PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 28, No. 1, April 1971

ON IDEMPOTENT, COMMUTATIVE, AND NONASSOCIATIVE GROUPOIDS

G. GRÄTZER AND R. PADMANABHAN[1]

ABSTRACT. For an algebra $\mathfrak{A}=\langle A;\ F\rangle$ and for $n\geqq 2$, let $p_n(\mathfrak{A})$ denote the number of essentially n-ary polynomials of $\mathfrak{A}$. J. Dudek has shown that if $\mathfrak{A}$ is an idempotent and nonassociative groupoid then $p_n(\mathfrak{A})\geqq n$ for all $n>2$. In this paper this result is improved for the commutative case to show that for such groupoids $\mathfrak{A}$, $p_n(\mathfrak{A})\geqq\frac{1}{3}(2^n-(-1)^n)$ for all $n\geqq 2$ (Theorem 1) and that this is the best possible result. Those groupoids for which this lower bound is attained are completely characterized. In fact, the relevant result proved below is much stronger (Theorem 3). From these and other known results it is deduced that the sequence $\langle 0,\ 0,\ 1,\ 3\rangle$ has the minimal extension property.

1. **Introduction.** Let $\mathfrak{A}=\langle A;\ \circ\ \rangle$ be a groupoid, that is, A is a nonvoid set and $\circ$ is a binary operation on A. Functions composed from $x_0,\cdots,x_{n-1}$ using $\circ$ are called n-ary polynomials; an n-ary polynomial is *essentially n-ary* if it depends on all n variables. For $n\geqq 2$ let $p_n(\mathfrak{A})$ denote the number of essentially n-ary polynomials.

J. Dudek [1] proved that $p_n(\mathfrak{A})\geqq n$ in any idempotent groupoid other than the semilattice and the diagonal algebra. Idempotent groupoids with $p_n(\mathfrak{A})=n$ are given in J. Płonka [8]; these are necessarily noncommutative.

In this paper we investigate $p_n(\mathfrak{A})$ for idempotent and commutative groupoids. If, in addition, $\circ$ is also associative, then $p_n(\mathfrak{A})=1$ for all $n\geqq 2$ (and $\mathfrak{A}$ is a semilattice). Therefore, to get something interesting we have to assume that $\mathfrak{A}$ is nonassociative. To provide an example, let $\langle G;\ +\rangle$ be an abelian group satisfying $3x=0$ and define

(1) $x\circ y=2x+2y$.

Then $\mathfrak{G}=\langle G;\ \circ\rangle$ is an idempotent, commutative, and nonassociative groupoid, and

(2) $p_n(\mathfrak{G})=\frac{1}{3}(2^n-(-1)^n)$.

Our main result states that this number is minimal, and equality is achieved only by the groupoid given in this example.

Received by the editors April 1, 1970.

AMS 1970 *subject classifications*. Primary 08A25, 08A05.

Key words and phrases. n-ary polynomials and essentially n-ary polynomials of a universal algebra, representable sequence, minimal extension property, idempotent reduct of an abelian group.

[1] This research of both authors was supported by the National Research Council of Canada.

In §2 we prove that $p_n(\mathfrak{G})$ is a lower-bound for any $p_n(\mathfrak{A})$. Groupoids in which equality is attained are described in §3.

An application of these results is given in §4.

NOTATION. We use the standard notation, see [2]. For an algebra $\mathfrak{A}$ let $P_n(\mathfrak{A})$ denote the set of essentially n-ary polynomials of $\mathfrak{A}$. As in [4], for a groupoid $\mathfrak{A}=\langle A;\circ\rangle$ and for $p\in P_n(\mathfrak{A})$ we define

(3) $pM_i=p(x_0,\cdots,x_i\circ x_n,\cdots,x_{n-1})$,

(4) $pS_n=p(x_0,\cdots,x_{n-1})\circ x_n$.

For $n\geqq 2$ let q_n denote the number $\frac{1}{3}(2^n-(-1)^n)$.

