Commentationes Mathematicae Universitatis Carolinae

Pavel Křivka

On representations of monoids as monoids of polynomials

Commentationes Mathematicae Universitatis Carolinae, Vol. 13 (1972), No. 1, 121--136

Persistent URL: http://dml.cz/dmlcz/105400

Commentationes Mathematicae Universitatis Carolinae

13,1 (1972)

ON REPRESENTATIONS OF MONOIDS AS MONOIDS OF POLYNOMIALS

P. KŘIVKA, Praha

Introduction. The problem of representations of monoids (or groups) as monoids (or groups) of structure preserving mappings (in particular, homomorphisms of algebras) was dealt with in a number of papers(e.g. Frucht [1], de Groot [2], Hedrlín and Pultr [3], Sabidussi [4], etc.). In the present paper, a different approach of representing monoids by means of algebras is studied. Given an algebra the family of all its mapping into itself given by polynomials in one variable obviously forms a monoid under composition.

The aim of this paper is to prove: first, that every abstract finite or countable group can be obtained this way using an algebra with one binary operation (see § 2), further, we show that in general finite monoids are not always representable this way (see § 3). Also, we show that finite transformation groups are not always representable in their concrete form (see § 2).

To the first of the mentioned results let us point

AMS, Primary 08A05 Ref. Ž. 2.726.3

out that the representability of groups is understood here in the stronger of the possible senses, namely, as a monoid of all polynomials in the given operation (not as the group of a priori invertible ones).

§ 1. Preliminaries

An algebraic monoid is a set with a binary operation which is associative and has a unity element. A transformation monoid is a pair (X, M), where X is a set and M is a set of mappings $F : X \longrightarrow X$ which contains the identity mapping and is closed under composition. It is called a concrete representation of an algebraic monoid $\mathfrak{M}$ if M is isomorphic to $\mathfrak{M}$.

Two transformation monoids (X, M) and (Y, N) are said to be isomorphic if there exists a 1-1 mapping $F : X \longrightarrow Y$ such that the mapping $\mathcal{F} : M \longrightarrow N$ defined by $\mathcal{F}(f)(F(x)) = F(f(x))$ is an algebraic isomorphism of the monoids M and N.

A left translation of an algebraic monoid $\mathfrak{M}$ is a mapping $L_a : \mathfrak{M} \longrightarrow \mathfrak{M}$ given by $L_a(x) = ax$ with $a \in \mathfrak{M}$ fixed. With every algebraic monoid $\mathfrak{M}$ we can associate the transformation monoid of all its left translations which is obviously isomorphic to $\mathfrak{M}$ (the mapping sending a to L_a is an isomorphism). It is called the Cayley representation of $\mathfrak{M}$. A transformation monoid (X, M) is said to be regular if it is isomorphic with Cayley representation of its algebraic part.

The following two statements will be often used:

Lemma 1. Cayley representation of every algebraic monoid is regular.

Lemma 2. Transformation monoid (X, M) is regular if and only if there exists an $x_0 \in X$ such that $f(x_0) = x$ (x_0 is then said to be an exact source of the regular monoid (X, M)).
(To the second one - in case (X, M) is regular it suffices to put $x_0 = F^{-1}(id)$, if (X, M) has an exact source x_0 it suffices to define an isomorphic mapping $F: X \longrightarrow M$ by $F(x) = f_x$ where $f_x(x_0) = x$. Such an f_x is exactly one.)

Let ω be a binary operation on a set X; polynomials of one variable in (X, ω) are defined recursively as follows:

a) the identity mapping is a polynomial,

b) if p, q are polynomials then the function $\overline{\omega}(p, q)$ defined by $\overline{\omega}(p, q)(x) = \omega(p(x), q(x))$ is a polynomial, too.

The system $P(X, \omega)$ of all polynomials in (X, ω) is obviously closed under composition (do not confuse this with the, in general non-associative, operation $\overline{\omega}$ above).

