Commentationes Mathematicae Universitatis Carolinae

Pavel Goralčík

One remarkable property of the bicyclic semigroup

Commentationes Mathematicae Universitatis Carolinae, Vol. 12 (1971), No. 3, 503--518

Persistent URL: http://dml.cz/dmlcz/105361

Commentationes Mathematicae Universitatis Carolinae

12,3 (1971)

ONE REMARKABLE PROPERTY OF THE BICYCLIC SEMIGROUP

P. GORALČÍK, Praha

Given an algebraic monoid $M = (X, e, \cdot)$ - a set X together with an associative multiplication possessing an identity element e, it may happen that from our knowledge of the multiplication on the left by a single element a in X, i.e. from the amount of "information" about M represented by its left translation f_a,

(1) $$f_a(x) = a \cdot x \quad \text{for all } x \text{ in } X ,$$

we can determine M uniquely. That means, we can say, in a unique way, which element e in X is the identity element of M, and, what is the product $x \cdot y$ of an arbitrary ordered pair (x, y) of elements of X. Let us call such an element a in X a <u>left determining element</u> and the left translation f_a corresponding to it a <u>determining left translation</u> of M. Replacing M by the monoid M^{op} opposite to M we get the dual notions of a <u>right determining element</u> and of a <u>determining right translation</u>.

AMS Classification, Primary 20M20

Any monogeneous monoid $M = \langle a \rangle$ is an example of a commutative monoid having (both left and right) determining element - just the generator a, in this case. A question was, whether there existed any non-commutative monoids possessing both a left and a right determining element - we shall call them non-commutative (1,1)-monoids. The present paper aims in the proof that, essentially, the only one noncommutative (1,1)-monoid is the well known <u>bicyclic semigroup</u> $\mathcal{B} = \langle a, b \rangle$ with the identity e and the two generators a, b satisfying the defining relation

$$ab = e \; . \tag{2}$$

More precisely, we state

<u>Theorem 1</u>. There are exactly two non-commutative (1,1)-monoids: the bicyclic semigroup $\mathcal{B}$ and $\mathcal{B}^0$ - the $\mathcal{B}$ with zero adjoined.

More elementary description identifies $\mathcal{B}$ with the set $N \times N$ of all ordered pairs (m, n) of non-negative integers supplied with the multiplication

$$(m,n)(r,s) = \begin{cases} (r, s-m+n) & \text{for } s \geq m \; , \\ (r+m-s, n) & \text{for } s < m \; . \end{cases} \tag{3}$$

Then we have $a = (1,0)$, $b = (0,1)$, $e = (0,0)$. The left translation f_a has a form

$$f_a(r,s) = (1,0)(r,s) = \begin{cases} (r, s-1) & \text{for } s \geq 1 \; , \\ (r+1, 0) & \text{for } s = 0 \; , \end{cases} \tag{4}$$

and it is worth while to visualize it as follows:

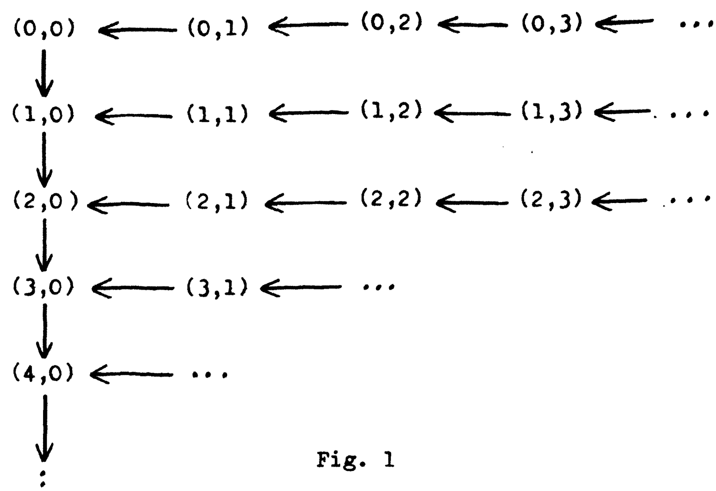

Fig. 1

To prove Theorem 1, we shall start with a general transformation $f: X \rightarrow X$ and, under the assumption that f be a left determining translation of some non-commutative (1,1)-monoid, we shall specify step by step its form, finally showing f to be isomorphic with f_a described by (4) (possibly extended by a single fixed point), and f_a, in its turn, to be a determining left translation of B (or of B^o when extended by a fixed point).

