COLLOQUIUM MATHEMATICUM

VOL. XXII 1970 FASC. 1

ON THE NUMBER OF POLYNOMIALS OF A UNIVERSAL ALGEBRA, II

BY

G. GRÄTZER AND J. PŁONKA (1) (WINNIPEG, CANADA)

1. Introduction. An n-ary polynomial of an algebra $\mathfrak{A}$ is *essentially n-ary* if it depends on all of its variables. Our main result (2) (Theorem 6) is that if an algebra $\mathfrak{A}$ has no constants and no essentially ternary polynomials, then the number of essentially n-ary polynomials is divisible by n.

This immediately yields a rather strong result on representability of sequences in the sense of [2]. Another application shows how our result extends a theorem of Wenzel [5].

The proof is based on finding variables with special properties. These are introduced in section 2. The case of 4-ary polynomials is discussed in section 3. The proof of the theorem is completed in section 4. The applications are given in section 5.

For the basic concepts and notations not defined in this paper the reader is referred to [1].

2. Distinguished and terminal variables. Let $p = p(x_0, \ldots, x_{n-1})$ be an n-ary polynomial over the algebra $\mathfrak{A}$. The *symmetry group of p*, denoted by $G(p)$, is the subgroup of the symmetric group $S(n)$ on n letters, consisting of all permutations a of $\{0, \ldots, n-1\}$ satisfying

$$p(a_0, \ldots, a_{n-1}) = p(a_{0a}, \ldots, a_{(n-1)a}) \ (= p^a(a_0, \ldots, a_{n-1})).$$

The variable x_i is a *distinguished variable* of p if $ia = i$ for all $a \in G(p)$.

The next result shows one method of proving that the number of essentially n-ary polynomials is divisible by n.

THEOREM 1. *If every essentially n-ary polynomial over $\mathfrak{A}$ has a distinguished variable, then the number of essentially n-ary polynomials is divisible by n.*

(1) This research of both authors was supported by the National Research Council of Canada.

(2) A weaker result was announced in the Notices of the American Mathematical Society 16 (1969), Number 4, p. 659.

Proof. For an essentially n-ary polynomial p set

$$Q(p) = \{p^{a} \mid a \in S(n)\}.$$

Obviously, the set of all essentially n-ary polynomials is a disjoint union of sets of the form $Q(p)$, hence it suffices to show that n divides $|Q(p)|$. Note that $|Q(p)|$ is the same as the index of $G(p)$ in $S(n)$. Let $S_i(n)$ denote the subgroup of $S(n)$ consisting of all $a \in S(n)$ with $ia = i$. Thus by assumption there exists an i with $G(p) \subseteq S_i(n)$. Hence the index of $G(p)$ in $S(n)$ equals the index of $G(p)$ in $S_i(n)$ multiplied by the index of $S_i(n)$ in $S(n)$, the latter being n. This completes the proof.

For $n = 2$ we shall use another trick:

THEOREM 2. *Let $\mathfrak{A}$ be an algebra without constants such that, for some $n \geqslant 2$, $\mathfrak{A}$ has no essentially n-ary polynomial. Then the number of essentially binary polynomials is divisible by two.*

Proof. If $p(x_0, x_1)$ is essentially binary, non-commutative, then $p(x_0, x_1) \neq p(x_1, x_0)$. Thus if the number of essentially binary polynomials is not divisible by two, then there exists an essentially binary commutative polynomial p. Since $\mathfrak{A}$ is assumed to have no constants, this implies [3] that

$$p\big(x_0, p(x_1, \ldots, p(x_{n-2}, x_{n-1}) \ldots)\big)$$

is essentially n-ary, contrary to assumption.

In order to apply Theorem 1 we have to find means of proving the existence of distinguished variables.

From now on we assume that the algebra $\mathfrak{A}$ has no constant and no essentially ternary polynomial.

Let $n > 3$, and let p be an n-ary polynomial over $\mathfrak{A}$. A variable x_i is *terminal* (3) in p if by equalizing the variables of p so that there are at most three left, the resulting polynomial depends only on x_i.

