Tatra Mountains Math. Publ. **5** (1995), 201–215

TATRA MOUNTAINS
*Mathematical Publications*

# CLONES ON A PRIME CARDINALITY UNIVERSE CONTAINING AN AFFINE ESSENTIAL OPERATION

IVO G. ROSENBERG

*Dedicated to Professor J. Jakubík on the occasion of his 70th birthday*

ABSTRACT. Let $p$ be an odd prime and let $\delta$ denote the number of divisors of $p-1$. We show that there are at most $2^{p\delta+2}$ clones on $\boldsymbol{p} := \{0,\dots,p-1\}$ containing at least one essential affine operation. These clones form the principal filter (in the lattice $\mathfrak{L}$ of clones on $\boldsymbol{p}$) generated by the minimal clone (i.e., an atom of $\mathfrak{L}$) of all idempotent affine operations. We determine this filter and show that each of its clones is finitely generated extending thus a result of Marchenkov ($p=3$) and Csikós ($p=5$). For every subset $J$ of $\boldsymbol{p}$ and the clone $K_J$ of all operations $f$ on $\boldsymbol{p}$ such that $f(j,\dots,j)=j$, for all $j \in J$, we give a canonical (or normal) representation for each $f \in K_J$.

## 1. Introduction

Let $p$ be an odd prime. An $n$-ary operation on $\boldsymbol{p} := \{0,\dots,p-1\}$ (i.e., a map from $\boldsymbol{p}^n$ into $\boldsymbol{p}$) is affine if there exist $a_0,\dots,a_n \in \boldsymbol{p}$ such that $f(x_1,\dots,x_n) \equiv a_0 + a_1x_1 + \dots + a_nx_n \pmod{p}$ holds for all $x_1,\dots,x_n \in \boldsymbol{p}$. Denote by $L_i$ the set of all idempotent affine operations on $\boldsymbol{p}$ (most of the concepts used in this section are defined in §2). $L_i$ is a minimal clone on $\boldsymbol{p}$ (i.e., an atom of the lattice $\mathfrak{L}$ of clones on $\boldsymbol{p}$). We describe completely the principal filter $[L_i)$ of $\mathfrak{L}$ generated by $L_i$ (i.e., the interval $[L_i, O]$ of $\mathfrak{L}$ where $O$ is the clone of all operations on $\boldsymbol{p}$) or, equivalently, all clones on $\boldsymbol{p}$ containing at least one essential (i.e., essentially nonunary) affine operation. This principal filter consists of at most $2^{p\delta+2}$ clones (where $\delta$ is the number of divisors of $p-1$) and each of them is finitely generated. The last fact was proved by *ad hoc* methods for $p=5$ and all clones containing a unary nonaffine operation in [Csi 84].

The filter $[L_i)$ contains the following $2^p-1$ clones. Let $J$ be a nonempty subset of $\boldsymbol{p}$ and $M$ the set of all operations $f$ on $\boldsymbol{p}$ such that $f(j,\dots,j)=j$

AMS Subject Classification (1991): 08A05, 08A40.
Key words: Clone, lattice of clones, minimal, maximal and finitely generated clone, affine and idempotent operation, relation, preservation of a relation.

for all $j \in J$ (i.e., $M = \bigcap_{j \in J} \mathrm{Pol}\{j\}$). In §3 we give explicitly a generating set $G$ of $M$ of cardinality $p^2 + p + 3 - |J|$ and a canonical (or normal) form for the representation of every operation from $M$. This is a more involved modification of the Post algebra generating set for $O$ (based on max, min, the peak functions and the constants) and is valid even for nonprime $p$.

The author benefited from numerous discussions with E. Fried on a subproblem of the main problem; namely, which clones on $\boldsymbol{p}$ contain the operation $+$ of $\mathbb{Z}_p$.

The author is also greatly indebted to Á. Szendrei for a very thorough referee's report which pointed out simplifications of the proofs of Lemmas 2.5–2.7 and 2.11, and many omissions and inaccuracies (in particular, in the proofs of Lemmas 2.6 and 2.12). Remarks 2.8–2) and 2.15–3) and the connection to McKenzie's results are also due to Á. Szendrei.

The partial financial support provided by NSERC operating grant 5407 and FCAR grant 93–ER–1647 is gratefully acknowledged.

## 2. Preliminaries and the main results

**DEFINITION 2.1.** Let $k$ be a positive integer and $\boldsymbol{k} := \{0, \dots, k-1\}$. For a positive integer $n$ an $n$-ary operation on $\boldsymbol{k}$ is a map $f\colon \boldsymbol{k}^n \to \boldsymbol{k}$. For $1 \le i \le n$ the $i$th $n$-ary *projection* $e_i^n$ is defined by setting $e_i^n(a_1, \dots, a_n) = a_i$ for all $a_1, \dots, a_n \in \boldsymbol{k}$. Denote by $O^{(n)}$ the set of all $n$-ary operations on $\boldsymbol{k}$ and set $O := \bigcup_{n=1}^{\infty} O^{(n)}$. Informally, a clone on $\boldsymbol{k}$ is a composition (i.e., substitution or superposition) closed subset of $O$ containing all projections; or, equivalently, the set of all term operations of an algebra on $\boldsymbol{k}$. Following Mal'tsev's approach [Mal 66] we give a precise definition. For $f \in O^{(m)}$ and $g \in O^{(n)}$ define $f * g \in O^{(m+n-1)}$ by setting

$$(f * g)(a_1, \dots, a_{m+n-1}) := f(g(a_1, \dots a_n), a_{n+1}, \dots, a_{m+n-1})$$

for all $a_1, \dots, a_{m+n-1} \in \boldsymbol{k}$. Let $f \in O^{(n)}$. Define

$$(\tau f)(a_1, \dots, a_n) := f(a_2, a_1, a_3, \dots, a_n);$$
$$(\zeta f)(a_1, \dots, a_n) := f(a_2, \dots, a_n, a_1),$$

for all $a_1, \dots, a_n \in \boldsymbol{k}$ (for $n = 1$ this is interpreted as $\tau f = \zeta f := f$). If $n > 1$, define $\Delta f \in O^{(n-1)}$ by setting

$$(\Delta f)(a_1, \dots, a_{n-1}) := f(a_1, a_1, a_2, \dots, a_{n-1}),$$

while $\Delta f := f$ for every $f \in O^{(1)}$. Clearly $*$ is a binary operation on $O$. A subset $C$ of $O$ is a *clone* on $\boldsymbol{k}$ if $C$ is closed under $*, \tau, \zeta$ and $\Delta$ (i.e., $C * C \subseteq C, \alpha C \subseteq C$ for every $\alpha \in \{\tau, \zeta, \Delta\}$) and $e_1^2 \in C$. Thus clones are exactly the subuniverses of the algebra $\langle O; *, \tau, \zeta, \Delta, e_1^2 \rangle$ (where $e_1^2$ is considered as a nullary operation on $O$) and therefore the set $\mathfrak{L}$ of all clones on $\boldsymbol{k}$ is closed under arbitrary intersections. In particular, for an arbitrary subset $F$ of $O$ there exists the least clone $\langle F \rangle$ containing $F$. The clone $\langle F \rangle$, called the clone *generated* by $F$, is the set of all term operations of the algebra $\langle \boldsymbol{k}; F \rangle$. The clones on $\boldsymbol{k}$, ordered by containment, form an algebraic lattice $\mathfrak{L}$. A dual atom (or co-atom) of $\mathfrak{L}$ is a *maximal* clone. Thus a clone $M$ is maximal if $M \neq O$ and $M \subset C \subset O$ for no clone $C$ (here $\subset$ denotes the strict inclusion).

EXAMPLE. Let $\phi \neq B \subset \boldsymbol{k}$. Denote by $\operatorname{Pol} B$ the set of all $f \in O^{(n)}$ such that $f(B^n) \subseteq B$ $(n = 1, 2, \ldots)$. It is well known that $\operatorname{Pol} B$ is a maximal clone (cf. [Iab 58]).

