Novi Sad J. Math.
Vol. 34, No. 2, 2004, 153-166
Proc. Novi Sad Algebraic Conf. 2003
(eds. I. Dolinka, A. Tepavčević)

ON CENTRALIZERS OF MONOIDS

Hajime Machida[1], **Ivo G. Rosenberg**[2]

Abstract. For a monoid M of k-valued unary operations, the centralizer M^* is the clone consisting of all k-valued multi-variable operations which commute with every operation in M. First we give a sufficient condition for a monoid M to have the least clone as its centralizer. Then using this condition we determine centralizers of all monoids containing the symmetric group.

AMS Mathematics Subject Classification (2000):

Key words and phrases: Clone; centralizer; monoid

1. Preliminaries

Let $\boldsymbol{k} = \{0, 1, \ldots, k-1\}$ for a fixed integer $k \geq 2$. For $n > 0$ let $\mathcal{O}_k^{(n)}$ be the set of all n-ary operations over $\boldsymbol{k}$, i.e., the set of all functions from $\boldsymbol{k}^n$ into $\boldsymbol{k}$. Set $\mathcal{O}_k = \bigcup_{n=1}^{\infty} \mathcal{O}_k^{(n)}$. A *projection* e_i^n over $\boldsymbol{k}$, for $1 \leq i \leq n$, is defined by $e_i^n(x_1, \ldots, x_i, \ldots, x_n) = x_i$ for every $(x_1, \ldots, x_n) \in \boldsymbol{k}^n$. The set of all projections over $\boldsymbol{k}$ is denoted by $\mathcal{J}_k$.

A subset C of $\mathcal{O}_k$ is a *clone* on $\boldsymbol{k}$ if (i) C is closed under (functional) composition and (ii) C contains $\mathcal{J}_k$. The set of all clones on $\boldsymbol{k}$ is a lattice with respect to inclusion. In this lattice, $\mathcal{O}_k$ is the greatest clone and $\mathcal{J}_k$ is the least clone. It is called the *lattice of clones* on $\boldsymbol{k}$ and is denoted by $\mathcal{L}_k$. The structure of $\mathcal{L}_2$ is completely known, but the structure of $\mathcal{L}_k$ for any $k \geq 3$ is still largely unknown.

An operation $f \in \mathcal{O}_k^{(n)}$ *commutes* (or *permutes*) with an operation $g \in \mathcal{O}_k^{(m)}$, denoted by $f \perp g$, if for every $m \times n$ matrix $B = (x_{ij})$ over $\boldsymbol{k}$ it holds that

$$f(g(x_{11}, \ldots, x_{m1}), \ldots, g(x_{1n}, \ldots, x_{mn})) = g(f(x_{11}, \ldots, x_{1n}), \ldots, f(x_{m1}, \ldots, x_{mn})).$$

For any subset G of $\mathcal{O}_k$, the *centralizer* G^* of G is defined to be the set of all operations f which commutes with every g in G, i.e.,

$$G^* = \{\ f \in \mathcal{O}_k \ \mid \ f \perp g \ \text{ for all } \ g \in G\ \}.$$

[1]Department of Mathematics, Hitotsubashi University, 2-1 Naka, Kunitachi, Tokyo 186-8601 Japan ⟨ machida@math.hit-u.ac.jp ⟩

[2]Départment de mathématiques et de statistique, Université de Montréal, C.P.6128, Succ. “Centre-ville”, Montréal, Québec, H3C 3J7, Canada ⟨ rosenb@DMS.UMontreal.CA ⟩

It is clear that G^* is a clone for any subset G of $\mathcal{O}_k$, i.e., $G^* \in \mathcal{L}_k$.

A *transformation monoid* (or, simply, a *monoid*) on $\boldsymbol{k}$ is defined as a composition-closed subset of unary operations on $\boldsymbol{k}$ containing the identity operation, that is, a subset M of $\mathcal{O}_k^{(1)}$ is a (transformation) monoid on $\boldsymbol{k}$ if (i) M is closed under composition and (ii) the identity operation $\mathrm{id}_{\boldsymbol{k}}$ $(= e_1^1)$ belongs to M. The set of all monoids on $\boldsymbol{k}$ is also a lattice with respect to inclusion. The lattice of monoids on $\boldsymbol{k}$ is denoted by $\mathcal{M}_k$. $\mathcal{M}_k$ is a finite lattice, but its structure is quite complicated when k is large.

The purpose of this paper is to study the centralizers of monoids of unary operations instead of centralizers of any subsets of $\mathcal{O}_k$. So, we examine more closely the definition of a centralizer of a monoid of unary operations. For a monoid M in $\mathcal{M}_k$, the centralizer of M is defined as follows:

$$\begin{aligned} M^* &= \{\, f \in \mathcal{O}_k \mid f \perp s \text{ for all } s \in M \,\} \\ &= \bigcup_{n>0} \{\, f \in \mathcal{O}_k^{(n)} \mid f(s(x_1), \ldots, s(x_n)) = s(f(x_1, \ldots, x_n)) \\ &\qquad\qquad \text{for every } (x_1, x_2, \ldots, x_n) \in \boldsymbol{k}^n \text{ and for all } s \in M \,\}. \end{aligned}$$

Note that a unary operation $s \in \mathcal{O}_k^{(1)}$ induces a binary relation $s^\square$ such that

$$s^\square = \{\, (x, s(x)) \mid x \in \boldsymbol{k} \,\}$$

and that, for $f \in \mathcal{O}_k^{(n)}$ and $s \in \mathcal{O}_k^{(1)}$, $f \in \mathrm{Pol}\, s^\square$ if and only if

$$f(s(x_1), s(x_2), \ldots, s(x_n)) = s(f(x_1, x_2, \ldots, x_n))$$

for every $(x_1, x_2, \ldots, x_n) \in \boldsymbol{k}^n$. In other words, $f \in \mathrm{Pol}\, s^\square$ if and only if s is an endomorphism of the algebra $\langle \boldsymbol{k}; \{f\} \rangle$.