Now, let us take a symbol $\sigma / \neq \theta /$. Words in σ are defined recursively as follows:

a) the empty set is a word,

b) σ is a word,

c) if w_1, w_2 are words, then $\sigma(w_1, w_2)$ is a word, too (these definitions are, of course, only particular cases of well known definitions of polynomials and words in general algebra).

The <u>interpretations</u> p_w of words w in a binary algebra (X, ω) are defined recursively by:

$$p_\emptyset = id, \quad p_{\sigma(w_1, w_2)} = \bar{\omega}(p_{w_1}, p_{w_2}).$$

The <u>degree of a word</u> is defined as follows:

a) the degree of the empty word is one,

b) the degree of the word σ is two,

c) if w_1 is a word degree i, w_2 is a word degree j, then $\sigma(w_1, w_2)$ is a word degree $i + j$.

The degree of a polynomial p is the minimal degree of a word w with $p_w = p$.

A transformation monoid (X, M) (an algebraic monoid $\mathfrak{M}$, resp.) is said to be representable if there is a binary operation ω on X with $M = P(X, \omega)$ (if there is a set X' with binary operation ω' such that $P(X', \omega')$ is isomorphic to $\mathfrak{M}$; the transformation monoid $(X', P(X', \omega'))$ is then a concrete representation of $\mathfrak{M}$, resp.). An algebraic monoid is said to be <u>strongly representable</u>, if every its concrete representation is representable.

§ 2. <u>Groups</u>

<u>Theorem 1</u>. Every finite or countable regular transformation group is representable.

__Proof__. Let (X, G) be any regular transformation group, let X be the set $\{1, 2, \ldots, m, \ldots\}$, let 1 be the exact source. For $i \in X$ denote by g_i the element of G with $g_i(1) = i$ (by the definition of an exact source, g_i is uniquely determined by i).

For every two $x, y \in X$ there is exactly one i with $g_i(x) = y$:

Really, we have $(g_y \cdot g_x^{-1})(x) = y$ and $g_y \cdot g_x^{-1} \in G$ and hence it has to be one of the g_i's (which are distinct). If $g_i(x) = g_j(x) = y$, we have $g_y^{-1} \cdot g_i \cdot g_x = g_y^{-1} \cdot g_j \cdot g_x$ and hence $g_i = g_j$.

Now, we can define an operation ω on X putting $\omega(x,x) = g_2(x), \omega(x, g_2(x)) = g_3(x), \ldots, \omega(x, g_m(x)) = g_{m+1}(x), \ldots$ (if X is finite, $\operatorname{card} X = m$, then $\omega(x, g_m(x)) = g_1(x) = x$, resp.). By this definition we see immediately that every $g \in G$ is a polynomial. On the other hand, let there exist a polynomial p in (X, ω) which is not in G. Take such a p with the least possible degree d. Obviously, $d > 2$. Thus, we have $p = \overline{\omega}(g_i, g_j)$ for some i, j. There is a k with $g_j = g_k \cdot g_i$. Hence, $p(x) = \omega(g_i(x), g_k(g_i(x))) = (g_{k+1} \cdot g_i)(x)$ so that $p \in G$ in a contradiction with the assumption, q.e.d.

Since the Cayley representation of an algebraic monoid is regular, we obtain

Corollary. Every finite or countable algebraic group is representable.

Theorem 2. Let X be a finite set, $card\ X > 2$. If G is the symmetric group on X (i.e. the group of all permutations), then the transformation group (X, G) is not representable.

Proof. Suppose (X, G) is representable, i.e. there exists a binary operation ω on X with $P(X, \omega) = G$.

Let $X = \{1, 2, \dots, p\}$. We shall prove the assertion $A = \{$ There exists $k_0 \in X$ with this characteristic: there exist $i, j, m, n \in X$ such that $\omega(i,j) = \omega(m,n) = k_0$ and $i \neq m$, $j \neq n$ holds.$\}$

Suppose $\mathrm{non}\,A$ holds and put

$K = \{x \in X \mid$ there exists at least p different pairs $(i, j) \in X^2$ with $\omega(i, j) = x\}$.

