Ivan Kopeček
Distinguishing subsets in general algebras

Časopis pro pěstování matematiky, Vol. 106 (1981), No. 1, 94--100

Persistent URL: http://dml.cz/dmlcz/108274

Časopis pro pěstování matematiky, roč. 106 (1981), Praha

DISTINGUISHING SUBSETS IN GENERAL ALGEBRAS

IVAN KOPEČEK, Brno

(Received February 21, 1979, in revised form July 3, 1979)

Distinguishing (also called disjunctive) subsets were considered for semigroups by E. J. Tully, Jr. [9], M. P. Schützenberger [7], B. M. Schein [5, 6] and in a slightly different sense by R. Pierce [4]. M. Novotný [2] and H. J. Shyr [8] discussed distinguishing subsets for monoids with respect to their relationship to languages and J. Zapletal [10, 11, 12] considered them for some special classes of semigroups.

In the present time languages are investigated not only as subsets of monoids but also as subsets of general algebras (see, for instance, [3]). Hence, it can be useful to generalize the notion of a distinguishing subset for universal algebras. This is the purpose of giving here a definition of distinguishing subsets in general algebras, which coincides with the original one for the case of semigroups.

Some elementary properties of distinguishing subsets on general algebras are discussed in this paper. The necessary and sufficient condition for the existence of distinguishing subsets in unary algebras would be of interest for characterizing the existence of distinguishing subsets in general algebras (see 3.7). In this paper, this problem is solved for a special case – mono-unary connected algebras.

I would like to express my thanks to Prof. M. Novotný. I am obliged to him for reading this paper and for many valuable suggestions.

1. PRELIMINARIES

Basic algebraic and set-theoretical notions are supposed to be known. Throughout the following text 'if and only if' is abbreviated as 'iff'. Proofs ot easily verifiable assertions are omitted.

Set-theoretical terms and notations. $R \subseteq S$ denotes that R is a subset of S. $R \subset S$ is equivalent to $R \subseteq S$ and $R \neq S$.

Let α be an equivalence on a set R. The factor set of R by α is denoted as R/α. If $r \in R$, then $[r]_\alpha$ is the element of R/α containing r. Hence, terms of the form $[x]_\alpha$,

where $x \in R$, represent classes of the equivalence α. For $L \subseteq R$ we put: $[L]_\alpha = \{[x]_\alpha; x \in L\}$.

The mapping from R onto R/α defined by $x \mapsto [x]_\alpha$ is denoted by $\mathrm{nat}(\alpha)$. Conversely, the equivalence on the set R induced by a mapping f is denoted by $\ker(f)$.

The empty set is denoted by $\emptyset$. By id_R we understand the identity on R (i.e., $\mathrm{id}_R = \{(x, x); x \in R\}$).

Let f be a mapping from R into S and g a mapping from S into T. Then gf denotes the composite of f and g. If $L \subseteq S$, then $f^{-1}(L) = \{x \in R; f(x) \in L\}$.

By N, the set of all positive integers is meant.

Algebraic terms and notation. An algebra will be denoted as a pair consisting of a support and a set of fundamental operations, for instance, $A = (M, F)$. By $x \in A$ we shall understand $x \in M$. We shall recall the notions of elementary translation and translation (see, for instance, [1]).

1.1. Definition. An *elementary translation* on an algebra $A = (M, F)$ is a function of the type

$$x \mapsto f(a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_n)$$

where $1 \leqq i \leqq n$, f is an arbitrary operation from F and $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n$ are arbitrary elements of M. A mapping g from M into M is said to be a *translation*, if $g = \mathrm{id}_M$ or g can be obtained as a composite of a finite number of elementary translations.

The set of all elementary translations on an algebra A will be denoted by Et_A and the set of all translations by T_A.

The following assertion will be useful in what follows ([1], Theorem 6.1.).

1.2. Proposition. *Let $A = (M, F)$ be an algebra and α an equivalence on the set M. Then the following assertions are equivalent.*

a) *α is a congruence relation,*

b) *α is closed with respect to Et_A,*

c) *α is closed with respect to T_A.*

Let us recal that the assertion b (c) means: for every $(x, y) \in \alpha$ and $g \in Et_A(T_A)$ the condition $(g(x), g(y)) \in \alpha$ holds.