As usual, a clone $C$ is *finitely generated* if $C = \langle F \rangle$ for some finite subset $F$ of $O$. In the remainder of §2 and §3, $k$ is an odd prime number $p$. For $x, y \in \boldsymbol{p}$ we denote by $x + y$ and $xy$ the elements of $\boldsymbol{p}$ congruent $\operatorname{mod} p$ to the arithmetical sum and product of $x$ and $y$. An $n$-ary operation $f$ on $\boldsymbol{p}$ is *affine* (also linear or quasilinear) if there exist $r_0, \ldots, r_n \in \boldsymbol{p}$ such that

$$f(x_1, \ldots, x_n) \approx r_0 + r_1 x_1 + \cdots + r_n x_n$$

(here and in the sequel $\approx$ denotes an identity over $\boldsymbol{p}$; i.e., both sides are equal for all $x_1, \ldots, x_n \in \boldsymbol{p}$). It is well known that the set $L$ of all affine operations on $\boldsymbol{p}$ is a maximal clone [Iab 58]. A clone $C$ is *unary* if $C = \{m * e_i^n : m \in M, 1 \leq i \leq n\}$ for some transformation monoid $M$ on $\boldsymbol{p}$; (i.e., $M \subseteq O^{(1)}$ such that $e_1^1 \in M$ and $M \circ M = M * M = M$). It is known ([Sal 64], [B-D 82], cf. also [Sze 86] Prop. 2.9) that the nonunary proper subclones of $L$ are exactly:

1) $A_q := \{f \in L : f(q, \ldots, q) = q\}$ $(q \in \boldsymbol{p})$,
2) $B := \{r_0 + r_1 x_1 + \cdots + r_n x_n : n > 0,\ r_0, \ldots r_n \in \boldsymbol{p}$ and $r_1 + \cdots + r_n = 1\}$, and
3) $L_i := \{f \in B : f(0, \ldots, 0) = 0\}$.

It is immediate that $L_i$ is the set of all idempotent affine operations on $\boldsymbol{p}$ (where, as usual, $f$ is idempotent if $f(x, \ldots, x) \approx x$). It follows that $L_i$ is the least nonunary clone of affine operations and so $L_i \subseteq \langle F \rangle$ whenever $\langle F \rangle$ contains an essentially nonunary affine operation.

S. V. Marchenkov [Mar 84] showed that every clone on $\mathbf{3}$ containing an essentially nonunary affine operation $f$ and a nonaffine operation $g$ is finitely generated. M. Csikós [Csi 84] gave another proof and generalized it to $p = 5$ provided $g$ is unary. Here we extend this result to all odd primes. Actually, we do much more by determining all clones containing the above clone $L_i$ (of all idempotent affine operations). The main result, Theorem 2.14 below, also follows from McKenzie's 1976 Theorem [MK 76], which is also a consequence of [MK 78] Theorem 22. We derive it directly using the relational description of clones.

**DEFINITION 2.2.** Let $h$ be a positive integer. A subset $\rho$ of $\boldsymbol{p}^h$ is an $h$-ary *relation* on $\boldsymbol{p}$. An $n$-ary operation $f$ on $\boldsymbol{p}$ *preserves* $\rho$ if for every $h \times n$ matrix $\mathbf{M} = [m_{ij}]$ whose columns belong to $\rho$, the values of $f$ on the rows of $\mathbf{M}$ form an $h$-tuple from $\rho$; in symbols,

$$\big(f(m_{11},\dots,m_{1n}),\dots f(m_{h1},\dots,m_{hn})\big) \in \rho$$

whenever $(m_{11},\dots,m_{h1}),\dots,(m_{1n},\dots,m_{hn}) \in \rho$. In algebraic terminology, $f$ preserves $\rho$ if $\rho$ is a subuniverse (i.e., the ground set of a subalgebra) of the power $\langle \boldsymbol{p}; f\rangle^h$. Notice that every projection preserves $\rho$. The set of all operations on $\boldsymbol{p}$ preserving $\rho$ is denoted $\operatorname{Pol}\rho$.

For an $h$-ary operation $f$ on $\boldsymbol{p}$ the *graph* of $f$ is the $(h+1)$-ary relation

$$f^\circ := \big\{\big(a_1,\dots,a_h,f(a_1,\dots,a_h)\big) : a_1,\dots,a_h \in \boldsymbol{p}\big\}.$$

For example, if $h = 1$, then the binary relation $f^\circ$ is the usual graph (or diagram) of the selfmap $f$. Let $g$ be an operation on $\boldsymbol{p}$. We say that $f$ and $g$ *commute* (or permute) if $g \in \operatorname{Pol} f^\circ$. It is well known and easy to check that $g \in \operatorname{Pol} f^\circ$ if and only if $f \in \operatorname{Pol} g^\circ$; and so the commutation relation on $O$ is symmetric.

EXAMPLE. Let $m$ be the ternary operation on $\boldsymbol{p}$ defined by $m(x,y,z) :\approx x - y + z$. It is known that $\operatorname{Pol} m^\circ = L$ (cf. [Sze 86] Prop. 2.1), and so $g$ and $m$ commute exactly if $g$ is affine. The next lemma gives a necessary and sufficient condition for the commutation of affine operations.

**LEMMA 2.3.** *The operations*

$$\begin{aligned} f(x_1,\dots,x_h) &\approx a_0 + a_1x_1 + \dots + a_hx_h\,, \\ g(x_1,\dots,x_n) &\approx b_0 + b_1x_1 + \dots + b_nx_n \end{aligned} \tag{2.1}$$

*commute if and only if*

$$a_0(b_1 + \dots + b_n - 1) = b_0(a_1 + \dots + a_h - 1)\,. \tag{2.2}$$

Proof. The operations $f$ and $g$ commute if and only if

$$g\big(f(M_{*1}),\dots,f(M_{*n})\big) = f\big(g(M_{1*}),\dots,g(M_{h*})\big) \tag{2.3}$$

holds for every $h \times n$ matrix $\mathsf{M}$ over $\boldsymbol{p}$ (where $M_{i*}$ and $M_{*j}$ denote the $i$th row vector and $j$th column vector of $M$). Set $\tilde{\mathbf{a}} := (a_1, \ldots, a_h)$ and $\tilde{\boldsymbol{b}} := (b_1, \ldots, b_n)$ and denote by $\tilde{\mathbf{e}}_i$ the $i$-vector $(1, \ldots, 1)$. Notice that

$$\big(f(M_{*1}), \ldots, f(M_{*n})\big) = \tilde{\mathbf{a}} \cdot \mathsf{M} + a_0 \tilde{\mathbf{e}}_n \quad \big(g(M_{1*}), \ldots, g(M_{h*})\big) = \tilde{\boldsymbol{b}} \cdot \mathsf{M}^T + b_0 \tilde{\mathbf{e}}_h$$

(where $\tilde{\mathbf{a}} \cdot \mathsf{M}$ is the product of the $1 \times h$ matrix $\tilde{\mathbf{a}}$ and the matrix $\mathsf{M}$, $a\tilde{\mathbf{e}}_n$ is the product of the $1 \times n$ matrix $\tilde{\mathbf{e}}_n$ by the scalar $a$, and $\mathsf{M}^T$ is the transpose of $\mathsf{M}$). Now (2.3) can be written as

$$\tilde{\boldsymbol{b}} \cdot (\tilde{\mathbf{a}} \cdot \mathsf{M} + a_0 \tilde{\mathbf{e}}_n)^T + b_0 = \tilde{\mathbf{a}} \cdot (\tilde{\boldsymbol{b}} \cdot \mathsf{M}^T + b_0 \tilde{\mathbf{e}}_h)^T + a_0 \tag{2.4}$$

which can be expressed as

$$\tilde{\boldsymbol{b}} \cdot \mathsf{M}^T \cdot \tilde{\mathbf{a}}^T + a_0 \tilde{\boldsymbol{b}} \cdot \tilde{\mathbf{e}}_n^T + b_0 = \tilde{\mathbf{a}} \cdot \mathsf{M} \cdot \tilde{\boldsymbol{b}}^T + b_0 \tilde{\mathbf{a}} \cdot \boldsymbol{e}_n^T + a_0 \,.$$

