Characterization of clones acting bicentrally and containing a primitive group

LÁSZLÓ SZABÓ

1. Introduction

For a set F of operations on a set A the centralizer F^* of F is the set of operations on A commuting with every member of F. If $F=F^{**}$ then we say that F acts bicentrally. The sets of operations on A acting bicentrally form a complete lattice $\mathcal{L}_A$ with respect to $\subseteqq$.

The clones acting bicentrally were characterized in [7] and [12]. The lattice $\mathcal{L}_A$ was completely described for $|A|=3$ in [3] and [4]. Some further properties of $\mathcal{L}_A$ can be found in [5] and [13].

In this paper for finite sets the clones acting bicentrally and generated by permutations and constant operations are characterized (Theorem 1) and the clones acting bicentrally and containing primitive groups are described (Corollary 2 and Theorem 5). As a corollary a characterization for basic groups is obtained (Corollary 6).

2. Preliminaries

Let A be an at least two element finite set which will be fixed in the sequel. The set of all n-ary operations on A will be denoted by $0_A^{(n)}$ $(n\geqq 1)$. Furthermore, we set $0_A=\bigcup\limits_{n\geqq 1} 0_A^{(n)}$. A set $F\subseteqq 0_A$ is said to be a *clone* if it contains all projections and is closed with respect to superposition of operations. Denote by $[F]$ the clone generated by $F\subseteqq 0_A$. Let f and g be operations on A of arities n and m, respectively. We say that f and g *commute* if for any elements $a_{11}, \dots, a_{mn}\in A$ we have $f(g(a_{11}, \dots, a_{m1}), \dots, g(a_{1n}, \dots, a_{mn}))=g(f(a_{11}, \dots, a_{1n}), \dots, f(a_{m1}, \dots, a_{mn}))$. It can be easily seen that f and g commute if and only if f is a homomorphism from $\langle A; g\rangle^n$ into $\langle A; g\rangle$ (or g is a homomorphism from $\langle A; f\rangle^m$ into $\langle A; f\rangle$).

By the *centralizer* of a set $F\subseteqq 0_A$ we mean the set $F^*\subseteqq 0_A$ consisting of all operations that commute with every member of F. The set F^{**} is called the *bicentralizer* of F. If $F=F^{**}$ then we say that F *acts bicentrally*.

The set of all projections, the set of all permutations on A, and the set of all unary constant operations will be denoted by P_A, S_A and C_A, respectively.

An operation $f\in 0_A$ *depends* on its i-th variable $(1\leqq i\leqq n)$ if there are elements $a_1, \ldots, a_n, a_i'\in A$ such that $f(a_1, \ldots, a_n)\neq f(a_1, \ldots, a_{i-1}, a_i', a_{i+1}, \ldots, a_n)$.

We adapt the terminology of [6] except that polynomials will be called *term functions*. Consequenltly, for an algebra $\mathfrak{A}=\langle A;\ F\rangle$ the set of its term functions and the set of its algebraic functions will be denoted by $T(\mathfrak{A})$ and $A(\mathfrak{A})$, respectively. The algebra $\mathfrak{A}$ is called *complete (functionally complete)* if $T(\mathfrak{A})=0_A$ $(A(\mathfrak{A})=0_A)$. $\mathfrak{A}$ is *trivial* if $T(\mathfrak{A})=P_A$.

Let A be a vector space over a field K. Then the algebra $\langle A; I\rangle$, where I is the set of all idempotent term functions of the vector space A, is said to be an *affine space* over K. By a *linear operation* over the vector space A we mean an operation of the form $\sum_{i=1}^{n} A_i x_i + a$ where $a\in A$ and the A_i are linear transformations of A. It is easy to check that I^* consists of all linear operations over A. If a clone $F\subseteqq 0_A$ consists of linear operations over a vector space with base set A, then we say that F is a *linear clone.*

For a natural number n denote by $\underset{\sim}{n}$ the set $\{1, \ldots, n\}$. Let B be a nonempty set and let $m\geqq 2$. An n-ary wreath operation w on the set B^m is associated to transformations p_i of B $(i=1, \ldots, m)$ and maps $r\colon \underset{\sim}{m}\to\underset{\sim}{n}$, $s\colon \underset{\sim}{m}\to\underset{\sim}{m}$ as follows. For $x_i=(x_{i1}, \ldots, x_{im})\in B^m$, $i=1, \ldots, n$, let

$$w(x_1, \ldots, x_n) = \big(p_1(x_{r(1)s(1)}), \ldots, p_m(x_{r(m)s(m)})\big).$$

If $E\subseteqq 0_B^{(1)}$ then $W_{E,m}$ denotes the set of all wreath operations on B^m with $p_i\in E$. Now a set of operations $F\subseteqq 0_A$ is said to be a *wreath clone* if there is a set B, a natural number $m\geqq 2$ and a transformation monoid $E\subseteqq 0_B^{(1)}$ containing id_B such that $\langle A;\ F\rangle\cong\langle B^m;\ W_{E,m}\rangle$.

