

Pacific Journal of Mathematics

ON THE NUMBER OF POLYNOMIALS OF AN IDEMPOTENT ALGEBRA. I

GEORGE GRÄTZER AND J. PŁONKA

ON THE NUMBER OF POLYNOMIALS OF AN IDEMPOTENT ALGEBRA I

G. GRÄTZER AND J. PŁONKA

This paper deals with the number $p_n(\mathfrak{A})$ of essentially n -ary polynomials of an idempotent universal algebra \mathfrak{A} . Under the condition that there is a commutative binary polynomial \cdot it is proved that $p_{n+1}(\mathfrak{A}) \geq p_n(\mathfrak{A}) + (n - 1)$, provided $p_n(\mathfrak{A}) \neq 1$. If \cdot is also associative this inequality is improved to

$$p_{n+1}(\mathfrak{A}) \geq p_n(\mathfrak{A}) + 1 + \max \{p_n(\mathfrak{A}), n + 1\}.$$

A sequence $\mathfrak{p} = \langle p_0, p_1, \dots \rangle$ is called *representable* (see [6]) if for some algebra \mathfrak{A} , $p_n = p_n(\mathfrak{A})$ for all $n \geq 0$. The basic problem is the characterization of representable sequences. Earlier results on representability (see [5] and [6]) were of the type that sequences satisfying some very mild condition (e.g., $p_0 > 0$) are all representable, and so the p_i are independent.

In this paper we make a first attack on the idempotent case ($p_0 = p_1 = 0$, in other words, $f(x, \dots, x) = x$ for every operation f). We conjecture that for idempotent algebras the $p_n(\mathfrak{A})$ are *not independent*. In fact, we think that with one exception the sequence $\langle p_n(\mathfrak{A}) \rangle$ is *increasing* from some m . Our general conjecture is the following:

Conjecture. Let \mathfrak{A} be an idempotent algebra different from the idempotent reduct of a Boolean group.¹ Then there exists an integer m such that $1 < p_n(\mathfrak{A}) < \aleph_0$ implies that $p_n(\mathfrak{A}) < p_{n+1}(\mathfrak{A})$ for every $n > m$.

To verify this conjecture one should make use of K. Urbanik's [9] classification of idempotent algebras using the set

$$Z(\mathfrak{A}) = \{n \mid n \geq 2, p_n(\mathfrak{A}) = 0\}.$$

The structure of \mathfrak{A} is quite well determined by $Z(\mathfrak{A})$ except if $Z(\mathfrak{A}) = \emptyset$, or $Z(\mathfrak{A}) = \{2\}$. In this paper we take up part of the case $Z(\mathfrak{A}) = \emptyset$. If $Z(\mathfrak{A}) = \emptyset$, then $p_2(\mathfrak{A}) \neq 0$, hence there exist binary polynomials; we shall discuss the case when there exist commutative binary polynomials.

THEOREM 1. *Let \mathfrak{A} be an idempotent algebra having a commutative binary polynomial. Then $p_n(\mathfrak{A}) \neq 1$ implies that*

¹ Let $\langle G; + \rangle$ be an abelian group; it is called *Boolean* if $2x = 0$ for all $x \in G$. The algebra $\langle G; g \rangle$, where g is a ternary operation defined by $g(x, y, z) = x + y + z$ is called the *idempotent reduct* of $\langle G; + \rangle$.

$$(1) \quad p_{n+1}(\mathfrak{A}) \geq p_n(\mathfrak{A}) + (n - 1).$$

The commutative binary polynomial that is assumed to exist is either associative or nonassociative. Accordingly, the proof of Theorem 1 splits into two completely different cases. In the nonassociative case one observes that for $n > 2$ the assumption $p_n(\mathfrak{A}) \neq 1$ is superfluous (since $p_3(\mathfrak{A}) \geq 3$). In the associative case we can prove a result that is much sharper:

THEOREM 2. *Let \mathfrak{A} be an idempotent algebra having a commutative and associative binary polynomial. Then $p_n(\mathfrak{A}) \neq 1 (n \geq 2)$ implies that*

$$(2) \quad p_{n+1}(\mathfrak{A}) \geq p_n(\mathfrak{A}) + 1 + \max \{p_n(\mathfrak{A}), n + 1\}.$$

The example given in § 2 will show that the two inequalities making up (2) are sharp.

Many conclusion can be drawn from Theorems 1 and 2.

Let us call a sequence $\langle p_i \rangle$ *conditionally strictly increasing* if $1 < p_i < \aleph_0$ implies $p_i < p_{i+1}$.

COROLLARY 1. *Let \mathfrak{A} be an idempotent algebra having a commutative and associative binary polynomial. If the sequence*

$$\langle p_n(\mathfrak{A}), p_{n+1}(\mathfrak{A}), \dots \rangle$$

is not conditionally strictly increasing for any $n \geq 2$, then \mathfrak{A} is equivalent to a semilattice.

COROLLARY 2. *The only representable sequence $\langle 0, 0, p_2, p_3, \dots \rangle$ satisfying $p_2 = 1, p_3 \leq 2$ for which $\langle p_n, p_{n+1}, \dots \rangle$ is not conditionally strictly increasing for any $n \geq 2$ is $\langle 0, 0, 1, \dots, 1, \dots \rangle$.*

The last condition of Corollary 2 is satisfied if the sequence $\langle p_n \rangle$ is assumed to be bounded. Under this assumption the conclusion of Corollary 2 is the same as the conclusion of the Theorem in [4] (however, the other assumptions in [4] are weaker than those in Corollary 2).

