Galois Connection between
Clones and Full Monoids

町田 元 (Machida, Hajime)
宮川正弘 (Miyakawa, Masahiro)
ローゼンバーグ (Ivo G. Rosenberg)

Abstract

An endoprimal clone is defined for a set of unary operations. It was known before that the endoprimal clone for the set $O_k^{(1)}$ of all unary operations on a $k$-element set is the least clone $J_k$ and that the endoprimal clone for the symmetric group $S_k$ strictly includes $J_k$. In this paper we consider monoids of unary operations and clones corresponding to such monoids. We define a descending sequence $\{N_i\}$ of monoids lying between $O_k^{(1)}$ and $S_k$, and show that the endoprimal clone for $N_{k-1}$ is distinct from $J_k$. We also give a characterization of the endoprimal clone for $S_k$.

1 Introduction

Let $k = \{0, 1, \ldots, k-1\}$ for $k > 1$. Let $O_k^{(n)}$ be the set of all $n$-ary operations from $k^n$ into $k$ and let $O_k = \bigcup_{n=1}^{\infty} O_k^{(n)}$. Denote by $J_k$ the set of all projections $pr_i^n$ (1 $\leq i \leq n$) over $k$ where $pr_i^n$ is defined as $pr_i^n(x_1, \ldots, x_i, \ldots, x_n) = x_i$ for every $(x_1, \ldots, x_n) \in k^n$.

A subset $C$ of $O_k$ is a clone on $k$ if (i) $C$ contains $J_k$ and (ii) $C$ is closed under (functional) composition. The set of all clones on $k$ is a lattice with respect to the inclusion relation. It is called the lattice of clones on $k$ and is denoted by $L_k$. Whereas the structure of $L_2$ is completely known, the structure of $L_k$ for $k \geq 3$ is extremely complex and our knowledge at present is still quite limited.

In [4], some properties of endoprimal clones were studied. (The definition of an endoprimal clone appears in Definition 2.5 of Section 2.) It was shown there, among others, that the endoprimal clone for $O_k^{(1)}$ is exactly the least clone $J_k$ and that the endoprimal clone for $R$ is distinct from $J_k$ if $R$ is a subset of the symmetric group $S_k$ of degree $k$.

This paper is a continuation of the work in [4]. We locate the work of [4] in the setting of Galois connection between clones and relations. For decades Galois connections between algebras and relations, or clones and relations, have been studied by many authors, e.g., [1, 7]. The target of this paper is some nicely restricted version of Galois connection, which aims at a particular type of relations defined for monoids of unary operations and clones corresponding to such relations. In particular, we investigate an interesting problem to determine at which points between $S_k$ and $O_k^{(1)}$ clones corresponding to them become strictly larger than the clone $J_k$. We give a partial solution to it. We also characterize the clone corresponding to the symmetric group $S_k$ of degree $k$ in terms of operations.
2 Definitions and Basic Properties

We start with introducing some terms and mappings which will play fundamental role in our study.

For $s,t \in \mathcal{O}_k^{(1)}$ we define composition $t \circ s$ of $s$ and $t$ as $(t \circ s)(x) = t(s(x))$ for every $x \in k$.

**Definition 2.1** A subset $M$ of $\mathcal{O}_k^{(1)}$ is a transformation monoid (or, simply, monoid) on $k$ if it satisfies the following two conditions:

1. For any $s,t \in M$, composition $t \circ s$ belongs to $M$, i.e., $t \circ s \in M$.
2. The identity operation $\mathrm{id}_k$ on $k$ belongs to $M$, i.e., $\mathrm{id}_k \in M$.

The set of all monoids on $k$ is denoted by $\mathcal{M}_k$.

Note that, since each element $s$ of $M(\in \mathcal{M}_k)$ is a transformation (selfmap) on $k$, the associative law automatically holds in $M$: $(u \circ t) \circ s = u \circ (t \circ s)$ for any $s,t,u \in M$.

**Example.** The monoid $\mathcal{O}_k^{(1)}$ is the greatest member of $\mathcal{M}_k$ and the monoid $\{\mathrm{id}_k\}$ is the least member of $\mathcal{M}_k$. Denote by $S_k$ the symmetric group $S_k$ on $k$, or the symmetric group of degree $k$, that is, the set of all permutations on $k$. Then $S_k$ is also a member of $\mathcal{M}_k$.