A pair of variables $\{x_i, x_j\}$, $i \neq j$, is a *terminal pair* in p if by equalizing the variables so that there are at most three left, the resulting polynomial depends exactly on x_i and x_j.

THEOREM 3. *A terminal variable is distinguished.*

Proof. Let x_i be terminal but not distinguished in p. Then there exists an $a \in G(p)$ with $ia \neq i$. Substitute, in p, $x_k = x_i$ for all $k \neq ia^{-1}$. Since $a \in G(p)$, we get

$$p(x_i, \ldots, x_i, \ldots, x_{ia^{-1}}, \ldots) = p(x_i, \ldots, x_{ia^{-1}}, \ldots, x_i, \ldots),$$

hence the left-hand side depends only on x_i, the right-hand side only on $x_{ia^{-1}}$, a contradiction since $\mathfrak{A}$ has no constants.

(3) This concept is used implicitly in [4].

THEOREM 4. *Both variables in a terminal pair are distinguished.*

Proof. Let $\{x_i, x_j\}$ be a terminal pair. If, for some $\alpha \in G(p)$, $i\alpha \notin \{i, j\}$, then we get a contradiction, similarly to the proof of Theorem 3. It remains to consider the case $i\alpha = j$ and $j\alpha = i$. By equalizing the rest of the variables we get a binary commutative polynomial. By the result quoted in the proof of Theorem 2 this would imply that there are essentially ternary polynomials, a contradiction.

3. 4-ary polynomials. In this section let $\mathfrak{A}$ be an algebra with no constants and no essentially ternary polynomials. We shall prove that every essentially 4-ary polynomial has a terminal variable or a terminal pair.

Let p be an essentially 4-ary polynomial. We distinguish three cases.

Case 1. There is a substitution $x_i = x_j$ $(i \neq j)$ such that p with $x_i = x_j$ depends only on a single x_k, $k \notin \{i, j\}$.

CLAIM. *x_k is a terminal variable.*

Proof. Let $i = 0$, $j = 1$, $k = 3$. Then

$$p(x_0, x_0, x_2, x_3) = g(x_3). \tag{1}$$

$p(x_0, x_1, x_1, x_3)$ cannot depend on x_0 or x_1, because if it depends on x_0 (and therefore not on x_1), then $p(x_0, x_0, x_0, x_3) = g(x_3)$ would depend on x_0. Thus

$$p(x_0, x_1, x_1, x_3) = g(x_3) \tag{2}$$

and, similarly,

$$p(x_0, x_1, x_0, x_3) = g(x_3). \tag{3}$$

$p(x_3, x_1, x_2, x_3)$ depends on x_3; thus it cannot depend both on x_1 and x_2. If it depends on x_1, then $p(x_3, x_1, x_1, x_3)$ depends on x_1, and so, by (2), $g(x_3)$ depends on x_1, a contradiction. Hence

$$p(x_3, x_1, x_2, x_3) = g(x_3). \tag{4}$$

Since the remaining two cases now follow trivially, this means that x_3 is a terminal variable.

Case 2. There is a substitution $x_i = x_j$ $(i \neq j)$ such that p with $x_i = x_j$ depends on both x_k, $k \notin \{i, j\}$.

CLAIM. *$\{x_k, x_m\}$ $(k, m \notin \{i, j\}$, $k \neq m)$ is a terminal pair.*

Proof. Let $i = 2$, $j = 3$, and so

$$p(x_0, x_1, x_2, x_2) = g_{23}(x_0, x_1), \tag{5}$$

where g_{23} is essentially binary.

Now we prove that $g_{12} = p(x_0, x_1, x_1, x_3)$ depends on x_0 and x_1 but not on x_3.