COROLLARY 3. *Let \mathfrak{A} be a commutative idempotent groupoid (i.e., an algebra with a single binary operation). If \mathfrak{A} is not equivalent to a semilattice, then for $n \geq 3$*

$$(3) \quad p_n(\mathfrak{A}) \geq \frac{(n-1)(n-2)}{2} + 2.$$

Since \mathfrak{A} is not equivalent to a semilattice the binary polynomial

is not associative. Hence $p_3(\mathfrak{A}) \geq 3$. Thus by (1):

$$\begin{aligned} p_n(\mathfrak{A}) &\geq p_{n-1}(\mathfrak{A}) + (n-2) \geq \dots \geq (n-2) + \dots + 2 + 3 \\ &= \frac{(n-1)(n-2)}{2} + 2. \end{aligned}$$

A weaker result, namely $p_n(\mathfrak{A}) > n$ was proved by J. Dudek [1].

A stronger result, namely

$$p_n(\mathfrak{A}) \geq \frac{1}{3}(2^n - (-1)^n)$$

is proved in [3].

A rather unexpected application of Theorem 2 is given in [3].

For the notation and basic concepts used in this paper see [2].

In §2 we present some facts concerning binary operations. Constructions of $(n+1)$ -ary polynomials from n -ary ones are given in §3. The inequality $p_{n+1} \geq 2p_n + 1$ is proved in §4, while $p_{n+1} \geq p_n + n + 2$ is proved in §5, concluding the proof of Theorem 2. Finally, Theorem 1 is verified in §6.

2. Binary operations. Let us consider an algebra $\mathfrak{A} = \langle A; \cdot, \circ \rangle$ with two binary operations \cdot and \circ satisfying the following set of identities:

$$(4) \quad x \cdot x = x, x \cdot y = y \cdot x, x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

$$(5) \quad x \circ x = x, x \circ (y \circ z) = (x \circ y) \circ z, x \circ (y \circ z) = x \circ (z \circ y)$$

$$(6) \quad (x \cdot y) \circ z = (x \circ z) \cdot (y \circ z), x \circ (y \cdot z) = (x \circ y) \cdot (x \circ z)$$

$$(7) \quad (x \cdot y) \circ x = x \cdot y,$$

that is $\langle A; \cdot \rangle$ is a semilattice and \circ is a partition function in the sense of J. Płonka [8]. It follows from the identities (4) – (7) (and more directly from Theorem 1 of [8]) that for $n \geq 2$ this algebra has exactly $2^n - 1$ essentially n -ary polynomials. These can be described as follows: Let $\{x_{i_0}, \dots, x_{i_k}\}, \{x_{i_{k+1}}, \dots, x_{i_{n-1}}\}$ be a partitioning of $\{x_0, \dots, x_{n-1}\}$ into two nondisjoint sets; then

$$(8) \quad (x_{i_0} \cdot x_{i_1} \cdot \dots \cdot x_{i_k}) \circ (x_{i_{k+1}} \cdot \dots \cdot x_{i_{n-1}})$$

is an essentially n -ary polynomial, and every essentially n -ary polynomial excepting $x_0 \cdot \dots \cdot x_{n-1}$ has a unique representation in this form, yielding $p_n(\mathfrak{A}) = 2^n - 1$.

Since $2^{n+1} - 1 = 2(2^n - 1) + 1$, the inequality $p_{n+1} \geq 2p_n + 1$ cannot be improved. Also, for $n = 2$ we get $p_2 = 3$, $p_3 = 7$, that is $p_3 = p_2 + 2 + 2$. Hence $p_{n+1} \geq p_n + n + 2$ cannot be sharpened to $p_{n+1} \geq p_n +$

$n + k$ for any $k > 2$.

All polynomials of the form (8) can be proved distinct under rather mild conditions:

LEMMA 1. *Let $\langle A; \cdot \rangle$ be a semilattice and let \circ be an idempotent essentially binary operation which is noncommutative, and satisfies*

$$(9) \quad (x \cdot y) \circ z = x \cdot (y \circ z) .$$

Then all the polynomials given in (8) are distinct, essentially n -ary, and different from $x_0 \cdot \dots \cdot x_{n-1}$.

Proof. If (8) does not depend on x_{i_j} then by symmetry, (8) does not depend on any variable in the same group. By identifying the variables in the same group we get that $x \circ y$ is not essentially binary. The first group of variables can be distinguished from the second by the fact that by (9) they can be brought outside. This cannot be done by any variable in the second group because it would imply the commutativity of \circ . This also shows that (8) is distinct from $x_0 \cdot \dots \cdot x_{n-1}$, completing the proof of Lemma 1.

Another lemma we need deals with commutative binary operations.

LEMMA 2. *Let \cdot and $+$ be distinct idempotent binary commutative operations, and let \cdot be associative. Then the polynomials*

$$(10) \quad \begin{aligned} &(x + y) + z, (y + z) + x, (z + x) + y, (x + y) \cdot z, (y + z) \cdot x, \\ &(z + x) \cdot y, (x \cdot y) + z, (y \cdot z) + x, (z \cdot x) + y \end{aligned}$$

are all essentially ternary and at least seven of them are distinct. The polynomial $x \cdot y \cdot z$ cannot equal any one of these.

The proof is a straightforward combination of Lemmas 1–4 of [7], including the statements made in the proofs of the same.

