FILOMAT (Niš) **12:1** (1998), 21–27

CANONIC SUBSETS IN SEMIGROUPS

O. S. Kashcheeva and B. V. Novikov

Abstract. In this work we introduce the notion of a canonic set, which arises in computing of semigroup cohomologies [n]. We investigate different properties of canonic sets and give examples of their applications to algorithmic problems.

1 Basic definitions and preliminary properties

It is well known that in studying of a semigroup it is advantageous to choose a generating set such that all elements of the semigroup have some canonic record. If we refuse the irreducibility of generating set (which is wanted usually) then this choice is always possible: it is sufficient to notice the whole semigroup being a generating set. Further we, certainly, don't appeal to this trivial example. We study the following question: in what way is possible to enlarge a given generating set in order to all elements of the semigroup have the unique (in some meaning) notion?

In the sequel the notation $S = \langle M|R\rangle$ means that the semigroup S is generated by the set M with the defining relation set R. If the set R is known or its type isn't important at this moment then we write $S = \langle M\rangle$.

Let $S = \langle M\rangle$ be some semigroup. A decomposition $x = x_1 \dots x_n$ ($x_i \in M$) of an element $x \in S \setminus M$ is called *reduced* , if $x_i x_{i+1} \dots x_j \notin M$ for each $i, j,\ 1 \le i \le j \le n$. We mean that a reduced decomposition of an element $x \in M$ is its decomposition into product of one multiplier. A set M is said to be *canonic*, if each element $x \in S$ has the unique reduced decomposition.

In the sequel we use the following criterion and its corollary.

Lemma 1 *A generating set M is canonic if and only if for each $s \in S$ the following condition holds:*

if $s = x_1 \dots x_m = y_1 \dots y_n$ are two decompositions of s ($x_i, y_j \in M$) with the first of them reduced, then there exist $1 = i_1 < i_2 <$

Received November 1, 1997
1991 *Mathematics Subject Classification:* 20M05.

$\ldots < i_m < i_{m+1} = n+1$ *such that* $x_k = y_{i_k} y_{i_k+1} \cdots y_{i_{k+1}-1}$ *for all* k, $1 \le k \le m$. ■

Corollary 1 *Let M be a canonic set in a semigroup S, $s = x_1 \ldots x_m$, $t = y_1 \ldots y_n$ $(x_i, y_j \in M)$ are reduced decompositions. Then the reduced decomposition of the element st is either $x_1 \ldots x_m y_1 \ldots y_n$ or $x_1 \ldots x_i z y_j \ldots y_n$, where $z = x_{i+1} \ldots x_m y_1 \ldots y_{j-1} \in M$.* ■

Let $S = \langle M|R\rangle$. If $x_1 \ldots x_m = y_1 \ldots y_n$ is a relation in R, then each of its parts is said to be *a defining word.*

Theorem 1 *Let a subset N of the semigroup $S = \langle M|R\rangle$ satisfies the conditions:*

1) $M \subseteq N$;

2) each defining word is contained in N;

3) for any $a, b, c \in S$ the inclusion $ab, bc \in N$ implies $abc \in N$.

Then N is a canonic set.

Proof. At first we note that it follows from condition 3)

3′) if $ab, bcd, de \in N$, then $abcde \in N$.

Let $s = x_1 \ldots x_m = y_1 \ldots y_n$ be two decompositions of an element s into products of elements of N, moreover the first of them is reduced. Then it is possible to go from the first decomposition to second one using defining relations from R. We consider the first step of this conversion.

Let $x_k = a_{k,1} \ldots a_{k,p_k}$ $(a_{k,l} \in M)$, $i < j$, the word $u = a_{i,r} a_{i,r+1} \ldots a_{j,t}$ be defining one and be replaced. Then $x_i = ab$, $u = b x_{i+1} \ldots x_{j-1} c$, $x_j = cd$ for some $a, b, c, d \in S$, and $x_i \ldots x_j \in N$ follows from 3′). This contradicts to assumption that $x_1 \ldots x_m$ is reduced. Therefore at the first step the replacement takes place inside one of x_i only and it is clear that the same is true for other steps. So as a result of the conversion we have

$$s = b_1 \ldots b_q \ (b_k \in M),$$

where $x_i = b_{\alpha_i} b_{\alpha_i+1} \ldots b_{\alpha_{i+1}-1}$, $y_j = b_{\beta_j} b_{\beta_j+1} \ldots b_{\beta_{j+1}-1}$ for α_i, β_j such that $1 = \alpha_1 < \ldots < \alpha_{m+1} = q+1$, $1 = \beta_1 < \ldots < \beta_{n+1} = q+1$.