For a permutation group G acting on A a subset $B\subseteqq A$ is called a *block* of G if for every $g\in G$, either $g(B)=B$ or $g(B)\cap B=\emptyset$. The one-element sets $\{a\}(a\in A)$ and A are called *trivial blocks.* A transitive permutation group G is said to be primitive if it has trivial blocks only.

Following Salomaa [10] a permutation group G on a finite set A is *basic* if the $\langle A;\ G\cup\{f\}\rangle$ is complete for every surjective operation $f\in 0_A$ depending on at least two variables.

Two algebras (on a common base set) are *equivalent* if they have the same set of term functions.

We shall use the following result from [8].

Theorem A. A nontrivial finite algebra with primitive automorphism group is functionally complete unless it is equivalent to one of the following algebras:

(i) $\mathfrak{B}^m$, where $m\geqq 2$ and $\mathfrak{B}$ is a functionally complete algebra with primitive automorphism group of composite order,

(ii) an affine space over a finite field,

(iii) $\langle A;\ x+1\rangle$, where $\langle A;\ +\rangle$ is a cyclic group of prime order and $1\in A\setminus\{0\}$,

(iv) $\langle A;\ x-y+z+1\rangle$, where $\langle A;\ +\rangle$ is a cyclic group of prime order and $1\in A\setminus\{0\}$,

(v) $\langle A;\ xy+xz+yz\rangle$, where $\langle A;\ +,\ \cdot\rangle$ is the two element field.

We also need the following characterization of basic groups given in [9] (see also [1, 2]).

Theorem B. A permutation group G on A is basic if and only if G is primitive and G is a subset of no linear clone and no wreath clone.

Results

Let G be a permutation group acting on A, and denote by G_a the stabilizer of the element $a\in A$ (that is $G_a=\{g\in G|g(a)=a\}$). For any $a\in A$ let $\bar{a}=\{x\in A|G_a\subseteqq G_x\}$. The next theorem describes the subclones of $[S_A\cup C_A]$ acting bicentrally.

Theorem 1. Let $F\subseteqq[S_A\cup C_A]$ be a clone and put $G=F\cap S_A$, $C=F\cap C_A$. Then F acts bicentrally if and only if C contains every unary constant operation $A\to\{a\}$ with $\bar{a}=\{a\}$.

Proof. For any $a\in A$ let us denote by c_a the unary constant operation with value a.

Let $F\subseteqq[S_A\cup C_A]$ be a clone. First suppose that F acts bicentrally. Let $f\in F^*$ and choose an element $a\in A$ such that $\bar{a}=\{a\}$. If $g\in G_a$ then $f(a, \dots, a)= =f(g(a), \dots, g(a))=g(f(a, \dots, a))$ showing that $f(a, \dots, a)\in\bar{a}$ and $f(a, \dots, a)=a$. It follows that $c_a\in F^{**}=F$.

Now suppose that $c_a\in C$ whenever $\bar{a}=\{a\}$. We have to show that $F=F^{**}$. In [11] it is proved that $[S_A\cup C_A]$ acts bicentrally. Thus we have $F^{**}\subseteqq[S_A\cup C_A]^{**}= =[S_A\cup C_A]$. Therefore it is enough to show that $F^{**}\cap(S_A\cup C_A)=G\cup C$.

Let $A=\{a_1, \dots, a_n\}$ and define an n-ary operation f as follows:

$$f(x_1, \dots, x_n)=\begin{cases} x_1 & \text{if } (x_1, \dots, x_n)=\big(g(a_1), \dots, g(a_n)\big) \text{ for some } g\in G,\\ x_2 & \text{otherwise.}\end{cases}$$

Now $f\in(G\cup C)^*=F^*$ and if $g\in S_A\setminus G$ then $g\notin\{f\}^*$. It follows that $F^{**}\cap S_A=G$.

