PACIFIC JOURNAL OF MATHEMATICS
Vol. 47, No. 1, 1973

ON THE NUMBER OF POLYNOMIALS OF AN IDEMPOTENT ALGEBRA, II

G. GRÄTZER AND J. PŁONKA

In part I of this paper a conjecture was formulated according to which, with a few obvious exceptions, the sequence $\langle p_n(\mathfrak{A})\rangle$ of an idempotent algebra is eventually strictly increasing. In this paper this conjecture is verified for idempotent algebras satisfying $p_2(\mathfrak{A}) = 0, p_3(\mathfrak{A}) > 0$, and $p_4(\mathfrak{A}) > 0$. In fact, somewhat more is proved:

THEOREM. Let $\mathfrak{A}$ be an idempotent algebra with no essentially binary polynomial and with essentially ternary and quaternary polynomials. Then the sequence

$$p_3(\mathfrak{A}), p_4(\mathfrak{A}), \cdots, p_n(\mathfrak{A}), \cdots$$

is strictly increasing, that is, for all $n \geqq 2$

$$p_n(\mathfrak{A}) + 1 \leqq p_{n+1}(\mathfrak{A}) .$$

The proof starts in §2 where a lemma of K. Urbanik is modified to show that the proof splits naturally into three cases. §§3 and 4 handle the first two cases. In §5 the third case is analyzed and it is proved that it splits into two further cases that are settled in §§6 and 7. In each of these sections examples are provided that the case under consideration is not void.

For the undefined concepts and basic results the reader is referred to [2].

Examples of algebras satisfying the conditions of the Theorem abound. On a two element Boolean algebra $\{0, 1\}$ the operation $(x \wedge y) \vee (y \wedge z) \vee (z \wedge x)$ defines such an algebra.

2. The classification. An algebra $\mathfrak{A} = \langle A; F\rangle$ is *idempotent* if every operation $f \in F$ has type (arity) > 0, and $f(a, \cdots, a) = a$ for all $a \in A$. All algebras considered in this paper are assumed to have more than one element. An n-ary polynomial p of $\mathfrak{A}$ (that is, an n-ary function or A composed from functions in F) *depends on* x_i $(1 \leqq i \leqq n)$ if there exist $a_1, \cdots, a_n, a'_i \in A$ with $p(a_1, \cdots, a_i, \cdots, a_n) \neq p(a_1, \cdots, a'_i, \cdots, a_n)$; p is *essentially n-ary*, if p depends on $x_1, \cdots, x_n$. For $n \geqq 2$, let $p_n(\mathfrak{A})$ denote the number of essentially n-ary polynomials.

In this paper we shall deal exclusively with idempotent algebras satisfying

$$p_2(\mathfrak{A}) = 0, p_3(\mathfrak{A}) \neq 0 , \quad \text{and} \quad p_4(\mathfrak{A}) \neq 0 .$$

The sequence $\langle p_n(\mathfrak{A})\rangle$ is strictly increasing because $\mathfrak{A}$ must have essentially ternary polynomials with very nice properties. This will be used to classify all algebras satisfying these conditions.

A ternary (idempotent) polynomial p is called a *minority polynomial* if

$$p(x, x, y) = p(x, y, x) = p(y, x, x) = y \;;$$

p is a *majority polynomial*, if

$$p(x, x, y) = p(x, y, x) = p(y, x, x) = x \;;$$

p is a *first projection* polynomial, if

$$p(x, x, y) = p(x, y, x) = p(x, y, y) = x \,.$$

Observe that a minority or majority ternary polynomial is essentially ternary.

LEMMA 1. *Let $p(x, y, z)$ be an essentially ternary polynomial satisfying $p(x, y, y) = y$. Then one of $p(z, y, x)$ and $p(y, x, z)$ is an essentially ternary first projection polynomial or one of $p(x, y, z)$ and $p(p(x, y, z), y, z)$ is a majority polynomial.*

This statement can be verified by easy computation, observing that $p(y, x, y) = x$ or y, $p(y, y, x) = x$ or y, and considering the four cases separately. This argument is the first half of the proof of Lemma 3 of K. Urbanik [6].

THEOREM 2. *Let $\mathfrak{A}$ be an idempotent algebra satisfying $p_2(\mathfrak{A}) = 0$ and $p_3(\mathfrak{A}) \neq 0$. Then $\mathfrak{A}$ satisfies one (or more) of the following three conditions:*

(a) *$\mathfrak{A}$ has a ternary majority polynomial;*

(b) *$\mathfrak{A}$ has an essentially ternary first projection polynomial;*

(c) *all essentially ternary polynomials of $\mathfrak{A}$ are minority polynomials.*

Proof. Since $p_3(\mathfrak{A}) \neq 0$, $\mathfrak{A}$ has an essentially ternary polynomial p. Since $\mathfrak{A}$ is idempotent and $p_2(\mathfrak{A}) = 0$, $p(x, y, y) = x$ or y, $p(y, x, y) = x$ or y, and $p(y, y, x) = x$ or y. If the second alternative occurs for any essentially ternary p, say $p(x, y, y) = y$, then by Lemma 1, $p(z, y, x)$ or $p(y, x, z)$ is an essentially ternary first projection polynomial, or one of $p(x, y, z)$ and $p(p(x, y, z), y, z)$ is a majority polynomial. Thus $\mathfrak{A}$ satisfies (a) or (b). This conclusion cannot be drawn only if for any essentially ternary polynomial p we have $p(x, y, y) = p(y, x, y) = p(y, y, x) = x$, which is (c).