We note that the q_n satisfiy the following two recursive relations:

(5) $q_n=2q_{n-1}-(-1)^n$,

(6) $q_n=q_{n-1}+2q_{n-2}$.

2. The lower-bound.

THEOREM 1. *Let $\mathfrak{A}$ be an idempotent, commutative, and nonassociative groupoid. Then, for $n\geqq 2$, $p_n(\mathfrak{A})\geqq q_n$.*

PROOF. $p_n(\mathfrak{A})\geqq q_n$ is obvious for $n=2$. Since $x\circ(y\circ z)$, $y\circ(z\circ x)$, $z\circ(x\circ y)$ are essentially ternary (see [6]) and pairwise distinct (the equality of any two would imply the associativity of $\circ$) we obtain $p_3(\mathfrak{A})\geqq q_3$.

Assume that $p_m(\mathfrak{A})\geqq q_m$ has been proved for all $m<n$, where n is an integer $\geqq 4$. By Lemmas 3 and 4 of [4]

(7) $P_{n-1}M_{n-2}\subseteq P_n$,

(8) $|P_{n-1}M_{n-2}|=|P_{n-1}|$,

(9) $(P_{n-2}S_{n-2})S_{n-1}\subseteq P_n$,

(10) $(P_{n-2}S_{n-1})S_{n-2}\subseteq P_n$,

(11) $|(P_{n-2}S_{n-2})S_{n-1}|=|(P_{n-2}S_{n-1})S_{n-2}|=|P_{n-2}|$.

The subsets of P_n given in (7), (9), and (10) are pairwise disjoint. Indeed, if

(12) $p\in(P_{n-2}S_{n-2})S_{n-1}\cap(P_{n-2}S_{n-1})S_{n-2}$,

then $p=(r\circ x_{n-2})\circ x_{n-1}=(s\circ x_{n-1})\circ x_{n-2}$ for some r, $s\in P_{n-2}$. Setting $x_0=\cdots=x_{n-3}$ this yields $(x_0\circ x_{n-2})\circ x_{n-1}=(x_0\circ x_{n-1})\circ x_{n-2}$, contradicting the nonassociativity of $\circ$. If $p\in P_{n-1}M_{n-2}\cap(P_{n-2}S_{n-2})S_{n-1}$, then

$$p=r(x_0,\cdots,x_{n-2}\circ x_{n-1})=(s(x_0,\cdots,x_{n-3})\circ x_{n-2})\circ x_{n-1}.$$

Thus x_{n-2} and x_{n-1} are symmetric in p, implying that p satisfies (12), a contradiction. The sets given in (7) and (10) are disjoint for the same reason. Hence, by (8) and (11),

(13) $p_n(\mathfrak{A})\geqq p_{n-1}(\mathfrak{A})+2p_{n-2}(\mathfrak{A})$.

Since $p_{n-1}(\mathfrak{A})\geqq q_{n-1}$ and $p_{n-2}\geqq q_{n-2}$, (6) and (13) yield $p_n(\mathfrak{A})\geqq q_n$, completing the proof of Theorem 1.

3. **Idempotent reduct of groups.** Let $\langle G; +\rangle$ be an abelian group of exponent 3. The groupoid $\mathfrak{G}=\langle G; \circ\rangle$, where $\circ$ is defined by (1) is called the *idempotent reduct* of $\langle G; +\rangle$. This terminology is justified by the following result of J. Płonka [7]: the polynomials of $\mathfrak{G}$ are exactly the idempotent polynomials of $\langle G; +\rangle$.

Hence, $P_n(\mathfrak{G})$ consists of all functions of the form

$$\sum_{i=0}^{n-1} \alpha_i x_i, \qquad \alpha_i = 1 \text{ or } 2, \qquad \sum \alpha_i \equiv 1 \pmod 3.$$

A simple computation (which is used in verifying this statement) shows that a polynomial given in this form belongs to $P_{n-1}M_{n-2}$ if $\alpha_{n-2}=\alpha_{n-1}$; it belongs to $(P_{n-2}S_{n-1})S_{n-2}$ if $\alpha_{n-2}=2$, $\alpha_{n-1}=1$.

