数理解析研究所講究録
第2008巻 2016年 81-85

A Note on Witnesses of Centralizing Monoids

Hajime Machida Ivo G. Rosenberg
Tokyo, Japan Montreal, Canada

Abstract

We consider multi-variable functions defined over a fixed finite set A. A centralizing monoid M is a set of unary functions on A which commute with all members of some set F of functions on A, where F is called a witness of M. We show that every centralizing monoid has a witness whose arity does not exceed $|A|$. Then we present a method to count the number of centralizing monoids which have sets of some specific functions as their witnesses. Finally, some results on the three-element set E_3 are reported concerning witnesses consisting of binary idempotent functions, majority functions or ternary semiprojections.

Keywords: commutation; centralizing monoid; witness

1 Preliminaries

Let A be a non-empty set. For $n \geq 1$ let $\mathcal{O}_A^{(n)}$ denote the set of n-variable functions defined on A, i.e., $\mathcal{O}_A^{(n)} = A^{A^n}$, and $\mathcal{O}_A$ denote the set of functions defined on A, i.e., $\mathcal{O}_A = \bigcup_{n=1}^{\infty} \mathcal{O}_A^{(n)}$. For $n > 0$ and $1 \leq i \leq n$ the i-th (n-variable) *projection* e_i^n is the function in $\mathcal{O}_A^{(n)}$ which always takes the value of the i-th variable. The set of projections is denoted by $\mathcal{J}_A$. A *clone* over A is a subset C of $\mathcal{O}_A$ which is closed under (functional) composition and includes $\mathcal{J}_A$.

For $m, n \geq 1$, $f \in \mathcal{O}_A^{(n)}$ and $g \in \mathcal{O}_A^{(m)}$, f *commutes* with g, or f and g *commute*, if the equation

$$f(g({}^t\boldsymbol{c}_1), \ldots, g({}^t\boldsymbol{c}_n)) = g(f(\boldsymbol{r}_1), \ldots, f(\boldsymbol{r}_m))$$

holds for every $m \times n$ matrix over A with the i-th row $\boldsymbol{r}_i$ $(1 \leq i \leq m)$ and the j-th column $\boldsymbol{c}_j$ $(1 \leq j \leq n)$. We write $f \perp g$ when f commutes with g.

In this paper we are concerned with a particular case of commutation, that is, commutation of an n-variable function with a unary function. It follows from the definition above that, for $f \in \mathcal{O}_A^{(n)}$ and $g \in \mathcal{O}_A^{(1)}$, f and g commute if

$$f(g(x_1), \ldots, g(x_n)) \;=\; g(f(x_1, \ldots, x_n))$$

holds for all $x_1, \ldots, x_n \in A$.

For a subset F of $\mathcal{O}_A$ the set of functions in $\mathcal{O}_A$ which commute with all members of F is denoted by F^*, i.e.,

$$F^* \;=\; \{\, g \in \mathcal{O}_A \;\mid\; g \perp f \;\text{ for all }\; f \in F \,\}.$$

When $F = \{f\}$ we write f^* instead of F^*. Also, we write F^{**} for $(F^*)^*$. The following property is straightforward.

Lemma 1.1 *For any F, $G \subseteq \mathcal{O}_A$, $F \subseteq G^*$ if and only if $G \subseteq F^*$.*

A subset C of $\mathcal{O}_A$ is a *centralizer* if there is a subset F of $\mathcal{O}_A$ satisfying $C = F^*$. For any subset F of $\mathcal{O}_A$, the centralizer F^* is clearly a clone. A subset M of $\mathcal{O}_A^{(1)}$ is a *monoid* if it is closed under composition and contains the identity. Since any centralizer F^* is a clone, the unary part of F^*, i.e., $F^* \cap \mathcal{O}_A^{(1)}$, is a monoid.

A subset M of $\mathcal{O}_A^{(1)}$ is a *centralizing monoid* if there exists a subset F of $\mathcal{O}_A$ which satisfies $M = F^* \cap \mathcal{O}_A^{(1)}$. In other words, a centralizing monoid is the unary part of some centralizer. The set F in the definition of a centralizing monoid M is called a *witness* of M. The centralizing monoid M will be denoted by $M(F)$ if F is a witness of M. When F is $\{f\}$ we simply write $M(f)$ for $M(\{f\})$.