3. Constructions of polynomials. In this section we deal with an idempotent algebra having a fixed binary commutative and associative polynomial \cdot ; for brevity, we sometimes write xy for $x \cdot y$. Let p be an n -ary polynomial. We define $n + 1$ constructions: M_0, \dots, M_{n-1} and S :

$$(11) \quad pM_i = p(x_0, \dots, x_{i-1}, x_i \cdot x_n, \dots, x_{n-1})$$

$$(12) \quad pS = p \cdot x_n .$$

Let P_n denote the set of all essentially n -ary polynomials.

The next six lemmas describe the behaviour of the M_i and of S .

LEMMA 3. M_i is a one-to-one map of P_n into P_{n+1} .

Proof. We prove the statement for $i = 0$. Let $p \in P_n$. Then $pM_0 = p(x_0x_n, x_1, \dots, x_{n-1}) = q$. Since the substitution $x_0 = x_n$ in q yields p we get immediately that (i) M_0 is one-to-one; (ii) pM_0 depends on x_1, \dots, x_{n-1} , and on at least one of x_0 and x_n . Since x_0 and x_n are symmetric in q , q depends on both, completing the proof.

LEMMA 4. S is a one-to-one map of P_n into P_{n+1} .

Proof. Let $p \in P_n$. Substituting $x_0 = \dots = x_{n-1}$ in $pS = px_n$ we get x_0x_n depending on x_0 and x_n ; thus px_n depends on x_n . If px_n does not depend on x_i ($0 \leq i < n$), then $p(x_0, \dots, x_{n-1}) \cdot p(y_0, \dots, y_{n-1})$ depends neither on x_i nor on y_i by the commutativity of \cdot , contradicting the fact that after the substitution $x_j = y_j$, $0 \leq j < n$, the polynomial depends on x_i . Now let $p, q \in P_n$, $pS = qS$, that is $px_n = qx_n$. Substituting $x_n = p$, then $x_n = q$ we get

$$p = p \cdot p = q \cdot p = p \cdot q = q \cdot q = q ,$$

completing the proof.

REMARK. Note that Lemmas 3 and 4 do not use the associativity of \cdot . These lemmas are applied in these more general forms in [3].

LEMMA 5. Let $i \neq j$, $p, q \in P_n$. Then $pM_i = qM_j$ implies $p = q$.

Proof. To simplify the notation let $i = 0, j = 1$. Then

$$(13) \quad p(x_0x_n, x_1, \dots, x_{n-1}) = q(x_0, x_1x_n, \dots, x_{n-1}) .$$

Compute:

$$p(x_0y_0, x_1y_1, x_2, \dots, x_{n-1}) = q(x_0, x_1y_1y_0, \dots) = p(x_0x_1, y_0y_1, \dots) .$$

Hence

$$(14) \quad p(x_0, x_1, \dots) = p(x_0x_1, x_0x_1, \dots) .$$

Similarly,

$$(15) \quad q(x_0, x_1, \dots) = q(x_0x_1, x_0x_1, \dots) .$$

Substituting x_0, x_1 and x_n by x_0x_1 (13) yields

$$(16) \quad \begin{aligned} p(x_0x_1, x_0x_1, \dots) &= p(x_0x_1 \cdot x_0x_1, x_0x_1, \dots) \\ &= q(x_0x_1, x_0x_1 \cdot x_0x_1, \dots) = q(x_0x_1, x_0x_1, \dots) . \end{aligned}$$

(14)–(16) give $p = q$, as required.

LEMMA 6. *Let $p, q \in P_n$. Then $pM_i = qS$ implies $p = q$.*

Proof. To simplify the notation let $i = 0$. Then

$$(17) \quad p(x_0x_n, x_1, \dots, x_{n-1}) = q(x_0, \dots, x_{n-1})x_n.$$

Therefore,

$$(18) \quad \begin{aligned} q(x_0y, x_1, \dots)x_n &= p(x_0x_ny, x_1, \dots) = q(x_0, \dots)x_ny \\ &= q(y, \dots)x_0x_n = q(x_0x_n, \dots)y. \end{aligned}$$

Now compute (applying (18) in every step):

$$\begin{aligned} qM_0 &= q(x_0x_n, x_1, \dots) = q(x_0x_n, \dots) \cdot q(x_0x_n, \dots) \\ &= q(x_0x_n, \dots) \cdot q(x_0x_n, \dots)x_0 = q(x_0x_n \cdot q(x_0x_n, \dots), \dots)x_0 \\ &= q(x_0x_n \cdot q(x_0, \dots), \dots)x_0 = q(x_0, \dots) \cdot q(x_0, \dots) \cdot x_0x_n \\ &= q(x_0, \dots)x_n = qS. \end{aligned}$$

Hence

$$pM_0 = qS = qM_0,$$

and so by Lemma 5 we conclude that $p = q$.

LEMMA 7. *Let $p, q \in P_n$, and $i \neq j$. Then $pM_i = pM_j$ if and only if*

$$(19) \quad \begin{aligned} &p(x_0, \dots, x_i, \dots, x_j, \dots, x_{n-1}) \\ &= p(x_0, \dots, x_ix_j, \dots, x_ix_j, \dots, x_{n-1}). \end{aligned}$$

Proof. Let $i = 0, j = 1$, and assume (19), that is,

$$(20) \quad p = p(x_0x_1, x_0x_1, x_2, \dots, x_{n-1}).$$

Then

$$\begin{aligned} pM_0 &= p(x_0x_n, x_1, \dots) = {}^{(20)}p(x_0x_nx_1, x_0x_nx_1, \dots) \\ &= {}^{(20)}p(x_0, x_1x_n, \dots) = pM_1. \end{aligned}$$

Conversely, if $pM_0 = pM_1$, then

$$(21) \quad p(x_0x_n, x_1, \dots) = p(x_0, x_1x_n, \dots),$$

and so

$$\begin{aligned} p(x_0, x_1, \dots) &= p(x_0x_0, x_1, \dots) = {}^{(20)}p(x_0, x_0x_1, \dots) \\ &= p(x_0, (x_0x_1)x_1, \dots) = p(x_0x_1, x_0x_1, \dots), \end{aligned}$$

completing the proof.

