Dokl. Akad. Nauk SSSR
Tom 178 (1968), No. 4

Soviet Math. Dokl.
Vol. 9 (1968), No. 1

ALGORITHMIC PROBLEMS FOR COMMUTATIVE SEMIGROUPS

UDC: 519.40

M. A. TAĬCLIN*

1. Algorithms for the solution of various problems in the theory of commutative semigroups have been given by A. I. Mal'cev [1], Ceĭtin, Birjukov [2–5], Emeličev [6], Halezov [7]. In the papers [8,9], the author described a universal algorithm which solves any problem which can be given in the language of the first-order predicate calculus with a certain signature. For a more precise formulation of these results, with every commutative semigroup $L(\mathfrak{A}, \mathfrak{B})$, given by a finite set of generators $\mathfrak{A}$ and a set of defining relations $\mathfrak{B}$, we associate the signature $\sigma(\mathfrak{A}) = \langle a, G_a | a \in \mathfrak{A} \rangle$, where, for $a \in \mathfrak{A}$, G_a is a symbol for a singulary predicate. We shall say that a certain algorithm *solves problem* A if, with respect to $\mathfrak{A}$, $\mathfrak{B}$ and any closed formula Φ of the first-order predicate calculus with signature $\sigma(\mathfrak{A})$, this algorithm determines whether the formula Φ is true in the semigroup $L(\mathfrak{A}, \mathfrak{B})$ in the case where, for each $a \in \mathfrak{A}$, the predicate $G_a(x)$ is interpreted in $L(\mathfrak{A}, \mathfrak{B})$ as "x is equal to some natural multiple of a". The basic content of papers [8,9] is a description of an algorithm solving problem A.

The indicated algorithm consists in deriving successively the consequences of a certain axiom system until the formula Φ or the formula $\neg\Phi$ is derived. A deficiency in papers [8,9] was the use of model-theoretic arguments for the completeness proof of the axiom system being used. This distinguished the description of the universal algorithm from the constructive descriptions of the algorithms for the solution of various problems in the papers cited above.

The present note describes another algorithm which also solves problem A. The description provided here is constructive and simpler. Of independent interest is the following result of this note. If by elements of a commutative semigroup with n generators we understand equivalence classes given on n-tuples of natural numbers, then the corresponding equivalence relation is always defined on the natural numbers by some formula of the first order predicate calculus not containing any extra-logical symbols other than the symbol for the addition operation.

2. We shall, in addition, employ without explanation the terminology introduced in section 1 of §1 of the survey [10]. Assume that an algebraic system $\mathfrak{M}$ of signature σ has a decidable theory. Assume that $\mathfrak{C}(x_1, \cdots, x_k, y_1, \cdots, y_k)$ is a formula of signature σ, not containing free variables different from $x_1, \cdots, x_k, y_1, \cdots, y_k$. Let a relation $\sim$, defined in the system $\mathfrak{M}^k$, $(x_1, \cdots, x_k) \sim (y_1, \cdots, y_k)$ if and only if $\mathfrak{C}(x_1, \cdots, x_k, y_1, \cdots, y_k)$ is true in $\mathfrak{M}$, be a congruence relation in $\mathfrak{M}^k$. Then the factor system $\mathfrak{M}^k/\sim$ also has a decidable theory. If the relation $\sim$ and the formula $\mathfrak{C}(x_1, \cdots, x_k, y_1, \cdots, y_k)$ are connected by the condition considered above, then we shall say that the relation $\sim$ is elementary in $\mathfrak{M}$ and that the formula $\mathfrak{C}(x_1, \cdots, x_k, y_1, \cdots, y_k)$ defines the relation $\sim$.

It is well known that the system $\mathfrak{N} = \langle N, + \rangle$, where $N = \{0, 1, 2, \cdots\}$ is the set of natural numbers and + is the usual addition operation on natural numbers, has a decidable theory. Hence, every factor system of the system $\mathfrak{N}^k$ with respect to an elementary equivalence relation also has a

* Editor's note. The present translation incorporates suggestions made by the author.

decidable theory.

