

ON THE NUMBER OF OPERATIONS IN A CLONE

JOEL BERMAN AND ANDRZEJ KISIELEWICZ

(Communicated by Jeffrey N. Kahn)

ABSTRACT. A clone C on a set A is a set of operations on A containing the projection operations and closed under composition. A combinatorial invariant of a clone is its p_n -sequence $(p_0(C), p_1(C), \dots)$, where $p_n(C)$ is the number of essentially n -ary operations in C . We investigate the links between this invariant and structural properties of clones. It has been conjectured that the p_n -sequence of a clone on a finite set is either eventually strictly increasing or is bounded above by a finite constant. We verify this conjecture for a large family of clones. A special role in our work is played by totally symmetric operations and totally symmetric clones. We show that every totally symmetric clone on a finite set has a bounded p_n -sequence and that it is decidable if a clone is totally symmetric.

1. INTRODUCTION

A clone on a nonvoid set A is a set of operations on A that contains all the projection operations and is closed under composition. Clones are common structures that appear in various contexts in discrete mathematics and algebra, e.g., the survey paper by Rosenberg [R] and the monograph by Szendrei [S] give some indication of the role of clones within these areas. An operation $f(x_1, \dots, x_n)$ on A is said to *depend on the variable* x_i if there exist a_1, \dots, a_n, b in A such that

$$f(a_1, \dots, a_n) \neq f(a_1, \dots, a_{i-1}, b, a_{i+1}, \dots, a_n).$$

An n -ary operation f is called *essentially n -ary* (or *essential*) if it depends on all n of its variables. For a clone C we denote by $E_n(C)$ the set of all essentially n -ary operations in C . By $E_0(C)$ we denote the set of constant unary operations in C . We follow the notation in [G] and write $p_n(C)$ for $|E_n(C)|$, and call the sequence of cardinals $\langle p_n(C) \rangle$ the p_n -sequence of the clone C . The essential operations in a clone determine the entire clone since any other operation in the clone can be obtained by adding one or more fictitious (i.e., not essential) variables to an essential operation. The p_n -sequence of a clone may therefore be viewed as an indication of the size of the clone. Our

Received by the editors July 11, 1990 and, in revised form, January 19, 1993.

1991 *Mathematics Subject Classification*. Primary 08A40, 08B20.

This work was done while the second author was visiting Professor George Grätzer at the University of Manitoba.

paper investigates a general conjecture that the p_n -sequence of a clone on a finite set is eventually strictly increasing or is bounded above by a finite constant.

An algebra $\mathbf{A} = \langle A, F \rangle$ consists of a nonvoid set A , called the universe of \mathbf{A} , together with a set F of operations on A . The smallest clone on A that contains F is denoted $\text{Clo } \mathbf{A}$ and an element of $\text{Clo } \mathbf{A}$ is called a *term operation* of \mathbf{A} . We write $E_n(\mathbf{A})$ for the essentially n -ary term operations of the algebra \mathbf{A} and we denote $|E_n(\mathbf{A})|$ by $p_n(\mathbf{A})$. Note that every clone C on a set A is the clone of all term operations of an algebra with universe A , for example, $C = \text{Clo}\langle A, C \rangle$. So without loss of generality we can restrict ourselves to clones of algebras.

The sequence $p_n(\mathbf{A})$ determines many algebraic properties of the algebra \mathbf{A} . In particular, it determines the cardinality of the free algebras in the equational class V generated by the algebra \mathbf{A} . Finitely generated algebras in V are all finite if and only if $p_n(\mathbf{A})$ is finite for all n . In this case the equational class V and the algebra \mathbf{A} are called *locally finite*. Of course, every finite algebra (i.e., with finite universe) is locally finite. An algebra \mathbf{A} is *idempotent* if every subalgebra of \mathbf{A} generated by a single element is a one-element algebra, and for nontrivial algebras this is equivalent to the condition that $p_0 = 0$ and $p_1 = 1$. For these and other less straightforward connections between the numerical properties of p_n -sequences and algebraic properties of algebras consult [B1, HM, T].

The following conjecture is presented in [GP]: Let \mathbf{A} be an idempotent algebra that is different from the idempotent reduct of a Boolean group (Example 2.2, below). Then there exists an integer m such that $p_n(\mathbf{A}) < p_{n+1}(\mathbf{A})$ whenever $n > m$ and $1 < p_n(\mathbf{A}) < \omega$. This conjecture was settled in the affirmative in [Ki, Ki1]. In particular, if an idempotent algebra \mathbf{A} is locally finite, then there exists an integer m such that for all $n > m$, $p_n(\mathbf{A}) < p_{n+1}(\mathbf{A})$ or for all $n > m$, $p_n(\mathbf{A}) \leq 1$, i.e., the p_n -sequence of \mathbf{A} is either eventually strictly increasing or is eventually bounded by the constant 1. This result in [Ki] and some other results concerning finite algebras prompted the following conjecture in [B]: If $\mathbf{A} = \langle A, F \rangle$ is a finite algebra, then the sequence $p_n(\mathbf{A})$ is either eventually strictly increasing or is bounded above by a finite constant. We verify this conjecture in the case that the algebra has a binary term operation that is strongly onto (Definition 3.1). As we point out in §3, the class of algebras having a strongly onto binary term operation is fairly robust and includes many familiar algebras.