Finally, we introduce some notations that will be useful in the sequel, and using these we characterize semilattice polynomials.

For $p \in P_n$ let $G(p)$ denote the group of all permutations α of

$\{0, \dots, n-1\}$ satisfying

$$(22) \quad p(x_0, \dots, x_{n-1}) = p(x_{0\alpha}, \dots, x_{(n-1)\alpha}) .$$

$G(p)$ is the *symmetry group* of p , and it is a subgroup of $S(n)$, the symmetric group on n letters. Then

LEMMA 8. *The index of $G(p)$ in $S(n)$ is the same as the number of polynomials arising from p by permuting the variables.*

Proof is obvious.

For $\alpha \in S(n)$, $p \in P_n$ define $p^\alpha \in P_n$ by

$$p^\alpha(x_0, \dots, x_{n-1}) = p(x_{0\alpha}, \dots, x_{(n-1)\alpha}) .$$

Note that $\alpha \in G(p)$ if and only if $p = p^\alpha$.

Let $P_{n+1}(i)$ denote the set of all $(n+1)$ -ary polynomials p which can be represented in the form

$$(23) \quad p = q(x_0, \dots, x_{i-1}, x_{i+1}, \dots, x_n)x_i$$

for some $q \in P_n$. It follows from Lemma 4 that $P_{n+1}(i) \subseteq P_{n+1}$, and that q is uniquely determined by p . If $p \in P_{n+1}(i)$ the variable x_i is said to *split* in p .

LEMMA 9. *If x_i splits in $p \in P_{n+1}$, and $\alpha \in G(p)$, then $x_{i\alpha}$ also splits in p .*

Proof. Obvious from (22) and (23).

LEMMA 10. *Let $p \in P_n$. Then $p = x_0 \cdot \dots \cdot x_{n-1}$ if and only if all x_i split in p .*

Proof. It is obvious that if $p = x_0 \cdot \dots \cdot x_{n-1}$, then all x_i split in p . Conversely, assume that all x_i split in p . Then, for some $q \in P_{n-1}$, $q(x_0, \dots, x_{i-1}, x_{i+1}, \dots, x_{n-1})x_i = p$, and so

$$(24) \quad \begin{aligned} p(x_0, \dots, x_i y_i, \dots, x_{n-1}) &= q(x_0, \dots, x_{i-1}, x_{i+1}, \dots, x_{n-1})x_i y_i \\ &= p(x_0, \dots, x_i, \dots, x_{n-1})y_i . \end{aligned}$$

Now compute using (24):

$$(25) \quad \begin{aligned} p(x_0 y_0, \dots, x_i y_i, \dots, x_{n-1} y_{n-1}) &= p(x_0, \dots, x_{n-1})y_0 \cdot \dots \cdot y_{n-1} \\ &= p(y_0, \dots, y_{n-1})x_0 \cdot \dots \cdot x_{n-1} . \end{aligned}$$

Setting $y_0 = \dots = y_{n-1} = y$ we get

$$(26) \quad p(x_0, \dots, x_{n-1})y = y \cdot x_0 \cdot \dots \cdot x_{n-1} .$$

And so

$$\begin{aligned}
 p(x_0, \dots, x_{n-1}) &= p(x_0, \dots, x_{n-1}) \cdot p(x_0, \dots, x_{n-1}) \\
 &= {}^{(26)} p(x_0, \dots, x_{n-1}) \cdot x_0 \cdot \dots \cdot x_{n-1} \\
 &= x_0 \cdot \dots \cdot x_{n-1} \cdot x_0 \cdot \dots \cdot x_{n-1} \\
 &= x_0 \cdot \dots \cdot x_{n-1} ,
 \end{aligned}$$

which was to be proved.

4. The inequality $p_{n+1} \geq 2p_n + 1$. In this and the next section let \mathfrak{A} be an algebra satisfying the conditions of Theorem 2, and let n be a fixed integer with $p_n(\mathfrak{A}) \neq 1$. Now we proceed to proving the inequality given in the title of the section.

For $p \in P_n$ let $R(p)$ denote the set of all polynomials of the form pM_i , or pS . By Lemmas 3 and 4, $R(p) \subseteq P_{n+1}$. If $p = x_0 \cdot \dots \cdot x_{n-1}$, then $|R(p)| = 1$, in fact, $R(p) = \{x_0 \cdot \dots \cdot x_{n-1} \cdot x_n\}$.

LEMMA 11. *If $p \neq x_0 \cdot \dots \cdot x_{n-1}$, then $|R(p)| \geq 2$.*

Proof. Let $|R(p)| = 1$. Then $pM_0 = pM_1 = \dots = pM_{n-1}$. Thus by Lemma 7 any pair of variables can be replaced by their products. Applying this a number of times we get

$$p = p(x_0 \cdot \dots \cdot x_{n-1}, \dots, x_0 \cdot \dots \cdot x_{n-1}) = x_0 \cdot \dots \cdot x_{n-1} ,$$

as claimed.