It is well-known and easy to see that, for a subset M of $\mathcal{O}_A^{(1)}$, M is a centralizing monoid if and only if M is the unary part of M^{**}, i.e., $M = M^{**} \cap \mathcal{O}_A^{(1)}$.

2 Arity of Witnesses

We shall consider a fundamental problem on the arity of witnesses: How small can the arity of a witness be?

Definition 2.1 *For a (non-empty) finite subset W of $\mathcal{O}_A$, the* arity *of W is defined to be the maximal arity of all functions in W.*

We establish the following theorem.

Theorem 2.1 *Every centralizing monoid M on A has a witness whose arity is less than or equal to $|A|$.*

Proof follows after a definition and a lemma.

Definition 2.2 *For $n > 1$ let $f \in \mathcal{O}_A^{(n)}$ be an n-variable function and $i, j \in \mathcal{N}$ satisfy $1 \leq i < j \leq n$. Define $(n-1)$-variable function $f_{i\equiv j} \in \mathcal{O}_A^{(n-1)}$ by*

$$f_{i\equiv j}(x_1, \ldots, x_{n-1}) \quad = \quad f(x_1, \ldots, x_i, \ldots, x_{j-1}, x_i, x_{j+1}, \ldots, x_{n-1})$$

*for all $x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n \in A$. The function $f_{i\equiv j}$ is called (i, j)-*minor *of f. Denote by* Minor(f) *the set of all minors of f, i.e.,*

$$\text{Minor}(f) \quad = \quad \{\, f_{i\equiv j} \mid 1 \leq i < j \leq n \,\}$$

Lemma 2.2 *Let $f \in \mathcal{O}_A^{(n)}$ be an n-variable function. If $n > |A|$ then $M(f) = M(\text{Minor}(f))$, i.e., $f^* \cap \mathcal{O}_A^{(1)} = \text{Minor}(f)^* \cap \mathcal{O}_A^{(1)}$.*

Proof ($\subseteq$): Let $s \in \mathcal{O}_A^{(1)}$ be in $M(f)$. It follows that $s \perp f$, which is equivalent to saying that

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

holds for all $x_1, \ldots, x_n \in A$. In particular, for any pair (i, j) such that $1 \leq i < j \leq n$ we have

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

for all $x_1, \ldots, x_n \in A$ satisfying $x_i = x_j$. This implies $s \perp f_{i\equiv j}$. Hence s belongs to $M(\text{Minor}(f))$, which concludes $M(f) \subseteq M(\text{Minor}(f))$.
($\supseteq$): We prove the contraposition, that is, if $s \notin f^*$ then $s \notin \text{Minor}(f)^*$ for any $s \in \mathcal{O}_A^{(1)}$. Now the condition $s \notin f^*$ implies $s \not\perp f$, which means that

$$s(f(a_1, \ldots, a_n)) \neq f(s(a_1), \ldots, s(a_n))$$

holds for some $a_1, \ldots, a_n \in A$. Since $n > |A|$, there exist $i, j \in \mathcal{N}$ satisfying $1 \leq i < j \leq n$ and $a_i = a_j$. For notational simplicity, let $i = n - 1$ and $j = n$. Then we have

$$s(f_{n-1\,\equiv\,n}(a_1, \ldots, a_{n-1})) \neq f_{n-1\,\equiv\,n}(s(a_1), \ldots, s(a_{n-1})),$$

which implies $s \not\perp f_{n-1\equiv n}$. Thus $s \notin \text{Minor}(f)^*$ and, consequently, $M(f) \supseteq M(\text{Minor}(f))$. □

Proof of Theorem 2.1 Let W be a witness of a centralizing monoid M. For each f in W, if $f \in \mathcal{O}_A^{(n)}$ and $n > |A|$, replace f with all minors of f. The set $(W \setminus \{f\}) \cup \text{Minor}(f)$ is a witness of M, due to Lemma 2.2. Repeat this procedure until no function in the witness has arity greater than $|A|$. Then we get a desired witness for M. □

3 Strategy

Let H be a subset of $\mathcal{O}_A$. Suppose we want to determine all centralizing monoids on A which have subsets of H as their witnesses, or simply the number of such centralizing monoids. If h is the number of elements in H the number of subsets of H is 2^h, which tends to be huge and, therefore, in such cases, it requires some trick to achieve the task above.