For any $a\in A$ with $c_a\notin C$ and for any $u\in\bar{a}$ define a unary operation $h_{a,u}$ as follows:

$$h_{a,u}(x)=\begin{cases} g(u) & \text{if } x=g(a) \text{ for some } g\in G,\\ x & \text{otherwise.}\end{cases}$$

Remark that h is well-defined. Indeed, if $g_1(a)=g_2(a)$ for some $g_1, g_2\in G$ then $g_1^{-1}\circ g_2\in G_a$ which implies $g_1^{-1}\circ g_2\in G_u$ and $g_1(u)=g_2(u)$.

We show that $h_{a,u}\in F^*=(G\cup C)^*$. Let $t\in G$ and $x\in A$. If $x=g(a)$ for some $g\in G$ then $t\big(h_{a,u}(x)\big)=t\big(h_{a,u}(g(a))\big)=t\big(g(u)\big)=h_{a,u}\big(t(g(a))\big)=h_{a,u}\big(t(x)\big)$. If $x\notin\{g(a)|g\in \in G\}$ then $t(x)\notin\{g(a)|g\in G\}$, and therefore $t\big(h_{a,u}(x)\big)=t(x)=h_{a,u}\big(t(x)\big)$. Hence $h_{a,u}$ commutes with t. Now let $c_b\in C$. Then $b\notin\{g(a)|g\in G\}$ since $b=g(a)$ implies $c_a=g^{-1}\circ c_b\in F\cap C_A=C$. Therefore for any $x\in A$ we have $c_b\big(h_{a,u}(x)\big)=b=h_{a,u}(b)= =h_{a,u}\big(c_b(x)\big)$. Hence $h_{a,u}\in F^*$.

Finally let $c_a\in C_A\setminus C$. By assumption there is an element $u\in\bar{a}$ with $u\neq a$. Now $h_{a,u}\in F^*$ and $c_a\big(h_{a,u}(u)\big)=a\neq u=h_{a,u}(a)=h_{a,u}\big(c_a(u)\big)$ showing that $h_{a,u}$ and c_a do not commute. Thus we have $F^{**}\cap C_A=C$ and $F^{**}\cap(S_A\cup C_A)=(F^{**}\cap S_A)\cup \cup(F^*\cap C_A)=G\cup C$, which completes the proof. □

Corollary 2. Let $F\subseteq[S_A\cup C_A]$ be a clone such that $G=F\cap S_A$ is a primitive permutation group. Then F acts bicentrally if and only if either $F\cap C_A=C_A$, or $F\cap C_A=\emptyset$ and G is a regular group of prime order.

Proof. Since G is transitive and F is a clone, we have either $F\cap C_A=C_A$ or $F\cap C_A=\emptyset$.

Suppose that $F\cap C_A$ contains every unary constant operation c_a with $\bar{a}=\{a\}$. If $F\cap C_A=\emptyset$ then $\bar{a}\neq\{a\}$ for any $a\in A$. Let $a\in A$ and $x\in\bar{a}$ with $x\neq a$. Then $G_a\subseteq G_x$. Since the stabilizer subgroups of two distinct elements cannot coincide in a primitive group of composite order (see [14; Prop. 8.6]), it follows that G has prime order. Hence G is a regular group of prime order. In this case $\bar{a}=A$ for any $a\in A$. Finally apply Theorem 1. □

Next we prove two lemmas.

Lemma 3. If $\mathfrak{A}=\langle A;\, F\rangle$ is a functionally complete algebra then $F^*\subseteq\subseteq[S_A\cup C_A]$ and consequently $F^*=[\mathrm{End}\,\mathfrak{A}]$.

Proof. Using the functional completeness of $\mathfrak{A}$, it is not hard to show that $(*)$ if θ is a congruence on $\mathfrak{A}^n$ $(n\geqq 1)$ then there exist $i_1, \dots, i_k$ $(k\geqq 0,\ 1\leqq i_1<\dots<<i_k\leqq n)$ such that

$$\theta = \{((a_1, \dots, a_n), (b_1, \dots, b_n))\in(A^n)^2\colon\ a_{i_1} = b_{i_1}, \dots, a_{i_k} = b_{i_k}\}.$$

Clearly, then θ has $|A|^k$ classes.