LEMMA 12. *Let $p, q \in P_n, p \neq q$. Then $R(p)$ and $R(q)$ are disjoint.*

Proof. By Lemmas 3, 4, 5, and 6.

By Lemmas 11 and 12,

$$(27) \quad p_{n+1} \geq |\bigcup (R(p) \mid p \in P_n)| \geq 2p_n - 1 .$$

LEMMA 13. *If $p_{n+1} < 2p_n + 1$, then $|R(p)| = 2$ for all $p \in P_n, p \neq x_0 \cdot \dots \cdot x_{n-1}$.*

Proof. It follows from (27) that $p_{n+1} = 2p_n$ or $p_{n+1} = 2p_n - 1$, and so $|R(p)| = 2$ for all $p \in P_n, p \neq x_0 \cdot \dots \cdot x_{n-1}$, with at most one exception. Let p be this exception; then $|R(p)| = 3$.

Partition $\{0, \dots, n-1\}$ into (at most) three classes, X_0, X_1, X_2 as follows:

$i, j \in X_a$ for some a , if $pM_i = pM_j$; furthermore, if $i \in X_2$, then $pM_i = pS$.

Since $|R(p)| = 3$, $|X_0| \neq 0$, $|X_1| \neq 0$, but X_2 could be empty. Note that by Lemma 7 $i, j \in X_a$, if and only if x_i and x_j can be substituted by $x_i x_j$; hence if $i \in X_a$, $j \in X_b$, $a \neq b$, then this cannot hold for x_i and x_j .

Now we distinguish some cases:

Case 1. For some a $|X_a| \geq 2$. Then choose $i, j \in X_a$, $i \neq j$, $k \in X_b$, $a \neq b$. To simplify the computation let $0, 1 \in X_a$, $2 \in X_b$. Let τ be the transposition $(0, 2)$. We claim that $p \neq p^\tau$. Indeed, if $p = p^\tau$, then

$$\begin{aligned} p(x_0, x_1, x_2, \dots) &= p(x_0 x_1, x_0 x_1, x_2, \dots) \\ &= p(x_2, x_0 x_1, x_0 x_1, \dots) \\ &= p(x_0 x_1 x_2, x_0 x_1 x_2, x_0 x_1, \dots) \\ &= p(x_0 x_1, x_0 x_1 x_2, x_0 x_1 x_2, \dots) \\ &= p(x_0 x_1 x_2, x_0 x_1 x_2, x_0 x_1 x_2, x_3, \dots). \end{aligned}$$

Similarly,

$$p(x_0 x_2, x_1, x_0 x_2, \dots) = p(x_0 x_1 x_2, x_0 x_1 x_2, x_0 x_1 x_2, \dots),$$

and so $p(x_0, x_1, x_2, \dots) = p(x_0 x_2, x_1, x_0 x_2, \dots)$, contradicting $0 \in X_a, 2 \in X_b$, $a \neq b$.

Thus $p \neq p^\tau$. Since $|R(p)| = |R(p^\tau)|$, we get a contradiction with the uniqueness of p .

Case 2. $|X_a| \leq 1$ for $a = 0, 1, 2$, and $X_2 \neq \emptyset$. Since $|X_2| = n$ is impossible, let $|X_0| \neq 0$, and take $i \in X_0$, $j \in X_2$, $\tau = (i, j)$. Then $p = p^\tau$ would imply $pM_i = pS$; since $pM_j = pS$, we obtain $pM_i = pM_j$, contradicting the definition of X_2 , and $i \notin X_2$. Hence $p \neq p^\tau$, $|R(p^\tau)| = |R(p)| = 3$, a contradiction.

Case 3. $|X_0| = |X_1| = 1$, and $X_2 = \emptyset$. Thus in this case $n = 2$, and pM_0, pM_1, pS are all distinct. Take $\tau = (0, 1)$. If $p \neq p^\tau$, then $|R(p)| = |R(p^\tau)| = 3$, a contradiction. Hence, $p(x_0, x_1) = p(x_1, x_0)$. Let us denote $p(x_0, x_1)$ by $x_0 + x_1$. Then \cdot and $+$ satisfy the requirements of Lemma 2. Since $p_3 \leq 2p_2$, all essentially ternary with at most one exception are accounted for by $\bigcup (R(t) | t \in P_2)$. But the seven polynomials listed in (10) can belong to no $R(t)$ excepting $R(+)$. (The verification of this statement is tedious but straightforward.) Hence either $|R(+)| > 3$, or there are at least five essentially ternary polynomials outside of $\bigcup (R(t) | t \in P_2)$, contradicting the assumptions.

Cases 1–3 exhaust all possibilities, thus completing the proof of Lemma 13.

LEMMA 14. If $|R(p)| \leq 2$ for all $p \in P_n$, then all $p \in P_n$, $p \neq x_0 \cdot \dots$

$\cdot x_{n-1}$, have a unique representation in the form (8), where \circ is an essentially binary noncommutative polynomial satisfying (9); this polynomial \circ is uniquely determined by p .

Proof. Let $p \in P_n$, $p \neq x_0 \cdot \dots \cdot x_{n-1}$, and so $|R(p)| = 2$. Thus $\{0, \dots, n-1\}$ splits into two nonvoid sets X_0, X_1 such that for $i, j \in X_0$, $pM_i = pM_j$, and for $i \in X_1$, $pM_i = pS$. Thus by Lemma 7, for $i \in X_0$, x_i can be replaced by the product of all $x_j, j \in X_0$, for $i \in X_1$, x_i can be replaced by the product of all $x_j, j \in X_1$, and all these variables split in px_n . Define \circ by

$$x \circ y = p(z_0, \dots, z_{n-1}),$$

where $z_i = x$ for $i \in X_1$, $z_i = y$ for $i \in X_0$. Setting $X_1 = \{i_0, \dots, i_k\}$, (8) gives p . The uniqueness of \circ , and (9) follow from the fact that the $x_i, i \in X_0$ do not split, while the $x_i, i \in X_1$ do in px_n .