Notice that the $1 \times 1$ matrix $C := \tilde{\boldsymbol{b}} \cdot \mathsf{M}^T \cdot \tilde{\mathbf{a}}^T$ satisfies $\tilde{\boldsymbol{b}} \cdot \mathsf{M}^T \cdot \tilde{\mathbf{a}}^T = C = C^T = \tilde{\mathbf{a}} \cdot \mathsf{M} \cdot \tilde{\boldsymbol{b}}^T$ and so (2.4) simplifies to

$$a_0(b_1 + \cdots + b_n) + b_0 = a_0 \tilde{\boldsymbol{b}} \cdot \tilde{\mathbf{e}}_n^T + b_0 = b_0 \tilde{\mathbf{a}} \cdot \boldsymbol{e}_h^T + a_0 = b_0(a_1 + \ldots a_h) + a_0 \,,$$

which is equivalent to (2.2). □

**DEFINITION 2.4.** Let $\rho$ be an $h$-ary relation on $\boldsymbol{p}$ and let $\pi$ be a permutation of $\{1, \ldots, h\}$. Set

$$\rho^{(\pi)} := \big\{(a_{\pi(1)}, \ldots a_{\pi(h)}) \colon \ (a_1, \ldots a_h) \in \rho\big\} \,. \tag{2.5}$$

It is well known and easy to verify that

$$\operatorname{Pol} \rho = \operatorname{Pol} \rho^{(\pi)} .$$

In the next lemma we characterize the relations $\sigma$ such that $L_i$ is a subclone of $\operatorname{Pol} \sigma$.

**LEMMA 2.5.** *Let $\sigma$ be an $h$-ary relation on $\mathbf{p}$ such that $1 < |\sigma| < p^h$. Then $L_i \subseteq \operatorname{Pol} \sigma$ if and only if there are:* (i) $1 \le j \le h$, (ii) *affine $(h-j)$-ary operations $f_1, \ldots f_j$ on $\mathbf{p}$, and* (iii) *a permutation $\pi$ of $\{1, \ldots, h\}$ such that*

$$\sigma^{(\pi)} = \big\{\big(\tilde{\mathbf{x}}, f_1(\tilde{\mathbf{x}}), \ldots f_j(\tilde{\mathbf{x}})\big) \colon \ \tilde{\mathbf{x}} \in \boldsymbol{p}^{h-j}\big\} \,. \tag{2.6}$$

Proof. ($\Rightarrow$) Consider the $h$-ary relation $\sigma$ as a subset of the vector space $GF(p)^h$, and suppose $L_i \subseteq \operatorname{Pol} \sigma$. Since $L_i$ is generated by $x - y + z$, we have $L_i \subseteq \operatorname{Pol} \sigma$ if and only if $\sigma$ is closed under $x - y + z$, and this is equivalent to $\sigma$ being a coset of a subspace of $GF(p)^h$. Therefore $\sigma = \rho + v$ for some subspace $\rho$ of $GF(p)^h$, and some element $v$ of $GF(p)^h$. Using elementary transformations for bases one can easily see that for some permutation $\pi$ of the coordinates, $\rho^{(\pi)}$ has a basis of the form

$$(0,\dots,0,\underbrace{1}_{i\text{th place}},0,\dots,0,a_{i,t+1},\dots,a_{ih}),\quad i=1,\dots,t,$$

(where $t=\dim\rho$), which immediately implies that $\sigma^{(\pi)}$ is of the required form. ($\Leftarrow$) Let $\sigma$ be of the form (2.6) and let $g\in L_i$ be $n$-ary. By the definition $g(\tilde{\mathbf{x}})\approx\tilde{\boldsymbol{a}}\cdot\tilde{\mathbf{x}}^T$ for some $\tilde{\boldsymbol{a}}=(a_1,\dots,a_n)\in\boldsymbol{p}^n$ such that $a_1+\dots+a_n=1$. To prove that $g$ preserves $\sigma$, we must show that $g$ commutes with every $f_l$. The affine $(h-j)$-ary operation $f_l$ satisfies $f_l(\tilde{\mathbf{x}})\approx b_0+\tilde{\boldsymbol{b}}\cdot\tilde{\mathbf{x}}^T$ for some $b_0\in\boldsymbol{p}$ and some $\tilde{\boldsymbol{b}}=(b_1,\dots,b_{h-j})\in\boldsymbol{p}^{h-j}$. Clearly $g$ and $f_l$ commute by Lemma 2.3. □

**LEMMA 2.6.** *Let $f_1,\dots,f_j$ be $n$-ary operations on $\boldsymbol{p}$ and let*

$$\sigma:=\{(\tilde{\mathbf{x}},f_1(\tilde{\mathbf{x}}),\dots,f_j(\tilde{\mathbf{x}})):\tilde{\mathbf{x}}\in\boldsymbol{p}^n\}.$$

*Then*

$$\operatorname{Pol}\sigma=\operatorname{Pol}f_1^\circ\cap\dots\cap\operatorname{Pol}f_j^\circ.\tag{2.7}$$

P r o o f . The reader can check directly that an operation preserves $\sigma$ if and only if it preserves each $f_l^\circ$. □

The next lemma determines all clones $\operatorname{Pol}f^\circ$ for $f$ affine. For $a,b\in\boldsymbol{p}$ define the selfmap $s_{ab}$ of $\boldsymbol{p}$ by setting $s_{ab}(x):\approx ax+b$. Set $\pi:=s_{11}$. The clones $A_q$ and $B$ were introduced in 2.1.

**LEMMA 2.7.** *Let $f$ be an affine operation on $\boldsymbol{p}$. Then* $\operatorname{Pol}f^\circ$ *is one of the following clones:*

(i) $\operatorname{Pol}s_{ab}^\circ$ with $a\in\boldsymbol{p}\setminus\mathbf{2}$ and $b\in\boldsymbol{p}$,
(ii) $O,B$ and $A_q$ $(q\in p)$, and
(iii) $L,\operatorname{Pol}\pi^\circ$, and $\operatorname{Pol}\{q\}$ $(q\in\boldsymbol{p})$.

P r o o f . Case I: $f$ is (essentially) unary. Then $\operatorname{Pol}f^\circ$ is one of the clones $\operatorname{Pol}s_{ab}^\circ$ $(a\neq 0)$ or $\operatorname{Pol}\{q\}$ depending on whether $f$ is a permutation or a constant; moreover all clones $\operatorname{Pol}s_{1b}^\circ$ with $b\neq 0$ are equal to $\operatorname{Pol}\pi^\circ$, while $\operatorname{Pol}s_{10}^\circ$ is of course equal to $O$.

Case II: $f$ is not essentially unary. Then $\operatorname{Pol}f^\circ\subseteq\operatorname{Pol}m^\circ=L$; i.e., by the description of the subclones of $L$ the clone $\operatorname{Pol}f^\circ$ is one of the clones $L$, $A_q$, $B$, $L_i$. Here $L_i$ is not of the form $\operatorname{Pol}f^\circ$. □

R e m a r k s 2.8. 1) The clones $L$, $\operatorname{Pol}\pi^\circ$ and $\operatorname{Pol}\{q\}$ $(q\in\boldsymbol{p})$ listed in Lemma 2.7 (iii), are maximal clones ([Iab 58] §§ 16, 18, 19, cf. [P-K79] 4.3.9–15) while it can be easily seen that $L_i$ is a minimal clone (the maximal and minimal clones were defined in 2.1).

2) Notice the following connection between the subclones of $L$ and the superclones of $L_i$:

$$(L] \to [L_i), \quad \langle f_1, \dots, f_j \rangle \mapsto \mathrm{Pol}\, f_1^\circ \cap \dots \cap \mathrm{Pol}\, f_j^\circ$$

is a surjective, order reversing mapping, which is bijective when restricted to those subclones of $L$ which are themselves of the form $\bigcap_k \mathrm{Pol}\, h_k^\circ$ for some — not necessarily affine — operations $h_k$ on $\boldsymbol{p}$ (the so-called bicentrally closed, or primitive positive subclones of $L$). Obviously, the not essentially unary subclones of $L$ are all of this kind, while among the essentially unary ones, a submonoid $M$ of the unary part of $L$ is the unary part of a bicentrally closed clone if and only if $M$ contains every constant which is a fixed point of a permutation in $M$ (cf. [Sza 84]).