Hence, for a monoid M in $\mathcal{M}_k$, the centralizer M^* of M is characterized as

$$M^* = \bigcap_{s \in M} \mathrm{Pol}\, s^\square.$$

For a subset S of $\mathcal{O}_k^{(1)}$ the monoid *generated* by S is defined to be the least monoid containing S, and is denoted by $\langle S \rangle$. The following property justifies us to consider centralizers only of monoids instead of centralizers of all subsets of $\mathcal{O}_k^{(1)}$. The proof is straightforward from the definition.

Proposition 1.1 *For a subset S of $\mathcal{O}_k^{(1)}$ let $M \in \mathcal{M}_k$ be the monoid generated by S, i.e., $M = \langle S \rangle$. Then $S^* = M^*$.*

2. Useful Conditions

Hereafter, we assume $k \geq 3$, unless otherwise stated.

In [MR 04] we presented a sufficient condition for a monoid M to satisfy $M^* = \mathcal{J}_k$, i.e., a condition which induces the centralizer M^* to be the least clone.

Properties: Let $M \in \mathcal{M}_k$.

I. (Partial separation property)
For all $a, b, c, d \in \boldsymbol{k}$, if $\{a, b\} \neq \{c, d\}$ and $c \neq d$ then M contains f $(= f^{ab}_{cd})$ which satisfies the following:

$$f(a) = f(b) \quad \text{and} \quad f(c) \neq f(d).$$

II. (Fixed-point-free property)
For every $i \in \boldsymbol{k}$, M contains g_i which satisfies $g_i(i) \neq i$.

The next theorem states a sufficient condition for a monoid M to satisfy $M^* = \mathcal{J}_k$, whose proof appears in [MR 04]. However, for the reader's convenience, we reproduce the proof, with certain modification, in the final section of this paper.

Theorem 2.1 *For any $M \in \mathcal{M}_k$, if M satisfies both Properties I and II then $M^* = \mathcal{J}_k$.*

There is another sufficient condition which is a bit weaker but, in most cases, more convenient to use than the above condition.

Additional Property: Let $M \in \mathcal{M}_k$.

I'. For every $i \in \boldsymbol{k}$, M contains f_i which satisfies $f_i^{-1}(\alpha) = \boldsymbol{k} \setminus \{i\}$ for some $\alpha \in \boldsymbol{k}$.

Corollary 2.2 *For any $M \in \mathcal{M}_k$, if M satisfies both Properties I' and II then $M^* = \mathcal{J}_k$.*

Proof. It is easy to see that f_c or f_d in Property I' serves as f^{ab}_{cd} in Property I and thus Property I follows from Property I'. □

3. Centralizers of Monoids Containing the Symmetric Group

We denote by S_k the symmetric group on $\boldsymbol{k}$. In this section we determine centralizers of all monoids which contain S_k.

Before we proceed, it is worth noting that the restriction of $*$-operator to the set of permutation groups, i.e., subgroups of S_k, on $\boldsymbol{k}$ is injective, that is, for any permutation groups G_1 and G_2 on $\boldsymbol{k}$, $G_1^* = G_2^*$ implies $G_1 = G_2$. This fact gives a clear contrast to what follows below.

3.1 The Symmetric Group S_k

We characterize the centralizer S_k^* of the symmetric group S_k. An operation f in S_k^* is called a *homogeneous* operation. Note that the following result was known by Marczewski [Marcz64]. The following definitions are from [MMR 01].

For n-tuples $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n) \in \boldsymbol{k}^n$, $(x_1, \ldots, x_n)$ is *similar* to $(y_1, \ldots, y_n)$ if the following is satisfied:

$$x_i = x_j \Longleftrightarrow y_i = y_j \quad \text{for} \quad \text{any} \quad 1 \leq i, j \leq n.$$

Definition 3.1 *An operation $f \in \mathcal{O}_k^{(n)}$ is* synchronous *(or,* pattern*) if the following condition is satisfied for any element $(x_1, \ldots, x_n)$ in $\boldsymbol{k}^n$:*
(i) If $|\{x_1, \ldots, x_n\}| \neq k-1$ then

(1) *$f(x_1, \ldots, x_n) = x_\ell$ for some $1 \leq \ell \leq n$, and*

(2) *$f(y_1, \ldots, y_n) = y_\ell$ for any $(y_1, \ldots, y_n) \in \boldsymbol{k}^n$ which is similar to $(x_1, \ldots, x_n)$.*

(ii) If $|\{x_1, \ldots, x_n\}| = k-1$ and $f(x_1, \ldots, x_n) = u$ for some $u \in \boldsymbol{k}$ then

(1) *$u = x_\ell$ for some $1 \leq \ell \leq n$ implies $f(y_1, \ldots, y_n) = y_\ell$ for any $(y_1, \ldots, y_n) \in \boldsymbol{k}^n$ which is similar to $(x_1, \ldots, x_n)$, and*

(2) *$u \in \boldsymbol{k} \setminus \{x_1, \ldots, x_n\}$ implies $f(y_1, \ldots, y_n) = v$, where $v \in \boldsymbol{k} \setminus \{y_1, \ldots, y_n\}$ for any $(y_1, \ldots, y_n) \in \boldsymbol{k}^n$ which is similar to $(x_1, \ldots, x_n)$.*

The set of all synchronous operations in $\mathcal{O}_k$ is denoted by $\mathcal{SYN}_k$.