Now let $f\in F^*$ be an n-ary operation $(n\geqq 1)$. Then f is a homomorphism from $\mathfrak{A}^n$ to $\mathfrak{A}$ and therefore $\ker f$ is a congruence on $\mathfrak{A}^n$. If $\ker f=(A^n)^2$ then f is constant and therefore $f\in[C_A]\subseteq[S_A\cup C_A]$. If $\ker f\neq(A^n)^2$ then (since $\ker f$ has at most $|A|$ classes), by $(*)$, there exists an i $(1\leqq i\leqq n)$ such that

$$\ker f=\{((a_1, \dots, a_n), (b_1, \dots, b_n))\in(A^n)^2\colon\ a_i=b_i\}.$$

From this it follows that f depends only on its i-th variable, and $f\in[S_A]\subseteq[S_A\cup C_A]$. □

Lemma 4. Let $\mathfrak{A}=\langle A;\, F\rangle$ be a functionally complete algebra and let $m\geqq 2$. Then the centralizer of F on A^m coincides with $W_{E,m}$ where $E=\mathrm{End}\,\mathfrak{A}$.

Proof. Let f be an n-ary operation on A^m that is $f\colon (A^m)^n\to A$. Let $f_1, \dots, f_m$ be the $m\cdot n$-ary operations on A defined as follows: For any $(a_{i1}, \dots, a_{im})\in A^m$, $i=1, \dots, n$, let $f((a_{11}, \dots, a_{1m}), \dots, (a_{n1}, \dots, a_{nm}))=(f_1(a_{11}, \dots, a_{nm}), \dots, f_m(a_{11}, \dots, a_{nm}))$. Observe that f is a wreath operation if and only if each f_j depends on at most one variable, $j=1, \dots, m$.

Now $f\in F^*$ on A^m if and onyl if f is a homomorphism from $(\mathfrak{A}^m)^n$ into $\mathfrak{A}^m$ which is equivalent to that $f_1, \dots, f_m$ are homomorphisms from $(\mathfrak{A}^m)^n$ into $\mathfrak{A}$. The latter means exactly that $f_1, \dots, f_m\in F^*$ on A. Taking into consideration Lemma 3, this is equivalent to that $f_1, \dots, f_m\in[\mathrm{End}\,\mathfrak{A}]$. This completes the proof. □

The following theorem completely describes those clones acting bicentrally and containing a primitive permutation group which are not contained in $[S_A\cup C_A]$.

Theorem 5. Let $F\subseteq O_A$ be aclone acting bicentrally and containing a primitive permutation group such that $F\nsubseteq[S_A\cup C_A]$. Then we have for F one of the following five possibilities:

(1) $\langle A;\ F\rangle \cong \langle B^m;\ W_{E,m}\rangle$ where B is a finite set, $m \geqq 2$, and $E = G \cup C_B$ with $G \subseteqq S_B$ a primitive group of composite order,

(2) F is the set of all linear operations over a vector space with base set A,

(3) $F = \{x+1\}^*$ where $\langle A;\ +\rangle$ is a cyclic group of prime order and $1 \in A \setminus \{0\}$,

(4) $F = [\{x-y+z+1\}]$ where $\langle A;\ +\rangle$ is a cyclic group of prime order and $1 \in A \setminus \{0\}$,

(5) $F = 0_A$.

Proof. Let F satisfy the hypothesis of the theorem. If $F^* = P_A$ then $F = F^{**} = P^* = 0_A$ that is we have case (5). Let us suppose that $F^* \neq P_A$. Then $\langle A;\ F^*\rangle$ is a nontrivial algebra with primitive automorphism group. If $\langle A;\ F^*\rangle$ is functionally complete then, according to Lemma 3, we have $F = F^{**} \subseteqq [S_A \cup C_A]$ contrary to our assumption on F. Hence $\langle A;\ F^*\rangle$ is not functionally complete. Therefore, taking into consideration Theorem A, we get for the algebra $\langle A;\ F^*\rangle$ one of the cases (i)—(v).

If $\langle A;\ F^*\rangle \cong \langle B^m;\ H\rangle$ where $m \geqq 2$ and $\mathfrak{B} = \langle B;\ H\rangle$ is a functionally complete algebra with primitive automorphism group of composite order, then Lemma 4 shows that $\langle A;\ F\rangle = \langle A;\ F^{**}\rangle \cong \langle B^m;\ W_{E,m}\rangle$ where $E = \operatorname{End} \mathfrak{B}$. In [8; Lemma 1] it was proved that a finite algebra with primitive automorphism group of composite order has idempotent term functions only. Therefore all unary constant operations on B belong to $\operatorname{End} \mathfrak{B}$. Hence $E = \operatorname{End} \mathfrak{B} = \operatorname{Aut} \mathfrak{B} \cup C_B$ and we have (1).