The whole proof will be carried out in a sequence of Statements 1 - 8 and it depends essentially on papers [1],[2],[3] whose results are restated here without proofs as Statements 1 - 4.

A <u>transformation system</u>, or shortly a T <u>-system</u>, is a couple (X, S), where X is a set and $S \subset X^X$ is a set of transformations of the set X, i.e. the

members of S are mappings of the form $f : X \to X$.
A T-system (X, F) is a T-monoid if

(5) $$1_X \in F$$

where 1_X is the identity transformation of X, and

(6) $$f, g \in F \implies fg \in F ,$$

where fg is a composite transformation written left-hand, i.e.

(7) $$fg(x) = f(g(x)) \text{ for } x \in X .$$

For any T-system (X, S) there is defined a T-monoid $(X, C(S))$ called the centralizer of (X, S) by

(8) $$C(S) = \{g \in X^X \mid fg = gf \text{ for all } f \text{ in } S\} .$$

A point s is a source (exact source) of a T-system (X, S) if for every x in X there exists (unique) f in S with $f(s) = x$. For an algebraic monoid $M = (X, e, \cdot)$ designate by $(X, L(M))$ and $(X, R(M))$ its T-systems of all the left and all the right translations, respectively. Call a T-monoid (X, F) a regular T-monoid if there exists an algebraic monoid $M = (X, e, \cdot)$ such that $F = L(M)$. A transformation f contained in some regular T-monoid will be called a (potential) translation.

Statement 1. The following three assertions about a T-system (X, S) are equivalent:

(A) (X, S) is a regular T-monoid,

(B) (X, S) is a T-monoid with an exact source,

(C) (X, S) and $(X, C(S))$ have a common source.

If these assertions hold, then for each exact source e of the regular T-monoid (X, S) there exists a unique algebraic monoid $M = (X, e, \cdot)$ with $L(M) = S$, whose multiplication is defined by

(9) $$x \cdot y = f_x(y) ,$$

where f_x is the unique member of S with $f_x(e) = x$.

Let a transformation $f : X \longrightarrow X$ be given. A subset A of X is <u>stable</u> with regard to f if $f(A) \subset A$. A transformation $g : A \longrightarrow A$ is <u>induced</u> by f on its stable subset A if $g(x) = f(x)$ for every x in A. The <u>kernel</u> Q_f of f is the union of all the subsets A of X such that $f(A) = A$, i.e. Q_f is the greatest stable subset such that the transformation induced on it by f is surjective. Of course, Q_f may be empty. The kernel Q_f of f is called an <u>increasing</u> kernel if the transformation induced on it by f is not injective and is called a <u>bijective kernel</u> otherwise.

For a given x in X, the intersection of all stable subsets of $f : X \longrightarrow X$ containing x is the <u>path</u> $P_f(x)$ of x formed by all <u>iterates</u> of x by f:

(10) $$P_f(x) = \{ f^m(x) \mid m \geq 0 \} .$$

Two elements x, y of X are E_f <u>-equivalent</u> if their paths meet, i.e. if $f^m(x) = f^n(x)$ for some non-negative integers m, n. The relation E_f on X thus defined is an equivalence relation by which X is decomposed into <u>components</u> of f. By $E_f(x)$ is denoted the component containing x. A transformation f is connected if all elements of X are mutually E_f -equivalent, otherwise it is disconnected. Call $f : X \to X$ a quasi-connected transformation if it either is connected or has exactly two components one of which consists of a single point.

Statement 2. Any quasi-connected potential translation with bijective kernel and no one with an increasing kernel is a translation of a commutative monoid.