It is known ([Marcz64]; Also see [Sze 86] and [MR 04]) that the centralizer S_k^* of S_k is the clone consisting of synchronous operations. Thus,

Proposition 3.1 *For $k \geq 2$, it holds that $S_k^* = \mathcal{SYN}_k$.*

3.2 The Union of S_k and CONST

For $a \in \boldsymbol{k}$, let $c_a \in \mathcal{O}_k^{(1)}$ be the unary constant operation such that $c_a(x) = a$ for all $x \in \boldsymbol{k}$. Denote by CONST the set of all constant operations in $\mathcal{O}_k^{(1)}$, i.e., $\mathrm{CONST} = \{ c_a \mid a \in \boldsymbol{k} \}$.

Lemma 3.2 *(i) The union $S_k \cup \mathrm{CONST}$ is a monoid and (ii) it covers S_k, i.e., for any $M \in \mathcal{M}_k$ if $S_k \subset M \subseteq S_k \cup \mathrm{CONST}$ then $M = S_k \cup \mathrm{CONST}$.*

Proof. (i) It is clear that $S_k \cup \mathrm{CONST}$ is a monoid. (ii) It is easy to see that $S_k \subset M \subseteq S_k \cup \mathrm{CONST}$ implies the existence of a unary constant operation in M. Suppose $c_a \in M$ for some $a \in \boldsymbol{k}$. Then, for any $b \in \boldsymbol{k}$, $c_b = (a\ b) \circ c_a$, where $(a\ b)$ is a transposition in S_k interchanging a and b. It follows that $c_b \in M$. Hence $\mathrm{CONST} \subseteq M$ holds and the claim (ii) follows. $\square$

An operation $f \in \mathcal{O}_k$ is *idempotent* if $f(a, \ldots, a) = a$ for all $a \in \boldsymbol{k}$. We observe without difficulty that the centralizer $(S_k \cup \mathrm{CONST})^*$ is the set of operations in $\mathcal{O}_k$ which are both synchronous and idempotent. However, it is easy to see that a synchronous operation is always idempotent when $k \geq 3$. Hence, $(S_k \cup \mathrm{CONST})^*$ is identical to the set of synchronous operations when $k \geq 3$.

Proposition 3.3 *For* $k = 2$, $(S_2 \cup \mathrm{CONST})^* = \{ f \in \mathcal{SYN}_2 \mid f : \text{idempotent} \}$. *For* $k \geq 3$, $(S_k \cup \mathrm{CONST})^* = \mathcal{SYN}_k\ (= S_k^*)$.

3.3 Other Monoids Containing S_k

Lemma 3.4 *Let M be a monoid in $\mathcal{M}_k$. If M strictly contains S_k, i.e., $S_k \subset M \subseteq \mathcal{O}_k^{(1)}$, then $S_k \cup \mathrm{CONST} \subseteq M$.*

Proof. Since M strictly contains S_k, there exists $u \in M$ such that $\#\,\mathrm{Im}(u) < k$. Here, $\mathrm{Im}(u)$ denotes the image of u and, for a finite set X, $\#X$ denotes the number of elements in X.

Claim 1 If $\#\,\mathrm{Im}(u) = 1$ then $S_k \cup \mathrm{CONST} \subseteq M$.

<u>Proof of Claim 1</u> Immediate from Lemma 3.2 (ii).

Claim 2 If $\#\,\mathrm{Im}(u) = r$ where $1 < r < k$ then there exists $v \in M$ such that $\#\,\mathrm{Im}(v) < r$.

<u>Proof of Claim 2</u> Let R be the range of u, and $u|_R$ be the restriction of u to R.

(i) Suppose that $u|_R$ is not a permutation on R. Then let $v = u \circ u$. It is clear that $\#\,\mathrm{Im}(v) < \#\,\mathrm{Im}(u) = r$.

(ii) Suppose that $u|_R$ is a permutation on R. Since $r < k$ by assumption, there exist $a \in R$ and $b \in \boldsymbol{k} \setminus R$ such that $u(a) = u(b)$. Let $c = u(a)(= u(b))$. Choose $d \in \boldsymbol{k}$ such that $d \in \mathrm{Im}(u)$ and $c \neq d$. Then construct v as $v = u \circ (b\ d) \circ u$ where $(b\ d)$ is a transposition in S_k interchanging b and d. For this v it clearly holds that $\#\,\mathrm{Im}(v) < \#\,\mathrm{Im}(u) = r$, because $u|_R$ is a permutation on R and $u(d) \notin \mathrm{Im}(v)$.

Claims 1 and 2 suffice to show the desired property: $S_k \cup \mathrm{CONST} \subseteq M$. $\square$

Lemma 3.5 *Let $k \geq 5$. Let M be a monoid in $\mathcal{M}_k$. If M strictly contains $S_k \cup \mathrm{CONST}$, i.e., $S_k \cup \mathrm{CONST} \subset M \subseteq \mathcal{O}_k^{(1)}$, then M satisfies Property I.*

Proof. The assumption $S_k \cup \mathrm{CONST} \subset M \subseteq \mathcal{O}_k^{(1)}$ asserts that there exists $u \in M$ such that $1 < \#\,\mathrm{Im}(u) < k$. Then the number $t\ (= t(u))$ of blocks of the equivalence relation $\ker u$ satisfies $1 < t < k$.

Now, suppose that a, b, c and d in $\boldsymbol{k}$ are given such that $\{a, b\} \neq \{c, d\}$ and $c \neq d$.

<u>Case 1</u>: $t = 2$

Since $k \geq 5$, one block B must have 3 or 4 elements. Choose a permutation $\sigma \in S_k$ which sends (mutually distinct elements of) a, b and c to mutually distinct elements in B, and d to an element in $\boldsymbol{k} \setminus B$. Then define $f = u \circ \sigma$.

Case 2: $2 < t < k$

Let a block B_1 consist of 2 or more elements and B_2 and B_3 be two other blocks. Choose a permutation $\tau \in S_k$ which sends a and b to mutually distinct elements in B_1 if $a \neq b$ and to an element if $a = b$, c to an element in B_2 and d to an element in B_3. Then define $f = u \circ \tau$.