Every semigroup $L(\mathfrak{A}, \mathfrak{B})$ can be considered as a factor semigroup of the semigroup $\mathfrak{N}^k$, where k is the number of elements of $\mathfrak{A}$. For a solution of problem A it suffices, therefore, to note that this factor semigroup is obtained by factorization of $\mathfrak{N}^k$ with respect to an elementary equivalence relation and that a formula defining this equivalence relation can be effectively constructed from $\mathfrak{A}$ and $\mathfrak{B}$.

In the case where $L(\mathfrak{A}, \mathfrak{B})$ is a semigroup with cancellation, this is a trivial observation. In fact, let $\mathfrak{A} = \{a_1, \cdots, a_k\}$, $\mathfrak{B} = \{c_i, d_i), i = 1, \cdots, q\}$, where

$$c_i = \sum_{j=1}^{k} \alpha_j^{(i)} a_j; \quad d_i = \sum_{j=1}^{k} \beta_j^{(i)} a_j; \quad \alpha_j^{(i)}, \beta_j^{(i)} \in N.$$

In this case, $(x_1, \cdots, x_k) \sim (y_1, \cdots, y_k)$ is equivalent to the condition

$$(\exists t_1) \ldots (\exists t_q) (\exists t_1') \ldots (\exists t_q') \Big(\bigwedge_{i=1}^{k} \Big[x_i + \sum_{j=1}^{q} t_j (\alpha_i^{(j)} - \beta_i^{(j)}) = y_i + \sum_{j=1}^{q} t_j' (\alpha_i^{(j)} - \beta_i^{(j)}) \Big] \Big).$$

This condition can, in an obvious way, be presented in the form of the required formula.

3. In this section we shall recall some definitions and results of §1 of paper [9]. By $L(\mathfrak{A})$ we shall denote the free semigroup with the set $\mathfrak{A}$ of free generators in the class of commutative semigroups with zero. We can think of the set $L(\mathfrak{A})$ as the set of all linear forms on the letters $a_1, \cdots, a_k$, where $\mathfrak{A} = \{a_1, \cdots, a_k\}$, with natural numbers as coefficients. A semigroup $L(\mathfrak{A}, \mathfrak{B})$, given in the class of commutative semigroups with zero, by finite sets of generators $\mathfrak{A}$ and defining relations $\mathfrak{B}$, will be considered a factor semigroup of the semigroup $L(\mathfrak{A})$. For $x \in L(\mathfrak{A})$, by $\bar{x}$ we shall denote the image of x under the canonical mapping $L(\mathfrak{A}) \to L(\mathfrak{A}, \mathfrak{B})$. By $M(\mathfrak{A}, \mathfrak{B})$ we shall denote the semigroup given in the class of commutative semigroups with cancellation and with zero by finite sets of generators $\mathfrak{A}$ and defining relations $\mathfrak{B}$. We treat $M(\mathfrak{A}, \mathfrak{B})$ also as a factor semigroup of the semigroup $L(\mathfrak{A})$. For $x \in L(\mathfrak{A})$, by $[x]$ we denote the image of x under the canonical mapping $L(\mathfrak{A}) \to M(\mathfrak{A}, \mathfrak{B})$.

For $a \in \mathfrak{A}$ and $f \in L(\mathfrak{A})$, we denote by $(f)_a$ the coefficient of the letter a in the form f. For $f, g \in L(\mathfrak{A})$, we write $f \geq g$ if $(f)_a \geq (g)_a$ for all $a \in \mathfrak{A}$. We write $\mathfrak{A}_1 \subset \mathfrak{A}$ if $\mathfrak{A}_1 \neq \mathfrak{A}$ and $\mathfrak{A}_1$ is a subset of the set $\mathfrak{A}$. By the symbol ϕ we denote the empty set. By $L(\phi)$ we denote the zero semigroup. If $\mathfrak{A}_1 \subset \mathfrak{A}$, we consider the semigroup $L(\mathfrak{A}_1)$ to be a subsemigroup of the semigroup $L(\mathfrak{A})$. We shall assume that $\mathfrak{A} \subseteq L(\mathfrak{A})$. For $\mathfrak{A}_1 \subset \mathfrak{A}$ and $f \in L(\mathfrak{A})$, we denote by $\mathfrak{A}_1(f)$ that form in $L(\mathfrak{A} - \mathfrak{A}_1)$ such that $(\mathfrak{A}_1(f))_a = (f)_a$ for all $a \in \mathfrak{A} - \mathfrak{A}_1$. Let $q(\mathfrak{B})$ be the number of relations in $\mathfrak{B}$, and let $\lambda(\mathfrak{B})$ be the largest coefficient in these relations. By $h(\mathfrak{A}, \mathfrak{B})$ we denote the form $\Sigma_{a \in \mathfrak{A}} \lambda(\mathfrak{B})(q(\mathfrak{B}) + 1)a$ in $L(\mathfrak{A})$.