3. Majority polynomial. Algebras satisfying condition (a) of Theorem 2 shall be handled in this section.

THEOREM 3. *Let* $\mathfrak{U}$ *be an idempotent algebra satisfying* $p_2(\mathfrak{U}) = 0$. *If* $\mathfrak{U}$ *has a ternary majority polynomial* f, *then*

$$p_n(\mathfrak{U}) + 1 \leqq p_{n+1}(\mathfrak{U})$$

for $n \geqq 2$.

Proof. For any n-ary polynomial p define an $(n+1)$-ary polynomial pF:

$$pF = f(p(x_1, \cdots, x_n), p(x_1, \cdots, x_{n-1}, x_{n+1}), p(x_1, \cdots, x_{n-1}, x_1)) .$$

Let $f_3 = f$ and for $n \geqq 3$ define recursively:

$$f_{n+1} = f_n F .$$

Finally, we define an $(n+1)$-ary polynomial g:

$$g = f(f_n(x_1, \cdots, x_n), f_n(x_1, \cdots, x_{n-1}, x_{n+1}), x_2) .$$

Now we make the following claims:

(i) For $n \geqq 3$,

$$f_n(x_1, \cdots, x_{n-1}, x_1) = x_1 .$$

(ii) For $n \geqq 3$,

$$f_n(x_1, x_2, \cdots, x_2) = x_2 .$$

(iii) If the polynomial p is essentially n-ary, then pF is essentially $(n+1)$-ary.

(iv) f_n is essentially n-ary.

(v) $pF = qF$ implies $p = q$.

(vi) g is essentially $(n+1)$-ary.

(vii) $g = pF$ for no polynomial p.

Statements (i)-(vii) easily imply the statement of Theorem 3. Indeed, consider the set

$$\{g\} \cup \{pF \mid p \text{ is an essentially } n\text{-ary polynomial of } \mathfrak{U}\} .$$

By (iii) and (vi) all elements of this set are essentially $(n+1)$-ary polynomials. (vii) shows that the union is a disjoint union, and so by (v) the set has $p_n(\mathfrak{U}) + 1$ elements. Thus, $p_{n+1}(\mathfrak{U}) \geqq p_n(\mathfrak{U}) + 1$.

Proof of (i). For $n = 3$ $f_3 = f$ is a majority polynomial, hence $f_3(x_1, x_2, x_1) = x_1$. Proceeding by induction, if $f_n(x_1, \cdots, x_{n-1}, x_1) = x_1$, then

$$\begin{aligned}
&f_{n+1}(x_1, \cdots, x_n, x_1)\\
&\quad = f(f_n(x_1, \cdots, x_n), f_n(x_1, \cdots, x_{n-1}, x_1), f_n(x_1, \cdots, x_{n-1}, x_1))\\
&\quad = f(f_n(x_1, \cdots, x_n), x_1, x_1) = x_1 .
\end{aligned}$$

Proof of (ii). For $n = 3$ (ii) is trivial. By induction, if f

$$f_n(x_1, x_2, \cdots, x_2) = x_2 ,$$

then

$$\begin{aligned}
&f_{n+1}(x_1, x_2, \cdots, x_2)\\
&\quad = f(f_n(x_1, x_2, \cdots, x_2), f_n(x_1, x_2, \cdots, x_2), f_n(x_1, x_2, \cdots, x_2, x_1))\\
&\quad = f(x_2, x_2, x_1) = x_2 .
\end{aligned}$$

Proof of (iii). Setting $x_n = x_{n+1}$ in pF we get p, since f is a majority polynomial. Hence pF depends on $x_1, \cdots, x_{n-1}$ and on one or both of x_n and x_{n+1}. Since pF is symmetric in x_n and x_{n+1} in any two element subalgebra the first possibility cannot occur, hence pF is essentially $(n + 1)$-ary.

Proof of (iv). Trivial induction using (iii).

Proof of (v). pF with $x_n = x_{n+1}$ yields p, from which the statement follows.

Proof of (vi). Same as the proof of (iv).

Proof of (vii). Let $g = pF$. Setting $x_n = x_{n+1}$ we conclude that $f_n = p$. Thus $g = f_nF = f_{n+1}$, in other words,

$$\begin{aligned}
&f(f_n(x_1, \cdots, x_n), f_n(x_1, \cdots, x_{n-1}, x_{n+1}), f_n(x_1, \cdots, x_{n-1}, x_1))\\
&\quad = f(f_n(x_1, \cdots, x_n), f_n(x_1, \cdots, x_{n-1}, x_{n+1}), x_2) .
\end{aligned}$$

Setting $x_1 = x_{n+1}$ and using (i) and that f is majority we get

$$x_1 = f(f_n(x_1, \cdots, x_n), x_1, x_2) .$$

Finally, setting $x_2 = x_3 = \cdots = x_n$ and using (ii) we obtain $x_1 = x_2$, a contradiction, proving (vii).