In the study of clones, it is often useful to describe clones via relations.

**Definition 2.2** For $h > 0$, an $h$-ary relation on $k$ is a subset of the Cartesian product $k^h$.

For an $n$-ary operation $f \in \mathcal{O}_k^{(n)}$ and an $h$-ary relation $\rho$ on $k$, $f$ is said to preserve $\rho$ if and only if $(x_{1j}, x_{2j}, \ldots, x_{hj}) \in \rho$ for all $j = 1, 2, \ldots, n$ imply $$(f(x_{11}, x_{12}, \ldots, x_{1n}), \ldots, f(x_{h1}, \ldots, x_{hn})) \in \rho.$$ The set of all operations $f \in \mathcal{O}_k$ that preserve relation $\rho$ on $k$ is denoted by $\text{Pol}(\rho)$.

It is easy to see that $\text{Pol}(\rho)$ is a clone in $\mathcal{L}_k$ for any relation $\rho$ on $k$.

In this work, we are mostly concerned with a special type of binary relations which are induced by unary operations.

**Definition 2.3** For an operation $s \in \mathcal{O}_k^{(1)}$ define the binary relation $s^\circ$ as $$s^\circ = \left\{ \left( \frac{x}{s(x)} \right) \mid x \in k \right\}.$$ Let $f \in \mathcal{O}_k^{(n)}$. For relation $s^\circ$ for $s \in \mathcal{O}_k^{(1)}$, $f \in \text{Pol}(s^\circ)$ is equivalent to saying that $$f(s(x_1), s(x_2), \ldots, s(x_n)) = s(f(x_1, x_2, \ldots, x_n))$$ for every $(x_1, x_2, \ldots, x_n) \in k^n$. Thus, to put it in algebraic terminology, $f \in \text{Pol}(s^\circ)$ is rephrased that $s$ is an endomorphism of the algebra $(k; f)$.

The next definition connects monoids to clones and clones to monoids, from which emerges a Galois connection between monoids and clones.

**Definition 2.4** A mapping $\varphi : \mathcal{M}_k \rightarrow \mathcal{L}_k$ is defined as $$\varphi(M) = \bigcap_{s \in M} \text{Pol}(s^\circ)$$ for every $M \in \mathcal{M}_k$. Conversely, a mapping $\psi : \mathcal{L}_k \rightarrow \mathcal{M}_k$ is defined as $$\psi(C) = \{ s \in \mathcal{O}_k^{(1)} \mid C \subseteq \text{Pol}(s^\circ) \}$$ for every $C \in \mathcal{L}_k$.

The validity of the above definitions of $\varphi$ and $\psi$ is certified by the following lemma.

**Lemma 2.1** (1) For any $M \in \mathcal{M}_k$, $\varphi(M)$ is a clone on $k$, i.e., $\varphi(M) \in \mathcal{L}_k$. 
(2) For any $C \in \mathcal{L}_k$, $\psi(C)$ is a monoid on $k$, i.e., $\psi(C) \in \mathcal{M}_k$.

Definition 2.5 For a subset $R$ of $\mathcal{O}_k^{(1)}$ and a clone $C \in \mathcal{L}_k$, $C$ is endoprimal for $R$ if $C = \bigcap_{s \in R} \text{Pol}(s)$.

Thus $\varphi(M)$ for $M \in \mathcal{M}_k$ is the endoprimal clone for $M$.

Lemma 2.2 (1) For any $M_1, M_2 \in \mathcal{M}_k$, if $M_1 \subseteq M_2$ then $\varphi(M_1) \supseteq \varphi(M_2)$.

(2) For any $C_1, C_2 \in \mathcal{L}_k$, if $C_1 \subseteq C_2$ then $\psi(C_1) \supseteq \psi(C_2)$.

Lemma 2.3 (1) For any $M \in \mathcal{M}_k$, $M \subseteq \psi(\varphi(M))$.

(2) For any $C \in \mathcal{L}_k$, $C \subseteq \varphi(\psi(C))$.

3 Full Monoids

In this paper, we shall concentrate on monoids which contain the symmetric group $S_k$ on $k$.