A special role in our paper is played by totally symmetric algebras. Let $f(x_1, \dots, x_n)$ be an n -ary operation on a set A . A permutation σ of $\{1, \dots, n\}$ is said to *preserve* f if $f(x_1, \dots, x_n) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$. The group of all permutations of $\{1, \dots, n\}$ that preserve f is denoted $G(f)$. An n -ary operation is called *totally symmetric* if $G(f)$ is the full symmetric group on $\{1, \dots, n\}$. Note that if an n -ary operation is totally symmetric, then either it is a constant operation or it depends on all n of its variables. An algebra \mathbf{A} is called *totally symmetric* if every f in every $E_n(\mathbf{A})$ is totally symmetric. In §2 we show that if \mathbf{A} is a finite algebra that is totally symmetric, then $p_n(\mathbf{A}) \leq |A|^{2^{|A|}}$. The hypothesis that the algebra be finite is crucial here since [GPS] contains a construction that shows, for any sequence of cardinals $\bar{c} = \langle c_0, c_1, \dots \rangle$ with $c_0 > 0$ and $c_1 > 0$, there is a totally symmetric algebra

whose p_n -sequence is \bar{c} . In §2 we also show that a k -element algebra is totally symmetric provided every essentially n -ary term operation for $n \leq k + 3$ is totally symmetric. It follows that there is an algorithm to decide if a finite set of operations on a finite set generates a totally symmetric clone.

In §3 we investigate algebras that possess a strongly onto term operation. Our main result is that if A is a finite algebra having a binary term operation that is strongly onto, then either $p_n(A)$ is strictly increasing for all $n \geq |A| + 2$ or A is totally symmetric.

We use the following notation and terminology. Let A be a nonvoid set and let $\bar{a} = (a_1, \dots, a_n) \in A^n$. Then $\text{supp}(\bar{a}) = \{a_i: 1 \leq i \leq n\}$ and for b in A , $\text{wt}(b, \bar{a}) = |\{i: a_i = b, 1 \leq i \leq n\}|$. We let $\text{oddsupp}(\bar{a}) = \{a_i: \text{wt}(a_i, \bar{a}) \text{ is odd}\}$. An n -ary operation f on A is called onto if for every b in A there is an \bar{a} such that $f(\bar{a}) = b$. For an algebra A , the n -ary term operations of A are denoted by $\text{Clo}_n A$.

Additional background on clones and algebras can be found in [MMT, S]. The papers [G, GK] survey the literature of p_n -sequences. Totally symmetric operations on a finite set A have been the focus of much research. We mention the texts [H, W] for the case $|A| = 2$ and [DDT] for the general case. The survey paper [SM] contains a bibliography of over 200 items pertaining to totally symmetric operations. However, since the composition of totally symmetric operations need not be totally symmetric, there is little in the literature on the general study of clones that have only totally symmetric essential operations.

2. TOTALLY SYMMETRIC ALGEBRAS

We first motivate our results by some examples of totally symmetric algebras. Examples 2.1 and 2.2 are from [U] and Example 2.3 is from [DK].

Example 2.1. Let $S = \langle S, \wedge \rangle$ be a nontrivial semilattice. It is known that

$$E_n(S) = \{x_1 \wedge \dots \wedge x_n\}$$

so $p_n = 1$ for all $n \geq 1$. More generally, let $U = \{c_1, \dots, c_m\}$ be any finite subuniverse of S and consider $S_U = \langle S, \wedge, c_1, \dots, c_m \rangle$ in which each c_i denotes a constant term operation. For S_U we have $p_0 = m$, and for $n > 0$ the value of p_n is m or $m+1$ depending on whether or not $\bigwedge S \in U$. We note that if $f(x_1, \dots, x_n) \in E_n(S_U)$, then $f(x_1, \dots, x_{n-2}, x_{n-1}, x_{n-1}) \in E_{n-1}(S_U)$.

Example 2.2. Let $G = \langle G, +, 0 \rangle$ be a Boolean group, i.e., a group satisfying the identity $x+x=0$. The algebra $M = \langle G, x+y+z \rangle$ has $p_n = 0$ for n even and $p_n = 1$ for n odd. The algebra M is called the idempotent reduct of G , i.e., $\text{Clo} M$ consists of all idempotent term operations of G . If H is a finite subuniverse of G and if M_H is the algebra $\langle G, c+x+y+z \rangle_{c \in H}$, then $p_n = 0$ for n even and $p_n = |H|$ for n odd. In contrast to Example 2.1 we note that if $f(x_1, \dots, x_n) \in E_n(M_H)$, then $f(x_1, \dots, x_{n-2}, x_{n-1}, x_{n-1}) \in E_{n-2}(M_H)$.

Example 2.3. In [DK] it is shown that if a semigroup $S = \langle S, \cdot \rangle$ satisfies $f(x_1, x_2) = f(x_2, x_1)$ for all $f \in E_2(S)$, then S is totally symmetric. A complete characterization of the equational classes of totally symmetric semigroups is given in [DK] and the p_n -sequence for each such equational class is provided. For each equational class of totally symmetric semigroups there exists an integer m such that for all $n \geq m$ either $p_n = 1$ or for all $n \geq m$, $p_n = 0$.

Example 2.4. It is possible to describe all totally symmetric clones on a two-element set. Let $A = \{0, 1\}$ and let $x_1 \wedge x_2 = \min\{x_1, x_2\}$, $x_1 \vee x_2 = \max\{x_1, x_2\}$ and $x_1 \oplus x_2 = x_1 + x_2 \pmod{2}$. Each of the three clones on A generated by the two constant operations together with one of \wedge , \vee , or \oplus is totally symmetric as are all subclones of these three clones. These are the only totally symmetric clones on A since from Post’s classification [P] (e.g., [S] or [R]) any other clone on A contains at least one of the ternary operations $x_1 \wedge (x_2 \vee x_3)$, $x_1 \vee (x_2 \wedge x_3)$, or $(x_1 \wedge x_2) \vee (x_1 \wedge x_3) \vee (x_2 \wedge x_3)$. Each of these operations generates a clone that is not totally symmetric. Note that in the clone generated by $(x_1 \wedge x_2) \vee (x_1 \wedge x_3) \vee (x_2 \wedge x_3)$ every essentially m -ary operation, for $m \leq 3$, is totally symmetric.