In case (ii) and (iii) F enjoys property (2) and (3), respectively. In case (iv) it is easy to show that $F = F^{**} = \{x-y+z+1\}^* = [\{x-y+z+1\}]$, that is we have (4).

Finally for $\langle A;\ F^*\rangle$ the case (v) cannot occur. Indeed, it can be shown easily that if $\langle A;\ +,\ \cdot\rangle$ is the two element field then $\{xy+xz+yz\}^* = [S_A \cup C_A]$ and $F = F^{**} = \{xy+xz+yz\}^* = [S_A \cup C_A]$ contradicts our assumption on F. □

Combining Theorem 5 with Theorem B we get the following characterization for basic groups.

Corollary 6. A permutation group G acting on A ($|A| \geqq 3$) is basic if and only if $(G \cup f)^{**} = 0_A$ for any operation $f \in 0_A \setminus [S_A \cup C_A]$.

Proof. If G is primitive then our statement follows immediately from Theorem 5 and Theorem B. If G is imprimitive then, by Theorem B, G is not basic. Let B be a nontrivial block of G and choose an element $a \in B$. Define a unary operation f and a binary operation g as follows:

$$f(x) = \begin{cases} a & \text{if } x \in B, \\ x & \text{otherwise,} \end{cases}$$

$$g(x, y) = \begin{cases} x & \text{if } (x, y) = (t(u),\ t(v)) \text{ for some } t \in G \text{ and } u, v \in B, \\ y & \text{otherwise.} \end{cases}$$

Then it is easy to check that $G \cup \{f\} \subseteqq \{g\}^*$. Furthermore, $\{g\}^* \neq 0_A$ since if $u, v \in B$, $u \neq v$, and $h \in 0_A^{(1)}$ is such that $h(u) \in B$ and $h(v) \in A \setminus B$ then $h \notin \{g\}^*$. Therefore $(G \cup \{f\})^{**} \subseteqq \{g\}^{***} = \{g\}^* \neq 0_A$, which completes the proof. □

References

[1] BAĬRAMOV, R. A., Fundamentality criteria for permutation groups and transformation semigroups, Dokl. Akad. Nauk SSSR, 9 (1969), 455—457 (Russian).

[2] BAĬRAMOV, R. A., Derivation of basicity criteria for permutation groups and transformation semigroups from a theorem of Rosenberg, Kibernetika (Kiev).

[3] DANIL'CENKO, A. F., On the parametrical expressibility of functions of three-valued logic, Algebra i logika, 16/4 (1977), 379—497 (Russian).

[4] DANIL'CENKO, A. F., Parametrically closed classes of functions of three-valued logic, Izv. Akad. Nauk Moldav. SSR, 1978, no. 2, 13—20 (Russian).

[5] DANIL'CENKO, A. F., On parametrical expressibility of the functions of k-valued logic, in: Finite Algebra and Multiple-valued Logic (Proc. Conf. Szeged, 1979), Colloq. Math. Soc. J. Bolyai, vol. 28, North-Holland (Amsterdam, 1981), 147—159.

[6] GRÄTZER, G., Universal algebra, 2nd ed., Birkhauser Verlag, 1979.

[7] KUZNECOV, A. V., On detecting non-deducibility and non-expressibility, in: Logical deduction, Nauka, Moscow (1979) 5—33 (Russian).

[8] PÁLFY, P. P., L. SZABÓ and Á. SZENDREI, Automorphism groups and functional completeness, Algebra Universalis, 15 (1982), 395—400.

[9] ROSENBERG, I. G., On closed classes, basic sets and groups, Preprint, CRMA Université de Montréal.

[10] SALOMAA, A. A., On basic groups for the set of functions over a finite domain, Proc. Camb. Phil. Soc., 62 (1966), 597—611.

[11] SZABÓ, L., Endomorphism monoids and clones, Acta Math. Acad. Sci. Hung., 26 (1975), 279—280.

[12] SZABÓ, L., Concrete representation of related structures of universal algebras I., Acta Sci. Math., 40 (1978), 175—184.

[13] SZABÓ, L., On the lattice of clones acting bicentrally, Acta Cybernetica, v. 6 (1984), 381—387.

[14] WIELANDT, H., Finite permutation groups, Academic Press (New York and London, 1964).

(Received Aug 30, 1983)