2. DISTINGUISHING SUBSETS IN GENERAL ALGEBRAS

2.1. Definition. Let M be a set, α an equivalence relation on the set M and $L \subseteq M$. We say that α *saturates* L, if L can be obtained as a union of a system of classes of the equivalence α.

2.2. Lemma. *Let α be an equivalence on a set M saturating a subset $L \subseteq M$ and β an equivalence on the set M/α saturating L/α. Let us denote $f_1 = \mathrm{nat}(\alpha)$ and $f_2 = \mathrm{nat}(\beta)$. Then $\ker(f_2 f_1)$ is an equivalence saturating L.*

2.3. Definition. Let $A = (M, F)$ be an algebra and $L \subseteq A$. We shall say that L *distinguishes* A if the following condition holds.
(*): For arbitrary elements $x, y \in M$, $x \neq y$, there exists a translation $f \in T_A$ such that exactly one of the elements $f(x), f(y)$ belongs to the subset L.

The set L satisfying the condition (*) is said to be a *distinguishing* (or *disjunctive*) (see [2], [6]) subset of the algebra A.

2.4. Remark. Let us recall the definition of a distinguishing subset for monoids ([2], Definition 1.1.): Let S be a monoid, $L \subseteq S$ its subset. We say that L distinguishes S if, for arbitrary elements $x, y \in S$, $x \neq y$, there exist such elements $u, v \in S$ that either $uxv \in L$, $uyv \in S - L$ or $uxv \in S - L$, $uyv \in L$.

Since translations on the monoid S are functions having the form $x \mapsto uxv$, where $u, v \in S$, it is seen immediately that Definition 2.3 is a generalized form of the above mentioned one. This means that for monoids, both definitions are equivalent.

For the case of semigroups, the previous definition taking monoids can be used if it is supposed that u, v can be void symbols (see, for instance, [6]). Hence, our definition coincides wit the original one for semigroups, too.

2.5. Definition. Let $A = (M, F)$ be an algebra and $L \subseteq M$. We define the relation $\Xi_{(A,L)}$ on the set M by:

$(x, y) \in \Xi_{(A,L)}$ iff for all $f \in T_A$, $f(x) \in L$ is equivalent to $f(y) \in L$.

2.6. Proposition. *$\Xi_{(A,L)}$ is a congruence relation on the algebra A.*

Proof. Clearly, $\Xi_{(A,L)}$ is an equivalence relation on A. Let $f \in T_A$ and $(x, y) \in \Xi_{(A,L)}$. For each $g \in T_A$, the assertion $gf \in T_A$ holds. Hence, the conditions $gf(x) \in L$, $gf(y) \in L$ are equivalent for each $g \in T_A$. We obtain $(f(x), f(y)) \in \Xi_{(A,L)}$, which by 1.2 implies that $\Xi_{(A,L)}$ is a congruence.

2.7. Proposition. *$\Xi_{(A,L)}$ saturates L.*

Proof. Let $x \in L$ and $(x, y) \in \Xi_{(A,L)}$. Since $\mathrm{id}_A \in T_A$ and $\mathrm{id}_A(x) \in L$, we have $y = \mathrm{id}_A(y) \in L$. Hence, $\Xi_{(A,L)}$ saturates L.

2.8. Theorem. *$\Xi_{(A,L)}$ is the greatest congruence relation on the algebra A saturating L.*

Proof. Assume α is a congruence saturating L and $(x, y) \in \alpha$. From 1.2, it follows that α is closed with respect to T_A. Hence, $(f(x), f(y)) \in \alpha$ holds for all $f \in T_A$ and,

since α saturates L, $f(x)$ and $f(y)$ simultaneously belong both to L or $A - L$. Hence, $(x, y) \in \Xi_{(A,L)}$. It means $(x, y) \in \alpha$ implies $(x, y) \in \Xi_{(A,L)}$, i.e. $\alpha \subseteq \Xi_{(A,L)}$, q.e.d.