**DEFINITION 2.9.** Let $C$ be a clone on $\boldsymbol{p}$. The clone $C$ is *rational* if $C = \mathrm{Pol}\, \rho$ for some finitary relation $\rho$ on $\boldsymbol{p}$. The clone $C$ is *irrational* if it is not rational. A set of clones on $p$ is *rational* if all its members are rational.

**COROLLARY 2.10.** *The interval* $[L_i) := [L_i, O]$ *(of the lattice* $\mathfrak{L}$ *of clones on* $\boldsymbol{p}$*) is finite and rational.*

Proof. According to Lemmas 2.5–2.7 and in view of $\mathrm{Pol}\, \phi = \mathrm{Pol}\, \boldsymbol{p}^h = O$, every rational clone from $[L_i)$ is the intersection of at most $p^2 + 5$ clones listed in Lemma 2.7. By [B-K-K-R 69] every irrational clone is the intersection of a countable chain of rational clones. Since $[L_i)$ contains at most $2^{p^2+5}$ rational clones, clearly $[L_i)$ is rational and finite. □

The next two lemmas describe the subinterval $J_q := \big[A_q, \mathrm{Pol}\{q\}\big]$ of $[L_i)$.

**LEMMA 2.11.** *Let* $q, b \in \boldsymbol{p}$ *and* $a \in \boldsymbol{p} \setminus \boldsymbol{2}$. *Then* $\mathrm{Pol}\, s_{ab}^\circ \in J_q$ *if and only if* $s_{ab}(q) = q$.

Proof. Let $C := \mathrm{Pol}\ s_{ab}^\circ$.
($\Rightarrow$) If $C \in J_q$, then for the constant function $q$ we have $q \in A_q \subseteq C = \mathrm{Pol}\, s_{ab}^\circ$, whence $s_{ab}(q) = q$.
($\Leftarrow$) Let $s_{ab}(q) = q$. Since $q$ is the unique fixed point of $s_{ab}$, it is straightforward to check that every function commuting with $s_{ab}$ fixes $q$. Thus $C \subseteq \mathrm{Pol}\{q\}$. The inclusion $A_q \subseteq C$ follows from the fact that $L_i$ and the constant $q$ belong to $C$, and that $L_i$ together with $q$ generates $A_q$. □

Denote by $D$ the set of all divisors of $p-1$ and set $\mathfrak{D} := (D, \sqsubseteq)$ where $d \sqsubseteq d'$ if $d$ divides $d'$. Fix a primitive $p$-th root $w$ (*i.e.*, $w \in \boldsymbol{p} \setminus \{0\}$ such that $\{w, w^2, \dots, w^{p-1}\} = \boldsymbol{p} \setminus \{0\}$). Fix $q \in \boldsymbol{p}$ and for each $d \in \{1, \dots, p-1\}$ set

$$a_d := w^d, \qquad b_d := q(1 - w^d), \qquad t_d := s_{a_d b_d}. \tag{2.8}$$

Observe that if $d \neq p-1$, then $t_d(x) :\approx a_d x + b_d$ is a permutation of $\boldsymbol{p}$ with a unique fixed point $q$. Further, $t_{p-1}(x) \approx x$. Set $C_d := \operatorname{Pol} t_d^\circ$ for $d \in \{1,\dots,p-2\}$. Finally, set $C_{p-1} := \operatorname{Pol}\{q\}$. The greatest common divisor of $a$ and $b$ will be denoted by g.c.d. $(a,b)$.

**LEMMA 2.12.** *For each $q \in \boldsymbol{p}$ the set $J_q \setminus \{A_q\}$ is lattice isomorphic to $\mathfrak{D}$.*

Proof. Apart from $A_q$ and $\operatorname{Pol}\{q\}$, among the clones listed in Lemma 2.7 only the clones of the form $\operatorname{Pol} s_{ab}^\circ$ may belong to $J_q$. According to Lemma 2.11 these are exactly the clones $C_d = \operatorname{Pol} t_d^\circ$ where $d \in \{1,\dots,p-2\}$ (and $t_d$ was defined in (2.8)). For all $n > 0$ let $t_d^n$ denote the usual $n$th iteration of the map $t_d$. An easy induction shows that $t_d^n = t_{nd}$ for all $n \geq 1$, where the subscript of $t$ is understood modulo $p-1$ (with $p-1$ replacing 0). Clearly $C_d = \operatorname{Pol} t_d^\circ \subseteq \operatorname{Pol} t_d^{n\circ} \cap \operatorname{Pol}\{q\} = C_{nd}$. If g.c.d. $(nd, p-1) =$ g.c.d. $(d, p-1)$, then $d \equiv \text{mnd} \pmod{p-1}$ for a suitable $m \in \boldsymbol{p}$ and $C_{nd} \subseteq C_{m(nd)} = C_d$ proving $C_d = C_{nd}$. Since there exists an $n \geq 1$ such that $nd \equiv$ g.c.d. $(d, p-1)$ $\pmod{p-1}$, we conclude that $C_d = C_{g.c.d.(d,p-1)}$. Thus every clone listed in Lemma 2.7 which belongs to $J_q \setminus \{A_q\}$ is of the form $C_d$ with $d \in \mathfrak{D}$. From the foregoing argument it follows also that $C_d \subseteq C_{d'}$ whenever $d \sqsubseteq d'$ $(d, d' \in \mathfrak{D})$. Here the inclusion is sharp if $d \neq d'$. Indeed, this is obvious if $d' = p-1$, and for $d' < p-1$ it can be verified by observing that every nontrivial cycle of $t_{d'}$ (as a permutation on $\boldsymbol{p}$) belongs to $C_{d'} \setminus C_d$. Let $d, d' \in \mathfrak{D}$ and let $\delta :=$ g.c.d. $(d, d')$. We show that $C_\delta = C_d \cap C_{d'}$. As this equality is trivial if $p-1 \in \{d, d'\}$, we assume that $d, d' < p-1$. The inclusion $\subseteq$ follows from the fact that $\delta$ divides both $d$ and $d'$. It is well known that $\delta \equiv ud + vd' \pmod{p-1}$ for suitable $u, v \in \boldsymbol{p}$. Clearly both $t_{ud}$ and $t_{vd'}$ are automorphisms of $A := \langle \boldsymbol{p}, C_d \cap C_{d'} \rangle$, hence $t_\delta = t_{ud} \circ t_{vd'} \in \operatorname{Aut} A$ proving the required $C_d \cap C_{d'} \subseteq C_\delta$. This, in fact, proves the lemma. □

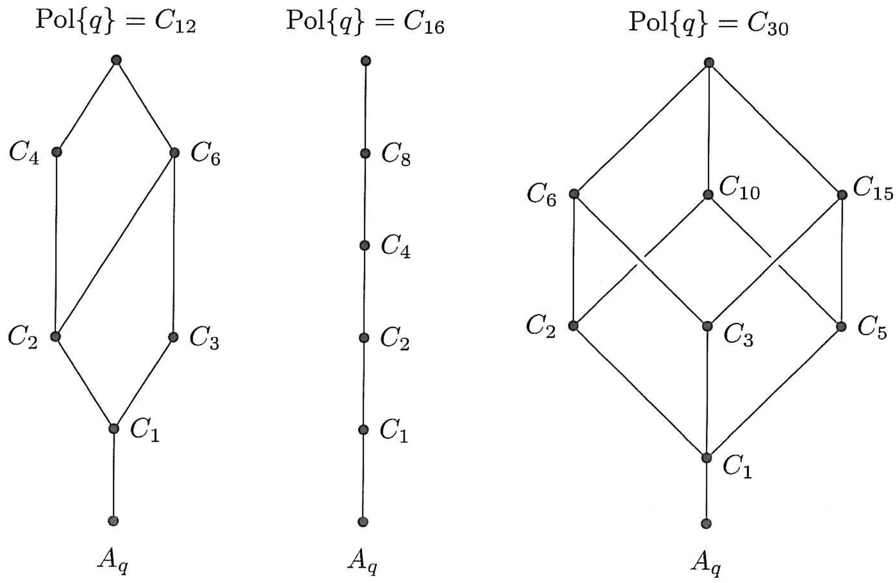
Remarks 2.13. 1) The (Hasse) diagrams of $J_q$ for $p = 13, 17, 31$ are in Fig. 1. a) – c).