In [Ko] there is a construction for every positive integer m , of an $(m + 2)$ -element idempotent algebra \mathbf{A}_m , for which $p_n(\mathbf{A}_m) = 1$ for $n \leq m$ and $p_{n+1}(\mathbf{A}_m) > p_n(\mathbf{A}_m)$ for $n \geq m$. So every $f \in E_n(\mathbf{A}_m)$ is totally symmetric for $n \leq m$. However, the algebra \mathbf{A}_m is not totally symmetric as the next lemma shows.

Lemma 2.5. *Let \mathbf{A} be a finite algebra of cardinality k . Suppose $n > 1$ and that $E_n(\mathbf{A})$ and $E_{n-1}(\mathbf{A})$ contain only totally symmetric terms. Then $|E_n(\mathbf{A})| \leq k^{2^k}$.*

Proof. We may assume $k \geq 2$ and that $A = \{1, \dots, k\}$. We first let $n \geq 3$ and we consider an arbitrary $f(x_1, \dots, x_n) \in E_n(\mathbf{A})$. Let $g(x_1, \dots, x_{n-1})$ denote the term obtained from f by replacing x_n by x_{n-1} , i.e., $f(x_1, \dots, x_{n-2}, x_{n-1}, x_{n-1})$.

Case 1. g depends on all $n - 1$ of its variables: By hypothesis $g \in E_{n-1}(\mathbf{A})$ is totally symmetric so $g(x_1, \dots, x_{n-2}, x_{n-1}) = g(x_1, \dots, x_{n-1}, x_{n-2})$ and hence

$$\begin{aligned} f(x_1, \dots, x_{n-2}, x_{n-1}, x_{n-1}) &= f(x_1, \dots, x_{n-1}, x_{n-2}, x_{n-2}) \\ &= f(x_1, \dots, x_{n-2}, x_{n-2}, x_{n-1}). \end{aligned}$$

For $\bar{u} \in A^n$ and $a, b \in \text{supp}(\bar{u})$ with $\text{wt}(a, \bar{u}) \geq 2$, if \bar{v} is obtained from \bar{u} by replacing one instance of a by b , then $f(\bar{u}) = f(\bar{v})$ since f is totally symmetric and $f(x_1, \dots, x_{n-2}, x_{n-1}, x_{n-1}) = f(x_1, \dots, x_{n-2}, x_{n-2}, x_{n-1})$. From this it follows that if $\text{supp}(\bar{u}) = \{a_1, \dots, a_m\}$ with $a_1 < a_2 < \dots < a_m$, then for $\bar{w} = (a_1, a_2, \dots, a_m, a_m, \dots, a_m) \in A^n$, we have $f(\bar{u}) = f(\bar{w})$, i.e., $f(\bar{u})$ is determined by $\text{supp}(\bar{u})$. So the number of $f \in E_n(\mathbf{A})$ for which g depends on all $n - 1$ of its variables is bounded above by $k^{2^{k-1}}$.

Case 2. $g(x_1, \dots, x_{n-1})$ does not depend on x_{n-1} : In this case $f(\bar{u}, a, a) = f(\bar{u}, b, b)$ for all $\bar{u} \in A^{n-2}$ and all $a, b \in A$. From the total symmetry of f we see that for every $\bar{v} \in A^n$ the value of $f(\bar{v})$ is completely determined by $\text{oddsupp}(\bar{v})$. For every n and every $\bar{v} \in A^n$ the parity of n is always the same as the parity of the cardinality of $\text{oddsupp}(\bar{v})$. So for a given n there are at most 2^{k-1} possible choices for $\text{oddsupp}(\bar{v})$. Therefore the number of $f \in E_n(\mathbf{A})$ for which g does not depend on x_{n-1} is bounded above by $k^{2^{k-1}}$, which is less than k^{2^k-1} .

Case 3. $g(x_1, \dots, x_{n-1})$ depends on x_{n-1} but does not depend on at least one x_i , $1 \leq i \leq n - 2$: In this case g must depend only on x_{n-1} since f is totally symmetric. So $f(x_1, \dots, x_{n-2}, x_{n-1}, x_{n-1}) = h(x_{n-1})$ for a unary term operation h . If $n \geq 4$, then let $a \neq b$ in A and $\bar{c} \in A^{n-4}$ and consider

$\bar{u} = (\bar{c}, a, a, b, b)$. Let $\bar{v} = (\bar{c}, b, b, a, a)$. We have $h(b) = f(\bar{u}) = f(\bar{v}) = h(a)$. This shows h is a constant function, contradicting the assumption that g depends on x_{n-1} . So for $n \geq 4$, Case 3 is vacuous. For $n = 3$ each f is determined by h and $f(a, b, c)$ for $a < b < c$. So the contribution of Case 3 for $n = 3$ is at most $k^{k+\binom{k}{3}}$.

For $n \geq 4$ the first two cases contribute at most $2k^{2^k-1}$ to $|E_n(\mathbf{A})|$ and this is less than k^{2^k} for $k \geq 2$. For $n = 2$, there are $k^{k(k+1)/2}$ totally symmetric binary operations on A and this value is less than k^{2^k} for all k . For $n = 3$, the three cases contribute $2k^{2^k-1} + k^{k+\binom{k}{3}}$, which is less than k^{2^k} for $k \geq 3$. For $n = 3$ and $k = 2$ an examination of all the possible two-element algebras completes the proof.

In the proof of Lemma 2.5, Case 1 and Case 2 are illustrated by Examples 2.1 and 2.2, respectively.

Corollary 2.6. *If \mathbf{A} is a totally symmetric algebra of cardinality k , then $p_n(\mathbf{A}) \leq k^{2^k}$ for all n .*

Another upper bound for $p_n(\mathbf{A})$ is given in Theorem 2.8.