In both cases, clearly f belongs to M and f serves as $f\,(= f_{cd}^{ab})$ in Property I, namely, f satisfies the required property: $f(a) = f(b)$ and $f(c) \neq f(d)$. $\square$

Let $k = 4$. For a unary operation u in $\mathcal{O}_4^{(1)}$ the **kernel** of u is defined by

$$\ker u \;=\; \{(x, y) \in \mathbf{4}^2 \mid u(x) = u(y)\}.$$

Clearly, $\ker u$ is an equivalence relation on $\boldsymbol{k}$. An equivalence class is called a **block**.

Let M_2 be the monoid consisting of unary operations u of $\mathcal{O}_4^{(1)}$ satisfying one of the following:

(i) $\ker u$ has four singleton blocks. (i.e., u is a permutation on $\mathbf{4}$.)

(ii) $\ker u$ has one block. (i.e., u is a constant function on $\mathbf{4}$.)

(iii) $\ker u$ has two blocks of size 2. (i.e., u sends two elements in $\mathbf{4}$ to an element in $\mathbf{4}$ and the other two to another element in $\mathbf{4}$.)

Analogously to Lemma 3.5, we have the following, excluding M_2.

Lemma 3.6 *Let $k = 4$. Let M be a monoid in $\mathcal{M}_4 \setminus \{M_2\}$. If M strictly contains $S_4 \cup \mathrm{CONST}$ then M satisfies Property I.*

Proof. M contains u whose kernel has either (i) two blocks, one of which consists of 3 elements, or (ii) three blocks, one of which consists of 2 elements. Then, the proof is carried out similarly to that of the previous lemma. $\square$

Proposition 3.7 *Let M be a monoid in $\mathcal{M}_k$ which strictly contains $S_k \cup \mathrm{CONST}$. Then the following holds.*

(i) *If $k = 3$ then $M^* = \mathcal{J}_k$.*

(ii) *If $k = 4$ and $M \neq M_2$ then $M^* = \mathcal{J}_k$.*

(iii) *If $k \geq 5$ then $M^* = \mathcal{J}_k$.*

Proof. (i) Let $k = 3$. If M strictly contains $S_k \cup \mathrm{CONST}$, then M is clearly the set of all unary operations, i.e., $M = \mathcal{O}_3^{(1)}$. Hence $M^* = \mathcal{J}_k$. (ii) By Lemma 3.6, M satisfies Property I. Clearly, M also satisfies Property II. Hence, the result follows from Theorem 2.1. (iii) Similarly, the result follows from Lemma 3.5 and Theorem 2.1. $\square$

Remark Let $k = 4$. The centralizer M_2^* of the monoid M_2 is *not* the least clone. In fact, M_2 contains, e.g., the following ternary operation $m \in \mathcal{O}_4^{(3)}$.

$$m(x_1, x_2, x_3) = \begin{cases} x_1 & \text{if } \ x_1 = x_2 = x_3 \\ x_1 & \text{if } \ x_1 \neq x_2 = x_3 \\ x_2 & \text{if } \ x_2 \neq x_1 = x_3 \\ x_3 & \text{if } \ x_3 \neq x_1 = x_2 \\ y & \text{if } \ \{x_1, x_2, x_3, y\} = \mathbf{4}. \end{cases}$$

For each element x of $\mathbf{4}$ let x^1, x^0 in $\mathbf{2}$ be elements satisfying $x = 2x^1 + x^0$. Let $q \in \mathcal{O}_4^{(m)}$ be an operation defined by

$$q(x_1, \ldots, x_m) \approx 2\cdot(x_{i_1}^1 + x_{i_2}^1 + \cdots + x_{i_{2\ell+1}}^1) \bmod 2 + \cdot(x_{i_1}^0 + x_{i_2}^0 + \cdots + x_{i_{2\ell+1}}^0) \bmod 2$$

where $m \geq 1$, $\ell \geq 0$ and $1 \leq i_1 < \cdots < i_{2\ell+1} \leq m$. Denote by Q_2 the set of all such operations q. Then it follows that $M_2^* = Q_2$. (Proof will appear elsewhere.)

We summarize as follows:

Theorem 3.8 *Let $k \geq 3$. For any monoid $M \in \mathcal{M}_k$ containing S_k, the centralizer M^* of M is as follows:*

(1) $S_k^* = \mathcal{SYN}_k$.

(2) $(S_k \cup \mathrm{CONST})^* = \mathcal{SYN}_k$.

(3A) *For $k = 3$ or $k \geq 5$, if $M \notin \{S_k, S_k \cup \mathrm{CONST}\}$ then $M^* = \mathcal{J}_k$.*

(3B) *For $k = 4$, if $M \notin \{S_4, S_4 \cup \mathrm{CONST}, M_2\}$ then $M^* = \mathcal{J}_4$.*

(3C) *For $k = 4$, $M^* = Q_2$.*

4. An Application of Corollary 2.2

Here we show a typical application of Corollary 2.2 to prove $M^* = \mathcal{J}_k$ for some monoid M.