Definition 3.1 Let $M \subseteq \mathcal{O}_k^{(1)}$ be a monoid. $M$ is a full monoid if and only if $S_k \subseteq M$. The set of all full monoids in $\mathcal{O}_k^{(1)}$ is denoted by $\overline{\mathcal{M}}_k$.

Definition 3.2 For every $i = 0, 1, \ldots, k - 1$, a unary operation $d_i : k \rightarrow k$ is defined as

$$d_i(x) = \begin{cases} 0 & \text{if } 0 \leq x \leq i, \\ x & \text{if } i < x \leq k - 1 \end{cases}$$

for every $x \in k$.

Figure 1 shows how elements in $k$ are mapped by operation $d_i$.

Remark. (1) By definition, $d_0 = \text{id}_k$ and $d_{k-1} = c_0$ (the constant operation taking value 0).

(2) $\#(\text{Im}(d_i)) = k-i$ for every $i = 0, 1, \ldots, k-1$.

Definition 3.3 For every $i = 0, 1, \ldots, k - 1$, $N_i$ is the monoid generated by the set $S_k \cup \{d_i\}$, i.e.,

$$N_i = \langle S_k \cup \{d_i\} \rangle.$$

Remark. It is clear that $N_0 = S_k$.

The sequence of $N_i$'s and that of corresponding clones $\varphi(N_i)$'s is depicted in Figure 2.

Definition 3.4 For a unary operation $s \in \mathcal{O}_k^{(1)}$, the width of $s$ is defined to be the maximum cardinality of preimages $s^{-1}(z)$ for all $z \in k$ and denoted by $\omega(s)$, i.e.,

$$\omega(s) = \max\{\#(s^{-1}(z)) \mid z \in k\}.$$
Lemma 3.1  (1) For any $s \in O_k^{(1)}$, $1 \leq \omega(s) \leq k$.

(2) For any $s \in O_k^{(1)}$, $\omega(s) = 1$ if and only if $s \in S_k$.

(3) For any $s \in O_k^{(1)}$, $\omega(s) = k$ if and only if $s$ is a constant operation.

(4) For $d_i (i = 0, 1, \ldots, k - 1)$ defined in Definition 3.2, $\omega(d_i) = i + 1$.

Definition 3.5 For a unary operation $s \in O_k^{(1)}$, the characteristic sequence $(c_1, \ldots, c_m)$ of $s$ is the sorted sequence in non-ascending order of all non-zero elements in

$(\#s^{-1}(0), \#s^{-1}(1), \ldots, \#s^{-1}(k - 1))$.

Remark. For the characteristic sequence $(c_1, \ldots, c_m)$ of $s \in O_k^{(1)}$,

$\omega(s) = c_1 \geq c_2 \geq \ldots \geq c_m > 0$

and

$\sum_{i=1}^{m} c_i = k$.

As an example, the characteristic sequence of $d_i$ is $(i+1, 1, \ldots, 1)$ with 1's appearing $k-i-1$ times after $i+1$.

Lemma 3.2 For any $s \in O_k^{(1)}$ and $i = 1, 2, \ldots, k - 1$, if $\omega(s) \geq i + 1$ then $s \in N_i$.

Proof The proof follows from Claims 1 - 3.

Claim 1 For $i, j \in \{1, 2, \ldots, k - 1\}$, if $i \leq j$ then $d_j \in N_j$. Accordingly, $N_j \subseteq N_i$.

Claim 2 ("Canonical form" of unary operation)

Let $s$ be a unary operation in $O_k^{(1)}$ whose characteristic sequence is $(c_1, \ldots, c_m)$. Suppose that $c_1 \geq c_2 \geq \ldots \geq c_i > 1$ and $c_{i+1} = \ldots = c_m = 1$. Let $t$ be the unary operation in $O_k^{(1)}$ with the same characteristic sequence as $s$ and defined as

$t(0) = t(1) = \cdots = t(c_1 - 1) = 0,$

t(c_1) = t(c_1 + c_2 - 1) = c_1,$

$\cdots$,

$t(c_1 + \cdots + c_{\ell - 1}) = \cdots = t(c_1 + \cdots + c_{\ell - 1}) = c_1 + \cdots + c_{\ell - 1}$

and

$t(x) = x$ for $\forall x = c_1 + \cdots + c_\ell, \ldots, k - 1$.