2) A part of the (Hasse) diagram of the above clones is in Fig. 2. Here $I_d := \operatorname{Pol}\{0\} \cap \dots \cap \operatorname{Pol}\{p-1\}$ is the clone of all idempotent operations on $\boldsymbol{p}$. The interval $[I_d, O]$ is formed by the clones $\bigcap_{q \in Q} \operatorname{Pol}\{q\}$ with $Q \subseteq \boldsymbol{p}$, and is lattice isomorphic to the dual of the boolean lattice of all subsets of $\boldsymbol{p}$.

3) Fig. 2 does not show the clones

$$E_\delta := I_d \cap \operatorname{Pol} u_\delta^\circ \cap \operatorname{Pol} \pi^\circ,$$

where $\delta$ is a divisor of $p-1$ and $u_\delta(x) \approx w^\delta x$ ($w$ is a primitive root of $p$; notice that $E_\delta \subseteq \operatorname{Pol} s_{ab}^\circ$ whenever $a = w^m$ and $\delta =$ g.c.d. $(m, p-1)$). The clone $\operatorname{Pol} \pi^\circ$ has exactly two maximal subclones: $B$ and $I_d \cap \operatorname{Pol} \pi^\circ = E_{p-1}$ [Sza 84], the least clone containing $L_i$ and the ternary discriminator. The interval $[E_1, E_{p-1}]$ is lattice isomorphic to $\mathfrak{D}$.




a) $p = 13$ b) $p = 17$ c) $p = 31$

FIG. 1.

**THEOREM 2.14.** *Every clone on* $\boldsymbol{p}$ *containing an essentially nonunary affine operation is the intersection of a subset of*

$$\{L, \operatorname{Pol} \pi^\circ\} \cup \{\operatorname{Pol}\{q\}\colon q \in \boldsymbol{p}\} \cup \bigcup_{q \in \boldsymbol{p}} J_q . \tag{2.9}$$

Proof. Corollary 2.10, Lemmas 2.11–12 and $B = L \cap \operatorname{Pol} \pi^\circ$. □

Remarks 2.15. 1) There is a redundancy in (2.9). Indeed, due to $A_q = L \cap \operatorname{Pol}\{q\}$ we can replace $J_q$ by the set $J_q \setminus \{A_q, \operatorname{Pol}\{q\}\}$ consisting of $\delta - 1$ clones, where $\delta$ denotes the number of divisors of $p-1$. After this reduction we are left with $2 + p + p(\delta - 1) = p\delta + 2$ clones and so the filter $[L_i)$ consists of at most $2^{p\delta+2}$ clones. This upper bound could be improved but this would necessitate a study of the intersections of the clones from $\bigcup_{q \in \boldsymbol{p}} J_q$.

2) The clone $L_i$ is a minimal clone. As there are only finitely many minimal clones ([Csá 83] for $k = 3$, [Ros 83] for $k > 3$, cf. [Qua 92]) while the lattice $\mathfrak{L}$ of all clones is of cardinality $2^{\aleph_0}$ [I-M 59], clearly $[M)$ is of cardinality $2^{\aleph_0}$ for some minimal clone $M$. It seems that the size of $[M)$ for $M$ minimal clone has not yet been investigated even for the case $p = 3$, where all minimal clones are

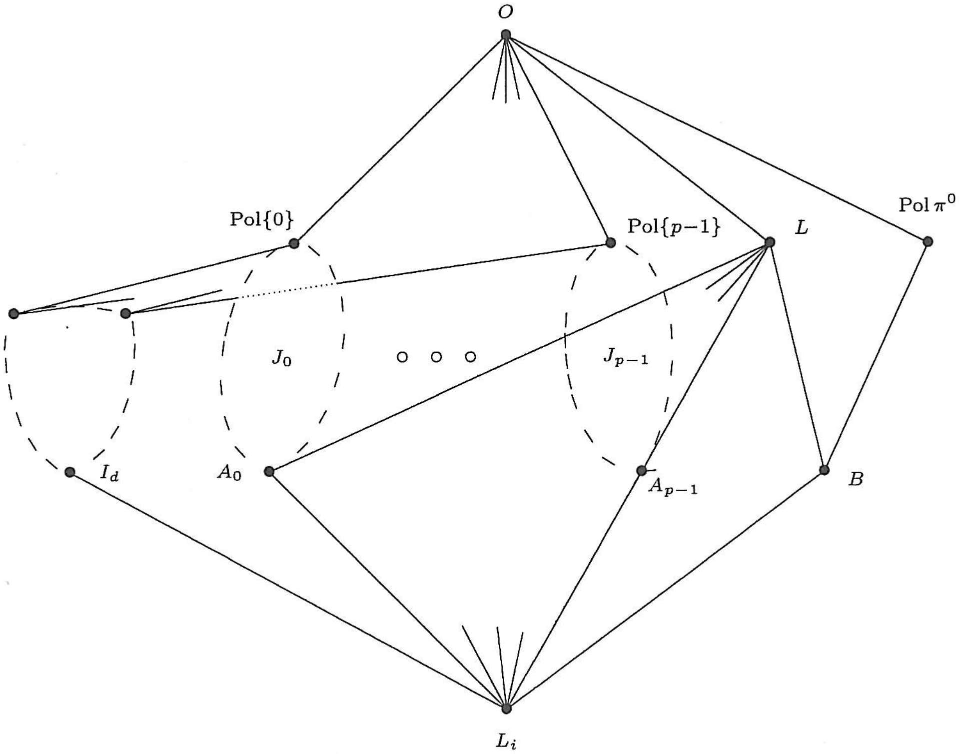



FIG. 2.

explicitly known [Csá 83]. The finiteness of $[L_i)$ seems to be rather exceptional among $[M)$, $M$ minimal clone.

3) A similar question for the maximal clones on $\boldsymbol{k}$ was completely settled. The ideals $(M]$, where $M$ is a maximal nonaffine clone, are all of size $2^{\aleph_0}$. For a maximal affine clone $L$ on $\boldsymbol{k}$ the ideal $(L]$ is finite if $k$ is prime ([D-H 83, Mar 79, Mar 83]) and countably infinite if $k = p^m$, $p$ prime and $m > 1$ [Lau 78].

**THEOREM 2.16.** *Every clone from $[L_i)$ is finitely generated.*

Proof. $[L_i)$ is finite and $L_i$ is finitely generated. □

## 3. A canonical form of $j$–idempotent operations

Remark 3.1. Let $k > 1$ and $\boldsymbol{k} := \{0, \ldots, k-1\}$. Let $J \subseteq \boldsymbol{k}$ and $K_J := \bigcap_{j \in J} \mathrm{Pol}\{j\}$. Clearly $K_J$ is the clone of all operations $f$ on $\boldsymbol{k}$ such that $f(j, \ldots, j)$

$= j$ for all $j \in J$. In this section we find a set $G$ of cardinality $k^2+k+3-|J|$ generating $K_J$ as well as a canonical (or normal) form expressing every $f \in K_J$ as a term operation of $\langle \boldsymbol{k}; G\rangle$. Here $G$ is a natural adaption of the standard complete set for $O$ consisting of max, min, the $k$ peak functions and the $k$ constants, often called the $k$-element Post algebra.