If x_i doesn't coincide with a subword of the word $y_1 \ldots y_n$ then the following variants are possible:

a) $x_i = ab$, $y_j = b x_{i+1} \ldots x_{k-1} c$, $x_k = cd$ for some $i < k$ and $a, b, c, d \in S$. Then by condition 3′) $x_i \ldots x_k \in M$.

b) $x_i = ab$, $y_j = bx_{i+1} \dots x_k$ for some $i < k$ and $a, b \in S$. Therefore $x_i \dots x_k \in M$ from 3).

c) $y_j = x_i \dots x_{k-1}c$, $x_k = cd$ for some $i < k$ and $c, d \in S$. Hence $x_i \dots x_k \in M$.

d) $y_j = x_i \dots x_k$ for some $1 < k$, i.e. $x_i \dots x_k \in M$.

Thus the variants we consider contradict the assumption that the decomposition $x_1 \dots x_m$ is reduced. Now by Lemma 1 the set N is canonic. ■

2 Hard canonic sets

In this section we construct an efficient way of enlargement of given generating set to canonic one.

As above, let $S = \langle M|R\rangle$. We define binary relations λ, ρ and π on M by the following way. Let $x_1 \dots x_m = y_1 \dots y_n$ be an arbitrary relation from R ($x_i, y_j \in M$). Then λ consists of all pairs (x_1, y_1) for all defining relations. Similarly, ρ consists of all pairs (x_m, y_n), and π does of all pairs (x_i, x_{i+1}), (y_j, y_{j+1}), $1 \le i < m$, $1 \le j < n$.

We denote by λ^* (resp. ρ^*) the least equivalence, which contains λ (resp. ρ), by $\overline{\pi}$ the relation $\rho^*\pi\lambda^*$ and by M^h the subset of all elements which are decomposed into product $t_1 \dots t_k$, where $t_i \in M$, $(t_i, t_{i+1}) \in \overline{\pi}$ for each i, $1 \le i < k$.

Lemma 2 *If $t = t_1 \dots t_k \in M^h$ ($t_i \in M$), then $(t_i, t_{i+1}) \in \overline{\pi}$ for each i, $1 \le i < k$.*

Proof. By the condition $t = t_1 \dots t_k = u_1 \dots u_l$ where $u_i \in M$ and $(u_i, u_{i+1}) \in \overline{\pi}$ for each i. Consider the first step of conversion from the right part of this equality to the left one.

Let the defining relation we use be of the following type:

$$u_\alpha \dots u_\beta = v_1 \dots v_m \ (1 \le \alpha \le \beta \le l).$$

Then $(u_{\alpha-1}, u_\alpha) \in \overline{\pi}$ implies $(u_{\alpha-1}, v_1) \in \overline{\pi}\lambda = \overline{\pi}$. In the same way we have $(v_m, u_{\beta+1}) \in \overline{\pi}$. Hence after the first step (and therefore throughout the whole conversion) neighboring elements stay in relation $\overline{\pi}$. ■

Corollary 2 *If $s = a_1 \dots a_m$, $t = b_1 \dots b_n$ ($a_i, b_j \in M^h$) are reduced decompositions with respect to M^h then the reduced decomposition of the st is:*

a) $a_1 \dots a_m b_1 \dots b_n$, if $a_m b_1 \notin M^h$,

b) $a_1 \dots a_{m-1} c b_2 \dots b_n$, if $c = a_m b_1 \in M^h$. ■

Theorem 2 *M^h is a canonic set.*

Proof. Evidently, conditions 1), 2) of Theorem 1 hold. Let $a, b, c \in S$, $ab, bc \in M^h$. Decomposing a and b into product of elements from M, we see (Lemma 2) that the last letter of the element a and the first letter of the element b are in the relation $\overline{\pi}$. Similar statement is true for b and c. Hence $abc \in M^h$ and by Theorem 1 M^h is a canonic set. ■

Further we say that canonic sets of the type M^h are *hard*.