Assume $\mathfrak{A}_1 \subset \mathfrak{A}$. By $\mathfrak{N}(\mathfrak{A}_1, \mathfrak{B})$ we denote the set of all $x \in L(\mathfrak{A} - \mathfrak{A}_1)$ such that the inequality $\overline{x + y} \neq \overline{h(\mathfrak{A}, \mathfrak{B}) + z}$ holds in $L(\mathfrak{A}, \mathfrak{B})$ for all $y \in L(\mathfrak{A}_1)$, $z \in L(\mathfrak{A})$. By $\mathfrak{M}(\mathfrak{A}_1, \mathfrak{B})$ we denote the set of maximal elements of $\mathfrak{N}(\mathfrak{A}_1, \mathfrak{B})$ in the sense of the relation $\geq$. By $\mathfrak{M}_1(\mathfrak{A}, \mathfrak{B})$ we denote the set

$$\{x \in L(\mathfrak{A} \setminus \mathfrak{A}_1) \mid (\exists y)(y \in \mathfrak{M}(\mathfrak{A}_1, \mathfrak{B}) \& y \geqslant x)\}.$$

The sets $\mathfrak{M}(\mathfrak{A}_1, \mathfrak{B})$ and $\mathfrak{M}_1(\mathfrak{A}_1, \mathfrak{B})$ are finite.

We divide the set $\mathfrak{M}_1(\mathfrak{A}_1, \mathfrak{B})$ into reduction classes, assigning $x, y \in \mathfrak{M}_1(\mathfrak{A}_1, \mathfrak{B})$ to the same class if there exist z, $u \in L(\mathfrak{A}_1)$ such that $\overline{x+z} = \overline{y+u}$ in $L(\mathfrak{A}, \mathfrak{B})$. By $i(\mathfrak{A}_1, \mathfrak{B})$ we denote the number of reduction classes, and by $\mathfrak{M}_{2,1}(\mathfrak{A}_1, \mathfrak{B}), \cdots, \mathfrak{M}_{2,i(\mathfrak{A}_1,\mathfrak{B})}(\mathfrak{A}_1, \mathfrak{B})$ all the different classes.

For $x, y \in \mathfrak{M}_{2,j}(\mathfrak{A}_1, \mathfrak{B})$, $j \in \{1, \cdots, i(\mathfrak{A}_1, \mathfrak{B})\}$ and for $\mathfrak{A}_3 \subset \mathfrak{A}_1$, we denote by $\mathfrak{N}(\mathfrak{A}_1, \mathfrak{A}_3, x, y, \mathfrak{B})$ the set of all those $z \in L(\mathfrak{A}_1 - \mathfrak{A}_3)$ such that, for all $u \in L(\mathfrak{A}_3)$ and $v \in L(\mathfrak{A}_1)$, the inequality $\overline{x+z+u} \neq \overline{y+v}$ holds in $L(\mathfrak{A}, \mathfrak{B})$. By $\mathfrak{M}(\mathfrak{A}_1, \mathfrak{A}_3, x, y, \mathfrak{B})$ we denote the set of maximal elements of $\mathfrak{N}(\mathfrak{A}_1, \mathfrak{A}_3, x, y, \mathfrak{B})$. The set $\mathfrak{M}(\mathfrak{A}_1, \mathfrak{A}_3, x, y, \mathfrak{B})$ is finite. We recall that:

(1) the sets $\mathfrak{M}(\mathfrak{A}_1, \mathfrak{B})$, $\mathfrak{M}_1(\mathfrak{A}_1, \mathfrak{B})$, $\mathfrak{M}(\mathfrak{A}_1, \mathfrak{A}_3, x, y, \mathfrak{B})$ are effectively constructible from $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{A}_1$, $\mathfrak{A}_3$, x, y [9];