An example of an algebra satisfying the conditions of Theorem 3 was given in §1. Further examples are easy to construct.

4. First projections polynomial. In this section the Theorem is proved, in a somewhat sharper form, for algebras having an essentially ternary first projection polynomial.

THEOREM 4. *Let* $\mathfrak{A}$ *be an idempotent algebra with* $p_2(\mathfrak{A}) = 0$. *If* $\mathfrak{A}$ *has an essentially ternary first projection polynomial* f, *then for* $n \geqq 3$

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

REMARK. Since, for $n \geqq 3$, $(n-1)p_n(\mathfrak{A}) \geqq 2p_n(\mathfrak{A}) \geqq p_n(\mathfrak{A}) + 1$, Theorem 4 is stronger than the corresponding special case of the Theorem.

Proof. For an n-ary polynomial p and $1 \leqq i \leqq n$ set

$$pF_i = f(p(x_1, \cdots, x_n), x_i, x_{n+1}) .$$

Then we make the following claims:

(i) $pF_i = qF_i$ implies $p = q$.

(ii) If $i \neq j$, then $pF_i \neq qF_j$.

(iii) pF_i depends on $x_1, \cdots, x_n$.

Since substituting $x_i = x_{n+1}$ in pF_i yields p, we see that if pF_i is not essentially $(n+1)$-ary, then by (iii) $pF_i = p$. By (ii), $pF_i \neq pF_j$ if $i \neq j$; hence for $i \neq j$ we cannot have both pF_i and pF_j not essentially $(n+1)$-ary. Thus for an essentially n-ary p

$$\{pF_i \mid i = 1, 2, \cdots, n\}$$

contains at least $n-1$ essentially $(n+1)$-ary polynomials. Furthermore, by (i) and (ii) the sets

$$\{pF_i \mid i = 1, 2, \cdots, n\} \quad \text{and} \quad \{qF_i \mid i = 1, 2, \cdots, n\}$$

are disjoint if p and q are distinct essentially n-ary polynomials, from which Theorem 4 follows trivially.

Proof of (i). pF_i with $x_i = x_{n+1}$ yields p, hence (i) is trivial.

Proof of (ii). Let us assume that $i \neq j$ and $pF_i = qF_j$, that is,

$$f(p(x_1, \cdots, x_n), x_i, x_{n+1}) = f(q(x_1, \cdots, x_n), x_j, x_{n+1}) .$$

Set $x = x_k$ for $k \neq i$, $1 \leqq k \leqq n$, in this identity; since $p_2(\mathfrak{A}) = 0$ after the substitution $p = x$ or x_i and $q = x$ or x_i. The four possibilities yield the following identities:

$$\begin{aligned} f(x, x_j, x_{n+1}) &= f(x, x, x_{n+1}) , \\ f(x, x_j, x_{n+1}) &= f(x_j, x, x_{n+1}) , \\ f(x, x_j, x_{n+1}) &= f(x, x, x_{n+1}) , \\ f(x, x_j, x_{n+1}) &= f(x_j, x, x_{n+1}) . \end{aligned}$$

The first and third contradict that f is essentially ternary, while the second and fourth mean that f is symmetric in its first and second variable, contradicting that f is a first projection polynomial.

Proof of (iii). Setting $x_i = x_{n+1}$ in pF_i gives p, hence pF_i depends on $x_1, \cdots, x_{i-1}, x_{i+1}, \cdots, x_n$. Assume that pF_i does not depend on x_i. Then

$$\begin{aligned} &f(p(x_1, \cdots, x_n), x_i, x_{n+1}) \\ &\quad = f(p(x_1, \cdots, x_{i-1}, x_{n+1}, x_{i+1}, \cdots, x_n), x_{n+1}, x_{n+1}) \\ &\quad = p(x_1, \cdots, x_{i-1}, x_{n+1}, x_{i+1}, \cdots, x_n) . \end{aligned}$$

Substituting $x = x_j$ for $j \neq i, 1 \leqq j \leqq n$ and using $p_2(\mathfrak{U}) = 0$ we get one of

$$\begin{aligned} f(x, x_i, x_{n+1}) &= x , \\ f(x_i, x_i, x_{n+1}) &= x_{n+1} . \end{aligned}$$

The first contradicts that f is essentially ternary, while the second is $x_i = x_{n+1}$, a contradiction.

An example of an algebra satisfying the condition of Theorem 4 can be defined on the two element set $\{0, 1\}$ taking

$$x + (x + y)(x + z)(y + z)$$

as operation

$$(u + v = (u \wedge v') \vee (u' \wedge v)) .$$

Taking both

$$(x \wedge y) \vee (y \wedge z) \vee (z \wedge x) \quad \text{and} \quad x + (x + y)(x + z)(y + z)$$

as operations we get an algebra satisfying the conditions of Theorems 3 and 4.