For each $i \in \boldsymbol{k}$ let $\chi_i \in \mathcal{O}_k^{(1)}$ be defined by $\chi_i(i) = 1$ and $\chi_i(x) = 0$ if $x \neq i$. Set $\Gamma_k = \{\chi_i \mid i \in \boldsymbol{k}\ \}$. For each $i \in \boldsymbol{k}$ let $\overline{\chi}_i(x) = 1 - \chi_i(x)$ for all $x \in \boldsymbol{k}$. The elements of the monoid $\langle \Gamma_k \rangle$ generated by Γ_k is as follows:

$$\langle \Gamma_k \rangle = \{\chi_0, \chi_1, \ldots, \chi_{k-1}, \overline{\chi}_0, \overline{\chi}_1, \ldots, \overline{\chi}_{k-1}, c_0, c_1, \mathrm{id}_{\boldsymbol{k}}\}.$$

Define a submonoid H_k of $\langle \Gamma_k \rangle$ by

$$H_k = \{\chi_1, \ldots, \chi_{k-1}, \overline{\chi}_0, \overline{\chi}_2, \ldots, \overline{\chi}_{k-1}, c_0, c_1, \mathrm{id}_{\boldsymbol{k}}\},$$

that is, $H_k = \langle \Gamma_k \rangle \setminus \{\chi_0, \overline{\chi}_1\}$. It is easy to see that H_k is also a monoid. We prove the following:

Proposition 4.1 *For every $k \geq 3$, it holds that $H_k^* = \mathcal{J}_k$.*

Proof. We show that Properties I' and II hold for H_k. Property I' is verified by the following table which gives an example of f_i in Property I' belonging to H_k for every $i \in \boldsymbol{k}$.

i	0	1	2	$\cdots$	$k-2$	$k-1$
f_i	$\overline{\chi}_0$	χ_1	χ_2	$\cdots$	χ_{k-2}	χ_{k-1}

Next, it is easy to see that Property II holds for H_k. □

Since H_k is a subset of $\langle \Gamma_k \rangle$, the above proposition immediately implies:

Corollary 4.2 $\langle \Gamma_k \rangle^* = \mathcal{J}_k$ *for every $k \geq 3$.*

Moreover, by looking at the table in the proof of Proposition 4.1, we can readily find even a smaller monoid M which satisfies $M^* = \mathcal{J}_k$. Define H'_k as

$$H'_k = \{\chi_1, \ldots, \chi_{k-1}, \overline{\chi}_0, c_0, c_1, \mathrm{id}_{\boldsymbol{k}}\}.$$

H'_k is a monoid. It is clear that Properties I' and II hold for H'_k. Hence we have:

Corollary 4.3 $(H'_k)^* = \mathcal{J}_k$ *for every $k \geq 3$.*

5. Proof of Theorem 2.1

In this section we present a proof of Theorem 2.1. We shall prove Propositon A. It is straightforward that Theorem 2.1 follows from Proposition A.

Proposition A For any $M \in \mathcal{M}_k$, the following holds.

(1) If M satisfies Property I then, for every $f \in M^*$, f is either a projection or a constant operation.

(2) If M satisfies Property II then, for every $f \in M^*$, f is *not* a constant operation.

The proof of Proposition A begins with the next lemma.

Lemma 5.1 *Let* $f \in \mathcal{O}_k^{(n)}$. *If* $|\mathrm{Im} f| \geq 2$ *then there exist* $i \in \{1, 2, \ldots, n\}$, $a, b \in \boldsymbol{k}$, $\boldsymbol{u} \in \boldsymbol{k}^{i-1}$ *and* $\boldsymbol{v} \in \boldsymbol{k}^{n-i}$ *such that*

$$f(\boldsymbol{u}, a, \boldsymbol{v}) \neq f(\boldsymbol{u}, b, \boldsymbol{v}).$$

Proof. Consider the (undirected) graph $G = (V, E)$ where the vertex set V is $\boldsymbol{k}^n$ and the edge set E consists of all $(\boldsymbol{x}, \boldsymbol{y})$ such that $\boldsymbol{x}$ and $\boldsymbol{y}$ differ exactly at one place, i.e., the "Hamming distance" of $\boldsymbol{x}$ and $\boldsymbol{y}$ is one. To each vertex $\boldsymbol{x} = (x_1, \ldots, x_n)$ in V, put the label $f(x_1, \ldots, x_n) (\in \boldsymbol{k})$. Denote this labeled graph by $\mathcal{H}(f)$.

Now the assumption $|\mathrm{Im} f| \geq 2$ implies that there are at least two different labels in $\mathcal{H}(f)$. Hence there must be a pair $(\boldsymbol{x}, \boldsymbol{y})$ of neighboring vertices of $\mathcal{H}(f)$ such that the label of $\boldsymbol{x}$ is different from the label of $\boldsymbol{y}$. For these $\boldsymbol{x} = (\boldsymbol{u}, a, \boldsymbol{v})$ and $\boldsymbol{y} = (\boldsymbol{u}, b, \boldsymbol{v})$, we have $f(\boldsymbol{u}, a, \boldsymbol{v}) \neq f(\boldsymbol{u}, b, \boldsymbol{v})$ as desired. $\square$

Let $f \in \mathcal{O}_k^{(n)}$ and $s \in \mathcal{O}_k^{(1)}$ be n-ary and unary operations. Suppose that $f(a_1, \ldots, a_n) = \alpha$ for some $a_1, \ldots, a_n, \alpha \in \boldsymbol{k}$. Then by saying '*apply s to f*' we mean to construct the expression $f(s(a_1), \ldots, s(a_n)) = s(\alpha)$.

Lemma 5.2 *Let* $f \in \mathcal{O}_k^{(n)}$ *satisfy Property I. For* $i \in \{1, 2, \ldots, n\}$, $a, b \in \boldsymbol{k}$, $\boldsymbol{u} \in \boldsymbol{k}^{i-1}$ *and* $\boldsymbol{v} \in \boldsymbol{k}^{n-i}$, *let*

$$\begin{cases} f(\boldsymbol{u}, a, \boldsymbol{v}) &= \alpha \\ f(\boldsymbol{u}, b, \boldsymbol{v}) &= \beta \end{cases}$$

for some $\alpha, \beta \in \boldsymbol{k}$. *If* $\alpha \neq \beta$, *then it follows that* $\alpha = a$ *and* $\beta = b$.

Proof. Note that $\alpha \neq \beta$ forces $a \neq b$. We divide the case into two.