Consider any $k \in K$ and $(i_1, j_1) \in X^2$ with $\omega(i_1, j_1) = k$. Put

$$I = \{(x, y) \in X^2 \mid \omega(x, y) = k,\ x = i_1,\ y \neq j_1\},$$

$$J = \{(x, y) \in X^2 \mid \omega(x, y) = k,\ x \neq i_1,\ y = j_1\}.$$

Either I or J is empty. (Really, let both be nonempty. Take $(i_2, j_2) \in I$, $(i_3, j_3) \in J$. Then $i_2 = i_1$, $j_2 \neq j_1 = j_3$, $i_3 \neq i_1$ hence $i_2 \neq i_3$, $j_2 \neq j_3$

in a contradiction with $non\ A$.) Let I be the non-empty one. For another $k' \neq k$, $k' \in K$ I' is again non-empty (otherwise there would be an (i, j) in $I \cap \cap J'$ and therefore $\omega(i, j) = k = k'$ which is impossible).
Since $card\ I = p - 1$ for every I (for $(x, y) \neq \neq (i_1, j_1)$ and $(x, y) \notin I \cup J$ we have $\omega(x, y) \neq k$ - see $non\ A$) we have $card\ K = p$.
If we take any stable $x \in K$, then, for any $y, z \in X$, $\omega(x, y) = \omega(x, z)$ (since (x, y), (x, z) belong to the same I). If we put $g(x) = = \omega(x, x)$, we have the operation ω described by $\omega(x, y) = g(x)$. But such operation forms a monoid with one generator g (see Theorem 5, § 4) and as we suppose g to be a permutation, this monoid is a cyclic group and we have a contradiction. Thus A holds. Consider an $f \in G$ with $f(i) = j$, $f(m) = m$. By our assumption there exists a polynomial $p' = f$. If we put $\xi =$ the identity polynomial, then for the polynomial $p = \bar{\omega}(\xi, p')$ we obtain

$$p(i) = \omega(i, f(i)) = \omega(i, j) = k_0,\ p(m) = \omega(m, f(m)) = \omega(m, m) = k_0 .$$

Thus $p(i) = p(m)$, which means that p is not one-to-one i.e. $p \notin G$ in a contradiction with our assumption $P(X, \omega) = G$, q.e.d.

Remark. It would be, however, representable in the weaker sense mentioned above, since the monoid of all mappings is representable - see Theorem 7 below.

§ 3. Monoids

Lemma 3. Let (X, M) be a transformation monoid, let $X' \subset X$ be such that $f(X') \subset X'$ for every $f \in M$. Denote by M / X' the system of all restrictions of the elements of M on X'. If (X, M) is representable, then $(X', M/X')$ is representable, too.

Proof. Let ω be an operation on X with $P(X, \omega) = M$ and define an operation ω' on X' by this way:

$\omega'(x, y) = \omega(x, y)$ if $\omega(x, y) \in X'$, otherwise, $\omega'(x, y)$ may be any element of X'.

Now, the following assertion will be proved:

If p'_w is the interpretation of a word w in (X', ω') and p_w is the interpretation of w in (X, ω), then $p'_w = p_w / X'$ holds (p_w / X' is the restriction of p_w on X') which means $p'_w \in M / X'$ for every w.

Let there exist a word w such that $p'_w \neq p_w / X'$. Take such a w with the least possible degree d. Obviously, $d > 2$. Thus we have $w = \sigma(w_1, w_2)$, $\deg w_1$, $\deg w_2 < d$. For the interpretations we obtain $p'_w = \bar{\omega}(p'_{w_1}, p'_{w_2}) = \bar{\omega}(p_{w_1} / X', p_{w_2} / X') = p_w / X'$ which is a contradiction.

On the other hand, consider any $f' \in M / X'$. There exists at least one $f \in M$ with $f' = f / X'$. Since

$M = P(X, \omega)$, there exists at least one word w such that $f = p_w$. By the first part of our proof, $p'_w = p_w / X' = f / X' = f'$, q.e.d.