Lemma 2.7. *Let \mathbf{A} be a finite, totally symmetric algebra and let $f \in E_n(\mathbf{A})$ with $n > |A|$. If $g(x_1, \dots, x_{n-1})$ denotes $f(x_1, x_2, \dots, x_{n-2}, x_{n-1}, x_{n-1})$, then g depends on all of x_1, \dots, x_{n-2} , and*

- (i) g depends on x_{n-1} if and only if for all $\bar{v} \in A^n$, $f(\bar{v})$ is determined by $\text{supp}(\bar{v})$;
- (ii) g does not depend on x_{n-1} if and only if for all $\bar{v} \in A^n$, $f(\bar{v})$ is determined by $\text{oddsupp}(\bar{v})$.

Proof. If $|A| = 2$ then the remarks in Example 2.4 suffice. So we assume $n > |A| \geq 3$. The argument in Lemma 2.5 applies. Case 3 in that argument does not hold for f so either g depends on all its variables (Case 1) or g does not depend on x_{n-1} (Case 2). If g does not depend on x_i , for an $i < n - 1$, then g depends on no variable, since f is totally symmetric. Thus g is a constant, say c . Since $n > |A|$, every $\bar{v} \in A^n$ has at least one repeated coordinate. Thus $f(\bar{v}) = c$ by the total symmetry of f . This contradicts $f \in E_n(\mathbf{A})$, and hence g depends on every x_i , $1 \leq i \leq n - 2$. One direction of (i) and (ii) is contained in the proof of Case 1 and Case 2 of Lemma 2.5. For the other direction it suffices to show that no $f \in E_n(\mathbf{A})$ has the property that for all $\bar{v} \in A^n$, the value $f(\bar{v})$ is determined by both $\text{supp}(\bar{v})$ and $\text{oddsupp}(\bar{v})$. This is true since $n > |A|$ so for every \bar{v} and $\bar{w} \in A^n$ there is a sequence $\bar{u}^0, \bar{u}^1, \dots, \bar{u}^m \in A^n$ such that $\bar{u}^0 = \bar{v}$, $\bar{u}^m = \bar{w}$ and for every $i = 1, \dots, m$ either $\text{supp}(\bar{u}^{i-1}) = \text{supp}(\bar{u}^i)$ or $\text{oddsupp}(\bar{u}^{i-1}) = \text{oddsupp}(\bar{u}^i)$.

Theorem 2.8. *Let \mathbf{A} be a finite totally symmetric algebra with $|A| = k$ and let $n > k$. If $n - k$ is odd, then $p_n(\mathbf{A}) \leq p_{k+1}(\mathbf{A})$ and if $n - k$ is even, then $p_n(\mathbf{A}) \leq p_{k+2}(\mathbf{A})$.*

Proof. For $k = 2$ the result is true by inspection of the algebras in Example 2.4. We may assume $n > k \geq 3$ and that Lemma 2.7 applies. We say $f \in E_n(\mathbf{A})$ is of type i if (i) of Lemma 2.7 holds, and f is of type ii, otherwise.

Let $n - k$ be odd. Define $\mu f \in \text{Clo}_{k+1} \mathbf{A}$ by

$$(\mu f)(x_1, \dots, x_{k+1}) = f(x_1, x_2, \dots, x_k, x_{k+1}, \dots, x_{k+1}).$$

Note that every variable appears an odd number of times in $f(x_1, x_2, \dots, x_k, x_{k+1}, \dots, x_{k+1})$. Hence $\mu f \in E_{k+1}(\mathbf{A})$. We show μ is one-to-one. We see that μf is of type i if and only if $(\mu f)(x_1, x_2, \dots, x_k, x_k)$ depends on x_k if and only if $f(x_1, x_2, \dots, x_{k-1}, x_k, \dots, x_k)$ depends on x_k if and only if f is of type i. So f and μf are always of the same type. Let $f \neq g$ in $E_n(\mathbf{A})$. If f and g are of different types then μf and μg are also of different types, so $\mu f \neq \mu g$. We may assume f and g are both of type i or both of type ii. Let $\bar{u} \in A^n$ with $f(\bar{u}) \neq g(\bar{u})$. If f and g are both of type i, then let $\{b_1, \dots, b_m\} = \text{supp}(\bar{u})$. Consider $\bar{u}' = (b_1, b_2, \dots, b_{m-1}, b_m, \dots, b_m) \in A^n$ and $\bar{u}'' = (b_1, b_2, \dots, b_{m-1}, b_m, \dots, b_m) \in A^{k+1}$. Then $f(\bar{u}) = f(\bar{u}') = (\mu f)(\bar{u}'')$; so \bar{u}'' witnesses $\mu f \neq \mu g$. If f and g are both of type ii, then let $\{b_1, \dots, b_m\} = \text{oddsupp}(\bar{u})$. Consider $\bar{u}' = (b_1, b_2, \dots, b_{m-1}, b_m, \dots, b_m) \in A^n$ and $\bar{u}'' = (b_1, b_2, \dots, b_{m-1}, b_m, \dots, b_m) \in A^{k+1}$. Since m is the cardinality of $\text{oddsupp}(\bar{u})$, the difference $n - m$ is even. Hence b_m appears an odd number of times in \bar{u}' . Since $n - k$ is odd, we have $f(\bar{u}) = f(\bar{u}') = (\mu f)(\bar{u}'')$ and again \bar{u}'' witnesses that $\mu f \neq \mu g$.

If $n - k$ is even then a similar argument applies with

$$\mu f = f(x_1, x_2, \dots, x_k, x_{k+1}, x_{k+2}, \dots, x_{k+2}).$$

As we already remarked, the composition of totally symmetric operations need not be totally symmetric. In contrast to the bound obtained in Corollary 2.6 the next result shows that the number of totally symmetric n -ary operations grows exponentially as n increases.