2.9. Proposition. *L is a distinguishing subset on an algebra A iff $\Xi_{(A,L)} = \mathrm{id}_A$.*

2.10. Theorem. *Let $A = (M, F)$ be an algebra, $L \subseteq M$, and α a congruence saturating L. Then the following assertions are equivalent.*

(i) *α is the greatest congruence on the algebra A saturating L.*

(ii) *L/α distinguishes A/α.*

Proof. Let us denote $\beta = \Xi_{(A/\alpha, L/\alpha)}$, $h_1 = \mathrm{nat}\,(\alpha)$ and $h_2 = \mathrm{nat}\,(\beta)$. Then $\ker(h_2 h_1)$ is a congruence on the algebra A. From 2.2 it follows that this congruence saturates L. Hence, (i) is equivalent with the assertion $\ker(h_2 h_1) \subseteq \alpha = \ker(h_1) = \ker(h_2 h_1)$, i.e., $\ker(h_1) = \alpha = \ker(h_2 h_1)$. This is equivalent to the assertion that h_2 is an injective mapping, i.e., $\beta = \mathrm{id}_{A/\alpha}$, and this is, by 2.11, equivalent to (ii).

3. DISTINGUISHING SUBSETS IN CONNECTED MONO-UNARY ALGEBRAS

3.1. Notation. Throughout this section, we shall suppose that A is a mono-unary algebra with a support M and the set of operations consisting from one unary operation f. Further, we shall use the following notation. If $x \in M$, then

$$x^0 = x\,,$$
$$x^n = f(x^{n-1}) \quad \text{for all} \quad n \in N\,.$$

3.2. Remark. Directly from Definition 1.1, it can be easily verified that the set of all translations on A coincides with the set of all functions of the type $x \mapsto x^{n-1}$, where $n \in N$.

3.3. Definition. A is said to be *connected*, if for all $x, y \in M$ there exist $m, n \in N$ such that $x^m = y^n$.

3.4. Definition. A *cycle of a mono-unary algebra A* is a subalgebra C of A such that there exists $n \in N$ satisfying $x^n = x$ for every $x \in C$.

3.5. Lemma. *Let A be connected. Then the following assertions are equivalent.*

a) *A includes no cycle.*

b) *Each subalgebra of A is infinite.*

3.6. Theorem. *Let A be connected. Then A includes a distinguishing subset iff there is no triplet of elements $a, b, c \in A$ $a \neq b \neq c \neq a$, satisfying $a^1 = b^1 = c^1$.*

Proof. a) Assume there are elements $a, b, c \in M$, $a \neq b \neq c \neq a$, satisfying $a^1 = b^1 = c^1$, and let R be a distinguishing subset of A. Then for each translation $f \neq \mathrm{id}_M$, we have $f(a) = f(b) = f(c)$, and simultaneously two of the elements a, b, c belong to R or $M - R$, so that they cannot be distinguished by id_M. However, by 2.3 this contradicts the assumption that R distinguishes A. Hence, if there is a distinguishing subset in A, there are no elements $a, b, c \in M$, $a \neq b \neq c \neq a$, with the property $a^1 = b^1 = c^1$.

b) Let there exist no elements $a, b, c \in M$, $a \neq b \neq c \neq a$, satisfying $a^1 = b^1 = c^1$. We have to prove that there is a distinguishing subset of the algebra A.

b1) Let us suppose that there is no cycle in A and let z be an arbitrary element of A. The subalgebra generated by the element z will be denoted by $P(z)$. From 3.5 it follows that $P(z)$ is infinite (hence, $z^m \neq z^n$ iff $m \neq n$). We put $R_1 = \{z^{2^n}; n \in N\}$. Further, we put $R_2 = \{y; y \notin P(z)$ and there exists $x \in P(z) - R_1$ such that $x^1 = y^1\}$, and $S = \{\{x, y\}; x \neq y, x^1 = y^1$ and $\{x, y\} \cap (R_1 \cup R_2) = \emptyset\}$. By the assumption (there are no elements $a, b, c \in M$, $a \neq b \neq c \neq a$, satisfying $a^1 = b^1 = c^1$) and the axiom of choice there exists a set R_3 with the following property: $R_3 \subseteq \bigcup_{s \in S} s$ and $R_3 \cap s$ contains exactly one element for each $s \in S$. The definition of S yields $R_3 \cap \cap (R_1 \cup R_2) = \emptyset$ and $R_3 \cap P(z) = \emptyset$.

We shall show that the set $R = R_1 \cup R_2 \cup R_3$ is a distinguishing subset of A.

Let $p, q \in M$, $p \neq q$. Since A is connected, there are numbers $k_1, k_2, k_3, k_4 \in N$ such that $z^{k_1} = p^{k_2}$ and $z^{k_3} = q^{k_4}$. Let $k = \max(k_2, k_4)$. Then $p^k, q^k \in P(z)$.