Our strategy to avoid this difficulty is the following. Instead of starting from a function f in H and determine $M(f) = f^* \cap \mathcal{O}_A^{(1)} = \{ s \in \mathcal{O}_A^{(1)} \mid f \perp s \}$, we do it in the reverse way. Namely, we start from a unary function $s \in \mathcal{O}_A^{(1)}$, and consider the following set.

$$C_H(s) \quad = \quad s^* \cap H \quad (= \{ f \in H \mid f \perp s\})$$

Due to the next proposition, we asserts: There exists a bijection between the set of centralizing monoids having subsets of H as their witnesses and the set consisting of $C_H(s_1) \cap \cdots \cap C_H(s_r)$ for $1 \leq r \leq |A|^{|A|}$ and $s_1, \ldots, s_r \in \mathcal{O}_A^{(1)}$.

Proposition 3.1 *Let H be a non-empty subset of $\mathcal{O}_A$ and $C_H(s) = s^* \cap H$ for every $s \in \mathcal{O}_A^{(1)}$.*

(1) *For any non-empty subset F of H, let G be the set of functions defined by*

$$G = \bigcap \{C_H(s) \mid s \in \mathcal{O}_A^{(1)},\ F \subseteq s^*\}.$$

Then, $M(F) = M(G)$, that is, the centralizing monoid having F as its witness is the same as the centralizing monoid having G as its witness. (A witness F can be replaced with a witness G.)

(2) *For any* $s_1, \ldots, s_r, t_1, \ldots, t_q \in \mathcal{O}_A^{(1)}$, *let*

$$G_1 = \bigcap_{i=1}^{r} C_H(s_i) \quad \text{and} \quad G_2 = \bigcap_{j=1}^{q} C_H(t_j).$$

If $M(G_1) = M(G_2)$ *then* $G_1 = G_2$.

Proof (1) It suffices to show the following (i) and (ii) for any $s \in \mathcal{O}_A^{(1)}$: (i) $s \in G^*$ implies $s \in F^*$ and (ii) $s \in F^*$ implies $s \in G^*$.

(i) Obvious from $F \subseteq G$. (ii) Condition $s \in F^*$ implies $F \subseteq s^*$ (Due to Lemma 1.1). Then, by the definition of G, we have $G \subseteq C_H(s)$, which implies $G \subseteq s^*$ and, hence, $s \in G^*$.

(2) Proof by contraposition. Assume that G_1 and G_2 are different. Then, w.l.o.g., we may assume that there exists f in $G_2 \setminus G_1$. Then we have $f \not\perp s_i$ for some $i \in \{1, \ldots, r\}$, which implies $s_i \notin M(G_2)$. However, since $G_1 \subseteq C_H(s_i)$, we have $s_i \in M(G_1)$. Hence the conclusion, $M(G_1) \neq M(G_2)$, follows. □

Corollary 3.2 *The number of the centralizing monoids having subsets of* H *as their witnesses is equal to the number of sets* $\bigcap_{s \in S} C_H(s)$ *for all* $S \subseteq \mathcal{O}_A^{(1)}$.

Proof is immediate from Proposition 3.1.

In this paper, we are concerned only with the numbers of centralizing monoids having specific sets as their witnesses. However, if we want, not only to obtain the numbers of such centralizing monoids, but also to determine explicitly elements of each of such centralizing monoids, the following property is useful.

For unary functions $s_1, \ldots, s_r \in \mathcal{O}_A^{(1)}$ let $S = \{s_1, \ldots, s_r\}$. Then S is said to be $*$-*maximal* if $C_H(s_1) \cap \cdots \cap C_H(s_r) \not\subseteq C_H(t)$ for any $t \in \mathcal{O}_A^{(1)} \setminus S$.