Thus, in view of the results of the last section,

(14) $p_n(\mathfrak{G})=p_{n-1}(\mathfrak{G})+2p_{n-2}(\mathfrak{G})$.

Since $p_2(\mathfrak{G})=1$, $p_3(\mathfrak{G})=3$, (6) and (14) yield $p_n(\mathfrak{G})=q_n$.

THEOREM 2. *Let $\mathfrak{G}$ be the idempotent reduct of an abelian group of exponent* 3. *Then $p_n(\mathfrak{G})=q_n$ for all $n\geqq 2$.*

This formula was first obtained by T. J. Dickson and B. Wolk.[2]

4. **The characterization theorem.** In this section we shall prove the converse of Theorem 2. In fact the result we prove is much stronger:

THEOREM 3. *Let $\mathfrak{A}=\langle A; \circ\rangle$ be an idempotent groupoid satisfying $p_n(\mathfrak{A})=q_n$ for $n=2$, 3, and 4. Then a binary operation $+$ can be defined on A such that*

(i) *$\langle A; +\rangle$ is an abelian group of exponent* 3;

(ii) *for all $a, b\in A$, we have $a\circ b=2a+2b$.*

The group $\langle A; +\rangle$ is determined by $\mathfrak{A}$ up to isomorphism.

PROOF. First we verify that the identity

(15) $(x\circ y)\circ y=x$

holds in $\mathfrak{A}$. Obviously,

(16) $(x\circ y)\circ y\in\{x, y, x\circ y\}$.

Assume that

(17) $(x\circ y)\circ y=y$,

then $(x\circ y)\circ((x\circ y)\circ y)=(x\circ y)\circ y$, and so $x\circ y=y$, contradicting $p_2(\mathfrak{A})=1$. Now assume that

(18) $(x\circ y)\circ y=x\circ y$.

We claim that (18) implies that $p_3(\mathfrak{A})\geqq 6$. Indeed, consider the six polynomials $f_1=(x\circ y)\circ z$, $f_2=(y\circ z)\circ x$, $f_3=(z\circ x)\circ y$, f_4

[2] Oral communication.

$=(x \circ y) \circ (y \circ z)$, $f_5=(y \circ z) \circ (z \circ x)$, $f_6=(z \circ x) \circ (x \circ y)$. We already noted that f_1, f_2, and f_3 are essentially ternary. The same is true of f_4, f_5 and f_6. Indeed, if f_4, or f_5, or f_6 does not depend on one variable we set the other two equal, and obtain that $u \circ v$ does not depend on u, a contradiction.

We have already noted that f_1, f_2 and f_3 are pairwise distinct. If two of f_4, f_5 and f_6 are equal, then one of them, hence all, are symmetric. But if f_4 is symmetric, then

$$\begin{aligned} a \circ (b \circ c) &= (a \circ (b \circ c)) \circ (b \circ c) \quad \text{by (18)} \\ &= (a \circ (b \circ c)) \circ (b \circ (b \circ c)) \quad \text{by (18)} \\ &= (a \circ b) \circ (b \circ c) \quad \text{(by the symmetry of } f_4\text{)}, \end{aligned}$$

thus $a \circ (b \circ c)$ is symmetric in a and c, which is associativity. For the same reason if f_1 equals one of f_4, f_5, f_6, it has to be f_5. So let $f_1=f_5$, then

$$\begin{aligned} f_1 &= (a \circ b) \circ c = ((a \circ b) \circ c) \circ (a \circ b) \\ &= ((a \circ b) \circ c) \circ ((a \circ b) \circ b) = (a \circ b) \circ (b \circ c) \quad (\text{by } f_1 = f_5) \\ &= f_4, \end{aligned}$$

implying associativity. Similarly, f_2 and f_3 cannot equal any of f_4, f_5, and f_6. This completes the proof of $p_3(\mathfrak{A}) \geqq 6$. Since we assumed that $p_3(\mathfrak{A})=3$, this shows that (18) is false. Thus (17) and (18) have been eliminated and by (16), only (15) is left. This completes the proof of the claim that (15) holds in $\mathfrak{A}$.

