (1), because f is movable. Thus we have (3).

LEMMA 3. *If $f(x_1,\dots,x_n)$, where $n\geqslant 3$, is a movable polynomial in $\mathfrak{A}$, $g(x_1,\dots,x_s)$ is a polynomial in $\mathfrak{A}$, and there exist two indices $i<j$ such that the operation*

$$g\big(x_1,\dots,x_{i-1},f^k(x_i),x_{i+1},\dots,x_{j-1},f^l(x_j),x_{j+1},\dots,x_s\big)$$

is essentially s-ary $(k,l\geqslant 1)$, then there exists in $\mathfrak{A}$ an essentially $(s+2)$-ary operation being of one of the forms (1) or (2) or of the form

$$(5)\quad g\big(x_1,\dots,x_{i-1},f\big(f^{k-1}(x),f^{k-1}(y),\dots,f^{k-1}(y)\big),x_{i+1},\dots,$$
$$x_{j-1},f\big(f^{l-1}(v),\dots,f^{l-1}(v),f^{l-1}(u),f^{l-1}(v),\dots,f^{l-1}(v)\big),x_{j+1},\dots,x_s\big).$$

Proof. First consider index i and forget about j. By lemma 2, we obtain either $(s+2)$-ary operation of the form (1), (2), or $(s+1)$-ary operation (3). Now in the same way consider index j. If considering i we get operation of the form (3) and considering j we get $(s+1)$-ary operation of the form

$$g\big(x_1,\dots,x_{i-1},f^k(x_i),x_{i+1},\dots,x_{j-1},f\big(f^{l-1}(y),\dots$$
$$\dots,f^{l-1}(y),f^{l-1}(x),f^{l-1}(y),\dots,f^{l-1}(y)\big),x_{j+1},\dots,x_s\big),$$

then an operation of the form (5) is essentially $(s+2)$-ary. Putting $x=y$ we get dependence on u and v. Putting $u=v$ dependence on x and y.

THEOREM 1. *If in an algebra $\mathfrak{A}$ without algebraic constants there exists an n-ary algebraic operation f, where $n\geqslant 2$, such that $S(f)$ is movable, then, for each $m=1,2,\dots$, there exists in $\mathfrak{A}$ an essentially $(2m+1)$-ary operation.*

Proof. If $n = 2$, then f is symmetrical and, by Theorem 1 in [4], there exist essentially j-ary operations for each $j = 3, 4, \ldots$. Suppose $n \geqslant 3$. We shall construct essentially $(2m+1)$-ary operation. Take for g the operation $e_1^{(1)}(x) = x$ and put $k = m$ in Lemma 2.

By lemma 2, either there exists in $\mathfrak{A}$ an essentially binary symmetrical operation of the form (3) (then we are ready as above), or there exists an essentially ternary operation being of one of the forms

$$f\big(f^{k-1}(x), f^{k-1}(y), f^{k-1}(z), f^{k-1}(z), \ldots, f^{k-1}(z)\big), \tag{6}$$

$$f\big(f^{k-1}(x), \ldots, f^{k-1}(x), f^{k-1}(y), f^{k-1}(z), \ldots, f^{k-1}(z)\big). \tag{7}$$

If $m = 1$, we are ready. If $m > 1$, we can use Lemma 2 or 3 by taking $k = l = m-1$.

THEOREM 2. *If in an algebra $\mathfrak{A}$ there is $p_0 = 0$ and $p_{2m+1} = 0$ for some $m \geqslant 1$, then n divides p_n for $n > 0$.*

Proof. Suppose $n \nmid p_n$ for some $n > 1$. By Lemma 1, there exists in $\mathfrak{A}$ an operation $f(x_1, \ldots, x_n)$ such that $S(f)$ is movable. By Theorem 1, $p_{2m+1} > 0$ for $m = 1, 2, \ldots$ a contradiction.

It was proved in Theorem 1 of [1] that if $a_0 = 0$, $a_1 \geqslant 1$, and n divides a_n for each n, then the sequence $a_0, a_1, \ldots$ is representable. Hence we have

COROLLARY. *A sequence $a_0, a_1, \ldots$, in which $a_0 = 0$, $a_1 \geqslant 1$, and $a_{2m_0+1} = 0$ for some $m_0 \geqslant 1$, is representable if and only if n divides a_n for each n.*

Remark. For idempotent algebras ($p_1 = 0$) this divisibility condition is only a necessary one. In fact, the sequence $0, 0, 4, 0, 0, \ldots$ is not representable, because $p_3(\mathfrak{A}) = 0$ implies $p_2(\mathfrak{A}) = 0$ or $p_2(\mathfrak{A}) = 2$ (see Urbanik [5]).

REFERENCES

[1] G. Grätzer, J. Płonka, A. Sekanina, *On the number of polynomials of a universal algebra I*, Colloquium Mathematicum 22 (1970), p. 1-7.

[2] G. Grätzer, J. Płonka, *On the number of polynomials of a universal algebra II*, ibidem 22 (1970), p. 13-19.

[3] J. Płonka, *On the number of polynomials of a universal algebra III*, ibidem 22 (1971), p. 177-180.

[4] — *On the number of independent elements in finite abstract algebras having a binary operation*, ibidem 14 (1966), p. 189-201.

[5] K. Urbanik, *On algebraic operations in idempotent algebras*, ibidem 13 (1965), p. 129-157.

Reçu par la Rédaction le 4. 1. 1971