Proposition 2.9 (see, e.g., [LL]). *The number of totally symmetric n -ary operations on a k -element set is $k^{\binom{k+n-1}{k-1}}$.*

Proof. Let $A = \{1, \dots, k\}$ and consider $n > 0$. Define an equivalence relation \sim on A^n by $\bar{u} \sim \bar{v}$ if and only if $\text{wt}(b, \bar{u}) = \text{wt}(b, \bar{v})$ for all $b \in A$. It is easily verified that $f: A^n \rightarrow A$ is totally symmetric if and only if f is constant on each equivalence class of \sim . There exists a bijection between the equivalence classes of \sim and the set of all k -tuples of nonnegative integers (n_1, \dots, n_k) with $\sum n_i = n$, given by $\bar{a}/\sim \mapsto (\text{wt}(1, \bar{a}), \dots, \text{wt}(k, \bar{a}))$ for every $\bar{a} \in A^n$. A standard combinational result states that there are $\binom{k+n-1}{k-1}$ such k -tuples.

Each totally symmetric algebra \mathbf{A} described in Examples 2.1, 2.2, 2.3, and 2.4 has a p_n -sequence that is eventually bounded by $|A|$. The bound given in Corollary 2.6 is $|A|^{2^{|A|}}$. We do not know if there exists a finite totally symmetric algebra whose p_n -sequence realizes the bound in Corollary 2.6. Our final example in this section provides an example of a finite totally symmetric algebra with a p_n -sequence that is close to the bound in Corollary 2.6.

Example 2.10. Let $1 < r < k$ be arbitrary integers and let $A = \{1, \dots, k\}$. For each $n > 0$ let F_n denote the set of all n -ary operations f on A such that for every $\bar{a} \in A^n$, $f(\bar{a}) \leq r$ and $f(\bar{a})$ is uniquely determined by $\text{supp}(\bar{a}) \cap \{r + 1, \dots, k\}$. Every member of F_n is totally symmetric and $|F_n| = r^{2^{k-r}}$, for $n \geq k - r$. For $f \in F_n$ and $g \in F_m$ the operation $f(x_1, \dots, x_{n-1}, g(x_n, \dots, x_{n+m-1}))$ does not depend on x_j for $j \geq n$. Let $F = \bigcup_{n \geq 1} F_n$ and let $\mathbf{A} = \langle A, F \rangle$. Then for $n \geq 1$, $E_n(\mathbf{A})$ consists of the nonconstant members of F_n so $p_n(\mathbf{A}) = r^{2^{k-r}} - r$, for $n \geq k - r$.

We conclude this section by showing that a finite algebra A is totally symmetric if and only if for every $m < |A| + 4$ every essentially m -ary term operation of A is totally symmetric. Thus there is an algorithm to decide if a finite set of operations on a finite set A generates a totally symmetric clone on A , since for any m the set of all m -ary operations on A generated by a given finite set of operations is readily computable.

Lemma 2.11. *Let A be a finite algebra, $|A| = k$. Let $n \geq k + 4$ and suppose that for every $m < n$ all members of $E_m(A)$ are totally symmetric. If $f(y, z, x_1, \dots, x_{n-2}) \in E_n(A)$ and if $1 \leq r \leq n - 2$, then there exists $s \neq r$, $1 \leq s \leq n - 2$, such that the term operation obtained from f by replacing x_r by x_s depends on z . A similar statement is true for y as well.*

Proof. If A is trivial, then there is nothing to prove, so we assume $k \geq 2$. For $1 \leq i, j \leq n - 2$ let f^{ij} denote the $(n - 1)$ -ary term operation obtained from f by replacing x_j by x_i . There exist $a, b, b' \in A$ and $\bar{c} \in A^{n-2}$ such that $f(a, b, \bar{c}) \neq f(a, b', \bar{c})$. It suffices to show that \bar{c} can be chosen so that $c_r = c_s$ for an $s \neq r$. Since $n - 2 \geq k + 2$ there exists $i \neq j$ with $c_i = c_j$. If $r \in \{i, j\}$ we are done. If f^{ij} does not depend on x_r , then we can replace c_r by c_i , say, and we are done. If f^{ij} does not depend on an x_s for $s \neq r$, then we can replace c_s by c_r . Therefore, we may assume f^{ij} depends on all x_s , $s \notin \{i, j\}$, and that f^{ij} is totally symmetric with respect to all these variables. Let $1 \leq s, t \leq n - 2$ be such that $c_s = c_t$ and $\{s, t\} \neq \{i, j\}$ with, say, $t \notin \{i, j\}$. We have $n - 2 \geq k + 2$ and $k + 2 \geq 4$, so such a choice is possible. Let \bar{d} be obtained from \bar{c} by interchanging c_r and c_t . Then $f(a, b, \bar{c}) = f(a, b, \bar{d})$ and $f(a, b', \bar{c}) = f(a, b', \bar{d})$, which shows that f^{rs} depends on z .

Theorem 2.12. *If A is a k -element algebra such that, for every $m < k + 4$, all members of $E_m(A)$ are totally symmetric, then A is totally symmetric.*

Proof. If $k = 1$ the claim is immediate and if $k = 2$ the remarks in Example 2.4 suffice. So we assume $k \geq 3$. We induct on n for $n \geq k + 4$. So assume that for all $m < n$ every member of $E_m(A)$ is totally symmetric. We prove that every $f \in E_n(A)$ is totally symmetric. Let $f \in E_n(A)$ and $\bar{c} \in A^{n-2}$ be arbitrary. It suffices to show that $f(y, z, \bar{c}) = f(z, y, \bar{c})$. We write f as $f(y, z, x_1, \dots, x_{n-2})$ and we denote $f(y, z, \bar{c})$ by $g(y, z)$. The $(n - 1)$ -ary term operation obtained from f by replacing x_j by x_i is denoted f^{ij} . By the induction hypothesis f^{ij} is totally symmetric in all of its essential variables.

If $g(y, z)$ depends on neither y nor z , then we are done since $g(y, z) = g(z, y)$. So we may assume that g depends on at least one of its variables. Suppose $1 \leq i < j \leq n - 2$ and $c_i = c_j$. Note that if f^{ij} does not depend on y then g does not either. A similar remark holds for z . If f^{ij} depends on both y and z , then $g(y, z) = g(z, y)$ and we are done. So suppose f^{ij} depends on y and not z . In this case g depends on y and not z , as well. Moreover, by a similar argument, we may assume this is true for any f^{ij} provided there is a \bar{d} with $d_i = d_j$ such that $g(y, z) = f(y, z, \bar{d})$ for all y and z . We show this leads to a contradiction.