Then it holds that $s \in (S_k \cup \{t\})$.

Claim 3 Let $s$ be a unary operation in $O_k^{(1)}$ whose characteristic sequence is $(c_1, \ldots, c_m)$. Let $i = \omega(s) - 1$. (Note that $\omega(s) = c_1$.) Then $s \in N_i$.

Due to Claims 1 and 3, we conclude that, for any $s \in O_k^{(1)}$ with characteristic sequence $(c_1, \ldots, c_m)$ ($c_1 = \omega(s)$), if $i \leq \omega(s) - 1$ then $s \in N_i$ as desired.

Proposition 3.1 For each $i = 0, 1, \ldots, k - 1$, let $W_i \subseteq O_k^{(1)}$ be the set of all permutations and all unary operations with width greater than $i$, that is, $W_i = S_k \cup \{f \in O_k^{(1)} | \omega(f) > i\}$. Then $N_i = W_i$ for every $i = 1, 2, \ldots, k - 1$.

Remark. Obviously, $W_0 = W_1 = O_k^{(1)}$.

Corollary 3.1 (1) $N_1 = O_k^{(1)}$

(2) $S_k \subset N_{k-1} \subset N_{k-2} \subset \cdots \subset N_3 \subset N_2 \subset O_k^{(1)} (= N_1)$

Here the symbol $\subset$ denotes proper inclusion.

4 Clones corresponding to Full Monoids

Definition 4.1 Pixley's discriminator function $p \in O_k^{(3)}$ is defined as

$p(x, y, z) = \begin{cases} x, & \text{if } x = y, \\ z, & \text{if } x \neq y \end{cases}$

for every $(x, y, z) \in k^3$.

Lemma 4.1 ([4]) Pixley's discriminator function $p$ belongs to $\varphi(S_k)$, i.e., $p \in \varphi(S_k)$. 

Proof Let \( s \) be arbitrary permutation in \( S_k \). If \( x = y \) then \( s(x) = s(y) \) and consequently \( p(s(x), s(y), s(z)) = s(p(x, y, z)) \). On the other hand, if \( x \neq y \) then \( s(x) \neq s(y) \), since \( s \) is a permutation. Then it follows that \( p(s(x), s(y), s(z)) = s(x) = s(p(x, y, z)) \). □

Theorem 4.1 ([4])

(1) \( \varphi(O_k^{(1)}) = J_k \), and

(2) \( \varphi(S_k) \supset J_k \). (Inclusion is proper.)

Proof Refer to [4] for the proof of (1). The proof of (2) is immediate from the previous lemma. □

The above results give rise to an interesting problem: Find maximal monoids satisfying

(1) \( S_k \subseteq M \subset O_k^{(1)} \) and (2) \( \varphi(M) \neq J_k \).

The following theorem provides an initial clue toward solving this problem.

Theorem 4.2
For Pixley's discriminator function \( p \), it holds that

(1) \( p \in \varphi(N_{k-1}) \), and

(2) \( p \notin \varphi(N_{k-2}) \).

Proof (1) Let \( c_i \in O_k^{(1)} \) denote the constant operation taking value \( i \) for \( i = 0, 1, \ldots, k - 1 \). By definition, \( N_{k-1} = \{ S_k \cup \{ d_{k-1} \} \} = \{ S_k \cup \{ c_0 \} \} \). Thus \( \varphi(N_{k-1}) = \varphi(S_k) \cap (\bigcap \varphi(c_i)) \).

Lemma 4.1 implies that \( p \in \varphi(S_k) \). On the other hand, it is straightforward that \( p \in Pol(c_i^O) \) for every \( i = 0, 1, \ldots, k - 1 \). (2) It suffices to show that \( p \notin Pol((d_{k-2})^O) \). According to the definition of discriminator function it follows that \( p(0,1,k-1) = 0 \) and \( p(d_{k-2}(0), d_{k-2}(1), d_{k-2}(k-1)) = p(0,0,k-1) = k-1 \). Since \( d_{k-2}(0) = 0 \neq k-1 \), it is concluded that \( p \notin Pol((d_{k-2})^O) \). □

Corollary 4.1 \( \varphi(N_{k-1}) \neq J_k \).

Finally, we characterize the clone \( \varphi(S_k) \).