Note that in Theorems 3 and 4 $p_4(\mathfrak{U}) \neq 0$ follows from the assumptions.

5. **The second classification.** In this and the subsequent sections we consider an idempotent algebra $\mathfrak{U}$ with $p_2(\mathfrak{U}) = 0$ in which all essentially ternary polynomials are minority polynomials.

LEMMA 5. *$\mathfrak{U}$ has exactly one essentially ternary polynomial.*

Proof. Let f and g be essentially ternary polynomials, and consider the polynomial $f(g(x, y, z), y, z) = h$. Then $h(x, y, x) = f(g(x, y, x), y, x) = f(y, y, x) = x$. Thus h cannot be essentially ternary, because it is not minority. Due to $p_2(\mathfrak{A}) = 0$, $h(x, y, z) = x$, or y, or z. $h(x, y, x) = x$ eliminates $h = y$. Furthermore,

$$h(x, x, z) = f(g(x, x, z), x, z) = f(z, x, z) = x ,$$

eliminating $h = z$. Hence, $h = x$, that is, we proved the identity

$$f(g(x, y, z), y, z) = x .$$

Now let $a, a', b, c \in A$ and $f(a, b, c) = f(a', b, c)$. Then

$$a = f(f(a, b, c), b, c) = f(f(a', b, c), b, c) = a' ,$$

by the above identity (used with $f = g$)

$$(a =) f(f(a, b, c), b, c) = (a =) f(g(a, b, c), b, c) ,$$

and so by the above remark, $f(a, b, c) = g(a, b, c)$, proving that $f = g$, completing the proof of Lemma 5.

The only essentially ternary polynomial shall be denoted by f. Keep in mind that

$$f(f(x, y, z), y, z) = x ,$$

and that f is fully symmetric.

The next important step is again due to K. Urbanik. We call a ternary function g on A a *Boolean group reduct* if a Boolean group operation $+$ can be defined on A(i.e., $\langle A; +\rangle$ is an abelian group satisfying $2x = 0$) such that $g(x, y, z) = x + y + z$. The proof of the next lemma is identical with the proof of Lemma 5 of K. Urbanik [6].

LEMMA 6. *f is a Boolean group reduct if and only if*

$$f(f(x, y, z), x, u)$$

does not depend on x. If this is the case $+$ is defined by fixing an arbitrary element $0 \in A$ and $x + y = f(x, y, 0)$.

Accordingly, the proof of the Theorem in the minority polynomial case splits into two completely different cases according to whether or not $f(f(x, y, z), x, u)$ depends on x.

6. The minority polynomial is not a Boolean group reduct.

THEOREM 7. *Let $\mathfrak{A}$ be an idempotent algebra satisfying $p_2(\mathfrak{A}) = 0$. Let f be the unique essentially ternary minority polynomial of $\mathfrak{A}$. If $f(f(x, y, z), x, u)$ depends on x, then for $n \geqq 2$*

$$p_n(\mathfrak{A}) + 1 \leqq p_{n+1}(\mathfrak{A}) .$$

Proof. We define $f_3 = f$ and, inductively, for $n \geqq 3$

$$f_{n+1} = f(f_n(x_1, \cdots, x_n), x_1, x_{n+1}) .$$

For an n-ary polynomial p and $2 \leqq i \leqq n$ we set

$$pG_1 = f(p(x_1, \cdots, x_n), x_1, x_{n+1}) ,$$
$$pG_i = p(x_1, x_2, \cdots, x_{i-1}, f(x_i, x_1, x_{n+1}), x_{i+1}, \cdots, x_n) .$$

Observe that pG_i with $x_1 = x_{n+1}$ yields p.

We make the following claims:

(i) f_n is essentially n-ary, and

$$f_3(x_1, x_2, x_2) = x_1, f_4(x_1, x_2, x_2, x_4) = x_4 .$$
$$f_n(x_1, x_2, x_2, x_4, \cdots, x_n) = f_{n-2}(x_1, x_4, \cdots, x_n) \quad \text{for} \quad n \geqq 5 .$$

(ii) If p and q are essentially n-ary polynomials and $1 \leqq i, j \leqq n$, then $pG_i = qG_j$ implies $p = q$.

(iii) For an essentially n-ary polynomial p, at least one of $pG_1, \cdots, pG_n$ is essentially $(n + 1)$-ary.