First suppose $c_i = c_j$ and there is an r , $1 \leq r \leq n - 2$, $r \neq i, j$, such that f^{ij} does not depend on x_r . We apply Lemma 2.11 to f and r to find an index s such that the term operation f^{rs} depends on z . (Note that $s \in \{i, j\}$

is possible.) Let $\bar{d} \in A^{n-2}$ be obtained from \bar{c} by replacing c_r by c_s . Then $g(y, z) = f(y, z, \bar{c}) = f(y, z, \bar{d})$. Since $d_r = d_s$ we see that f^{rs} depends on y and not z , but this contradicts the choice of s . So we conclude that f^{ij} depends on all $x_r, r \neq i, j$.

We next apply Lemma 2.11 to find an index s for which f^{is} depends on z . We complete the proof by showing no such s exists. From the remarks above we cannot have $c_i = c_s$ else f^{is} would depend on y and not z . So $s \notin \{i, j\}$. We choose indices u and w so that $c_u = c_w$ and $j \notin \{u, w\}$. Since $n - 2 \geq k + 2 \geq 5$ this is possible. If $s \in \{u, w\}$, with $s = w$ say, then choose $t \notin \{i, j, u, w\}$. Use the induction hypothesis on f^{ij} to interchange x_t and x_w . Let $\bar{d} \in A^{n-2}$ be obtained from \bar{c} by interchanging c_t and c_w . Then $g(y, z) = f(y, z, \bar{d})$, $d_i = d_j$, $d_u = d_t$, and $s \notin \{i, j, u, t\}$. So we may as well assume $s \notin \{i, j, u, w\}$, $c_i = c_j$, and $c_u = c_w$ at the outset. Let \bar{e} be obtained from \bar{c} by interchanging c_j and c_s . Note $g(y, z) = f(y, z, \bar{c}) = f(y, z, \bar{e})$. From $e_i = e_s$ we see that f^{is} depends on y and not z , but this contradicts our original choice of s .

3. STRICTLY INCREASING p_n -SEQUENCES

In this section we define strongly onto binary operations and we show that if a finite algebra A has a strongly onto term operation and if A is not totally symmetric, then there exists an m such that the sequence $p_n(A)$ is strictly increasing for $n > m$.

Definition 3.1. A binary operation $x \cdot y$ on a set A is *strongly onto* if both of the following conditions hold for the elements of A :

(C1) $\forall a \exists b_1, b_2 (a = b_1 b_2 = b_2 b_1)$.

(C2) $\forall a, b (\exists c, d_1, d_2 (a = c d_1 \text{ and } b = c d_2) \text{ if and only if } \exists d, c_1, c_2 (a = c_1 d \text{ and } b = c_2 d))$.

Strongly onto binary operations occur frequently as the term operations of algebras. Any commutative binary operation that is onto is strongly onto. Every binary operation on A that has an identity element e (i.e., $a = ae = ea$ for all $a \in A$) is strongly onto. Thus groups, rings, lattices, and monoids all have strongly onto binary term operations.

The main result in [GP] is that if an idempotent algebra A has a commutative binary term operation, then $p_n(A) \neq 1$ implies $p_{n+1}(A) \geq p_n(A) + (n - 1)$. In particular, the p_n -sequence of A is strictly increasing. Note that every idempotent operation is onto, and hence the commutative operation in question is strongly onto.

Definition 3.2. Let h be a binary term operation on an algebra A . For $1 \leq n$ and $1 \leq i \leq n$ define the function $\lambda(h, n, i): E_n(A) \rightarrow \text{Clo}_{n+1} A$ by

$$f(x_1, \dots, x_n) \mapsto f(x_1, \dots, x_{i-1}, h(x_{n+1}, x_i), x_{i+1}, \dots, x_n).$$

If h and n are clear from the context we write λ_i instead of $\lambda(h, n, i)$. The definition of $\rho(h, n, i)$ is analogous, using $h(x_i, x_{n+1})$ in place of $h(x_{n+1}, x_i)$.

In the literature on the p_n -sequences of idempotent algebras, the λ_i and ρ_i have been used in various ways. For example, the function $\rho(h, n, i)$ appears in §3 of [GP] for a term operation h that is commutative and associative in an idempotent algebra.

We collect in the next lemma some facts about $\lambda(h, n, i)$ and $\rho(h, n, i)$ for arbitrary algebras in which h is strongly onto.

Lemma 3.3. *Let h be a strongly onto, binary term operation in an algebra \mathbf{A} . Let $1 \leq i \leq n$ be arbitrary and let λ_i and ρ_i denote $\lambda(h, n, i)$ and $\rho(h, n, i)$, respectively. All of the following are true:*

- (i) *The functions λ_i and ρ_i are one-to-one from $E_n(\mathbf{A})$ to $E_{n+1}(\mathbf{A})$.*
- (ii) *For all $f, g \in E_n(\mathbf{A})$, if $\lambda_i(f) = \rho_i(g)$, then $f = g$.*
- (iii) *For $n \geq 3$, if $f \in E_n(\mathbf{A})$ is such that $\rho_n(f)$ and $\rho_1(f)$ are totally symmetric, then f is totally symmetric.*