Definition 4.2
For \( (x_1, \ldots, x_n), (y_1, \ldots, y_n) \in k^n \), we say that \( (x_1, \ldots, x_n) \) is similar to \( (y_1, \ldots, y_n) \), denoted as \( (x_1, \ldots, x_n) \sim (y_1, \ldots, y_n) \), if the following condition is satisfied:

\[ x_i = x_j \iff y_i = y_j \text{ for any } 0 \leq i, j < n. \]

Definition 4.3 An operation \( f \in O_k^{(n)} \) is synchronous if and only if the following condition is satisfied: Let \( (x_1, \ldots, x_n) \) be any element in \( k^n \).

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 \( (y_1, \ldots, y_n) \in k^n \) which is similar to \( (x_1, \ldots, x_n) \),

and if \( |(x_1, \ldots, x_n)| = k-1 \) and \( f(x_1, \ldots, x_n) = u \) for some \( u \in k \) then

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

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

The set of all synchronous operations in \( O_k \) is denoted by \( SYN_k \).

Example. Pixley's discriminator function \( p \) is synchronous.

Theorem 4.3 For the symmetric group \( S_k \) on \( k \), it holds that

\[ \varphi(S_k) = SYN_k. \]
Proof First, we prove that $S \mathcal{Y} N_k \subseteq \varphi(S_k)$. Let $f$ be any operation in $S \mathcal{Y} N_k$. As $\varphi(S_k)$ is defined to be the intersection of $\mathrm{Pol}(s^\circ)$'s for all $s \in S_k$, it suffices to show that $f$ belongs to $\mathrm{Pol}(s^\circ)$ for all $s \in S_k$. Let $s \in S_k$ and $(x_1, \ldots, x_n) \in k^n$. Suppose that $\{x_1, \ldots, x_n\} \neq k-1$ and $f(x_1, \ldots, x_n) = x_\ell$ for some $0 \leq \ell < k$. Since $s$ is a permutation, $x_i = x_j$ is equivalent to $s(x_i) = s(x_j)$ for any $0 \leq i, j < k$. Thus it follows from the assumption that $f$ is synchronous that $f(s(x_1), \ldots, s(x_n)) = s(x_\ell)$. Therefore $f \in \varphi(S_k)$ holds in this case. The case of $\{x_1, \ldots, x_n\} = k-1$ can be handled in the analogous way.

Secondly, in order to prove the converse, we assume that $f \in \mathcal{O}_k^{(n)}$ does not belong to $S \mathcal{Y} N_k$ and show that $f$ is not a member of $\varphi(S_k)$. Suppose that $\{x_1, \ldots, x_n\} \neq k-1$. Since $f \not\in S \mathcal{Y} N_k$, there exist vectors $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n)$ in $k^n$ which satisfy (1) $x_i = x_j$ if and only if $y_i = y_j$ for any $0 \leq i, j < k$ and (2) either $f(x_1, \ldots, x_n) = x_\ell$ for some $0 \leq \ell < k$ and $f(y_1, \ldots, y_n) \neq y_\ell$ or $f(x_1, \ldots, x_n) = u$ for $v \in k \setminus \{x_1, \ldots, x_n\}$ and $f(y_1, \ldots, y_n) \neq v$ for $v \in k \setminus \{y_1, \ldots, y_n\}$. Then it is easy to see that $f$ does not belong to $\mathrm{Pol}(s^\circ)$ for the permutation $s$ which maps $x_i$ to $y_i$ for each $i = 1, \ldots, n$ and $u$ to $v$. This proves the contraposition of $\varphi(S_k) \subseteq S \mathcal{Y} N_k$. □

5 Conclusion

We have considered some properties of (transformation) monoids and clones corresponding to such monoids. It was known before that the endoprimal clone for $\mathcal{O}_k^{(1)}$ is the least clone $\mathcal{J}_k$ and that the endoprimal clone for the symmetric group $S_k$ is distinct from $\mathcal{J}_k$. In this paper, we defined a descending sequence $\{N_i\}$ of monoids lying between $\mathcal{O}_k^{(1)}$ and $S_k$, and proved that the endoprimal clone for $N_{k-1}$ is distinct from $\mathcal{J}_k$. We also characterized the endoprimal clone for $S_k$ without appealing to monoids.

References