An element x in X is called a cylic element of $f : X \to X$ if $x \in P_f(f(x))$. The set Z_f of all cyclic elements of f may be empty in the case X is infinite. If f has no cyclic elements then an equality $f^m(x) = f^n(x)$ holds if and only if $m = n$.

Statement 3. A connected non-surjective transformation $f : X \to X$ with an increasing kernel is a potential translation if and only if

(i) $Z_f = \emptyset$,

(ii) there exist e in X and $h : Q_f \to Q_f$ such that $f^m(X) \subset Q_f$ whenever $f^m(e) \in Q_f$,

(11) $fh(x) = x$ for all x in Q_f,

(12) $h(Q_f) \cap P_f(e) = \emptyset$.

Call $f : X \to X$ an increasing transformation if it is surjective but not injective. It is "increasing" in the sense that for some proper subset Y of X it is $f(Y) = X$.

Statement 4. A connected increasing transformation $f : X \to X$ is a potential translation if and only if

$Z_f = \emptyset$ and there exists an element e in X and an injection g in $C(f)$ such that

(13) $f(e) = g(e)$ and $g(t) \neq e$ for any t in X with $f(t) = e$.

Moreover, for any fixed e and g satisfying (13) there exists a regular T-monoid (X, F) such that $f \in F$ and $g \in C(F)$.

For proofs of Statements 1 - 4 see [1], [2], [3].

Statement 5. Any determining left translation $f: X \longrightarrow X$ of some (1,1)-monoid $M = (X, e, \cdot)$ is quasi-connected. If it is disconnected, then $X - E_f(e) = \{z\}$ and $M = K^0$ (a monoid K with zero adjoined), where $K = (E_f(e), e, \cdot)$ is a (1,1)-submonoid of M with the same determining elements (left or right) as M and z is the zero adjoined.

Proof: Assume f disconnected and define a monoid $M' = (X, e, *)$ by

$$(14) \qquad x * y = \begin{cases} x \cdot y & \text{for } x \in E_f(e), \\ x & \text{for } x \in X - E_f(e) . \end{cases}$$

The left translation f of M corresponds to the element $f(e)$ contained in $E_f(e)$, hence f is, by (14), also a left translation of M', and, since f is a determining left translation of M, it is $M = M'$. By (14), $K = (E_f, e, \cdot)$ is a submonoid of M and all elements in $X - E_f(e)$ are left zeros of M .

Now, M has also a determining right translation g which is disconnected, since $E_f(e)$ and $X - E_f(e)$ are disjoint stable subsets of every right translation of M. So g is a disconnected determining left translation of a (1,1)-monoid M^{op} opposite to M. By the same argument as applied above to f, we conclude that M^{op} must have a left zero, i.e. M has a right zero. It follows that $X - E_f(e)$ contains exactly one point, the bothsided outer zero z of M. Clearly, elements determining M are the same as those determining $K = M - \{z\}$.

Statement 5 enables us to regard only connected determining translations of (1,1)-monoids since all disconnected ones can be obtained from them by a single fixed point extension.

<u>Statement 6</u>. A connected determining left translation $f : X \to X$ of a non-commutative (1,1)-monoid M must be surjective.

Proof: Assume f not to be surjective. By Statement 2, f must have an increasing kernel, hence Statement 3 applies.

Starting with e and $h : Q_f \to Q_f$ satisfying the condition of Statement 3, we shall give a construction of a regular T-monoid (X, F_h) containing f:

For every x in X define a non-negative integer

$$(15) \qquad u(x) = \min \{ k \mid f^k(x) \in Q_f \} .$$

Designate by Y_f the set of all x in X such that $f^{u(x)}(x) \in P_f(e)$, i.e. $f^{u(x)}(x) = f^m(e)$ for some $m \geq 0$. Since $Z_f = \emptyset$ by Statement 3, such m is unique and we can define for every x in Y_f a non-negative integer $d(x)$ by

(16) $$d(x) = m - u(x) \text{ if } f^m(e) = f^{u(x)}(x) .$$

Since $Z_f = \emptyset$, we can decompose X into classes $T_{p,q}$ so that

$x \in T_{p,q}$ if and only if p, q are the least non-negative integers such that

(17) $$f^{u(e)+p}(e) = f^q(x) ,$$

i.e. if for some p', q', $p' \leq p$, $q' \leq q$, it holds $f^{u(e)+p'}(e) = f^{q'}(x)$, then $p' = p$ and $q' = q$.