<u>Case 1</u> $\{a, b\} \neq \{\alpha, \beta\}$:

By assumption M contains $f_{\alpha\beta}^{ab}$. Apply $f_{\alpha\beta}^{ab}$ to

$$\begin{cases} f(\boldsymbol{u}, a, \boldsymbol{v}) &= \alpha \\ f(\boldsymbol{u}, b, \boldsymbol{v}) &= \beta \end{cases}$$

Then we have a contradiction because $f_{\alpha\beta}^{ab}(a) = f_{\alpha\beta}^{ab}(b)$ and $f_{\alpha\beta}^{ab}(\alpha) \neq f_{\alpha\beta}^{ab}(\beta)$.

<u>Case 2</u> $\{a, b\} = \{\alpha, \beta\}$:

Since $a \neq b$ and $\alpha \neq \beta$, we have either "$a = \alpha$ and $b = \beta$" or "$a = \beta$ and $b = \alpha$".

<u>Subcase 2–1</u> $a = \alpha$ and $b = \beta$:

In this case, we are done.

<u>Subcase 2–2</u> $a = \beta$ and $b = \alpha$:

We have

$$\begin{cases} f(\boldsymbol{u}, a, \boldsymbol{v}) &= b \quad (1) \\ f(\boldsymbol{u}, b, \boldsymbol{v}) &= a. \quad (2) \end{cases}$$

Since $k \geq 3$ by assumption, $\boldsymbol{k} \setminus \{a, b\}$ is non-empty. Take any $c \in \boldsymbol{k} \setminus \{a, b\}$ and let

$$f(\boldsymbol{u}, c, \boldsymbol{v}) \;=\; d. \tag{3}$$

If $d \notin \{a, b\}$, apply f^{ac}_{bd} to (1) and (3). Then we have a contradiction because $f^{ac}_{bd}(a) = f^{ac}_{bd}(c)$ and $f^{ac}_{bd}(b) \neq f^{ac}_{bd}(d)$.

If $d = a$, then $b \neq d$. Apply f^{ac}_{bd} to (1) and (3). Then we have a contradiction as above.

If $d = b$, then $a \neq d$. Apply f^{bc}_{ad} to (2) and (3). Then we have a contradiction because $f^{bc}_{ad}(b) = f^{bc}_{ad}(c)$ and $f^{bc}_{ad}(a) \neq f^{bc}_{ad}(d)$.

To conclude, we must have $a = \alpha$ and $b = \beta$ (Subcase 2–1). □

Lemma 5.3 *Let $f \in \mathcal{O}^{(n)}_k$ satisfy Property I. For $i \in \{1, 2, \ldots, n\}$, $a, b \in \boldsymbol{k}$, $\boldsymbol{u} \in \boldsymbol{k}^{i-1}$ and $\boldsymbol{v} \in \boldsymbol{k}^{n-i}$, suppose that $a \neq b$ and that f satisfies the following:*

$$\left\{\begin{array}{lcll} f(\boldsymbol{u}, a, \boldsymbol{v}) & = & a & \quad (4)\\ f(\boldsymbol{u}, b, \boldsymbol{v}) & = & b. & \quad (5)\end{array}\right.$$

Then it follows that $f(\boldsymbol{u}, x, \boldsymbol{v}) = x$ for every $x \in \boldsymbol{k}$.

Proof. Suppose that

$$f(\boldsymbol{u}, x, \boldsymbol{v}) \;=\; y \tag{6}$$

for some $x, y \in \boldsymbol{k}$ where $x \neq y$.

If $y \neq a$, apply f^{ax}_{ay} to the equations (4) and (6). Then we have

$$\left\{\begin{array}{lcll} f(\boldsymbol{u}\text{'}, f^{ax}_{ay}(a), \boldsymbol{v}\text{'}) & = & f^{ax}_{ay}(a) & \quad (4)\text{'}\\ f(\boldsymbol{u}\text{'}, f^{ax}_{ay}(x), \boldsymbol{v}\text{'}) & = & f^{ax}_{ay}(y) & \quad (6)\text{'}\end{array}\right.$$

which is a contradiction because $f^{ax}_{ay}(a) = f^{ax}_{ay}(x)$ and $f^{ax}_{ay}(a) \neq f^{ax}_{ay}(y)$.

If $y \neq b$, apply f^{bx}_{by} to the equations (5) and (6). Then we have

$$\left\{\begin{array}{lcll} f(\boldsymbol{u}\text{'}, f^{bx}_{by}(b), \boldsymbol{v}\text{'}) & = & f^{bx}_{by}(b) & \quad (5)\text{'}\\ f(\boldsymbol{u}\text{'}, f^{bx}_{by}(x), \boldsymbol{v}\text{'}) & = & f^{bx}_{by}(y) & \quad (6)\text{''}\end{array}\right.$$

which is a contradiction because $f^{bx}_{by}(a) = f^{bx}_{by}(x)$ and $f^{bx}_{by}(a) \neq f^{bx}_{by}(y)$.

Since $a \neq b$, either $y \neq a$ or $y \neq b$ holds, and the assertion is proved. □

To summarize, Lemmas 5.1, 5.2 and 5.3 imply:

Lemma 5.4 *Let $f \in \mathcal{O}^{(n)}_k$ satisfy Property I. If $|\mathrm{Im} f| \geq 2$ then there exist $i \in \{1, 2, \ldots, n\}$, $\boldsymbol{u} \in \boldsymbol{k}^{i-1}$ and $\boldsymbol{v} \in \boldsymbol{k}^{n-i}$ such that*

$$f(\boldsymbol{u}, x, \boldsymbol{v}) \;=\; x$$

for every $x \in \boldsymbol{k}$.