3 Applications to algorithmic problems.

It is known (see [ev]) that in investigation of the algorithmic problems it is convenient to consider a generating set of a semigroup as a partial gropouid with induced operation. In the case of using of a canonic set it means that many algorithmic questions reduce to similar problems for the corresponding groupoids. In this section we consider two such examples. Below N is a canonic set in the semigroup $S =< M >$.

The word problem.

Since N is a canonic set, a reduced decomposition of each element is uniquely defined by any its decomposition into product of elements from N. In the case $N = M^h$, the word problem in S is decidable if and only if it is decidable in the partial groupoid N. In particular it is decidable when the set N is finite. Thus we obtain the following assertion:

Theorem 3 *If a semigroup S is finitely generated and the graph of the relation $\overline{\pi}$ doesn't contain (oriented) cycles then the word problem is decidable in S.* ■

Example. Consider a series of Malcev's semigroups, which aren't embedded into groups [ma]. Let a semigroup S is generated by the set

$$M = \{a_i, b_i, c_i, d_i, A_j, B_j, C_j, D_j | i \in I, j \in J\}$$

and its defining relations set is Malcev's system (following by [cp]). Suppose

$$P = \{c_i, d_i, A_j, B_j | i \in I, j \in J\},\ Q = \{a_i, b_i, C_j, D_j | i \in I, j \in J\}.$$

Then $\pi \subset P \times Q, \lambda^* \subset (Q \times Q) \cup \Delta$ and $\rho^* \subset (Q \times Q) \cup \Delta$. Therefore $\overline{\pi} \subset P \times Q$, $\overline{\pi}$ doesn't contain cycles and in the semigroup S the word problem is decidable.

The use of canonic sets makes it possible to obtain an analog of well known result about $C(3)$-semigroups. We remind some necessary definitions [hi].

Let F_M be the free semigroup on an alphabet M and the set of defining relations R be given. The word $w \in F_M$ is called *a piece*, if there are $u_1, u_2, v_1, v_2 \in F_M^1$ such that $u_1 w v_1, u_2 w v_2$ are defining words and either $u_1 \neq u_2$ or $v_1 \neq v_2$. The semigroup $S = \langle M|R\rangle$ is called *a $C(n)$-semigroup* if no defining word is a product of fewer than n pieces.

The set R defines a relation γ on the set of defining words: $(u, v) \in \gamma$ if and only if $u = v$ is a defining relation from R. We shall say that the words u and v are equivalent if $(u, v) \in \gamma^*$, where γ^* is the least equivalence which contains γ.

It is proved by Remmers [re], that in finitely defined $C(3)$- semigroups the word problem is decidable. Below we establish a solution of this problem for some class of semigroups, in which the condition $C(3)$ does not hold.

Theorem 4 *Let $S = \langle M|R\rangle$ be a $C(2)$-semigroup, where R is finite, and no defining word begins by a proper end of another defining word (as elements of F_M). Then the word problem is decidable in S.*

Proof. Note that if $S = \langle M|R\rangle$ is $C(2)$-semigroup then no defining word is a proper segment of another defining word. Therefore, if w is a defining word then each transition from w to w' touches the word w completely. Hence, w' is a defining word which is equivalent to w. Moreover, if w is a defining word and a word w' equals to w in the semigroup S then w' is a defining word which is equivalent to w.

At first let us consider the particular case when each relation from R has the form $x_1 \dots x_n = y$ where $x_1, \dots, x_n, y \in M$. We prove that the set M is canonic. It is sufficient for proving to verify that the conditions of Theorem 1 hold. Only the third condition requires verifying.

Let $x, y \in M$ and there exist $a, b, c \in S$ such that $x = ab$, $y = bc$ and $a, b, c \in S$ $a = a_1 \dots a_n$, $b = b_1 \dots b_m$, $c = c_1 \dots c_k$, where $a_i, b_j, c_l \in M$. Then it is possible to pass from the decomposition x to the decomposition $a_1 \dots a_n b_1 \dots b_m$ using defining relations from R. Hence, the word x is defining and therefore, the word $a_1 \dots a_n b_1 \dots b_m$ is also defining. Similarly the word $b_1 \dots b_m c_1 \dots c_k$ is defining and it begins by the proper end of another defining word. We receive a contradiction to the condition of the theorem.