For notational simplicity we assume that $J = \boldsymbol{j} := \{0,\dots,j-1\}$. Indeed, let $\pi$ be a permutation of $\boldsymbol{k}$. For each $n$-ary operation $f$ on $\boldsymbol{k}$ define an $n$-ary operation $f^\pi$ on $\boldsymbol{k}$ by setting

$$f^\pi(x_1,\dots,x_n) :\approx \pi^{-1}\big(f\big(\pi(x_1),\dots,\pi(x_n)\big)\big)\,.$$

Clearly $\pi$ is an isomorphism between the algebras $\langle \boldsymbol{k}; f\rangle$ and $\langle \boldsymbol{k}; f^\pi\rangle$. The self-map $\varphi\colon f \mapsto f^\pi$ of $O$ is an automorphism of the algebra $\langle O; *, \zeta, \tau, \Delta, e_1^2\rangle$ [Mal 66]; in other words, $\varphi$ is compatible with composition. Thus results for $\boldsymbol{j}$ can be transferred to $J$ by choosing $\pi$ so that $\pi$ maps $\boldsymbol{j}$ onto $J$. We say that an operation $f$ on $\boldsymbol{k}$ is *$\boldsymbol{j}$-idempotent* if $f(x,\dots,x) = x$ for all $x \in \boldsymbol{j}$. For $x, y \in \boldsymbol{k}$ denote by $x \vee y$ and $x \wedge y$ the greatest and the least of $x, y$. Clearly $\vee$ and $\wedge$ are the lattice operations of the chain $0 < \dots < k-1$. For $n > 0$ set $K_n := \boldsymbol{k}^n \setminus \{(0,\dots,0),\dots,(j-1,\dots,j-1)\}$. For $\tilde{\mathbf{a}} \in K_n$ the nary *$\boldsymbol{j}$-idempotent peak operation* $\chi^n_{\tilde{\mathbf{a}}}$ at $\tilde{\mathbf{a}}$ is defined by $\chi^n_{\tilde{\mathbf{a}}}(x,\dots,x) := x$ for all $x \in \boldsymbol{j}$, $\chi^n_{\tilde{\mathbf{a}}}(\tilde{\mathbf{a}}) := k-1$ and $\chi^n_{\tilde{\mathbf{a}}}(\tilde{\mathbf{x}}) := 0$ otherwise. In Lemmas 3.2–6 we construct all $\boldsymbol{j}$–idempotent peak operations from (i) the binary ones, (ii) $\vee, \wedge$, and (iii) 4 additional binary $\boldsymbol{j}$–idempotent operations. For $n = 1$ clearly $K_1 = \boldsymbol{k} \setminus \boldsymbol{j}$ and for each $a \in \boldsymbol{k} \setminus \boldsymbol{j}$ obviously $\chi^1_a(x) \approx \chi^2_{(a,a)}(x,x)$. Thus let $n > 2$ and let $\tilde{\mathbf{a}} = (a_1,\dots,a_n) \in K_n$. Denote by $A$ the set consisting of $a_1,\dots,a_n$ and put

$$P := \{(r,s)\colon (a_r,a_s) \in K_2\}\,,$$

$$[x_1,\dots,x_n]_{\tilde{\mathbf{a}}} :\approx \bigwedge_{(r,s)\in P} \chi^2_{a_r a_s}(x_r,x_s)\,. \tag{3.1}$$

**LEMMA 3.2.** *If $A \not\subseteq \boldsymbol{j}$ or $|A| > 2$, then $[x_1,\dots,x_n]_{\tilde{\mathbf{a}}} = \chi^n_{\tilde{\mathbf{a}}}$.*

Proof. Clearly $\chi^2_{ab}$ and $\wedge$ are $\boldsymbol{j}$–idempotent and so by (3.1) the operation $[x_1,\dots,x_n]_{\tilde{\mathbf{a}}}$ is also $\boldsymbol{j}$–idempotent. Next $\chi^2_{a_r a_s}(a_r,a_s) = k-1$ and $P \neq \phi$; and therefore $[a_1,\dots,a_n]_{\tilde{\mathbf{a}}} = k-1$. Finally, let $\tilde{\boldsymbol{b}} = (b_1,\dots,b_n) \in K_n$ satisfy $\beta := [b_1,\dots,b_n]_{\tilde{\mathbf{a}}} > 0$. We distinguish two cases.
(i) Let $A \not\subseteq \boldsymbol{j}$. Then some $a_i \geq j$ and so $(l,i) \in P$ for all $1 \leq l \leq n$, $l \neq i$. Set

$$Q := \{1 \leq l \leq n\colon l \neq i\,, (b_l,b_i) \neq (a_l,a_i)\}\,.$$

Consider $l \in Q$. From $\beta > 0$ we see that $\chi^2_{a_l a_i}(b_l,b_i) > 0$. Combined with $(b_l,b_i) \neq (a_l,a_i)$ this gives $b_l = b_i \in \boldsymbol{j}$. Suppose $Q$ is nonempty. Notice that $Q \subset \{1,\dots,n\} \setminus \{i\}$, since otherwise $\tilde{\boldsymbol{b}} = (b_1,\dots,b_n) \notin K_n$. Choose $m \in$

$\{1,\dots,n\}\setminus Q$, $m\neq i$. Then $(b_m,b_i)=(a_m,a_i)$, hence $b_i=a_i\geq j$ contrary to $b_i\in\boldsymbol{j}$. Thus $Q=\phi$ and $\tilde{\boldsymbol{b}}=\tilde{\mathbf{a}}$ by (3.1).

(ii) Thus let $A\subseteq\boldsymbol{j}$. Suppose that $\tilde{\boldsymbol{b}}\neq\tilde{\mathbf{a}}$. Then $M:=\{(r,s)\colon (b_r,b_s)\neq(a_r,a_s)\}$ is nonempty. Notice that due to $\beta>0$, clearly $b_r=b_s\in\boldsymbol{j}$ for every $(r,s)\in M$. Choose $1\leq i\leq n$ so that $a_i\neq b_i$ and set $C:=\{1\leq j\leq n\colon a_j=a_i\}$. For every $l\in\{1,\dots,n\}\setminus C$ clearly $(i,l)\in M$ and so $b_l=b_i$. By hypothesis $|A|>2$ and hence $a_i\neq a_j\neq b_i$ for some $1\leq j\leq n$. Let $c\in C$ be arbitrary. Clearly $(b_c,b_j)=(b_c,b_i)\neq(a_c,a_j)$ and again $b_c=b_j=b_i$. Together $\tilde{\boldsymbol{b}}=(b_i,\dots,b_i)\notin K_n$. This contradiction shows the required $\tilde{\boldsymbol{b}}=\tilde{\mathbf{a}}$. □

**DEFINITION 3.3.** For the remaining peak operations $\chi^n_{\tilde{\mathbf{a}}}$ with $A\subseteq\boldsymbol{j}$ and $|A|=2$ we need the following additional operations.

(1) Let $\psi$ be any binary $j$–idempotent operation on $\boldsymbol{k}$ satisfying $\psi(0,x)=\psi(x,0)=0$ and $\psi(x,k-1)=k-1$ for all $x\in\boldsymbol{k}\setminus\{0\}$.

(2) For each $d\in\{0,\dots,k-2\}$ set $c_d(x,x):=x$ for all $x\in\boldsymbol{j}$ and $c_d(x,y):=d$ for all $(x,y)\in K_2$.

(3) Let $n>1$, let $0\leq r<s<j$ and let $\tilde{\mathbf{a}}=(a_1,\dots,a_n)\in\{r,s\}^n$ satisfy $(r,\dots,r)\neq\tilde{\mathbf{a}}\neq(s,\dots,s)$. Let $R:=\{i\colon a_i=r\}$ and $S:=\{i\colon a_i=s\}$.