Proof. Immediate. □

Lemma 5.5 *Let $f \in \mathcal{O}_k^{(n)}$ satisfy Property I. If for some $i \in \{1, 2, \ldots, n\}$ and some $\boldsymbol{u} \in \boldsymbol{k}^{i-1}$ and $\boldsymbol{v} \in \boldsymbol{k}^{n-i}$ it holds that*

$$f(\boldsymbol{u}, x, \boldsymbol{v}) \;=\; x \qquad \text{for every } x \in \boldsymbol{k}$$

then for any $\boldsymbol{u}' \in \boldsymbol{k}^{i-1}$ and $\boldsymbol{v}' \in \boldsymbol{k}^{n-i}$ it holds that

$$f(\boldsymbol{u}', x, \boldsymbol{v}') \;=\; x \qquad \text{for every } x \in \boldsymbol{k}.$$

Proof. For brevity, we assume that

$$f(x, c, \boldsymbol{w}) \;=\; x$$

for some $c \in \boldsymbol{k}$ and $\boldsymbol{w} \in \boldsymbol{k}^{n-2}$ and for every $x \in \boldsymbol{k}$, that is, $i = 1$, $\boldsymbol{u}$ is null and $\boldsymbol{v} = (c, \boldsymbol{w})$. Then we shall show that for every $d \in \boldsymbol{k}$

$$f(x, d, \boldsymbol{w}) \;=\; x$$

holds for every $x \in \boldsymbol{k}$. It is clear that this suffices to prove the lemma. (By repeating this procedure, we obtain $f(x, \boldsymbol{v}') = x$ for any $\boldsymbol{v}' \in \boldsymbol{k}^{n-1}$ from $f(x, \boldsymbol{v}) = x$ for some particular $\boldsymbol{v} \in \boldsymbol{k}^{n-1}$.)

Moreover, we assume without loss of generality that $c = 0$. I.e., we have

$$f(x, 0, \boldsymbol{w}) \;=\; x \tag{7}$$

for every $x \in \boldsymbol{k}$. We shall show that for every $d \in \{1, 2, \ldots, k-1\}$ and every $x \in \boldsymbol{k}$ it holds that

$$f(x, d, \boldsymbol{w}) \;=\; x.$$

Without loss of generality, again, we may assume that $d = 1$.

<u>Case 1</u> $x \in \{2, 3, \ldots, k-1\}$:

Let

$$f(x, 1, \boldsymbol{w}) \;=\; y \tag{8}$$

for some $y \in \boldsymbol{k}$. Suppose $y \neq x$. Since $x \notin \{0, 1\}$, we have $\{x, y\} \neq \{0, 1\}$. So, apply f_{xy}^{01} to (7) and (8) and we obtain

$$\begin{cases} f(f_{xy}^{01}(x), f_{xy}^{01}(0), \boldsymbol{w}') \;=\; f_{xy}^{01}(x) & (7)' \\ f(f_{xy}^{01}(x), f_{xy}^{01}(1), \boldsymbol{w}') \;=\; f_{xy}^{01}(y) & (8)' \end{cases}$$

which is a contradiction because $f_{xy}^{01}(0) = f_{xy}^{01}(1)$ and $f_{xy}^{01}(x) \neq f_{xy}^{01}(y)$. Hence we have

$$f(x, 1, \boldsymbol{w}) \;=\; x \tag{9}$$

for any $x \in \{2, 3, \ldots, k-1\}$.

Case 2 $x = 0$:
Let $y := f(0,1,\boldsymbol{w})$. We consider two subcases.

Claim 2–1. $y \notin \{2,3,\ldots,k-1\}$.
(Proof) It is enough to show that $y \neq 2$, because proof of $y \neq j$ for $j \in \{3,\ldots,k-1\}$ can be carried out analogously. Suppose to the contrary that

$$f(0,1,\boldsymbol{w}) = 2. \tag{10}$$

Then apply f^{01}_{02} to (7) and (10). We obtain

$$\begin{cases} f(f^{01}_{02}(0), f^{01}_{02}(0), \boldsymbol{w}\text{'}) = f^{01}_{02}(0) & (7)\text{'} \\ f(f^{01}_{02}(0), f^{01}_{02}(1), \boldsymbol{w}\text{'}) = f^{01}_{02}(2) & (10)\text{'} \end{cases}$$

which is a contradiction because $f^{01}_{02}(0) = f^{01}_{02}(1)$ and $f^{01}_{02}(0) \neq f^{01}_{02}(2)$. Thus we have proved $y \neq 2$.

Similarly, we can show that $f(0,1,\boldsymbol{w}) \neq y$ for any $y \in \{3,4,\ldots,k-1\}$. $\diamond$

Claim 2–2. $y \neq 1$.
(Proof) Suppose to the contrary that

$$f(0,1,\boldsymbol{w}) = 1. \tag{11}$$

Then apply f^{02}_{12} to (9) with $x = 2$ and to (11). We obtain

$$\begin{cases} f(f^{02}_{12}(2), f^{02}_{12}(1), \boldsymbol{w}\text{'}) = f^{02}_{12}(2) & (9)\text{'} \\ f(f^{02}_{12}(0), f^{02}_{12}(1), \boldsymbol{w}\text{'}) = f^{02}_{12}(1) & (11)\text{'} \end{cases}$$

which is a contradiction because $f^{02}_{12}(0) = f^{02}_{12}(2)$ and $f^{02}_{12}(1) \neq f^{02}_{12}(2)$. Thus we have shown $y \neq 1$. $\diamond$

The remaining possibility for the value of $f(0,1,\boldsymbol{w})$ is 0, i.e., $f(0,1,\boldsymbol{w}) = 0$.

Case 3 $x = 1$:
Let $z := f(1,1,\boldsymbol{w})$. We consider two subcases.