Corollary. If (X, M) is a transformation monoid and M / X' is the symmetric group on X' for an $X' \subset X$, then (X, M) is not representable.

Lemma 4. Let (X, M) be a representable transformation monoid, $M = P(X, \omega)$. If a polynomial $p \in M$ is an interpretation of a word w in (X, ω) , then for the interpretation p' of w in $(M, \overline{\omega})$ (see the definition of polynomial) holds $p'(f) = p \cdot f$.

Proof. Let there exist a word w such that $p'_w(f_0) \neq p_w \cdot f_0$ for some $f_0 \in M$. Take such a w with the least possible degree d . Obviously, $d > 2$. Thus, we have $w = \sigma(w_1, w_2)$, $deg\, w_1$, $deg\, w_2 < d$.

For the interpretations we obtain

$$p'_w(f_0) = \overline{\overline{\omega}}(p'_{w_1}, p'_{w_2})(f_0) = \overline{\omega}(p_{w_1} \cdot f_0, p_{w_2} \cdot f_0) .$$

Thus we have for every $x \in X$

$$p'_w(f_0)(x) = \overline{\omega}(p_{w_1} \cdot f_0, p_{w_2} \cdot f_0)(x) = \omega(p_{w_1}(f_0(x)) ,$$

$$p_{w_2}(f_0(x))) = \overline{\omega}(p_{w_1}, p_{w_2})(f_0(x)) = p_w(f_0(x)) = (p_w \cdot f_0)(x)$$

so that $p'_w(f_0) = p_w \cdot f_0$ in a contradiction with the assumption, q.e.d.

Theorem 3. An algebraic monoid $\mathcal{M}$ is representable if and only if its Cayley representation is representable.

Proof. Let (X, M) be a concrete representation of $\mathfrak{M}$ such that there exists an operation ω on X with $P(X, \omega) = M$. Let (M, L_M) be the Cayley representation of M. Consider a polynomial $p' \in P(M, \bar{\omega})$. There exists a word w with $p' = p'_w$. If $p_w \in M = P(X, \omega)$ is the interpretation of w in (X, ω), then, by Lemma 4, $p'_w(f) = p_w \cdot f = L_{p_w}(f)$. Thus, $P(M, \bar{\omega}) \subset L_M$.

To prove that $L_M \subset P(M, \bar{\omega})$ consider any $L_f \in L_M$. Then $f \in M = P(X, \omega)$ and hence there exists a word w with $p_w = f$. Hence $L_f(g) = L_{p_w}(g) = p_w \cdot g = p'_w(g)$ (again by Lemma 4) for every $g \in M$. As $p'_w \in P(M, \bar{\omega})$, we have $L_M = P(M, \bar{\omega})$. On the other hand, if Cayley representation is representable, $\mathfrak{M}$ is representable by the definition, q.e.d.

Theorem 4. The set $M = \{1, 2, 3, \ldots, n\}$ $(n > 4)$ with the binary operation of minimum is a nonrepresentable algebraic monoid.

Proof. Let M be representable. By Theorem 3 the Cayley representation (M, L_M) is representable, too. Let ω be an operation on M with $L_M = P(M, \omega)$. $\xi^2 \in P(M, \omega)$ defined by $\xi^2(x) = \omega(x, x)$ is equal to L_1 if we define $L_i(j) = \min(i, j)$. Really, if $\xi^2 = L_i$, $i \geq 2$, then $\xi^2(2) = \omega(2, 2) = \min(i, 2) = 2$

and thus we have for every $p \in P(M, \omega)$ that $p(2) = 2$ while $L_1(2) = 1$. Let $\bar{\omega}(\xi^2, \xi) = L_i$, $\bar{\omega}(\xi, \xi^2) = L_j$ (evidently $L_m = id = \xi$).