Denote by $\rho$ and $\sigma$ the least elements of the nonempty sets $R$ and $S$. Set $R':=R\setminus\{\rho\}$ and $S':=S\setminus\{\sigma\}$ and define an $n$-ary operation $\varepsilon$ on $\boldsymbol{k}$ by

$$\varepsilon(x_1,\dots,x_n):\approx\bigwedge_{\nu\in R'}c_0(x_\rho,x_\nu)\wedge\bigwedge_{\nu\in S'}c_0(x_\sigma,x_\nu)\tag{3.2}$$

(where $\bigwedge_{\nu\in\phi}\nu:=k-1$). It is easy to verify that $\varepsilon(b_1,\dots,b_n)=z\wedge t$ if $b_u=z$, $b_v=t$ for all $u\in R$, $v\in S$ while $\varepsilon(b_1,\dots,b_n)=0$ otherwise. Finally, set

$$\nu_{\tilde{\mathbf{a}}}(x_1,\dots,x_n):\approx\psi\big(\varepsilon(x_1,\dots,x_n),[x_1,\dots,x_n]_{\tilde{\mathbf{a}}}\big)\,.\tag{3.3}$$

**LEMMA 3.4.** *If* $0<r<s$, *then* $\nu_{\tilde{\mathbf{a}}}=\chi^n_{\tilde{\mathbf{a}}}$.

P r o o f. $\nu_{\tilde{\mathbf{a}}}$ is obviously $\boldsymbol{j}$–idempotent. Notice that $\varepsilon(\tilde{\mathbf{a}})=r\wedge s=r>0$ and $[a_1,\dots,a_n]_{\tilde{\mathbf{a}}}=k-1$ and therefore $\nu_{\tilde{\mathbf{a}}}(\tilde{\mathbf{a}})=\psi(r,k-1)=k-1$. Let $\tilde{\boldsymbol{b}}=(b_1,\dots,b_n)\in K_n$ be such that $\nu_{\tilde{\mathbf{a}}}(\tilde{b})>0$. By Definition 3.3–1) clearly $\beta:=\varepsilon(\tilde{\boldsymbol{b}})>0$. By 3) there are distinct $z,t\in\boldsymbol{k}$ such that $\beta=z\wedge t$, $b_u=z$ for all $u\in R$ and $b_v=t$ for all $v\in S$. Let $\tilde{\boldsymbol{b}}\neq\tilde{\mathbf{a}}$. From the shape of $\tilde{\boldsymbol{b}}$ and (3.1) it follows that $[b_1,\dots,b_n]_{\tilde{\mathbf{a}}}=0$; and therefore $\nu_{\tilde{\mathbf{a}}}(\tilde{\boldsymbol{b}})=\psi(\beta,0)=0$. □

We turn to the case $r=0$. First we consider the case $s<k-1$. Let $\tau$ be the binary $\boldsymbol{j}$–idempotent operation on $\boldsymbol{k}$ satisfying $\tau(0,k-1)=k-1$ and $\tau(x,y)=0$ elsewhere on $K_2$. Set

$$\lambda_{\tilde{\mathbf{a}}}(x_1,\dots,x_n):\approx\tau\big(\varepsilon(x_1,\dots,x_n),[x_1,\dots,x_n]_{\tilde{\mathbf{a}}}\big)\,.$$

**Lemma 3.5.** *Let $r = 0$, let $s < k-1$ and let $\tilde{\mathbf{a}}$ be as in Definition 3.3. Then $\lambda_{\tilde{\mathbf{a}}} = \chi^n_{\tilde{\mathbf{a}}}$.*

Proof. Clearly $\lambda_{\tilde{\mathbf{a}}}(\tilde{\mathbf{a}}) = \tau(0, k-1) = k-1$. Let $\tilde{\boldsymbol{b}} = (b_1, \dots, b_n) \in K_n$ be such that $\tilde{\boldsymbol{b}} \neq \tilde{\mathbf{a}}$ and $l := \lambda_{\tilde{\mathbf{a}}}(\tilde{\boldsymbol{b}}) > 0$. Let $e := \varepsilon(\tilde{\boldsymbol{b}})$. Observe that $e < k-1$ since $\tilde{\boldsymbol{b}} \in K_n$ is distinct from $(k-1, \dots, k-1)$. Notice that $e > 0$ because otherwise $0 < \lambda_{\tilde{\mathbf{a}}}(\tilde{\boldsymbol{b}}) = \tau(0, [b_1, \dots, b_n]_{\tilde{\mathbf{a}}}) = 0$. Thus $l = z \wedge t$ where $b_u = z$ for all $u \in R$ and $b_v = t$ for all $v \in S$. As $\tilde{\boldsymbol{b}} \neq \tilde{\mathbf{a}}$, clearly $[b_1, \dots, b_n]_{\tilde{\mathbf{a}}} = 0$, and $\lambda_{\tilde{\mathbf{a}}}(\tilde{\boldsymbol{b}}) = \tau(e, 0) = 0$. □

Finally, we turn to the remaining case $r = 0$ and $s = k-1$. Since $\{0, k-1\} = A \subseteq \boldsymbol{j}$, clearly $j = k$. Let

$$\xi(x_1, \dots, x_n) :\approx \bigwedge_{\nu \in R'} c_1(x_\rho, x_\nu)\,, \tag{3.4}$$

$$\mu_{\tilde{\mathbf{a}}}(x_1, \dots, x_n) :\approx \tau\big(\xi(x_1, \dots, x_n), [x_1, \dots, x_n]_{\tilde{\mathbf{a}}}\big)\,.$$

**Lemma 3.6.** *Let $\tilde{\mathbf{a}}$ be an $n$-tuple from Definition 3.3 corresponding to $r = 0$, $s = k-1$ and $j = k$. If $R = \{\rho\}$ then $[x_1, \dots, x_n]_{\tilde{\mathbf{a}}} = \chi^n_{\tilde{\mathbf{a}}}$. If $|R| > 1$ then $\mu_{\tilde{\mathbf{a}}} = \chi^n_{\tilde{\mathbf{a}}}$.*

Proof. 1) Let $R = \{\rho\}$. Clearly $[a_1, \dots, a_n]_{\tilde{\mathbf{a}}} = k-1$. Suppose that $\beta := [b_1, \dots, b_n] \neq 0$ for some $\tilde{\boldsymbol{b}} = (b_1, \dots, b_n) \in K_n$. Since $\tilde{\boldsymbol{b}} \neq (b_\rho, \dots, b_\rho)$, we have $(b_\rho, b_w) = (0, k-1)$ for some $w \in S$; and so $b_\rho = 0$. By the same argument $b_v = k-1$ for all $v \in S$ proving $\tilde{\boldsymbol{b}} = \tilde{\mathbf{a}}$.
2) Let $|R| > 1$. Observe that $c_1(a_\rho, a_\nu) = c_1(0,0) = 0$ for all $\nu \in R'$ and therefore $\xi(\tilde{\mathbf{a}}) = 0$. Next by (3.1) we have $[a_1, \dots, a_n]_{\tilde{\mathbf{a}}} = k-1$ and so $\mu_{\tilde{\mathbf{a}}}(a_1, \dots, a_n) = \tau(0, k-1) = k-1$. Suppose to the contrary that $\beta := \mu_{\tilde{\mathbf{a}}}(b_1, \dots, b_n) > 0$ for some $\tilde{\boldsymbol{b}} = (b_1, \dots, b_n) \in K_n$, $\tilde{\boldsymbol{b}} \neq \tilde{\mathbf{a}}$. Let $z := \xi(b_1, \dots, b_n)$ and $t := [b_1, \dots, b_n]_{\tilde{\mathbf{a}}}$. From the definition of $\tau$ either $(z,t) = (0, k-1)$ or $z = t \in \boldsymbol{j}$.
(i) Let $z = 0$ and $t = k-1$. From (3.1) we obtain $b_u \in \{0, k-1\}$ for all $u \in R$ and $b_v = k-1$ for all $v \in S$. Since $\tilde{\boldsymbol{b}} \neq \tilde{\mathbf{a}}$, clearly $\{b_\rho, b_\nu\} = \{0, k-1\}$ for some $\nu \in R'$; hence $c_1(b_\rho, b_\nu) = 1$ and $z = \xi(b_1, \dots, b_n) = 1$ in contradiction to the assumption $z = 0$.
(ii) Thus let $z = t \in \boldsymbol{j}$. By (3.1) clearly $\tilde{\boldsymbol{b}} = (z, \dots, z)$ in contradiction to $\tilde{\boldsymbol{b}} \in K_n$. □

Using the $\boldsymbol{j}$–idempotent peak operations, the $\boldsymbol{j}$–idempotent constants, $\wedge$ and $\vee$ we can easily represent every $\boldsymbol{j}$–idempotent operation by the following canonical form.