Claim 3–1. $z \notin \{2,3,\ldots,k-1\}$.
(Proof) By the same reason as the proof of Claim 2-1, it is enough to show that $y \neq 2$. Suppose to the contrary that

$$f(1,1,\boldsymbol{w}) = 2. \tag{12}$$

Then apply f^{01}_{02} to (7) and (12). Then we get

$$\begin{cases} f(f^{01}_{02}(0), f^{01}_{02}(0), \boldsymbol{w}\text{'}) = f^{01}_{02}(0) & (7)\text{'} \\ f(f^{01}_{02}(1), f^{01}_{02}(1), \boldsymbol{w}\text{'}) = f^{01}_{02}(2) & (12)\text{'} \end{cases}$$

which is a contradiction because $f^{01}_{02}(0) = f^{01}_{02}(1)$ and $f^{01}_{02}(0) \neq f^{01}_{02}(2)$. Thus we have shown $z \neq 2$.

Similarly, we can show that $f(1, 1, \boldsymbol{w}) \neq z$ for any $z \in \{3, 4, \ldots, k-1\}$. $\diamond$

Claim 3–2. $z \neq 0$.

(Proof) Suppose to the contrary that

$$f(1, 1, \boldsymbol{w}) = 0. \tag{13}$$

Then apply f_{02}^{12} to (9) with $x = 2$ and to (13) we obtain

$$\begin{cases} f(f_{02}^{12}(2), f_{02}^{12}(1), \boldsymbol{w}') = f_{02}^{12}(2) & (9)' \\ f(f_{02}^{12}(1), f_{02}^{12}(1), \boldsymbol{w}') = f_{02}^{12}(0) & (13)' \end{cases}$$

which is a contradiction because $f_{02}^{12}(1) = f_{02}^{12}(2)$ and $f_{02}^{12}(0) \neq f_{02}^{12}(2)$. Thus we have shown $z \neq 0$. $\diamond$

The remaining possibility for the value of $f(1, 1, \boldsymbol{w})$ is 1, i.e., $f(1, 1, \boldsymbol{w}) = 1$.

Altogether, we have shown that $f(x, 1, \boldsymbol{w}) = x$ for every $x \in \boldsymbol{k}$.

Analogously, we can verify that for every $d \in \{2, 3, \ldots, k-1\}$ and every $x \in \boldsymbol{k}$ we have

$$f(x, d, \boldsymbol{w}) = x$$

as desired. $\square$

Proof of Proposition A (1) :

From Lemmas 5.4 and 5.5 it follows that if f is not a constant operation, that is, if f satisfies $|\mathrm{Im}\, f| \geq 2$, then f is a projection. $\square$

Proof of Proposition A (2) :

For $f \in M^* \cap \mathcal{O}_k^{(n)}$, suppose that f is a constant operation taking value $i \in \boldsymbol{k}$, i.e., $f(x_1, \ldots, x_n) = i$ for all $(x_1, \ldots, x_n) \in \boldsymbol{k}^n$. Property II asserts that there exists g_i in M which satisfies $g_i(i) \neq i$. Then we have $f(g_i(x_1), \ldots, g_i(x_n)) = i$ and $g_i(f(x_1, \ldots, x_n)) = g_i(i) \neq i$ which contradicts the assumption $f \in M^*$. $\square$

Acknowledgment: The authors are grateful to an anonymous referee for a valuable remark which led to improve the contents of the paper.

References

[BKKR 69] Bodnartchuk, V. G., Kaluzhnin, L. A., Kotov, V. N. and Romov, A. A. (1969). Galois theory for Post algebras I-II (in Russian), Kibernetika (Kiev), Part I: **3**, 1-10; Part II: **5**, 1-9; English translation: Cybernetics (1969), **3**, 243-252 and 531-539.

[Co 65] Cohn, P. M. (1965). Universal Algebra, Harper and Row, 412pp.

[Da 77] Danil'tchenko, A. F. (1977). Parametric expressibility of functions of three-valued logic (in Russian), Algebra i Logika, **16**, 397-416; English traslation: Algebra and Logic (1977), **16**, 266-280.

[Da 79] Danil'tchenko, A. F. (1979). On parametrical expressibility of the functions of k-valued logic, Colloquia Mathematica Societatis János Bolyai, **28**, Finite Algebra and Multiple-Valued Logic, 147-159.

[Ku 61] Kuznetsov, A. V. (1961). Lattices with closure and criteria for functional completeness (in Russian), Uspekhi Mat. Nauk, **16/2**(98), 201-202.

[MMR 01] Machida, H., Miyakawa, M. and Rosenberg, I. G. (2001). Relations between clones and full monoids, Proc. 31st Int. Symp. Multiple-Valued Logic, IEEE, 279-284.

[MMR 02] Machida, H., Miyakawa, M. and Rosenberg, I. G. (2002). Some results on the centralizers of monoids in clone theory, Proc. 32nd Int. Symp. Multiple-Valued Logic, IEEE, 10-16.

[MR 03] Machida, H. and Rosenberg, I. G. (2003). On the centralizers of monoids in clone theory, Proc. 33rd Int. Symp. Multiple-Valued Logic, IEEE, 303-308.

[MR 04] Machida, H. and Rosenberg, I. G. (2004). Monoids whose centralizer is the least clone, to appear in Proc. 34th Int. Symp. Multiple-Valued Logic, IEEE.

[March82] Marchenkov, S. S. (1982). Homogeneous algebras (Russian), Problemy Kibernetiki, **39**, 85-106.

[Marcz64] Marczewski, E. (1964). Homogeneous algebras and homogeneous operations, Fund. Math., **56**, 81-103.

[Ro 78] Rosenberg, I. G. (1978). On a Galois connection between algebras and relations and its applications, Contributions of General Algebra, 273-289.

[Sza 78] Szabó, L. (1978). Concrete representation of related structures of universal algebras. I, Acta. Sci. Math., **40**, 175-184.

[Sza 85] Szabó, L. (1985). Characterization of clones acting bicentrally and containing a primitive group, Acta. Cybernet., **7**, 137-142.

[Sze 86] Szendrei, Á. (1986). Clones in Universal Algebra, SMS Series **99**, Les Presses de L'Université de Montréal, 166pp.