(2) the set $\mathfrak{M}_1(\mathfrak{A}_1, \mathfrak{B})$ is effectively divisible into reduction classes with respect to $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{A}_1$ [9];

(3) there exists an effective procedure which, for $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{A}_1$, x such that $\mathfrak{A}_1 \subset \mathfrak{A}$ and $x \in L(\mathfrak{A} - \mathfrak{A}_1)$, constructs a finite set $\mathfrak{B}(\mathfrak{A}_1, x)$ of defining relations for $\mathfrak{A}_1$ such that, for $u, v \in L(\mathfrak{A}_1)$, $\bar{u} = \bar{v}$ in $L(\mathfrak{A}_1, \mathfrak{B}(\mathfrak{A}_1, x))$ when and only when $\overline{x+u} = \overline{x+v}$ in $L(\mathfrak{A}, \mathfrak{B})$ [9];

(4) for $x, y \in L(\mathfrak{A})$, $\overline{x + h(\mathfrak{A}, \mathfrak{B})} = \overline{y + h(\mathfrak{A}, \mathfrak{B})}$ in $L(\mathfrak{A}, \mathfrak{B})$ if and only if $[x] = [y]$ in $M(\mathfrak{A}, \mathfrak{B})$ (Lemma of Ceĭtin [7]);

(5) for $x \in L(\mathfrak{A})$, either there exists $z \in L(\mathfrak{A})$ such that $\bar{x} = \overline{h(\mathfrak{A}, \mathfrak{B}) + z}$ in $L(\mathfrak{A}, \mathfrak{B})$, or there exists $\mathfrak{A}_1 \subset \mathfrak{A}$ such that $\mathfrak{A}_1(x) \in \mathfrak{M}_1(\mathfrak{A}_1, \mathfrak{B})$ (9);

(6) for $\mathfrak{A}_1 \subset \mathfrak{A}$, $x, y \in \mathfrak{M}_{2,j}(\mathfrak{A}_1, \mathfrak{B})$, $j \in \{1, \cdots, i(\mathfrak{A}_1, \mathfrak{B})\}$, and $u \in L(\mathfrak{A}_1)$, either there exists $v \in L(\mathfrak{A}_1)$ such that $\overline{x+u} = \overline{y+v}$ in $L(\mathfrak{A}, \mathfrak{B})$, or there exist $\mathfrak{A}_3 \subset \mathfrak{A}_1$ and $v \in \mathfrak{M}(\mathfrak{A}_1, \mathfrak{A}_3, x, y, \mathfrak{B})$ such that $\mathfrak{A}_3(u) \leq v$ [9].

4. **Theorem.** *Let* $\mathfrak{A} = \{a_1, \cdots, a_k\}$. *The equivalence relation in* $\mathfrak{N}^k$, *defined by the condition that* $(\alpha_1, \cdots, \alpha_k) \sim (\beta_1, \cdots, \beta_k)$ *when and only when*

$$\sum_{i=1}^{k} \alpha_i \bar{a}_i = \sum_{i=1}^{k} \beta_i \bar{a}_i$$

in $L(\mathfrak{A}, \mathfrak{B})$, *is elementary in* $\mathfrak{N}$. *There exists an effective procedure which constructs from* $\mathfrak{A}$ *and* $\mathfrak{B}$ *a formula* $\mathfrak{C}(\mathfrak{A}, \mathfrak{B}; \alpha_a, \beta_a | a \in \mathfrak{A})$ *defining the relation* $\sim$.

The proof is carried out by induction with respect to the number of elements of $\mathfrak{A}$. For $\mathfrak{A}$ with one element, it is obvious. Let us suppose that we are able to construct $\mathfrak{C}(\mathfrak{A}, \mathfrak{B}; \alpha_a, \beta_a | a \in \mathfrak{A})$ in the case where $\mathfrak{A}$ contains fewer than k elements. Assume that $\mathfrak{A}$ contains k elements. Let $\mathfrak{C}^*(\mathfrak{A}, \mathfrak{B}; \alpha_a, \beta_a | a \in \mathfrak{A})$ denote a formula which defines a congruence relation $\sim_1$ on $\mathfrak{N}^k$ such that the semigroups $M(\mathfrak{A}, \mathfrak{B})$ and $\mathfrak{N}^k | \sim_1$ are isomorphic.