Assume $p^k = q^k$ and let r be the smallest number satisfying $p^r = q^r$. Hence, $p^{r-1} \neq q^{r-1}$. Assume further $p^{r-1}, q^{r-1} \in P(z)$. This means that there are numbers $m \neq n$ satisfying $p^{r-1} = z^m$, $q^{r-1} = z^n$. Then $z^{m+1} = p^r = q^r = z^{n+1}$ and this is a contradiction since A has no cycle. Hence, at most one of the elements p^{r-1}, q^{r-1} belongs to $P(z)$. Without loss of generality we can suppose that $P(z) \cap \{p^{r-1}, q^{r-1}\} = \{p^{r-1}\}$ if $P(z) \cap \{p^{r-1}, q^{r-1}\} \neq \emptyset$. Thus, the following cases can occur.

1) $p^{r-1} \notin P(z)$. Then, as we assume, $q^{r-1} \notin P(z)$. Therefore $p^{r-1} \notin R_1$, $q^{r-1} \notin R_1$. Since q^{r-1} is the only element different from p^{r-1} satisfying $(q^{r-1})^1 = (p^{r-1})^1$ and $q^{r-1} \notin P(z) - R_1$ holds, $p^{r-1} \notin R_2$ holds as well. Analogously $q^{r-1} \notin R_2$. This implies $\{p^{r-1}, q^{r-1}\} \in S$ and therefore exactly one of the elements p^{r-1}, q^{r-1} is in $R_3 \subseteq R$.

2) $p^{r-1} \in P(z)$ and $p^{r-1} \in R_1$. Then $q^{r-1} \notin P(z)$ and therefore $q^{r-1} \notin R_1$. Further, p^{r-1} is the only element from $P(z)$ satisfying $(p^{r-1})^1 = (q^{r-1})^1$. Since $p^{r-1} \in R_1$, we obtain $q^{r-1} \notin R_2$. Because of $p^{r-1} \in R_1$, we have $\{p^{r-1}, q^{r-1}\} \notin S$ and consequently $q^{r-1} \notin R_3$.

3) $p^{r-1} \in P(z)$ and $p^{r-1} \notin R_1$. Then $q^{r-1} \notin P(z)$ and $(p^{r-1})^1 = (q^{r-1})^1$ implies $q^{r-1} \in R_2$. Clearly, $p^{r-1} \in P(z)$ implies $p^{r-1} \notin R_2$ and $q^{r-1} \in R_2$ implies $\{p^{r-1}, q^{r-1}\} \notin \notin S$. Hence, $p^{r-1} \notin R_3$.

From 1), 2) and 3) it follows that exactly one of the elements p^{r-1}, q^{r-1} belongs

to R. Hence, if $p^k = q^k$, the condition $(*)$ (2.3) is satisfied for the translation $x \mapsto x^{r-1}$.

Now, assume $p^k \neq q^k$ and let $p^k = z^v$ and $q^k = z^w$. Without loss of generality we can suppose $w > v$. Let us denote $u = w - v$. Let d be a positive integer satisfying $d \geqq 2$ and $2^d - 2^{d-1} > u$. Then $p^{k+2^{(d-1)}-v} = z^{2^{(d-1)}} \in R_1 \subseteq R$ and $q^{k+2^{(d-1)}-v} = z^{w-v+2^{(d-1)}} = z^{2^{(d-1)}+u} \notin R_1$, whereby $q^{k+2^{(d-1)}-v} \notin R_2 \cup R_3$ because of $(R_2 \cup R_3) \cap P(z) = \emptyset$. Consequently, $q^{k+2^{(d-1)}-v} \notin R$. Hence, the condition $(*)$ (2.3) is satisfied for the translation $x \mapsto x^{k+2^{(d-1)}-v}$.

b2) Let a cycle C exists in A and suppose $z \in C$. We put $R_1 = \{z\}$ and $S = \{\{x, y\};\ x \neq y$ and $x^1 = y^1$ and $\{x, y\} \cap R_1 = \emptyset\}$. By our assumption (there are no elements a, b, c with the property $a \neq b \neq c \neq a$ and $a^1 = b^1 = c^1$), the axiom of choice and the fact that $s \nsubseteq C$ for each $s \in S$, there exists a set R_2 with the following properties: $R_2 \subseteq \bigcup_{s \in S} s$, $R_2 \cap s$ contains exactly one element for each $s \in S$, and $R_2 \cap C = \emptyset$. We shall show that the set $R = R_1 \cup R_2$ distinguishes A. Let $p, q \in M$ and $p \neq q$. Further, let k be the smallest positive integer satisfying $p^k, q^k \in C$.