Now let us verify two more identities:

(19) $(x \circ y) \circ z=(x \circ z) \circ (y \circ z)$,

(20) $(x \circ y) \circ (z \circ t)=(y \circ z) \circ (x \circ t)$.

As noted above, $f_1=f_4$ and $f_1=f_6$ both imply associativity. Since $p_3(\mathfrak{A})=3$, and so $P_3(\mathfrak{A})=\{f_1, f_2, f_3\}$, we conclude that $f_1=f_5$, which is (19).

It is proved in [9] that if $\circ$ is commutative, idempotent, and nonassociative, then $p_4(\mathfrak{A}) \geqq 5$, and

$$P_4(\mathfrak{A}) \supseteq \{((x \circ y) \circ z) \circ t, ((y \circ z) \circ t) \circ x, ((z \circ t) \circ x) \circ y, \\ ((t \circ x) \circ y) \circ z, (x \circ y) \circ (z \circ t)\}, \tag{21}$$

where the five polynomials listed are all distinct. Since we assumed that $p_4(\mathfrak{A})=5$ we obtain equality in (21). Therefore $(y \circ z) \circ (x \circ t)$ must equal one of these five polynomials; it cannot equal any of the first four because they cannot be symmetric in y, z and in x, t. Thus follows (20).

Now fix an element $e \in A$ and define

(22) $x+y=(x \circ y) \circ e$.

Then

(23) $x+y=y+x$,

since $\circ$ is commutative.

(24) $x+e=x$,

since $x+e=(x \circ e) \circ e=x$ by (15).

(25) $(x+x)+x=e$,

since $(x+x)+x=(((x \circ x) \circ e) \circ x) \circ e=e \circ e=e$ by (15).

Now compute:

$$\begin{aligned}(x+y)+z &= (((x \circ y) \circ e) \circ z) \circ e \\ &= (((x \circ y) \circ e) \circ e) \circ (z \circ e) \quad \text{by (19)} \\ &= (x \circ y) \circ (z \circ e) \quad \text{by (15)} \\ &= (x \circ e) \circ (y \circ z) \quad \text{by (20).}\end{aligned}$$

Thus, $(x+y)+z$ is symmetric in y and z, and $+$ is commutative, hence

(26) $(x+y)+z=x+(y+z)$.

Thus, by (22)$-$(26), $\langle A;+\rangle$ is an abelian group of exponent three, and

$$\begin{aligned}2x+2y &= (x+x)+(y+y) = (x \circ x) \circ e + (y \circ y) \circ e \\ &= (x \circ e) + (y \circ e) = ((x \circ e) \circ (y \circ e)) \circ e \\ &= ((x \circ y) \circ e) \circ e \quad \text{by (19)} \\ &= x \circ y \quad \text{by (15).}\end{aligned}$$

These prove statements (i) and (ii) of Theorem 3. The last statement of Theorem 3 follows from the observation that the choice of zero determines $+$; indeed, if $e \in A$ is chosen to be the zero of $\langle A;+\rangle$, and $x \circ y=2x+2y$, then $(x \circ y) \circ z=x+y+2z$, hence $x+y=(x \circ y) \circ e$ as in (22).

5. **Some applications.** A universal algebra $\mathfrak{A}=\langle A;F\rangle$ is *idempotent* if every $f \in F$ is of positive arity (i.e., not nullary) and satisfies $f(x, x, \cdots)=x$. Using the notations of [**5**], this is the same as $p_0(\mathfrak{A})=p_1(\mathfrak{A})=0$. For $n \geqq 2$, $p_n(\mathfrak{A})$ will again denote the number of essentially n-ary polynomials.