For $\mathfrak{A}_1 \subset \mathfrak{A}$, $j \in \{1, \cdots, i(\mathfrak{A}_1, \mathfrak{B})\}$, $u, v \in \mathfrak{M}_{2,j}(\mathfrak{A}_1, \mathfrak{B})$, we denote by $\Phi(\mathfrak{A}_1, u, v)$ the set of all those functions ϕ which, to each $\mathfrak{A}_3 \subset \mathfrak{A}_1$ and to each $e \in \mathfrak{M}(\mathfrak{A}_1, \mathfrak{A}_3, u, v, \mathfrak{B})$, associates an element $\phi(\mathfrak{A}_3, e) \in \mathfrak{A}_1 - \mathfrak{A}_3$. For $\phi \in \Phi(\mathfrak{A}_1, u, v)$ we consider the set $\mathfrak{A}(\phi) = \{\phi(\mathfrak{A}_3, e) | \mathfrak{A}_3 \subset \mathfrak{A}_1, e \in \mathfrak{M}(\mathfrak{A}_1, \mathfrak{A}_3, u, v, \mathfrak{B})\}$. For $a \in \mathfrak{A}(\phi)$ we denote by μ_a the natural number $\max\{(e)_a | \mathfrak{A}_3 \subset \mathfrak{A}_1, e \in \mathfrak{M}(\mathfrak{A}_1, \mathfrak{A}_3, u, v, \mathfrak{B}), \phi(\mathfrak{A}_3, e) = a\}$. By $F_\phi(u, v, \mathfrak{A}_1)$ we denote the conjunction of all formulas

$$\alpha_a = (u)_a, \quad \beta_a = (v)_a, \quad \alpha_c = \mu_c + z_c + 1$$

for all $a \in \mathfrak{A} - \mathfrak{A}_1$, $c \in \mathfrak{A}(\phi)$, where z_c, α_c, α_a, β_a are symbols for individual variables.

Let

$$d = \sum_{a \in \mathfrak{A} \setminus \mathfrak{A}_1} \alpha_a a + \sum_{a \in \mathfrak{A}(\varphi)} (\mu_a + 1) a.$$

From (6) it follows that $\bar{d} = \bar{v} + \bar{d}_1$ in $L(\mathfrak{A}, \mathfrak{B})$ for some $d_1 \in L(\mathfrak{A}_1)$. Now, in $\mathfrak{C}(\mathfrak{A}_1, \mathfrak{B}(\mathfrak{A}_1, v); \alpha_a, \beta_a | a \in \mathfrak{A}_1)$, instead of α_a we put $(d_1)_a + z_a$ if $a \in \mathfrak{A}(\phi)$ and we put $\alpha_a + (d_1)_a$ if $a \notin \mathfrak{A}(\phi)$. We obtain a formula $G_\phi(u, v, \mathfrak{A}_1)$. By $D_\phi(u, v, \mathfrak{A}_1)$ we denote the formula which is obtained if we prefix to the formula $F_\phi(u, v, \mathfrak{A}_1)$ & $G_\phi(u, v, \mathfrak{A}_1)$ existential quantifiers with respect to z_c for all $c \in \mathfrak{A}(\phi)$. By $D(\mathfrak{A}_1 u, v)$ we denote the disjunction of the formulas $D_\phi(u, v, \mathfrak{A}_1)$ for all $\phi \in \Phi(\mathfrak{A}_1, u, v)$.