Assume $p^k = q^k$. Let r be the smallest positive integer satisfying $p^r = q^r$. Hence, $p^{r-1} \neq q^{r-1}$. Assume $p^{r-1}, q^{r-1} \in C$. Then there exists $m \neq n$ such that $p^{r-1} = z^m$ and $q^{r-1} = z^n$. This implies $z^{m+1} = p^r = q^r = z^{n+1}$. We obtain $p^{r-1} = z^m = z^n = q^{r-1}$, but this is a contradiction. Hence, $\{p^{r-1}, q^{r-1}\} \nsubseteq C$. Without loss of generality we can suppose $C \cap \{p^{r-1}, q^{r-1}\} = \{p^{r-1}\}$ if $C \cap \{p^{r-1}, q^{r-1}\} \neq \emptyset$. Thus the following cases can occur.

1) $p^{r-1} \neq z$. Then $\{p^{r-1}, q^{r-1}\} \cap R_1 = \emptyset$ and therefore $\{p^{r-1}, q^{r-1}\} \in S$. This implies that exactly one of the elements p^{r-1}, q^{r-1} belongs to R_2. Hence, exactly one of the elements p^{r-1}, q^{r-1} belongs to R.

2) $p^{r-1} = z$. This implies $\{p^{r-1}, q^{r-1}\} \notin S$, i.e., $q^{r-1} \notin R_2$. Hence, exactly one of the elements p^{r-1}, q^{r-1} belongs to R.

From 1) and 2) it follows that if $p^k = q^k$, the condition $(*)$ (2.3) is satisfied for the translation $x \mapsto x^{r-1}$.

Assume $p^k \neq q^k$ and let u be a positive integer satisfying $p^{k+u} = z$. Then $q^{k+u} \neq z$. Hence, R distinguishes A because $R_2 \cap C = \emptyset$ implies $q^{k+u} \notin R_2$. This completes the proof.

3.7. Problem. Find a necessary and sufficient condition for the existence of distinguishing subsets in general unary algebras. Since a distinguishing subset is defined by means of translations and those are unary operations, solution of this problem would simultaneously characterize the existence of distinguishing subsets in general algebras, as far as the set of all translations could be suitably described.

References

[1] *Cohn P. M.:* Universal Algebra, Harper and Row, N.Y. 1965.

[2] *Novotný M.:* On some relations defined by languages, Prague Studies in Mathematical Linguistics *4*, 1972, 157—170.

[3] *Opp M.:* Charakterisierungen erkennbarer Termmengen in absolut freien universelen Algebren, Institut für Informatik, Hamburg, 1976.
[4] *Pierce R.:* Homomorphisms of semigroups, Ann. of Math. *59* (1954), 287—291.
[5] *Шайн Б. М.:* Вмещение полугруп в обобщение группы, Мат. сборник, (Н.С.) *55* (1961), 379—400.
[6] *Schein B. M.:* Homomorphisms and subdirect decompositions of semigroups, Pacific J. Math. *17* (1966), 529—547.
[7] *Schützenberger M. P.:* Une théorie algébrique du codage, C.R. Acad. Sci. Paris *242* (1956), 862—864.
[8] *Shyr H. J.:* Disjunctive languages on a free monoid, Information and Control *34* (1977), 123—129.
[9] *Tully E. J., Jr.:* Representation of semigroups by transformations of a set, Dissertation, Tulane University, 1960.
[10] *Zapletal J.:* Distinguishing subsets of semigroups and groups, Arch. Math. (Brno) *4* (1968), 241—250.
[11] *Zapletal J.:* Distinguishing subsets in semilattices, Arch. Math. (Brno) *2* (1973), 73—82.
[12] *Zapletal J.:* On the characterization of semilattices satisfying the descending chain condition and some remarks on distinguishing subsets, Arch. Math. (Brno) *2* (1973), 123—128.

Author's address: 602 00 Brno, Gorkého 60.