Putting $x_3 = x_1$ we get $g_{23}(x_0, x_1)$; hence g_{12} depends on x_0, and on exactly one of x_1 and x_3. Assume the latter:

$$(6) \qquad p(x_0, x_1, x_1, x_3) = g_{12}(x_0, x_3).$$

Now consider $h = p(x_0, x_1, x_2, x_0)$; substituting $x_1 = x_2$ into h, by (6) we get $g_{12}(x_0, x_0)$, hence h depends on x_0. We claim that h depends neither on x_1 nor on x_2; indeed, if h depends, say, on x_1, then (since $p_3 = 0$) h does not depend on x_2, hence $h(x_0, x_1, x_2) = h(x_0, x_1, x_1) = p(x_0, x_1, x_1, x_0) = g_{12}(x_0, x_0)$ by (6), contradicting the assumption. Thus

$$(7) \qquad p(x_0, x_1, x_2, x_0) = g_{03}(x_0);$$

in particular,

$$(8) \qquad p(x_0, x_1, x_0, x_0)$$

does not depend on x_1. However, substituting $x_2 = x_0$ into (5) we infer that (8) depends on x_1, a contradiction. Thus

$$(9) \qquad p(x_0, x_1, x_1, x_3) = g_{12}(x_0, x_1).$$

Similarly,

$$(10) \qquad p(x_0, x_1, x_0, x_3) = g_{02}(x_0, x_1), \qquad p(x_0, x_1, x_2, x_0) = g_{03}(x_0, x_1),$$

$$(11) \qquad p(x_0, x_1, x_1, x_3) = g_{12}(x_0, x_1), \qquad p(x_0, x_1, x_2, x_1) = g_{13}(x_0, x_1).$$

Finally, we consider $p(x_0, x_0, x_2, x_3)$. By (5) it depends on x_0. Suppose it depends on x_2 (and hence not on x_3). Then, by (5),

$$p(x_0, x_0, x_2, x_3) = p(x_0, x_0, x_2, x_2) = g_{23}(x_0, x_0),$$

hence it cannot depend on x_2. Similarly, $p(x_0, x_0, x_2, x_3)$ cannot depend on x_3. Thus

$$(12) \qquad p(x_0, x_0, x_2, x_3) = g(x_0).$$

Formulas (5) and (9)-(12) verify that $\{x_0, x_1\}$ is a terminal pair.

Negating the conditions of Cases 1 and 2 we get the final case:

Case 3. For all pairs i, j $(i \neq j)$, identifying x_i and x_j in p we get a polynomial depending on x_i.

CLAIM. *No polynomial satisfies this assumption.*

Proof. Let p satisfy the assumption of Case 3. Firstly we prove that p with $x_i = x_j$ cannot be unary. Again let $i = 0$, $j = 1$, and let

$$(13) \qquad p(x_0, x_0, x_2, x_3) = g(x_0).$$

If $p(x_0, x_1, x_2, x_2)$ is also unary, say $h(x_2)$, then

$$g(x_0) = p(x_0, x_0, x_2, x_2) = h(x_2),$$

contradicting that $\mathfrak{A}$ has no constants. Hence $p(x_0, x_1, x_2, x_2)$ depends on exactly one of x_0 and x_1, say on x_0, i.e.

$$p(x_0, x_1, x_2, x_2) = g(x_0, x_2). \tag{14}$$

Setting $x_2 = x_3$ in (13) and $x_0 = x_1$ in (14) we get that $g(x_0)$ depends on x_2, a contradiction.

Thus, for instance, $p(x_0, x_0, x_2, x_3)$ is binary, say

$$p(x_0, x_0, x_2, x_3) = g_{01}(x_0, x_2). \tag{15}$$

Then $p(x_0, x_1, x_0, x_3)$ cannot depend on x_3; indeed, if it does, that is, $p(x_0, x_1, x_0, x_3) = g_{02}(x_0, x_3)$, then $p(x_0, x_0, x_0, x_3) = g_{02}(x_0, x_3)$, contradicting (15) with $x_0 = x_2$. Thus

$$p(x_0, x_1, x_0, x_3) = g_{02}(x_0, x_1). \tag{16}$$

Finally, $p(x_0, x_1, x_2, x_0)$ cannot depend on x_2, because if $p(x_0, x_1, x_2, x_0) = g_{03}(x_0, x_2)$, then setting $x_3 = x_0$ in (16) we get

$$g_{02}(x_0, x_1) = p(x_0, x_1, x_0, x_0) = g_{03}(x_0, x_0),$$

a contradiction. Thus,

$$p(x_0, x_1, x_2, x_0) = g_{03}(x_0, x_1). \tag{17}$$

Then (15) and (17) yield

$$g_{01}(x_0, x_2) = p(x_0, x_0, x_2, x_0) = g_{03}(x_0, x_0);$$

this final contradiction completes the discussion.