Now, we shall prove that any $p \in P(M, \omega)$ must be one of L_1, L_i, L_j, L_m. We can suppose that no two of them coincide. Further, we can see that $\bar{\omega}(L_1, L_m) = L_i$, $\bar{\omega}(L_m, L_1) = L_j$, $\bar{\omega}(L_m, L_m) = L_1$ hold.

Moreover, for every

$L \in L_M$, $L_1 = L_1 \cdot L$, $L = L_m \cdot L$, $L \cdot L = L$.

Suppose there exists a $p \in P(M, \omega)$, $p \neq L_x$ $x = 1, i, j, m$. Take such a p with the least possible degree d. Obviously, $d > 3$. Thus, we have $p = \bar{\omega}(p_1, p_2)$, $\deg p_1$, $\deg p_2 < d$. Let $p_1 = L_1$, $p_2 = L_i$ hold: Then we have

$$p(x) = \omega(p_1(x), p_2(x)) = \omega(L_1(x), L_i(x)) = \omega(L_1(L_i(x)), L_m(L_i(x))) = \bar{\omega}(L_1, L_m)(L_i(x)) = L_i(L_i(x)) = L_i(x)$$

for every $x \in M$ – a contradiction. Suppose $p_1 = L_i$ and $p_2 = L_1$: We have again

$$p(x) = \omega(L_i(x), L_1(x)) = \bar{\omega}(L_m, L_1)(L_i(x)) = (L_j \cdot L_i)(x).$$

Thus if $i < j$, then $p(x) = (L_i \cdot L_j)(x) = L_i(x)$ holds, if $i > j$, then $p = L_j$ holds – a contradiction.

By the same procedure we obtain a contradiction in the cases $p_1 = L_1$, $p_2 = L_j$ and $p_1 = L_j$, $p_2 = L_1$.

Further, let $p_1 = L_i$, $p_2 = L_j$ (we suppose $i, j \neq 1$):

Then $p(2) = \omega(L_i(2), L_j(2)) = \omega(2,2) = \xi^2(2) = L_1(2) = 1$, thus $p_1 = L_1$ holds - again a contradiction.

We obtain the same result in the cases $p_1 = L_j$, $p_2 = L_i$; $p_1 = p_2 = L_i$ and $p_1 = p_2 = L_j$.

For $p_1 = p_2 = L_1$ we have $p(x) = \omega(L_1(x), L_1(x)) = \xi^2(L_1(x)) = L_1(L_1(x)) = L_1(x)$ - a contradiction.

Further, let $p_1 = L_m$, $p_2 = L_i$. We have $p(2) = \omega(L_m(2), L_i(2)) = \omega(2,2) = L_1(2) = 1$, thus $p = L_1$. We obtain the same result in the remaining cases:

$p_1 = L_i$, $p_2 = L$; $p_1 = L_j$, $p_2 = L_m$; $p_1 = L_m$, $p_2 = L_j$.

Thus, we have proved that $P(M, \omega) = \{L_1, L_i, L_j, L_m\} \neq L_M$. Hence, the Cayley representation of M is not representable and, by Theorem 3, M is not representable at all.

§ 4. Remarks

In this paragraph we give some special cases and concrete supplements as illustrations to general theorems from the preceding two paragraphs.

Theorem 5. An algebraic monoid with one generator is strongly representable.

Proof. Let M be an algebraic monoid with one generator and (X, M) any concrete representation of M. Let g be a generator of M. Define an operation ω on X by $\omega(x, y) = g(y)$. In particular, $\omega(x, x) = g(x)$, i.e. we have $\xi^2 = g$.

a) Take an $f \in M$. There is a k with $f = g^k$ and hence $f = g^k = Q_1 \cdot Q_2 \cdot \ldots \cdot Q_k$ where $Q_i = \xi^2 \in P(X, \omega)$. Thus $M \subset P(X, \omega)$.

b) Let there exist a $p \in P(X, \omega)$ which is not in M. Take such a p with the least possible degree d. Obviously, $d > 2$. Thus, we have $p(x) = \bar{\omega}(f_1, f_2)(x) = \omega(f_1(x), f_2(x)) = g(f_2(x)) = (g \cdot f_2)(x)$ by the definition of ω. Thus $p = g \cdot f_2$, i.e. $P(X, \omega) \subset M$, q.e.d.