Now, for every x in X define a transformation f_x:

For $x \in V_f$ put

(18) $$f_x(e) = x ,$$
$$f_x(t) = f^{d(x)}(t) \quad \text{for } t \neq e ;$$

for $x \in T_{p,q} - V_f$

(19) $$f_x(e) = x ,$$
$$f_x(t) = h^q f^{u(e)+p}(t) \text{ for } t \neq e .$$

The T-system (X, F_h), $F_h = \{f_x \mid x \in X\}$, has e for its source and its centralizer is formed by a system of transformations $C(F_h) = \{g_y \mid y \in X\}$, defined as follows:

Put $g_e = 1_X$ - the identity transformation, and for $y \neq e$ put

$$(20)\quad g_y(t) = \begin{cases} f^{d(t)}(y) & \text{for } t \in V_f\,, \\ h^n f^{u(e)+m(y)} & \text{for } t \in T_{m,n} - V_f\,. \end{cases}$$

After checking mutual commutativity of f_x and g_y for arbitrary x, y in X, it is seen immediately that e is a common source of both (X, F_h) and $(X, C(F_h))$, hence by the "regularity condition" (C) of Statement 1 (X, F_h) is a regular T-monoid, and $f = f_{f(e)}$.

Let $h' : Q_f \longrightarrow Q_f$ be another transformation satisfying, together with the same e as above, the conditions of Statement 3 and let us construct, by the construction just described, the corresponding regular T-monoid $(X, F_{h'})$, $F_{h'} = \{f'_x \mid x \in X\}$. If $h' \neq h$, then also $F_{h'} \neq F_h$: Assume $h'(t) \neq h(t)$ in some point t of Q_f. Choose some x in $T_{0,1} - V_f$, e.g. $x = h f^{u(e)}(e)$, and s in Q_f such that $f^{u(e)}(s) = t$. Then by (18) we have

$$f_x(s) = h f^{u(e)}(s) = h(t)\,,$$

whereas

$$f'_x(s) = h' f^{u(e)}(s) = h'(t)\,,$$

that is, $f_x \neq f'_x$ and hence $F_h \neq F_{h'}$.

Since f is, by assumption, a determining translation, the two regular T-monoids $F_{h'}$ and F_h cannot be distinct. This means that the transformation $h : Q_f \to Q_f$ satisfying the conditions of Statement 3 must be unique. On the other hand, every choice function on the disjoint family of sets

(21) $\quad (f^{-1}(x) \cap Q_f) - P_f(e), \quad x \in Q_f$

meets these conditions. It follows that each member of the family (21) must contain exactly one point, which amounts to saying that $T_{m,n} \cap Q_f$ consists of a single point $x_{m,n}$ for every pair (m,n) of non-negative integers. The assignment of (m,n) to $x_{m,n}$ establishes an isomorphism between the transformation induced by f on its kernel Q_f and the transformation f_a defined by (4). Note that (0,0) is assigned to $f^{u(e)}(e)$ - the first of iterates of e by f which is contained in the kernel Q_f of f.

We have proved, thus far, that the only regular T-monoid containing f is (X, F_h) described by (18), (19) with the only possible $h: Q_f \longrightarrow Q_f$ given by

(22) $\quad h(x_{m,n}) = x_{m,n+1}$ for every $m, n \geq 0$.