Theorem 4. *Let $\mathfrak{A}$ be an idempotent algebra satisfying $p_2(\mathfrak{A})=1$ and $p_3(\mathfrak{A}) \geqq 2$. Then $p_n(\mathfrak{A}) \geqq q_n$, for $n \geqq 4$.*

Proof. Since $p_2(\mathfrak{A})=1$, $\mathfrak{A}$ has a commutative, idempotent binary polynomial, $x \circ y$. If $\circ$ is nonassociative, then by Theorem 1,

$$p_n(\mathfrak{A}) \geqq p_n(\langle A;\circ\rangle) \geqq q_n.$$

If $\circ$ is associative, then we apply an inequality of [**4**]:

$$p_n(\mathfrak{A}) \geqq 2p_{n-1}(\mathfrak{A}) + 1 \quad \text{for } n \geqq 2. \tag{27}$$

By assumption $p_3(\mathfrak{A}) \geqq 2$, hence by (26), $p_4(\mathfrak{A}) \geqq 2 \cdot 2 + 1 = q_4$; since, by (5), $q_n = 2q_{n-1} \pm 1$, this implies that $p_n(\mathfrak{A}) \geqq q_n(\mathfrak{A})$ for all $n \geqq 4$.

We can reinterpret a special case of Theorem 4 using a concept introduced in [3]. Let us say that the sequence $\langle p_0, p_1, \cdots, p_{n-1}\rangle$ has the *minimal extension property* if for some algebra $\mathfrak{A}$: (i) $p_k(\mathfrak{A}) = p_k$ for $k < n$; (ii) if any algebra $\mathfrak{B}$ satisfies $p_k(\mathfrak{B}) = p_k$ for $k < n$, then $p_k(\mathfrak{A}) \leqq p_k(\mathfrak{B})$ for all k.

COROLLARY. *The sequence $\langle 0, 0, 1, 3\rangle$ has the minimal extension property.*

From the proof of Theorem 3 we get a corollary that the identities (15), (19) and (20) together with the commutative and idempotent laws form an equationally complete set; this was proved by S. O. Aliev (Algebra i Logika Sem. **5** (1966), 5–14). To see this observe that any such groupoid arises from an abelian group of exponent 3 and that every word in the basic groupoid operation is a word in the group operation (by property (1)). Since it is well known that any such group is equationally complete, the result follows immediately.

Using arguments similar to the ones in the proof of Theorem 3 one can show that $\mathfrak{A} = \langle A; \circ\rangle$ arises out of a commutative Moufang loop of exponent 3 if we just demand that $p_n(\mathfrak{A}) = q_n$ for $n = 2, 3$. Since such a loop need not be a group, our theorem cannot be strengthened by omiting the assumption $p_4(\mathfrak{A}) = q_4$.

REFERENCES

1. J. Dudek, *The number of algebraic operations in an idempotent groupoid*, Colloq. Math **21** (1970), 169–177.

2. G. Grätzer, *Universal algebra*, Van Nostrand, Princeton, N. J., 1968. MR **40** #1320.

3. ———, *Universal algebra*, Trends in Lattice Theory, Van Nostrand, Princeton, N. J., 1969.

4. G. Grätzer and J. Płonka, *On the number of polynomials of an idempotent algebra*. I, Pacific J. Math. **32** (1970), 697–709.

5. G. Grätzer, J. Płonka and A. Sekanina, *On the number of polynomials of a universal algebra*. I, Colloq. Math. **22** (1970), 9–11.

6. J. Płonka, *On the number of independent elements in finite abstract algebra having a binary operation*, Colloq. Math. **14** (1966), 189–201. MR **33** #88.

7. ———, *On the arity of idempotent reducts of groups*, Colloq. Math. **21** (1970), 35–37.

8. ———, *On algebras with n distinct essentially n-ary operations*, Algebra Universalis (to appear).

9. ———, *On algebras with at most n distinct essentially n-ary operations*, Algebra Universalis (to appear).

UNIVERSITY OF MANITOBA, WINNIPEG, MANITOBA, CANADA