4. The main result. The results of sections 2 and 3 combine to give the first step of an inductive argument:

THEOREM 5. *Let $\mathfrak{A}$ be an algebra with no constants and no ternary polynomials such that every 4-ary polynomial has a terminal variable or a terminal pair. Then the same is true of all essentially n-ary polynomials for $n > 4$.*

Proof. Let the statement be proved for all essentially m-ary polynomials for all $m < n$, where n is an integer, $n > 4$, and let p be an essentially n-ary polynomial. We distinguish three cases as in the discussion of section 3. Let p_{ij} denote p with the substitution $x_i = x_j$.

Case 1. There exist i, j $(i \neq j)$ such that p_{ij} has a terminal variable x_k, $k \notin \{i, j\}$.

CLAIM. *x_k is terminal in p.*

Proof. Let $i = 0, j = 1, k = 2$. To show that x_2 is terminal in p we have to consider all p_{qr}, $q \neq r$. Either (a) p_{qr} has a terminal variable x_a, or (b) p_{qr} has a terminal pair $\{x_a, x_b\}$. Let (a) hold and let q be p with

$x_0 = x_1$ and $x_q = x_r$. If $x_2 \neq x_a$ in q, then q has two terminal variables, a contradiction. If $x_2 = x_a$ in q but $a \neq 2$, then $\{0, 1\} \cap \{q, r\}$ is a singleton and $a \in \{0, 1\}$, e.g. $a = 0$, $q = 1$, $r = 2$. Then we set $x_3 = x_4 = \ldots = x_{n-1}$ in p; the resulting polynomial t has x_0 as a terminal variable if $x_1 = x_2$, and x_2 as a terminal variable if $x_0 = x_1$, clearly contradicting Case 1 of section 3. Hence $a = 2$.

Now if (b) holds for p_{qr}, and $x_a = x_b$ is not implied by $x_0 = x_1$ and $x_p = x_q$, then these substitutions yield a polynomial with a terminal variable and a terminal pair. However, if $x_a = x_b$ is implied by $x_0 = x_1$ and $x_p = x_q$, then (α) $\{0,1\} \cup \{p, q\}$ has 4 elements or (β) $\{0,1\} \cup \{p, q\}$ has 3 elements, including a and b. If (α) holds, then p with $x_0 = x_1$ and $x_p = x_q$ has x_2, x_a, and x_b as terminal variables but they are not all equal. If (β) holds, then by identifying all variables in p other than x_0, x_1, x_p, and x_q we get a 4-ary polynomial contradicting Case 1 of section 3.

Case 2. There exist i, j $(i \neq j)$ such that p_{ij} has a terminal pair x_k, x_l, $k, l \notin \{i, j\}$.

CLAIM. *$\{x_k, x_l\}$ is a terminal pair in p.*

Proof. Let $i = 0$, $j = 1$, $k = 2$, $l = 3$. To show that $\{x_2, x_3\}$ is a terminal pair in p, we have to consider all p_{qr}. Either p_{qr} has (a) a terminal variable x_a or (b) a terminal pair $\{x_a, x_b\}$. If (a) holds, then p with $x_0 = x_1$, $x_q = x_r$ has x_a as a terminal variable and $\{x_2, x_3\}$ as a terminal pair, which is a contradiction unless $\{q, r\} = \{2, 3\}$ and $a = 2$ $(a = 3)$, in which case we get that p_{23} has x_2 as a terminal variable, as required. If (b) holds for p_{qr} and $\{a, b\} = \{2, 3\}$, then we are done. If $\{a, b\} \neq \{2, 3\}$, then p with $x_0 = x_1, x_q = x_r$ has two terminal pairs, a contradiction, unless $x_a = x_2$ and $x_b = x_3$ (or the other way around) after the substitution. This is possible only if $\{0, 1\} \cup \{q, r\}$ has 3 elements and, say, it includes a and 2, and $b = 3$ (or a similar combination). In this case we set $x_3 = x_4 = \ldots = x_{n-1}$ in p and get a polynomial contradicting Case 2 of section 3.