Proposition 3.3 *For* $s_1, \ldots, s_r \in \mathcal{O}_A^{(1)}$, *if* $\{s_1, \ldots, s_r\}$ *is* $*$-*maximal then* $\{s_1, \ldots, s_r\}$ *is a centralizing monoid having* $C_H(s_1) \cap \cdots \cap C_H(s_r)$ *as its witness.*

4 Specific Types of Centralizing Monoids on E_3

From now on, we deal with the case where the base set A is $E_3 = \{0, 1, 2\}$. We write $\mathcal{O}_3^{(n)}$ and $\mathcal{O}_3$ for $\mathcal{O}_A^{(n)}$ and $\mathcal{O}_A$, respectively. In the past work, centralizers on E_3 were discussed, e.g., in [Da79].

Due to Theorem 2.1 in Section 2, every centralizing monoid on E_3 has a witness whose arity is less than or equal to 3.

We have considered witnesses which consist of sets of functions in each of the following three classes: Binary idempotent functions, majority functions and ternary semiprojections. The reason behind the selection of these classes of functions comes from the fact that minimal functions on E_3, except unary functions, all belong to these classes, which is the result of B. Csákány ([Cs83]) obtained in 1983.

For the reader's sake, we review the definition of each of these functions.

(i) For $f \in \mathcal{O}_3^{(2)}$, f is a *binary idempotent function* if $f(x, x) = x$ for all $x \in E_3$.

(ii) For $f \in \mathcal{O}_3^{(3)}$, f is a *majority function* if $f(x, x, y) = f(x, y, x) = f(y, x, x) = x$ for all $x, y \in E_3$.

(iii) For $f \in \mathcal{O}_3^{(3)}$, f is a *semiprojection* if there exists $i \in \{1, 2, 3\}$ such that $f(x_1, x_2, x_3) = x_i$ whenever $|\{x_1, x_2, x_3\}| < 3$ for all $x_1, x_2, x_3 \in E_3$.

Thus, for the set H in Section 3, we took up the set of majority functions, the set of ternary semiprojections and the set of binary idempotent functions, and enumerated all centralizing monoids which have those sets as their witnesses ([GMR15], [MR16]).

Proposition 4.1 (i) *The number of centralizing monoids on E_3 which have sets of binary idempotent functions as their witnesses is* 67.

(ii) *The number of centralizing monoids on E_3 which have sets of majority functions as their witnesses is* 15.

(iii) *The number of centralizing monoids on E_3 which have sets of ternary semiprojections as their witnesses is* 13.

More detailed description concerning the statements (ii) and (iii) (respectively, (i)) is found in [GMR15] (respectively, [MR16]).

Note that the number of binary idempotent functions on E_3, as well as the number of ternary majority functions on E_3, is $3^6 = 729$. Also, if we mean by a ternary semiprojection only such ternary semiprojection p which takes the value of the first argument whenever at least two of the arguments coincide, i.e., $p(x_1, x_2, x_3) = x_1$ whenever $|\{x_1, x_2, x_3\}| < 3$, then the number of such functions on E_3 is $3^6 = 729$. We observe that the numbers 67, 15 and 13 are small as compared with the number 729 and remarkably small as compared with the cardinality of the power set of each class of such functions, which is 2^{729}.

References

[Cs83] Csákány, B., All minimal clones on the three element set, *Acta Cybernet.*, **6**, 1983, 227-238.

[Da79] Danil'čenko, A. F., On parametrical expressibility of the functions of k-valued logic, *Colloquia Mathematica Societatis János Bolyai*, **28**, Finite Algebra and Multiple-Valued Logic, 1979, 147-159.

[GMR15] Goldstern, M., Machida, H. and Rosenberg, I. G., Some classes of centralizing monoids on a three-element set, *Proceedings 45th International Symposium on Multiple-Valued Logic*, IEEE, 2015, 205-210.

[MR16] Machida, H. and Rosenberg, I. G., Centralizing monoids on a three-element set related to binary idempotent functions, *Proceedings 46th International Symposium on Multiple-Valued Logic*, IEEE, 2016, 84-89.