Now it is sufficient for solving the word problem in S to enumerate the equal letters from M and to answer the question: for what $x_1, \dots, x_k \in M$ $(k > 1)$ does the product $x_1 \dots x_k$ lie in M and what letter is it represented

by. The answer is quite clear. Two different letters from M are equal in S only if they are defining words and are equivalent, $x_1 \dots x_k \in M$ only if there is a letter y such that $x_1 \dots x_k = y$ is a defining relation out of R.

Finally we consider the general case. Let us denote the classes of equivalence on the set of defining words by letters and so we enlarge the alphabet M. Now we change the defining relations by evident way such that the condition of the particular case holds. ■

Example. Let us consider the following semigroup

$$S = \langle a, b, c, d \,|\, ab = cd, ad = cb \rangle.$$

This semigroup is not a $C(3)$-semigroup, but by Theorem 4 the word problem is decidable in S.

The cancellativity problem

Since cancellativity is Marcov's property [bo] the problem of its establishment is algorithmic undecidable. But as above it is possible to consider the canonic set only.

Regarding M^h as a partial groupoid we call it *left cancellative* if for all $a, b, c \in M^h$

$$ab = ac \in M^h \Rightarrow b = c,$$

$$ab = a \in M^h \Rightarrow bc = c.$$

Theorem 5 *S is left cancellative if and only if M^h is left cancellative.*

Proof. The implication $\Rightarrow$ is obvious.

Let M^h be left cancellative and $st = su$, where $s, t, u \in S$. It is sufficient to consider the case when $s \in M^h$. Let $t = a_1 \dots a_m, u = b_1 \dots b_n$ be reduced decompositions. Then according to Corollary 2 the reduced decomposition of the element st is either $sa_1 \dots a_m$(when $sa_1 \notin M^h$) or $(sa_1) \dots a_m$ (when $sa_1 \in M^c$). In the same way the reduced decomposition of the element su is either $sb_1 \dots b_n$ or $(sb_1) \dots b_n$. Since there is the unique reduced decomposition we should consider the following four variants:

1) $sa_1, sb_1 \notin M^h$. Then $a_i = b_i$ for each $i \geq 1$, i.e. $t = u$.

2) $sa_1, sb_1 \in M^h$. Then $a_i = b_i$ for each $i \geq 2$ and $sa_1 = sb_1 \in M$. It follows by cancellation in M^h that $a_1 = b_1$, whence $t = u$.

3) $sa_1 \in M^h$, $sb_1 \notin M^h$. Then $sa_1 = s, a_2 = b_1, \dots$ and the cancellativity of M^h implies $a_1 a_2 = a_2$. This is impossible, so $a_1 a_2 \notin M^h$.

4) $sa_1 \notin M^h$, $sb_1 \in M^h$. It is impossible as before. ■

Clearly, the similar statement is true for the right cancellativity.

Corollary 3 *If M^h is finite then S has the decidable cancellativity problem.*

Refrences

[bo] Bokut' L.A., Kukin G.P. *Unsolvable algorithmic problems for semigroups, groups and rings.* Itogi nauki i tekhn. Algebra. Topologiya. Geometriya. **25**(1987), 3-66 (in Russian).

[cp] Clifford A.H., Preston G.B. *The Algebraic Theory of Semigroups.* vol.1, 2, AMS Math. Surveys, 1964, 1967.

[ev] Evans T. *Word problem.* Bull Amer. Math. Soc., **84**(1978), N5, 789-802.

[hi] Higgins P.M. *Techniques of semigroup theory.* Oxford Univ. Press, 1992.

[ma] Mal'cev A.I. *On including of associative systems into groups. II.* Matem. sbornik, **8**(1940), N2, 251-264 (in Russian).

[n] Novikov B.V. *Partial semigroup cohomologies and their application.* Izv. vyssh. uchebn. zaved. Matem., 1988, N11, 25-32 (in Russian).

[re] Remmers J. *On the geometry of semigroup presentations.* Adv. Math. **36**(1980), 283-296.

av. Traktorostroiteley 83g, apt.10, 310123 Kharkov, Ukraine
Saltovskoye shosse 258, apt.20, 310178 Kharkov, Ukraine
boris.v.novikovuniver.kharkov.ua