Case 3. For every $i \neq j$ either x_i is the terminal variable for p_{ij} or p_{ij} has a terminal pair $\{x_i, x_k\}$, $k \neq i$, $k \neq j$.

CLAIM. *No polynomial satisfies this assumption.*

Proof. The assumption is that if $x_i = x_j$ is followed by other substitutions, the resulting polynomial will always depend on x_i. Substitute $x_3 = \ldots = x_{n-1}$ in p. The resulting polynomial q satisfies Case 3 of section 3, consequently, it cannot exist.

This completes the proof of Theorem 5.

Now we are ready to state and prove the main result.

THEOREM 6. *Let $\mathfrak{A}$ be an algebra without constants and with no essentially ternary polynomial. Then, for every $n \geqslant 2$, the number of essentially n-ary polynomials is divisible by n.*

Proof. For $n = 2$, this is Theorem 2; for $n = 3$ this holds vacuously. For $n = 4$ this follows by combining section 3 with Theorems 1, 3 and 4. For $n \geqslant 4$ the statement follows from Theorems 1, 3, 4 and 5.

5. Applications. For an algebra $\mathfrak{A}$ and $n \geqslant 2$ let $p_n(\mathfrak{A})$ denote the number of essentially n-ary polynomials; let $p_1(\mathfrak{A})$ denote the number of non-constant unary polynomials excepting $p(x) = x$, and $p_0(\mathfrak{A})$ the number of constant unary polynomials. Let us call a sequence $\langle p_0, p_1, \ldots, p_n, \ldots\rangle$ *representable* if, for some algebra $\mathfrak{A}$ and all $n \geqslant 0$, $p_n = p_n(\mathfrak{A})$. The following result was proved in [2]:

Any sequence $\langle 0, p_1, p_2, \ldots, p_n, \ldots\rangle$ is representable if $p_1 > 0$ and n divides p_n for $n \geqslant 2$.

Combining this with Theorem 6 we get

THEOREM 7. *Let $p_1 > 0$; the sequence $\langle 0, p_1, p_2, 0, p_4, \ldots\rangle$ is representable if and only if n divides p_n for all $n \geqslant 2$.*

Let K be an equational class of algebras, and let F_n denote the number of elements of the free algebra over K on n generators. Let $\mathfrak{A}$ be the free algebra over K on ω generators, $p_n = p_n(\mathfrak{A})$.

The following formula is evident: if $p_0(\mathfrak{A}) = 0$, then

$$F_n = p_n + nF_{n-1} - \binom{n}{n-2}F_{n-2} + \binom{n}{n-3}F_{n-3} - \ldots + (-1)^n nF_1.$$

Since n divides $\binom{n}{k}$ for $1 \leqslant k < n$, we conclude that p_n is divisible by n if and only if F_n is divisible by n. Thus Theorem 6 gives the following result:

THEOREM 8. *Let $\mathfrak{A}$ be a free algebra on n generators with $p_0(\mathfrak{A}) = p_3(\mathfrak{A}) = 0$. Then n divides the cardinality of $\mathfrak{A}$.*

Under the additional assumption $p_1(\mathfrak{A}) = p_2(\mathfrak{A}) = 0$, this is the result of Wenzel [5].

REFERENCES

[1] G. Grätzer, *Universal algebra*, The University Series in Higher Mathematics, Princeton, N. J. 1968.

[2] — J. Płonka and A. Sekanina, *On the number of polynomials of a universal algebra I*, this fascicle, p. 9-11.

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

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

[5] G. H. Wenzel, *Konstanten in endlichen, freien universellen Algebren*, Mathematische Zeitschrift 102 (1967), p. 205-215.

UNIVERSITY OF MANITOBA

Reçu par la Rédaction le 12. 9. 1969