Using (i)–(iii) it is easy to prove Theorem 7. Indeed, by (ii) and (iii),

$$P = \{pG_i \mid p \text{ is essentially } n\text{-ary, } i = 1, \cdots, n\}$$

contains at least $p_n(\mathfrak{A})$ essentially $(n + 1)$-ary polynomials. By (i),

$$g = f_{n+1}(x_2, x_1, x_{n+1}, x_3, x_4, \cdots, x_n)$$

is also essentially $(n + 1)$-ary. If $g \in P$, that is,

$$g = pG_i ,$$

for some essentially n-ary p and $1 \leqq i \leqq n$, then the substitution $x_1 = x_{n+1}$ yields

$$f_{n+1}(x_2, x_1, x_1, x_3, \cdots, x_n) = p(x_1, x_2, \cdots, x_n) .$$

By the second part of (i) the left-hand side does not depend on x_1 while the right-hand side does, a contradiction. Thus $g \notin P$, and so $P \cup \{g\}$ contains at least $p_n(\mathfrak{A}) + 1$ essentially $(n + 1)$-ary polynomials, proving Theorem 7.

Proof of (i). We start by proving the formulas in (i). Obviously,

$$f_3(x_1, x_2, x_2) = x_1$$

and

$$f_4(x_1, x_2, x_2, x_4) = f(f_3(x_1, x_2, x_2), x_1, x_4) = f(x_1, x_1, x_4) = x_1 .$$

Thus, for $n \geqq 5$, by induction,

$$\begin{aligned} f_n(x_1, x_2, x_2, x_4, \cdots, x_n) &= f(f_{n-1}(x_1, x_2, x_2, x_4, \cdots, x_{n-1}), x_1, x_n) \\ &= f(f_{n-3}(x_1, x_4, \cdots, x_{n-1}), x_1, x_n) \\ &= f_{n-2}(x_1, x_4, \cdots, x_n) . \end{aligned}$$

(For $n = 5$ interpret f_{n-3} as x_1.)

f_3 is essentially ternary by assumption. $f_4(x_1, x_2, x_3, x_1) = f_3(x_1, x_2, x_3)$, hence f_4 depends on x_2, x_3. By assumption, f_4 depends on x_1. Finally, $f_4(x_1, x_2, x_2, x_4) = x_4$, hence f_4 depends on x_4. Thus f_4 is essentially 4-ary. Proceeding by induction for $n \geqq 5$, f_n with $x_1 = x_n$ yields $f_{n-1}(x_1, \cdots, x_{n-1})$, hence f_n depends on $x_2, \cdots, x_{n-1}$. Finally, f_n with $x_2 = x_3$ gives

$$f_{n-2}(x_1, x_4, \cdots, x_n) ,$$

which depends on x_1 and x_n, hence f_n depends on x_1 and x_n.

Proof of (ii). Obvious; by setting $x_1 = x_{n+1}$ in $pG_i = qG_j$ we get $p = q$.

Proof of (iii). pG_i with $x_1 = x_{n+1}$ gives $p(x_1, \cdots, x_n)$, hence pG_i depends on $x_2, \cdots, x_n$. Furthermore, pG_1 with $x_1 = x_2 = \cdots = x_n$ gives $f(x_1, x_1, x_{n+1}) = x_{n+1}$ and $pG_i (i > 1)$ with $x_1 = x_{n+1}$ gives

$$p(x_1, \cdots, x_{i-1}, x_{n+1}, x_{i+1}, \cdots, x_n) ,$$

hence all pG_i, $1 \leqq i \leqq n$ depend on x_{n+1}. Thus if none of $pG_1, \cdots, pG_n$ is essentially $(n + 1)$-ary then none of them depend on x_1.

So assume that none of $pG_1, \cdots, pG_n$ depend on x_1. Then by substituting $x_1 = x_{n+1}$ in pG_1 we get the identity

$$(*) \qquad f(p(x_1, \cdots, x_n), x_1, x_{n+1}) = p(x_{n+1}, \cdots, x_n) .$$

For $i > 1$ we obtain

$$\begin{aligned} p(x_{n+1}, x_2, \cdots, x_i, \cdots, x_n) &= p(x_1, \cdots, x_{i-1}, f(x_i, x_1, x_{n+1}), \cdots, x_n) \\ &= p(x_1, \cdots, x_i, \cdots, x_n) . \end{aligned}$$

Since this holds for all $i > 1$, p is symmetric. Then, using the identity (*) repeatedly we obtain

$$\begin{aligned} p(x_1, \cdots, x_n) = p(x_n, x_{n-1}, \cdots, x_1) &= f(p(x_1, x_{n-1}, \cdots, x_1), x_1, x_n) \\ &= f(f(p(x_1, x_1, x_{n-2}, \cdots, x_1), x_1, x_{n-1}), x_1, x_n) \\ &= f(\cdots f(p(x_1, x_1, \cdots, x_1), x_1, x_2) \cdots) \\ &= f_n(x_1, x_2, \cdots, x_n) . \end{aligned}$$

Hence, $p = f_n$. But then (*) states that $f_{n+1}(x_1, \cdots, x_{n+1})$ does not depend on x_1, a contradiction.

Idempotent algebras satisfying $p_2 = 0$ and having a unique ternary minority polynomial can be constructed from Steiner quadruple systems and vice versa. A *Steiner quadruple system* is a set A and a set S of four element subsets of A with the property that any three element subset of A belongs to one and only one member of S. For such a system define an algebra $\langle A; f\rangle$ as follows:

f is a minority function and for three distinct elements $a, b, c \in A$ there is a unique member $B \in S$ with $a, b, c \in B$; let $B = \{a, b, c, d\}$; set $f(a, b, c) = d$.