**DEFINITION 3.7.** Let $f$ be a $\jmath$–idempotent $n$-ary operation on $\boldsymbol{k}$. For $0 < b < k$ set $F(b) := f^{-1}(b) \cap K_n$ and

$$\varphi_b(x_1, \ldots, x_n) :\approx \bigvee_{\tilde{\mathbf{a}} \in F(b)} \chi^n_{\tilde{\mathbf{a}}}(x_1, \ldots, x_n)\,.$$

Clearly $\varphi_b$ is $\jmath$–idempotent, takes the value $k-1$ on $F(b)$ and vanishes elsewhere on $K_n$. Now for all $0 < b < k-1$ set

$$c^n_b(x) :\approx c_b\bigl(c_b(\ldots c_b(x_1, x_2), \ldots, x_{n-1})x_n\bigr)\,. \tag{3.5}$$

Clearly $c^n_b$ is the $\jmath$–idempotent $n$-ary constant with value $b$ on $K_n$. Set $\gamma_{k-1} := \varphi_{k-1}$ and $\gamma_b := c^n_b \wedge \varphi_b$ for all $0 < b < k-1$. Obviously $\gamma_b$ is the $\jmath$–idempotent $n$-ary operation taking the value $b$ on $F(b)$ and vanishing elsewhere on $k_n$. From 3.7 we obtain:

**THEOREM 3.8.** *Let $0 < j < k$. If $f$ is an $n$-ary $\jmath$–idempotent operation on $\boldsymbol{k}$ distinct from $c^n_0$, then*

$$f = \gamma_1 \vee \cdots \vee \gamma_{k-1} \tag{3.6}$$

*(where $\gamma_1, \ldots, \gamma_{k-1}$ are defined in 3.7).*

R e m a r k s 3.9. 1) $c^n_0$ has the representation (3.5).

2) The canonical form (3.6) is based on the following binary $\jmath$–idempotent operations: i) 2 lattice operations: $\wedge$ and $\vee$, ii) $k^2 - j$ operations $\chi^2_{ab}$, (iii) $k-1$ operations $c_0, \ldots, c_{k-2}$ and (iv) $\psi$ and $\tau$. It follows that the clone of $\jmath$–idempotent operations is generated by $k^2 + k + 3 - j$ binary operations.

3) The fact that the operations listed in 2) generate $K_J$ can be verified from the completeness criterion for $K_J$ from [Sze 89] Cor. 2 and [Lau 92].

## REFERENCES


[B-D 82] BAGYINSZKI, J.—DEMETROVICS, J.: *The lattice of linear classes in prime valued logics*, in: Discrete Mathematics, Banach Center Publications, Vol. 7, 1982, pp. 101–123.

[B-K-K-R 69] BODNARCHUK, V. G.—KALUZHNIN, L. A.—KOTOV, V. N.—ROMOV, B. A.: *Galois theory for Post algebras Part I*, Kibernetika **3** (1969), 1–10; *Part II*, ibid **5** (1969), 1–9 (Russian), English translation Cybernetics (1969) 243–252, 531–539.

[Csá 83] CSÁKÁNY, B.: *All minimal clones on the three-element universe*, Acta Cybernet. **6** (1983), 227–238.

[Csi 84] CSIKÓS, M.: *Finitely generated clones with linear functions in $P_3$ and $P_5$*, Közl. MTA Számitástech. Automat. Kutató Int. Budapest **31** (1984), 7–21.

[Dan 81] DANILCHENKO, A. F.: *On parametrical expressibility of the functions of k-valued logic*, in: Finite Algebra and multiple-valued Logic (Csákány, B.; Rosenberg, I. G., eds.), Szeged, Hungary, 1979, Coll. Math. Soc. J. Bolyai, Vol. 28, North Holland 1981, pp. 147–160.

[D-H 83] DEMETROVICS, J.—HANNÁK, L.: *The number of reducts of a preprimal algebra*, Algebra Universalis **16** (1983), 178–185.

[Iab 58] IABLONSKII, S. V.: *Functional constructions in $k$-valued logic*, Trudy Mat. Inst. Steklov **51** (1958), 5–142. (Russian)

[I-M 59] IANOV, Iu. I.—MUCHNIK, A. A.: *Existence of $k$-valued closed classes without a finite basis*, Doklady Akad. Nauk SSSR **127** (1959), 44–46. (Russian)

[Lau 78] LAU, D.: *Über die Anzahl von abgeschlossenen Mengen linearer Funktionen der $n$-wertigen Logik*, Elektron. Informationsvearb. Kybernet. EIK **14** (1978), 567–569.

[Lau 91] LAU, D.: *Die maximalen Klassen von* $\bigcap_{a\in Q} \mathrm{Pol}_k\{a\}$ *für* $Q \subseteq E_k$ *(Ein Kriterium für endliche semi-primale Algebren mit nur trivialen Unteralgebren)*, preprint Univ. Rostock 1991, rev. 1992, 27 pp.

[MK 76] McKENZIE, R.: *On minimal locally finite varieties with permuting congruence relations*, preprint, 1976.

[MK 78] McKENZIE, R.: *Para primal varieties: A study of finite axiomatizability and definable principal congruences in locally finite varieties*, Algebra Universalis **8** (1978), 336–348.

[Mal 66] MAL'TSEV, A. I.: *Iterative algebras and Post's varieties*, Algebra i Logika **5** (1966), 5–24. English translation: *The mathematics of algebraic systems*, in: Collected papers 1936–67, Studies in Logics and Foundations of Mathematics, Vol. 66, North Holland, Amsterdam, 1971.

[Mar 79] MARCHENKOV, S. S.: *On closed classes of selfdual functions in $k$-valued logics*, Problemy kibernetiki **36** (1979), 5–22. (Russian)

[Mar 83] MARCHENKOV, S. S.: *On closed classes of selfdual functions in manyvalued logics II*, Problemy kibernetiki **40** (1983), 261–266. (Russian)

[Mar 84] MARCHENKOV, S. S.: *On clones in $P_k$ containing homogeneous functions*, preprint Inst. Appl. Math. Acad. Sci. U. S. S. R. **35** (1984), 1–28. (Russian)

[Qua 92] QUACKENBUSH, R. W.: *A survey of minimal clones*, preprint Univ. of Manitoba 1992; Aequationes Math. (to appear).

[Ros 83] ROSENBERG, I. G.: *Minimal clones I: the five types*, in: Lectures in Universal Algebra, Szeged, (Szabó, L.; Szendrei, A., eds.); Colloquia Math. Soc. J. Bolyai, Vol. 43, 1983, pp. 405–427.

[Sal 64] SALOMAA, A.: *On infinitely generated sets of operations in finite algebras*, Ann. Acad. Sc. Fenn., Ser A I **363** (1965), 1–12.

[Sze 84] SZABÓ, L.: *Characterization of clones acting bicentrally and containing a primitive permutation group*, Acta Cybernet. **7** (1984), 137–142.

[Sze 82] SZENDREI, Á.: *Algebras of prime cardinality with a cyclic automorphism*, Arch. Math. (Basel) **39** (1982), 417–427.

[Sze 86] SZENDREI, Á.: *Clones in universal algebra*, NATO Adv. Study Inst. (Montréal 1984), SMS vol 99. Les presses de l'Université de Montréal, 1986.

[Sze 89] SZENDREI, Á.: *A classification of strictly simple algebras with trivial subalgebras*, Demonstr. Math. **24** (1991), 149–173.

Received March 15, 1994

*Département de mathématiques et de Statistique*
*Université de Montréal*
*CANADA*

*E-mail*: rosenb@ere.umontreal.ca