It remains to show that $(X, C(F_h))$ does not contain any determining translation. Using the description (20) of $C(F_h)$, we can easily see that for every y in V_f or in $T_{p,q} - V_f$ with $u(e) + p - q \neq 1$ the transformations g_y are not quasi-connected: For y in V_f as well as for any y in $T_{p,q} - V_f$ with $u(e) + p - q \geq 0$ the sets V_f and $X - V_f$ are disjoint infinite stable sets of g_y; for y in $T_{p,q} - V_f$ with $d = q - (u(e) + p) \geq 2$ we have $\bigcup_{i=0}^{\infty} T_{p,id}$ and $\bigcup_{i=0}^{\infty} T_{p,id+1}$ disjoint stable sets of g_y.

Our last step it will be to show that also g_y for an arbitrary y in $T_{n,u(e)+n+1}$, $n \geq 0$, fail to be determining translations of $C(F_h)$. Using (20), we have

$$(23)\quad g_y(x_{n+i+1,j}) = h^j f^{u(e)+n+i+1}(y) = h^j(x_{n+i,0}) = x_{n+i,j}$$

for all $i \geq 0$ and arbitrary $j \geq 1$. This means that all the points $x_{n+i,j}$ for $i \geq 0$ and $j \geq 1$ are contained in the kernel Q_{g_y} of g_y. Since we have

$$g_y(x_{n,u(e)+n+1}) = x_{n,u(e)+n+2} = g_y(x_{n+1,u(e)+n+2}),$$

the point $x_{n,u(e)+n+2} = g_y^2(e)$ cannot be the first iterate of e by g_y contained in the kernel of g_y. If $y = x_{n,u(e)+n+1}$ we are in precisely the same situation because of

$$g_y(x_{n,u(e)+n}) = x_{n,u(e)+n+1} = g_y(x_{n+1,u(e)+n+1}).$$

In the case $y \neq x_{n,u(e)+n+1}$ y is not in Q_f, therefore by (20) it is $g_y(t) = y$ only if $t \in V_f$ and $d(t) = 0$. Since there is no s with $g_y(s) = t$ for such a t, it follows that neither $y = g_y(e)$ nor $e = g_y^0(e)$ is in the kernel of g_y.

So in $(X, C(F_h))$ there is no determining translation - a contradiction due to the assumption that f is not surjective.

<u>Statement 7</u>. A connected and surjective determining left translation of a non-commutative (1,1)-monoid M must be isomorphic to the transformation f_a given by (4).

Proof: By Statement 2, f must be increasing. By Statement 4, we can choose an element e in X and an injection g in $C(f)$ satisfying (13). Since, by Statement 4, f has no cyclic points, every x in X determines uniquely the least non-negative integers $m(x), n(x)$ such that

$$f^{m(x)}(e) = f^{n(x)}(x) \quad . \tag{24}$$

This defines a decomposition of X into classes $T_{m,n}$ such that $x \in T_{m,n}$ if and only if $m(x)=m,\ n(x)=n$.

Next we shall prove that

$$g(T_{m,n}) \subset T_{m+1,n} \tag{25}$$

for all $m, n \geq 0$.

From (13) it follows that for every m, $m \geq 0$, it is $gf^m(e) = f^m g(e) = f^{m+1}(e) = ff^m(e)$, thus $g(T_{m,0}) = T_{m+1,0}$, since clearly $T_{m,0} = \{f^m(e)\}$. From $fg(t) = gf(t)$ we get

$$g(t) \in f^{-1}(gf(t)) \quad \text{for} \quad t \in X \quad . \tag{26}$$

If $t \in T_{0,1} = f^{-1}(e)$, then $gf(t) = g(e) = f(e)$, and, by (26), $g(t) \in f^{-1}(f(e)) = T_{1,1} \cup \{e\}$. But by (13) it is $g(t) \neq e$, thus $g(t) \in T_{1,1}$ and hence $g(T_{0,1}) \subset$ $\subset T_{1,1}$.

If $t \in T_{m,1}$ for $m \geq 1$, then it is $gf(t) = gf^m(e) =$ $= f^{m+1}(e)$, and, by (26), $g(t) \in f^{-1}(f^{m+1}(e)) = T_{m+1,1} \cup \{f^m(e)\}$. Since g is injective, it follows from $gf^{m-1}(e) = f^m(e)$ and from $t \neq f^{m-1}(e)$ that $g(t) \neq f^m(e)$. Thus

$g(t) \in T_{m+1,1}$, and we conclude that $g(T_{m,1}) \subset$
$\subset T_{m+1,1}$.