Conversely, if an idempotent algebra $\langle A; F\rangle$ satisfies $p_2 = 0$ and f is the unique ternary minority polynomial, then set

$$S = \{\{a, b, c, f(a, b, c)\} \mid a, b, c \in A, \mid \{a, b, c\} \mid = 3\} .$$

Then this defines a Steiner quadruple system.

The smallest Steiner quadruple system which is associated with an algebra satisfying the conditions of Theorem 7 can be defined on $A = \{1, 2, \cdots, 10\}$ as follows (see [1]):

1	2	3	10	1	3	5	8
4	5	6	10	4	5	7	8
7	8	9	10	1	2	6	9
1	4	7	10	2	3	8	9
2	5	8	10	1	5	6	7
3	6	9	10	1	3	7	9
1	5	9	10	2	4	6	8
2	6	7	10	1	2	7	8
3	4	8	10	3	4	5	9
3	5	7	10	2	3	5	6
2	4	9	10	1	4	8	9
1	6	8	10	1	3	4	6
2	3	4	7	2	5	7	9
5	6	8	9	1	2	4	5
4	6	7	9	3	6	7	8

Obviously, the associated f is not a Boolean group reduct since $|A| = 10$ is not a power of two. However, an example, which is due to N.S. Mendelsohn, shows that even if $|A|$ is a power of two, examples of algebras satisfying the conditions of Theorem 7 can be defined on A provided that $|A| \geqq 16$. Let $A = \{1, 2, \cdots, 16\}$ and let S be given by the following table:

1	2	3	4	2	3	5	8
1	2	5	6	2	3	9	12
1	2	7	8	2	3	13	16
1	2	9	10	2	3	6	7

1	2	11	12	2	3	10	11
1	2	13	14	2	3	14	15
1	2	15	16	2	4	5	7
1	3	5	7	2	4	8	9
1	3	6	8	2	4	10	12
1	3	9	11	2	4	13	15
1	3	10	12	2	4	6	16
1	3	13	15	2	4	11	14
1	3	14	16	2	5	9	15
1	4	5	8	2	5	10	16
1	4	6	7	2	5	11	13
1	4	9	12	2	5	12	14
1	4	10	11	2	6	8	14
1	4	13	16	2	6	10	15
1	4	14	15	2	6	9	11
1	5	9	13	2	6	12	13
1	5	10	14	2	7	9	13
1	5	11	15	2	7	10	14
1	5	12	16	2	7	11	15
1	6	9	14	2	7	12	16
1	6	10	13	2	8	10	13
1	6	11	16	2	8	12	15
1	6	12	15	2	8	11	16
1	7	9	15	2	9	14	16
1	7	10	16	3	4	5	6
1	7	11	13	3	4	7	8
1	7	12	14	3	4	9	13
1	8	9	16	3	4	10	14
1	8	10	15	3	4	11	12
1	8	11	14	3	4	15	16
1	8	12	13	3	5	9	14
3	5	10	15	5	6	11	14
3	5	11	16	5	7	9	10
3	5	12	13	5	7	11	12
3	6	9	10	5	7	13	14
3	6	11	15	5	7	15	16
3	6	12	16	5	8	9	12
3	6	13	14	5	8	13	16
3	7	9	16	5	8	10	11
3	7	10	13	5	8	14	15
3	7	11	14	6	7	9	12
3	7	12	15	6	7	13	16
3	8	9	15	6	7	10	11
3	8	10	16	6	7	14	15

3	8	11	13	6	8	9	13
3	8	12	14	6	8	15	16
4	5	9	11	6	8	11	12
4	5	12	15	6	10	14	16
4	5	14	16	7	8	9	11
4	5	10	18	7	8	10	12
4	6	8	10	7	8	13	15
4	6	11	13	7	8	14	16
4	6	12	14	8	9	10	14
4	6	9	15	9	10	11	12
4	7	9	14	9	10	13	15
4	7	10	15	9	11	13	14
4	7	11	16	9	11	15	16
4	7	12	13	9	12	13	16
4	8	11	15	9	12	14	15
4	8	12	16	10	11	13	16
4	8	13	14	10	11	14	15
4	9	10	16	10	12	13	14
5	6	7	8	10	12	15	16
5	6	9	16	11	12	13	15
5	6	10	12	11	12	14	16
5	6	13	15	13	14	15	16

In this example,

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

and therefore

$$x + y = f(x, y, 0)$$

defines a Boolean group operation for any fixed $0 \in A$. However, $f(x, y, z) \neq x + y + z$. To prove this it suffices by Lemma 6 to illustrate that $f(f(x, y, z), x, u)$ depends on x. Indeed, $f(f(1, 4, 5), 1, 6) = 3$ and $f(f(9, 4, 5), 9, 6) = 2$.