Theorem 6. Every cyclic group is strongly representable by means of an operation depending on both arguments.

Proof. Let (X, G) be any concrete representation of a cyclic group, i.e. if g is a generator, then $G = \{\ldots, g^{-n}, \ldots, g^{-1}, g^0, g, \ldots, g^n, \ldots\}$. Define an operation ω on X by: $\omega(x, g^i(x)) = g^{i+1}(x)$ (if G is finite, $\operatorname{card} G = n+1$, then $\omega(x, g^n(x)) = x$, resp.) and for $x, y \in X$ such that there exists no $g^i \in G$ with $g^i(x) = y$ $\omega(x, y)$ can be any element from X. For every two $x, y \in X$ $\omega(x, y)$ is defined uniquely. Really, if $g^i(x) = g^j(x) = y$, we have

$$\omega(x, g^i(x)) = g(g^i(x)) = g(g^j(x)) = \omega(x, g^j(x)) .$$

By this definition we see immediately that every $f \in G$ is a polynomial. On the other hand, let there exist a polynomial p which is not in G. Take such a p with the least possible degree d. Obviously, $d > 2$. Thus, we we have $p = \bar{\omega}(f_1, f_2)$, $f_1, f_2 \in G$. There exists an i such that $f_2 = g^i \cdot f_1$ and hence $p(x) = \omega(f_1(x), f_2(x)) = \omega(f_1(x), g^i(f_1(x))) = g^{i+1}(f_1(x)) = (g \cdot f_2)(x)$ holds for every $x \in X$. Thus $M = P(X, \omega)$, q.e.d.

Theorem 7. Let M be the monoid of all mappings of a set X into itself (X finite or countable). Then (X, M) is representable and the binary operation can be chosen commutative.

Proof. Let $X = \{1, 2, \ldots, m, \ldots\}$. (If $card\ X = m$, the addition below is understood $mod\ m$.) By a well-known theorem monoid M can be generated by mappings g, c, t, given by: $g(x) = x + 1$; $c(1) = c(2) = 1$ and $c(x) = x$ for other $x \in X$; $t(1) = 2$, $t(2) = 1$ and $t(x) = x$ for other $x \in X$.

If $card\ X \geq 4$, define a commutative operation ω on X by:

$\omega(x,x) = q(x) = x+1$,

$\omega(x, x+1) = \omega(x+1, x) = c(x)$,

$\omega(x, x+2) = \omega(x+2, x) = t(x)$

and on the rest of X arbitrarily. Evidently, $P(X, \omega) \subset M$.

On the other hand, it is easy to see that every $f \in M$ is a polynomial. For $card\ X = 3$ take the commutative operation ω given by $\omega(x,x) = q(x) = x+1$, $\omega(x, x+1) = \omega(x+1, x) = t(x)$, for $card\ X = 2$ take the ω given by $\omega(x,x) = q(x) = x+1$, $\omega(1,2) = \omega(2,1) = 1$ (or $\omega(1,2) = \omega(2,1) = 2$). We check easily that these operations have the required properties, q.e.d.

I should like to thank most sincerely to A. Pultr for his kind advices and valuable help during the writing of this paper.

R e f e r e n c e s :

[1] R. FRUCHT: Herstellung von Graphen mit vorgegebener abstrakter Gruppe, Compos.Math.6(1938),239-250.

[2] J. de GROOT: Groups represented by homeomorphism groups I., Math.Annalen 138(1959),80-102.

[3] Z. HEDRLÍN, A. PULTR: Symmetric relations (Undirected graphs) with given semigroups. Mh.für Math. 69(1965),318-322.

[4] G. SABIDUSSI: Graphs with given infinite group, Mh.für Math.64(1960),64-67.

Matematicko-fyzikální fakulta

Karlova universita

Praha 8, Sokolovská 83

Československo

(Oblatum 5.10.1971)