Proof. For notational convenience we let $i = n$ and we denote $h(x, y)$ by xy . Let $f(x_1, \dots, x_n) \in E_n(\mathbf{A})$ be arbitrary. The term operation $\rho_n(f)$ depends on every x_i , $1 \leq i < n$, by virtue of condition (C1) of Definition 3.1. From condition (C2) we see that $\rho_n(f)$ depends on x_n if and only if it depends on x_{n+1} . So $\rho_n(f)$ either depends on both x_n and x_{n+1} or $\rho_n(f)$ depends on neither of these two variables. If $\rho_n(f)$ were to depend on neither x_n nor x_{n+1} , then for all $b_1, b_2, c_1, c_2 \in A$ and $\bar{a} \in A^{n-1}$ we would have $f(\bar{a}, b_1b_2) = f(\bar{a}, c_1c_2)$. This is impossible since f depends on x_n and for every $d \in A$ there exist $b_1, b_2 \in A$ such that $d = b_1b_2$. Hence $\rho_n(f)$ is in $E_{n+1}(\mathbf{A})$. Let $f, g \in E_n(\mathbf{A})$ and suppose $\bar{a} = (a_1, \dots, a_n) \in A^n$ is such that $f(\bar{a}) \neq g(\bar{a})$. There exist $b, c \in A$ such that $bc = a_n$ and thus $f(a_1, \dots, a_{n-1}, bc) \neq g(a_1, \dots, a_{n-1}, bc)$. Thus ρ_n is one-to-one. A similar argument that uses the full strength of condition (C1) shows $\rho_n(f) \neq \lambda_n(g)$.

In order to prove (iii), let $n \geq 3$ and assume $f \in E_n(\mathbf{A})$ is such that $\rho_n(f)$ and $\rho_1(f)$ are totally symmetric. So $\rho_n(f) = f(x_1, x_2, \dots, x_{n-1}, x_nx_{n+1}) = f(x_2, x_1, \dots, x_{n-1}, x_nx_{n+1})$. Since \cdot is onto it follows that the transposition $(1, 2)$ is in $G(f)$. Similarly, for every $1 \leq i < j < n$ the transposition $(i, j) \in G(f)$. The transpositions (i, n) for $i \geq 2$ are in $G(f)$ since $\rho_1(f)$ is totally symmetric. It follows that $G(f)$ contains all the transpositions.

Lemma 3.4. *Let \mathbf{A} be an algebra having a binary term operation that is strongly onto. If $n \geq 1$ is such that $|E_n(\mathbf{A})| = |E_{n+1}(\mathbf{A})| < \omega$, then every $g \in E_{n+1}(\mathbf{A})$ is totally symmetric.*

Proof. From Lemma 3.3(i) and the finiteness of $E_{n+1}(\mathbf{A})$ it follows that for every $g \in E_{n+1}(\mathbf{A})$ and for every $1 \leq i \leq n$, there exist $f_1, f_2 \in E_n(\mathbf{A})$ such that $g = \lambda_i(f_1) = \rho_i(f_2)$. Thus, for each i , $f_1 = f_2$ by Lemma 3.3(ii). So $G(g)$ contains all transpositions $(i, n+1)$, for $1 \leq i < n+1$, and hence $G(g)$ is the full symmetric group.

Lemma 3.5. *Let \cdot be an onto binary operation on a set A . If the operations $(x_1x_2)x_3$ and $x_1(x_2x_3)$ are totally symmetric, then \cdot is commutative and associative.*

Proof. From the total symmetry of $(x_1x_2)x_3$ and $x_1(x_2x_3)$ we see that $(x_1x_2)(x_3x_4) = (x_1(x_3x_4))x_2 = (x_3(x_1x_4))x_2 = (x_3x_2)(x_1x_4)$. By repeating this argument in order to interchange x_2 and x_4 we see that $(x_1x_2)(x_3x_4) = (x_3x_4)(x_1x_2)$. If $a, b \in A$ are arbitrary with $a = a_1a_2$ and $b = b_1b_2$, then we see that $ab = (a_1a_2)(b_1b_2) = (b_1b_2)(a_1a_2) = ba$. For associativity, we have by the total symmetry of $x_1(x_2x_3)$ and the commutativity of x_1x_2 , that $x_1(x_2x_3) = x_3(x_1x_2) = (x_1x_2)x_3$.

Theorem 3.6. *If \mathbf{A} is a locally finite algebra that has a strongly onto binary term operation, then $p_n(\mathbf{A})$ is monotonically nondecreasing for $n \geq 1$. Moreover, either \mathbf{A} is totally symmetric or there exists an $m \geq 1$ such that $p_{n+1}(\mathbf{A}) > p_n(\mathbf{A})$ for all $n \geq m$ and for every $1 \leq n \leq m$ every essentially n -ary term operation of \mathbf{A} is totally symmetric.*

Proof. The p_n -sequence of \mathbf{A} is monotonically nondecreasing for $n \geq 1$ by Lemma 3.3(i). Let $k \geq 2$ be such that $p_{k-1}(\mathbf{A}) = p_k(\mathbf{A})$. For every n with $3 \leq n$ and $n \leq k$ we have that every $f \in E_n(\mathbf{A})$ is totally symmetric by virtue of Lemmas 3.4 and 3.3(iii). We show that every member of $E_2(\mathbf{A})$ is totally symmetric. If $k = 2$, then it suffices to apply Lemma 3.4. Otherwise let $h(x_1, x_2)$ be a strongly onto term operation of \mathbf{A} . The term operations $\rho_2(h) = h(x_1, h(x_2, x_3))$ and $\rho_1(h) = h(h(x_1, x_3), x_2)$ are in $E_3(\mathbf{A})$ and are totally symmetric. From Lemma 3.5 it follows that h is commutative and associative. Let $f \in E_2(\mathbf{A})$ be arbitrary. Then $\rho_2(f) = f(x_1, h(x_2, x_3)) \in E_3(\mathbf{A})$ is totally symmetric. Thus

$$\begin{aligned} f(h(x_1, x_2), h(x_3, x_4)) &= f(x_4, h(x_3, h(x_1, x_2))) \\ &= f(x_4, h(x_2, h(x_1, x_3))) = f(x_2, h(x_4, h(x_1, x_3))) \\ &= f(x_2, h(x_1, h(x_3, x_4))) = f(h(x_3, x_4), h(x_1, x_2)). \end{aligned}$$

This shows f is commutative since h is onto A .