It may be of interest to note that recently C. Treash [5] has solved the word problem for algebras $\langle A; f\rangle$ of type $\langle 3\rangle$, where f is a minority function and

$$f(f(x, y, z), y, z) = x .$$

7. **Boolean reducts.** In this section we settle the final case of the Theorem.

THEOREM 8. *Let* $\mathfrak{A}$ *be an idempotent algebra satisfying* $p_2(\mathfrak{A}) = 0$, $p_3(\mathfrak{A}) \neq 0$, *and* $p_4(\mathfrak{A}) \neq 0$, *having a unique essentially ternary minority* *polynomial f. If $f(f(x, y, z), x, u)$ does not depend on x, then*

$$p_n(\mathfrak{U}) + 1 \leqq p_{n+1}(\mathfrak{U})$$

for $n = 2, 3, \cdots$.

Proof. By Lemma 6, a Boolean group operation $+$ can be defined on A such that $f(x, y, z) = x + y + z$. Let p be an essentially 4-ary polynomial of $\mathfrak{U}$ (recall that $p_4(\mathfrak{U}) \neq 0$). It follows from Lemma 6 of [6], that there exists a ternary polynomial p_0 of $\langle A; f\rangle$ such that $p(x, y, z, u) = p_0(x, y, z, u)$ whenever x, y, z, and u are not all distinct. If $p_0 = x$, then we can conclude that p is an *essentially 4-ary first projection polynomial*, that is, it satisfies

$p(x, y, z, u) = x$ whenever x, y, z, and u are not all distinct.

If $p_0 = y$, $p_0 = z$, or $p_0 = u$, we get a first projection polynomial by permuting the variables of p. If $p_0 = x + y + z$, then $p + y + z$ is the first projection polynomial. Observe that $p + y + z$ is essentially 4-ary, since otherwise $p + y + z$ would be a polynomial of f, implying that $p = (p + y + z) + y + z$ is a polynomial of f. If $p_0 = x + y + u, \cdots$ we proceed similarly.

Thus there exists in $\mathfrak{U}$ an essentially 4-ary first projection polynomial g. (This statement is a small part of Lemma 7 in [6].)

Now we start our constructions.

Let $p = p(x_1, \cdots, x_n)$ be an essentially n-ary polynomial, $n \geqq 4$. We construct an $(n+1)$-ary polynomial $\bar{p}$ as follows:

$p(x, x, \cdots, x, y, z)$ is a ternary polynomial of $\mathfrak{U}$, hence it is x, y, z, or $x + y + z$;

(1) if $p(x, \cdots, x, y, z) = x$, then $\bar{p} = g(p(x_1, \cdots, x_n), x_{n-1}, x_n, x_{n+1})$;

(2) if $p(x, \cdots, x, y, z) = y$, then $\bar{p} = g(p(x_1, \cdots, x_n), x_1, x_n, x_{n+1})$;

(3) if $p(x, \cdots, x, y, z) = z$, then $\bar{p} = g(p(x_1, \cdots, x_n), x_1, x_{n-1}, x_{n+1})$;

(4) if $p(x, \cdots, x, y, z) = x + y + z$, then

$$\bar{p} = g(p(x_1, \cdots, x_n) + x_{n-1} + x_n, x_{n-1}, x_n, x_{n+1}) + x_{n-1} + x_n.$$

Furthermore, for $n \geqq 4$ we define g_n by recursion: $g_4 = g$ and

$$g_{n+1} = g(g_n, x_2, x_3, x_{n+1}) .$$

Then we claim the following:

(i) For an essentially n-ary p, the polynomial $\bar{p}$ is essentially $(n+1)$-ary.

(ii) If p and q are essentially n-ary polynomials and $p \neq q$, then $\bar{p} \neq \bar{q}$.

(iii) For $n \geqq 4$, $g_n(x_1, \cdots, x_1, x_{n-1}, x_n) = g_n(x_1, x_2, x_3, \cdots, x_3) = x_1$.

(iv) g_n is essentially n-ary.

(v) $g_{n+1} = \bar{p}$ for no essentially n-ary polynomial p.

Now Theorem 8 is clear:

$$\{\bar{p} \mid p \text{ essentially } n\text{-ary}\} \cup \{g_{n+1}\}$$

is a set of $p_n(\mathfrak{A}) + 1$ essentially $(n + 1)$-ary polynomials by (i), (ii), (iv), and (v).

In the subsequent proofs Case 1, $\cdots$, Case 4 refer to the cases in the definition of $\bar{p}$.

Proof of (i). *Case* 1. $\bar{p}$ with $x_{n+1} = x_n$ yields $p(x_1, \cdots, x_n)$, hence $\bar{p}$ depends on $x_1, \cdots, x_{n-1}$. The substitution $x_{n+1} = x_{n-1}$ gives that $\bar{p}$ depends on x_n. Setting $x_1 = x_2 = \cdots = x_{n-1}$ in $\bar{p}$ (observe that $p(x_1, \cdots, x_1, x_{n-1}, x_n) = x_1$ by assumption) yields $g(x_1, x_{n-1}, x_n, x_{n+1})$, hence $\bar{p}$ depends on x_{n+1}.