Now we are ready to complete the proof of the inequality. If $p_{n+1} \geq 2p_n + 1$ does not hold, then $p_{n+1} \leq 2p_n$, hence by Lemma 13, $|R(p)| \leq 2$ for all $p \in P_n$. By Lemma 14, (8) gives a unique representation for every $p \in P_n$, $p \neq x_0 \cdot \dots \cdot x_{n-1}$, and Lemma 1 stated that every such polynomial is essentially n -ary. Let k denote the number of essentially binary polynomials satisfying the requirements of Lemma 1. Then it follows from what has been stated above that

$$p_n = k(2^n - 2) + 1.$$

Again applying Lemma 1, we obtain the inequality

$$p_{n+1} \geq k(2^{n+1} - 2) + 1.$$

Hence

$$k(2^{n+1} - 2) + 1 \leq p_{n+1} \leq 2p_n = 2k(2^n - 2) + 2,$$

yielding $2k \leq 1$, that is $k = 0$. Therefore $p_1 = 1$, contrary to assumption. This completes the proof of the inequality.

5. The inequality $p_{n+1} \geq p_n + n + 2$. Recall that $P_{n+1}(i)$ is the set of all polynomials with representation (23). By Lemma 4, $|P_{n+1}(i)| = p_n$. By Lemma 10, $\bigcap (P_{n+1}(i) \mid 0 \leq i \leq n) = \{x_0 \cdot \dots \cdot x_n\}$, hence we can choose

$$p(x_0, \dots, x_{n-1})x_n \in P_{n+1}(n) - P_{n+1}(n-1),$$

that is, $p \in P_n$ can be chosen such that x_{n-1} does not split in px_n . Define:

$$(28) \quad q = p(x_0, \dots, x_{n-1}x_n).$$

LEMMA 15. *Neither x_{n-1} nor x_n splits in q .*

Proof. x_{n-1} and x_n are symmetric in q , therefore it suffices to prove that x_n does not split in q . Let us assume that x_n splits in q , that is

$$(29) \quad q = r(x_0, \dots, x_{n-1})x_n.$$

Now substitute $x_n = x_{n-1}$ in (28) and (29); we obtain

$$(30) \quad p(x_0, \dots, x_{n-1}) = r(x_0, \dots, x_{n-1})x_{n-1}.$$

Substituting $x_{n-1}x_n$ for x_{n-1} , and comparing the result with (28) and (29) we obtain

$$(31) \quad r(x_0, \dots, x_{n-1}x_n)x_{n-1}x_n = r(x_0, \dots, x_{n-1})x_n.$$

Thus

$$p(x_0, \dots, x_{n-1})x_n = {}^{(30)}r(x_0, \dots, x_{n-1})x_{n-1}x_n = {}^{(31)}r(x_0, \dots, x_{n-1}x_n)x_{n-1}x_n.$$

This formula shows that px_n is symmetric in x_{n-1} and x_n , contradicting the assumption that x_{n-1} does not split in px_n .

Now we start proving the inequality. Let s denote the number of variables that split in q .

Case 1. $s \geq 2$. Let Q denote the set of all polynomials arising from q by permuting x_0, \dots, x_{n-1} . Note that $P_{n+1}(n) \cap Q = \emptyset$. Of the $n!$ permutations (by Lemma 9) at most $(n-s)! \cdot s!$ belong to $G(q)$, hence by Lemma 8,

$$|Q| \geq \frac{n!}{(n-s)! \cdot s!} = \binom{n}{s} \geq \binom{n}{2} \geq n+2, \quad \text{for } n \geq 4, \text{ and } s < n-1.$$

Thus, if $n \geq 4$, and $s < n-1$, then

$$|P_{n+1}| \geq |P_{n+1}(n) \cup Q| \geq |P_{n+1}(n)| + |Q| \geq P_n + n + 2.$$

Let $n = 3$; $s \geq 2$, hence $s = 2$ ($s = 3$ implies that $p = x_0 \cdot x_1 \cdot x_2$). Thus x_0 and x_1 split in $q(x_0, x_1, x_2, x_3) = p(x_0, x_1, x_2x_3)$, and so $q = p(x_0x_1, x_0x_1, x_2x_3)$. Set $x \circ y = p(x, x, y)$. Then \circ satisfies (9) and so (8) will produce seven essentially 4-ary polynomials in which x_3 does not split. Thus $p_4 \geq p_3 + 7 \geq p_3 + 3 + 2$. Finally, if $n \geq 4$, and $s = n-1$, then as in the previous case we set $x \circ y = p(x, \dots, x, y)$ and apply (8) to get $p_{n+1} \geq p_n + 2^{n-1} \geq p_n + n + 2$.