If there exist infinitely many k with $p_{k-1}(\mathbf{A}) = p_k(\mathbf{A})$, then \mathbf{A} is totally symmetric by the remarks in the previous paragraph. If there is at least one but only finitely many such k , then let m be the largest such. If there are no such k , then we let $m = 1$.

Now, combining Theorem 3.6 with the results of §2, we obtain the following result for finite algebras.

Corollary 3.7. *Let \mathbf{A} be a k -element algebra having a strongly onto binary term operation. Then either $p_{n+1}(\mathbf{A}) > p_n(\mathbf{A})$ for all $n \geq k + 2$ or \mathbf{A} is totally symmetric in which case $p_n(\mathbf{A}) \leq k^{2^k}$ for all n .*

Proof. If \mathbf{A} is totally symmetric, then the bound on $p_n(\mathbf{A})$ is from Corollary 2.6. If \mathbf{A} is not totally symmetric, then by Theorem 2.12 there is a $q \leq k + 3$ and an essentially q -ary operation that is not totally symmetric. Thus the m in Theorem 3.6 is less than $k + 3$.

In August, 1992, Ross Willard presented at the Alan Day Conference in Hamilton, Ontario, an example of a finite algebra \mathbf{A} for which $p_n(\mathbf{A})$ is neither bounded nor strictly increasing, thereby settling the conjecture in [B]. He also has proved that for any k -element algebra \mathbf{A} , either the sequence $p_n(\mathbf{A})$ is bounded above by a finite constant or $p_n(\mathbf{A}) \geq n$ for all $n \geq \max\{k + 1, 5\}$. One ingredient in Willard's proof is our result in §2 that a totally symmetric algebra has a bounded p_n -sequence.

REFERENCES

- [B] J. Berman, *Lecture notes: Free spectra of finite algebras*, manuscript, April, 1986.
- [B1] ———, *The combinatorics of free algebras*, Lattices, Semigroups and Universal Algebra, Plenum Press, New York, 1990.

- [DDT] M. Davio, J.-P. Deschamps, and A. Thayse, *Discrete and switching functions*, McGraw-Hill, New York, 1978.
- [DK] J. Dudek and A. Kisielewicz, *Totally commutative semigroups*, J. Austral. Math. Soc. Ser. A **51** (1991), 381–399.
- [G] G. Grätzer, *Composition of functions*, Proceedings of the Conference on Universal Algebra (October 1969), Queen's Papers in Pure and Appl. Math., no. 25, Queen's Univ., Kingston, ON, 1970.
- [GK] G. Grätzer and A. Kisielewicz, *A survey of some open problems on p_n -sequences and free spectra of algebras and varieties*, Universal Algebra and Quasigroup Theory (A. Romanowska and J. D. H. Smith, eds.), Heldermann Verlag, Berlin, 1992, pp. 57–88.
- [GP] G. Grätzer and J. Plonka, *On the number of polynomials of an idempotent algebra. I*, Pacific J. Math. **32** (1970), 697–709.
- [GPS] G. Grätzer, J. Plonka, and A. Sekanina, *On the number of polynomials of a universal algebra. I*, Colloq. Math. **22** (1970), 9–11.
- [H] M. Harrison, *Introduction to switching and automata theory*, McGraw-Hill, New York, 1965.
- [HM] D. Hobby and R. McKenzie, *The structure of finite algebras*, Contemp. Math., vol. 76, Amer. Math. Soc., Providence, RI, 1988.
- [Ki] A. Kisielewicz, *The p_n -sequences of idempotent algebras are strictly increasing*, Algebra Universalis **13** (1981), 233–250.
- [Ki1] ———, *The p_n -sequences of idempotent algebras are strictly increasing. II*, Algebra Universalis **28** (1991), 453–458.
- [Ko] K. M. Koh, *Idempotent algebras with one essentially binary polynomial*, Nanyang Univ. J. **6** (1972), 18–27.
- [LL] S. C. Lee and E. T. Lee, *On multivalued symmetric functions*, IEEE Trans. Comput. **C-21** (1972), 312–317.
- [MMT] R. McKenzie, G. McNulty, and W. Taylor, *Algebras, lattices, varieties*, Vol. I, Wadsworth, Belmont, CA, 1987.
- [P] E. L. Post, *The two-valued iterative systems of mathematical logic*, Ann. of Math. Stud., no. 5, Princeton Univ. Press, Princeton, NJ, 1941.
- [R] I. Rosenberg, *Completeness properties of multiple-valued logic algebras*, Computer Science and Multiple-Valued Logic, Theory and Applications, North-Holland, Amsterdam, 1977, pp. 144–186.
- [S] A. Szendrei, *Clones in universal algebra*, Université de Montréal Press, 1986.
- [SM] I. Stojmenović and M. Miyakawa, *Symmetric functions in many-valued logics*, Note on Multiple-Valued Logic in Japan **6** (1986), 1–26.
- [T] W. Taylor, *Equational logic*, Houston J. Math., Special Survey Issue, 1979. Abridged version in G. Grätzer, *Universal algebra*, 2nd ed., Springer-Verlag, Berlin and New York, 1979.
- [U] K. Urbanik, *Remarks on symmetrical operations*, Colloq. Math. **15** (1966), 1–9.
- [W] I. Wegner, *The complexity of Boolean functions*, Wiley, New York, 1987.

DEPARTMENT OF MATHEMATICS, STATISTICS, AND COMPUTER SCIENCE (M/C 249), UNIVERSITY OF ILLINOIS AT CHICAGO, 322 SCIENCE AND ENGINEERING OFFICES, CHICAGO, ILLINOIS 60607-7045
E-mail address: u10391@uicvm.uic.edu

INSTITUTE OF MATHEMATICS, UNIVERSITY OF WROCLAW, PL. GRUNWALDZKI 2/4, WROCLAW, POLAND
E-mail address: kisiel@math.impwr.wroc.edu.pl