Case 2. Use the substitutions

$$x_{n+1} = x_1,\ x_{n+1} = x_n, \quad \text{and} \quad x_1 = \cdots = x_{n-2}\ .$$

Case 3. Use the substitutions

$$x_{n+1} = x_1,\ x_{n+1} = x_{n-1}, \quad \text{and} \quad x_1 = \cdots = x_{n-2}\ .$$

Case 4. Just as in the previous cases,

$$x_{n+1} = x_n \quad \text{and} \quad x_{n+1} = x_{n-1}$$

establish that $\bar{p}$ depends on $x_1, \cdots, x_n$. Setting $x_1 = \cdots = x_{n-2}$ in $\bar{p}$ we get $h = g(x_1, x_{n-1}, x_n, x_{n+1}) + x_{n-1} + x_n$. Observe that $h + x_{n-1} + x_n = g(x_1, x_{n-1}, x_n, x_{n+1})$ depends on x_{n+1}, therefore so does h. Thus $\bar{p}$ depends on x_{n+1}.

Proof of (ii). Set $A_1 = \{n - 1, n, n + 1\}$, $A_2 = \{1, n, n + 1\}$, $A_3 = \{1, n - 1, n + 1\}$, and $A_4 = \{n - 1, n, n + 1\}$. If p belongs to Case i and $k, l \in A_i$, $k \neq l$, then $x_k = x_l$ substituted into $\bar{p}$ yields p. Observe that $|A_i \cap A_j| \geqq 2$ for $1 \leqq i, j \leqq 4$. Now if $\bar{p} = \bar{q}$, p belongs to Case i, q to Case j, then we can choose $k, l \in A_i \cap A_j$, $k \neq l$. Substituting $x_k = x_l$ into $\bar{p} = \bar{q}$ gives $p = q$.

Proof of (iii). For $n = 4$, $g_4(x_1, x_1, x_3, x_4) = g_n(x_1, x_2, x_3, x_3) = x_1$, since $g_4 = g$ is a first projection polynomial. Assuming the identities for n, we compute:

$$g_{n+1}(x_1, \cdots, x_1, x_n, x_{n+1}) = g(g_n(x_1, \cdots, x_1, x_n), x_1, x_1, x_{n+1}) = x_1$$

and

$$g_{n+1}(x_1, x_2, x_3, \cdots, x_3) = g(g_n(x_1, x_2, x_3, \cdots, x_3), x_2, x_3, x_3) = x_1\ .$$

Proof of (iv). $g_4 = g$ so the statement is true for $n = 4$. Assume it for n. Substituting $x_{n+1} = x_2$ or $x_{n+1} = x_3$ into g_{n+1} yields g_n, hence

g_{n+1} depends on $x_1, \cdots, x_n$. Substituting $x_3 = x_4 = \cdots = x_n$ into g_{n+1} gives by (iii) $g(g_n(x_1, x_2, x_3, \cdots, x_3), x_2, x_3, x_{n+1}) = g(x_1, x_2, x_3, x_{n+1})$, hence g_{n+1} depends on x_{n+1}.

Proof of (v). Observe that $g_{n+1}(x_1, x_2, x_2, x_4, \cdots, x_{n+1}) = x_1$. Hence, if $g_{n+1} = \bar{p}$, then $\bar{p}(x_1, x_2, x_2, x_4, \cdots, x_{n+1}) = x_1$. Further substituting $x_{n+1} = x_n$ or (Case 3) $x_{n+1} = x_{n-1}$, we conclude that

$$p(x_1, x_2, x_2, x_4, \cdots, x_n) = x_1 .$$

This is impossible if p belongs to Cases 2 or 3, and it immediately yields a contradiction in Case 1 (namely, $x_1 = g(x_1, x_{n-1}, x_n, x_{n+1})$) and in Case 4.

REFERENCES

1. R. D. Carmichael, *Groups of Finite Order*, Dover Publ. Inc. 1956.
2. G. Grätzer, *Universal Algebra*, The University Series in Higher Mathematics. D. Van Nostrand Co., Princeton, N. J., 1968.
3. ———, *Composition of Functions*, Proceedings of the Conference on Universal Algebra, October 1969. Queen's Papers in Pure and Applied Mathematics, No. 25, Queen's University, Kingston, Ont., 1970.
4. G. Grätzer and J. Płonka, *On the number of polynomials of an idempotent algebra. I*, Pacific J. Math., **32** (1970), 697-709.
5. C. Treash, *The Completion of Finite Incomplete Steiner Triple Systems with Applications to Loop Theory.*
6. K. Urbanik, *On algebraic operations in idempotent algebras*, Colloq. Math., **13** (1965), 129-157.

Received May 6, 1972. The work of both authors was supported by the National Research Council of Canada.

THE UNIVERSITY OF MANITOBA,
AND
THE MATHEMATICAL RESEARCH INSTITUTE OF THE POLISH ACADEMY OF SCIENCES,
WROCLAW, POLAND