By Ψ we denote the set of all those functions ψ which, to each $\mathfrak{A}_1 \subset \mathfrak{A}$ and to each $c \in \mathfrak{M}(\mathfrak{A}_1, \mathfrak{B})$, associates an element $\psi(\mathfrak{A}_1, c) \in \mathfrak{A} - \mathfrak{A}_1$. For $\psi \in \Psi$ we consider the set $\mathfrak{A}_\psi = \{\psi(\mathfrak{A}_1, c) | \mathfrak{A}_1 \subset \mathfrak{A}, c \in \mathfrak{M}(\mathfrak{A}_1, \mathfrak{B})$. For $a \in \mathfrak{A}_\psi$, we denote by ν_a the natural number $\max\{(c)_a | \mathfrak{A}_1 \subset \mathfrak{A}, c \in \mathfrak{M}(\mathfrak{A}_1, \mathfrak{B}), \psi(\mathfrak{A}_1, c) = a\}$. By $H_\psi(\alpha_c, z_c | c \in \mathfrak{A}_\psi)$ we denote the conjunction of all formulas $\alpha_c = \nu_c + z_c + 1$ for all $c \in \mathfrak{A}_\psi$, where α_c, z_c are symbols for individual variables.

Let

$$f_\psi = \sum_{a \in \mathfrak{A}_\psi} (\nu_a + 1) a.$$

From (5) it follows that $\bar{f}_\psi = \overline{h(\mathfrak{A}, \mathfrak{B})} + \bar{g}_\psi$ for some $\bar{g}_\psi \in L(\mathfrak{A})$. By $B(\psi, \tau)$ we denote the formula which is obtained if, in $\mathfrak{C}^*(\mathfrak{A}, \mathfrak{B}; \alpha_a, \beta_a | a \in \mathfrak{A})$ instead of α_c we put $z_c + (g_\psi)_c$ for $c \in \mathfrak{A}_\psi$, instead of α_a we put $\alpha_a + (g_\psi)_a$ for all $a \in \mathfrak{A} - \mathfrak{A}_\psi$, instead of β_d we put $y_d + (g_\tau)$ for all $d \in \mathfrak{A}_\tau$, and instead of β_a we put $\beta_a + (g_\tau)_a$ for all $a \in \mathfrak{A} - \mathfrak{A}_\tau$. By $E(\psi, \tau)$ we denote the formula which is obtained if, in the conjunction

$$H_\psi(\alpha_c, z_c | c \in \mathfrak{A}_\psi) \;\&\; H_\tau(\beta_d, y_d | d \in \mathfrak{A}_\tau) \;\&\; B(\psi, \tau)$$

we prefix existential quantifiers with respect to all z_c and y_d for $c \in \mathfrak{R}_\psi$ and $d \in \mathfrak{A}_\tau$.

From (4), (5), (6) it follows that, as $\mathfrak{C}(\mathfrak{A}, \mathfrak{B}; \alpha_a, \beta_a | a \in \mathfrak{A})$, one can take the disjunction of all formulas $E(\psi, \tau)$, $D(\mathfrak{A}_1, u, v)$ for all $\psi, \tau \in \Psi$, all $\mathfrak{A}_1 \subset \mathfrak{A}$, all $j \in \{1, \cdots, i(\mathfrak{A}_1, \mathfrak{B})\}$ and all $u, v \in \mathfrak{M}_{2,j}(\mathfrak{A}_1, \mathfrak{B})$.

Institute of Mathematics
Siberian Branch, Academy of Sciences of the USSR

Received 31/MAR/67

BIBLIOGRAPHY

[1] A. I. Mal'cev, Učen. Zap. Ivanovsk. Ped. Inst. 6 (1958), 227.

[2] A. P. Birjukov, Seventh All-Union Colloquium on General Algebra, Kishinev, 1965. (Russian)

[3] ______, Interuniv. Sci. Sympos. General Algebra, Tartu, 1966, pp. 5–6. (Russian) MR 34 #1422.

[4] ______, Sibirsk. Mat. Ž. 7 (1966), 523. MR 34 #1423.

[5] ______, Sibirsk. Mat. Ž. 8 (1967), 525.

[6] V. A. Emeličev, Sibirsk. Mat. Ž. 4 (1963), 788. MR 28 #2146.

[7] E. A. Halezov, Sibirsk. Mat. Ž. 7 (1966), 419. MR 35 #277.

[8] M. A. Taĭclin, Algebra i Logika Sem. 5 (1966), no. 1, 51. MR 33 #5486.

[9] ______, Algebra i Logika Sem. 5 (1966), no. 4, 55. MR 35 #2985.

[10] Ju. L. Eršov et al. Uspehi Mat. Nauk 20 (1965), no. 4, (124) 37. MR 32 #4012.

Translated by: Elliott Mendelson