We have yet proved the inclusion (25) for $n = 0, 1$ and all $m \geq 0$. Assume that (25) holds for some $n \geq 1$ and for all $m \geq 0$. Since for any t in $T_{m,n+1}$ it is $f(t) \in T_{m,n}$, we have $gf(t) \in T_{m+1,n}$, and, by (26), $g(t) \in f^{-1}(T_{m+1,n}) = T_{m+1,n+1}$, which completes the proof of (25).

From (25) it follows that no $T_{m,n}$ is void, since $T_{0,n} \neq \emptyset$ for all $n \geq 0$. On the other hand, each class $T_{m,n}$ contains at most one point: If $|T_{m,n}| > 1$ for some m, n , choose x in $T_{m,n}$ and y in $T_{m+1,n}$ so that $y \neq g(x)$ and define g' by

$$(27)\quad g'(t) = \begin{cases} f^k(y) \text{ for } t = f^k(x),\ k = 0, 1, \dots, n-1, \\ g(t) \text{ otherwise.} \end{cases}$$

We have $g'(x) \neq g(x)$ while g' is easily shown to satisfy the conditions (13). By Statement 4, there exist regular T-monoids (X, F) and (X, F') , both containing f , with g in $C(F)$ and g' in $C(F')$. Since $g' \neq g$, it is $C(F') \neq C(F)$ and thus $F' \neq F$, in contradiction with f being a determining translation of M .

Let us identify the set X with the set $N \times N$ of all ordered pairs of non-negative integers so that (m, n) denotes the single point contained in the class $T_{m,n}$. The transformation f then coincides with f_a described by (4).

Statement 8. The element (1,0) is a left determining element of the bicyclic semigroup $\mathcal{B}$ as defined by (3).

Proof: The only possible choice of e and of an injection g in $C(f_a)$ satisfying (13) for f_e given by (4) is $e = (0,0)$ and

(28) $\qquad g(m,n) = (m+1, n)$ for all $m, n \geq 0$.

By Statement 4, there exists a regular T-monoid $(N \times N, F)$ with f in F and g in $C(F)$. In F there must be a transformation h such that $h(0,0) = (0,1)$. Since $fh(0,0) = (0,0)$, it is $fh(m,n) = (m,n)$ for all m, n and therefore

(29) $\qquad h(0,n) = h(0,n+1)$ for all $n \geq 0$.

Using commutativity of g and h it follows from (28) and (29) that

(30) $\qquad h(m,n) = (m, n+1)$ for all $m, n \geq 0$.

By Statement 1, the unique multiplication on $N \times N$ with the identity (0,0) for which F is the system of all the left translations is given by

(31) $\qquad (m,n)(k,p) = f_{(m,n)}(k,p)$,

where $f_{(m,n)}$ is the only member of F with $f_{(m,n)}(0,0) = (m,n)$. But clearly $f_{(m,n)} = h^n f^m$ and (31) is easily checked to give the same multiplication as (3), i.e. the multiplication in $\mathcal{B}$.

References

[1] Z. HEDRLÍN, P. GORALČÍK: O sdvigach polugrupp I,

Periodičeskije i kvaziperiodičeskije preobrazovanija, Matem.časop.3(1968) 161-176.

[2] P. GORALČÍK, Z. HEDRLÍN: O sdvigach polugrupp II, Surjektivnyje preobrazovanija, Matem. časop.4(1968),263-272.

[3] P. GORALČÍK: O sdvigach polugrupp III, Preobrazovanija s uveličitělnoj i preobrazovanija s něpravilnoj surjektivnoj časť-ju, Matem.časop.4(1968),273-282.

Matematicko-fyzikální fakulta
Karlova universita
Sokolovská 83, Praha 8
Československo

(Oblatum 7.4.1971)