Case 2. $s = 1$. Let x_0 be the variable that splits in q . Let Q

be defined as in Case 1. Since by Lemma 9 one variable (the one that splits) has to be kept fixed by any $\alpha \in G(q)$ we get that at most $(n-1)!$ permutations of $\{0, \dots, n-1\}$ belong to $G(q)$, and therefore we get at least n polynomials from q by permuting x_0, \dots, x_{n-1} . We get exactly n , if every permutation not moving 0 belongs to $G(q)$. Thus if we get exactly n , all transpositions $(i, n) \in G(p)$, $i \neq 0$. But then

$$\begin{aligned}
 & q(x_0, x_1, \dots, x_n) \\
 &= p(x_0, x_1, \dots, x_{n-1}x_n) \\
 (32) \quad &= p(x_0, x_{n-1}x_n, \dots, x_1x_{n-1}x_n) \\
 &= p(x_0, x_1x_{n-1}x_n, \dots, x_1x_{n-1}x_n) = \dots \\
 &= p(x_0, x_1x_2 \dots x_n, x_1x_2 \dots x_n, \dots, x_1x_2 \dots x_n) .
 \end{aligned}$$

Also, since x_0 splits in q :

$$(33) \quad q(x_0, \dots, x_n) = r(x_1, \dots, x_n) \cdot x_0 .$$

From (32) and (33) we obtain,

$$\begin{aligned}
 q(x_0, \dots, x_n) &= r(x_1 \cdot \dots \cdot x_n, \dots, x_1 \cdot \dots \cdot x_n) \cdot x_0 \\
 &= x_0 \cdot x_1 \cdot \dots \cdot x_n .
 \end{aligned}$$

Thus $p = x_0 \cdot \dots \cdot x_{n-1}$, contrary to assumption. Thus we cannot get exactly n , hence we get at least $2n$, and so

$$p_{n+1} \geq p_n + 2n \geq p_n + n + 2 ,$$

because $n \geq 2$.

Case 3. Cases 1 and 2 do not apply to any

$$px_n \in P_{n+1}(n) - P_{n+1}(n-1) .$$

Firstly we claim that $p_{n-1} = 1$. Indeed, if $p_{n-1} \neq 1$, then let r be an essentially $(n-1)$ -ary polynomial different from $x_0 \cdot \dots \cdot x_{n-2}$. Then some x_i , say x_0 does not split in $r \cdot x_{n-1} \cdot x_n$, hence by permuting the variables we get a $px_n \in P_{n+1}(n) - P_{n+1}(n-1)$ such that some x_i splits in $p(x_0, \dots, x_{n-1}x_n)$.

Now choose an arbitrary $px_n \in P_{n+1}(n) - P_{n+1}(n-1)$ and take $q = p(x_0, \dots, x_{n-1}x_n)$. Note that in q the pair $\{x_{n-1}, x_n\}$ is the only one which can be substituted by their product, because if $\{x_i, x_j\}$ is any other such pair then by setting $x_{n-1} = x_n, x_i = x_j$ we would get an $(n-1)$ -ary polynomial different from $x_0 \cdot \dots \cdot x_{n-2}$, in contradiction with $p_{n-1} = 1$. Hence for every $\alpha \in G(q)$, $(n-1)\alpha = n-1$ and $n\alpha = n$, or $(n-1)\alpha = n, n\alpha = n-1$. Thus $|G(q)| \leq (n-1)!2!$, and so we get at least $\binom{n+1}{2} \geq n+2$ polynomials by permuting the variables of q ,

none of them in $P_{n+1}(n)$, provided $n \geq 3$.

If $n = 2$, then $p(x_0, x_1x_2)$ yields three polynomials in which no variable splits; $|P_3(2)| = p_2$ and we can choose a $t \in P_3(1) - P_3(2)$, obtaining $p_2 + 4$ polynomials. This completes the proof of the inequality.

6. The nonassociative case. In this section let \mathfrak{A} be an idempotent algebra, and \cdot a binary commutative and nonassociative polynomial. The following lemma is due to J. Dudek [1]:

LEMMA 16. *Let $n > 2$ and let f_n denote the polynomial*

$$(\cdots ((x_0x_1)x_2) \cdots) x_{n-1}.$$

Let τ be the transposition $(i, i+1)$, where $i \neq 0$, and let σ denote the cyclic permutation $(0, 1, \cdots, n-1)$. Then $f_n \neq f_n^\tau$, and the polynomials $f_n, f_n^\sigma, f_n^{\sigma^2}, \cdots, f_n^{\sigma^{n-1}}$ are all distinct.

Now we prove the inequality $p_{n+1} \geq p_n + (n-1)$. Observe that Lemma 3 applies, hence $|P_n M_{n-1}| = p_n$ and $P_n M_{n-1} \subseteq P_{n+1}$. We claim that $f_{n+1}, f_{n+1}^\sigma, \cdots, f_{n+1}^{\sigma^{n-2}} \notin P_n M_{n-1}$. Indeed, let $f_n^{\sigma^k} \in P_n M_{n-1}$. Then

$$(\cdots (((\cdots (x_k x_{k+1}) \cdots) x_n) x_0) \cdots) x_{k-1} = p(x_0, \cdots, x_{n-1} x_n).$$

Since x_{n-1} and x_n are symmetric in the right hand side, we get that f_{n+1} is invariant under some $\tau = (i, i+1)$, $i \neq 0$, contrary to Lemma 16. Thus we have found $p_n + (n-1)$ essentially $(n+1)$ -ary polynomials, completing the proof.

REFERENCES

1. J. Dudek, *The number of algebraic operations in an idempotent groupoid*, Bull. Acad. Polon. Sci. Sér. Math. Phys. Astr. (to appear).
2. G. Grätzer, *Universal algebra*, The University Series in Higher Mathematics, D. Van Nostrand Co. Inc., Princeton, N. J., 1968.
3. G. Grätzer and R. Padmanabhan, *On commutative, idempotent, and non-associative groupoids* (to appear).
4. G. Grätzer and J. Pionka, *A characterization of semilattices*, Colloq. Math. (to appear).
5. ———, *On the number of polynomials of a universal algebra II* (to appear).
6. G. Grätzer, J. Pionka, and A. Sekanina, *On the number of polynomials of a universal algebra I*, Colloq. Math. (to appear).
7. J. Pionka, *On the number of independent elements in finite abstract algebras with two binary symmetrical operations*, Colloq. Math. **19** (1968), 9-21.
8. ———, *On a method of construction of abstract algebras*, Fund. Math. **61** (1967), 183-189.
9. K. Urbanik, *On algebraic operations in idempotent algebras*, Colloq. Math. **13** (1965), 129-157.

Received July 28, 1969, and in revised form November 4, 1969. The research of both authors was supported by the National Research Council of Canada.

THE UNIVERSITY OF MANITOBA

PACIFIC JOURNAL OF MATHEMATICS

EDITORS

H. SAMELSON
Stanford University
Stanford, California 94305

J. DUGUNDJI
Department of Mathematics
University of Southern California
Los Angeles, California 90007

RICHARD PIERCE
University of Washington
Seattle, Washington 98105

BASIL GORDON*
University of California
Los Angeles, California 90024

ASSOCIATE EDITORS

E. F. BECKENBACH

B. H. NEUMANN

F. WOLF

K. YOSHIDA

SUPPORTING INSTITUTIONS

UNIVERSITY OF BRITISH COLUMBIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
UNIVERSITY OF CALIFORNIA
MONTANA STATE UNIVERSITY
UNIVERSITY OF NEVADA
NEW MEXICO STATE UNIVERSITY
OREGON STATE UNIVERSITY
UNIVERSITY OF OREGON
OSAKA UNIVERSITY
UNIVERSITY OF SOUTHERN CALIFORNIA

STANFORD UNIVERSITY
UNIVERSITY OF TOKYO
UNIVERSITY OF UTAH
WASHINGTON STATE UNIVERSITY
UNIVERSITY OF WASHINGTON

* * *

AMERICAN MATHEMATICAL SOCIETY
CHEVRON RESEARCH CORPORATION
TRW SYSTEMS
NAVAL WEAPONS CENTER

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be in typed form or offset-reproduced, double spaced with large margins. Underline Greek letters in red, German in green, and script in blue. The first paragraph or two must be capable of being used separately as a synopsis of the entire paper. It should not contain references to the bibliography. Manuscripts, in duplicate if possible, may be sent to any one of the four editors. Please classify according to the scheme of Math. Rev. **36**, 1539-1546. All other communications to the editors should be addressed to the managing editor, Richard Arens, University of California, Los Angeles, California, 90024.

50 reprints are provided free for each article; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published monthly. Effective with Volume 16 the price per volume (3 numbers) is \$8.00; single issues, \$3.00. Special price for current issues to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: \$4.00 per volume; single issues \$1.50. Back numbers are available.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley, California, 94708.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), 7-17, Fujimi 2-chome, Chiyoda-ku, Tokyo, Japan.

* Acting Managing Editor.

Shair Ahmad, <i>Dynamical systems of characteristic 0^+</i>	561
Charles A. Akemann and Bernard Russo, <i>Geometry of the unit sphere of a C^*-algebra and its dual</i>	575
Philip Bacon, <i>The compactness of countably compact spaces</i>	587
Richard Blaine Barrar and Henry Loeb, <i>On the continuity of the nonlinear Tschebyscheff operator</i>	593
L. Carlitz, <i>Factorization of a special polynomial over a finite field</i>	603
Joe Ebeling Cude, <i>Compact integral domains</i>	615
Frank Rimi DeMeyer, <i>On automorphisms of separable algebras. II</i>	621
James B. Derr, <i>Generalized Sylow tower groups</i>	633
Raouf Doss, <i>Some inclusions in multipliers</i>	643
Mary Rodriguez Embry, <i>The numerical range of an operator</i>	647
John Froese, <i>Domain-perturbed problems for ordinary linear differential operators</i>	651
Zdeněk Frolík, <i>Absolute Borel and Souslin sets</i>	663
Ronald Owen Fulp, <i>Tensor and torsion products of semigroups</i>	685
George Grätzer and J. Plonka, <i>On the number of polynomials of an idempotent algebra. I</i>	697
Newcomb Greenleaf and Walter Read, <i>Positive holomorphic differentials on Klein surfaces</i>	711
John Willard Heidel, <i>Uniqueness, continuation, and nonoscillation for a second order nonlinear differential equation</i>	715
Leon A. Henkin, <i>Extending Boolean operations</i>	723
R. Hirshon, <i>On hopfian groups</i>	753
Melvin Hochster, <i>Totally integrally closed rings and extremal spaces</i>	767
R. Mohanty and B. K. Ray, <i>On the convergence of a trigonometric integral</i>	781
Michael Rich, <i>On a class of nodal algebras</i>	787
Emile B. Roth, <i>Conjugate space representations of Banach spaces</i>	793
Rolf Schneider, <i>On the projections of a convex polytope</i>	799
Bertram Manuel Schreiber, <i>On the coset ring and strong Ditkin sets</i>	805
Edgar Lee Stout, <i>Some remarks on varieties in polydiscs and bounded holomorphic functions</i>	813
James Edward Ward, <i>Two-groups and Jordan algebras</i>	821