BULL. AUSTRAL. MATH. SOC. 20M05, 20M07
VOL. 47 (1993) [457–464]

A DECISION PROBLEM FOR VARIETIES OF COMMUTATIVE SEMIGROUPS

W.L. CAO

For a first order formula P: $\forall x_1 \ldots \forall x_n \exists y_1 \ldots \exists y_m (u(x_1, \ldots, x_n, y_1, \ldots, y_m) \equiv v(x_1, \ldots, x_n, y_1, \ldots, y_m))$, where u and v are two words on the alphabet $\{x_1, \ldots, x_n, y_1, \ldots, y_m\}$, and a finite set E of semigroup identities with $xy \equiv yx$ in it, we prove that it is decidable whether P follows from E, that is whether all the semigroups in the variety defined by E satisfy P.

1. INTRODUCTION

One of the fundamental decision problems in algebra is the so-called word problem: decide whether a identity P follows from a set E of identities. It has been proved that the word problems for semigroups and groups are both undecidable, but decidable for commutative semigroups and commutative groups [**1**].

Some important semigroup properties cannot be described by semigroup identities, for example, S is

(i) regular;
(ii) simple;
(iii) a group, et cetera.

But they can be described as S satisfies

(i) $\forall x \exists y (xyx \equiv x)$;
(ii) $\forall x \forall y \exists u \exists v (uxv \equiv y)$;
(iii) $\forall x \forall y \exists z (xz \equiv y) \wedge \forall x \forall y \exists z (zx \equiv y)$, et cetera.

In this paper, we consider the following decision problem for semigroups: decide whether P follows from a set E of semigroup identities, where P is the first order formula

$$\forall x_1 \ldots \forall x_n \exists y_1 \ldots \exists y_m (u(x_1, \ldots, x_n, y_1, \ldots, y_m) \equiv v(x_1, \ldots, x_n, y_1, \ldots, y_m))$$

and u, v are two words on the alphabet $\{x_1, \ldots, x_n, y_1, \ldots, y_m\}$. Notice P will reduce to an identity if the existential variables y_j do not appear in P.

Received 28 May 1992

We say a semigroup S satisfies P if for any $s_1, \ldots, s_n$ in S, there are $w_1, \ldots, w_m$ in S, such that

$$u(s_1, \ldots, s_n, w_1, \ldots, w_m) = v(s_1, \ldots, s_n, w_1, \ldots, w_m)$$

holds in S.

We say P follows from E, written as $E \Vdash P$, if whenever a semigroup S satisfies every identity in E, S satisfies P also, that is all semigroups in the variety $[E]$ defined by E satisfy P.

For any set Σ, let Σ^+ and Σ^* denote, respectively, the free semigroup and free monoid generated by Σ. For a word $w \in \Sigma^*$ and a letter $a \in \Sigma$, $\binom{w}{a}$ denotes the number of times the letter a appears in w.

We regard a semigroup identity $u \equiv v$ as a pair of words $(u, v) \in V^+ \times V^+$, where V is a countably infinite set of variables.

Let $A = \{a_1, a_2, \ldots, a_n, \ldots\}$, and $A_n = \{a_1, a_2, \ldots, a_n\}$, $n \geqslant 1$. We define the following binary relations on A_n^+:

(i) $w \rho_n^E w'$, if for some homomorphism $\varphi\colon V^+ \to A_n^+$, and $u \equiv v$ in E, $\varphi(u) = w$, $\varphi(v) = w'$;

(ii) $w \underset{E}{\leftrightarrow} w'$, if for some $u, v, x, y \in A_n^*$, $w = xuy$, $w' = xvy$, and $u \rho_n^E v$ or $v \rho_n^E u$;

(iii) $w \overset{*}{\underset{E}{\longleftrightarrow}} w'$, if $w = w'$ or for some $z_1, z_2, \ldots, z_k \in A_n^+$, $w = z_1$, $w' = z_k$, $z_i \underset{E}{\leftrightarrow} z_{i+1}$, $i \leqslant k - 1$.

So $\overset{*}{\underset{E}{\longleftrightarrow}}$ is the congruence generated by ρ_n^E, and $A_n^+ / \overset{*}{\underset{E}{\longleftrightarrow}}$ is the relatively free semigroup in $[E]$ over the set $\{[a_i] \mid 1 \leqslant i \leqslant n\}$, where $[a_i] = \{w \in A_n^+ \mid a_i \overset{*}{\underset{E}{\longleftrightarrow}} w\}$. P follows from E if and only if there are $w_1, w_2, \ldots, w_m \in A_n^+$, such that

$$u(a_1, \ldots, a_n, w_1, \ldots, w_m) \overset{*}{\underset{E}{\longleftrightarrow}} v(a_1, \ldots, a_n, w_1, \ldots, w_m).$$

2. The results

From now on, we assume that $xy \equiv yx$ is in E, that is $[E]$ is a variety of commutative semigroups.

Let $E' = \{u \equiv v \in E \mid \binom{u}{x} \neq \binom{v}{x}$ for some $x \in V\}$. Without loss of generality, we assume

$$E = E' \cup \{xy \equiv yx\},$$
$$E' = \{x_1^{p_{i1}} x_2^{p_{i2}} \ldots x_k^{p_{ik}} \equiv x_1^{p'_{i1}} x_2^{p'_{i2}} \ldots x_k^{p'_{ik}} \mid i = 1, 2, \ldots, L\}, \text{ (if } E' \neq \emptyset)$$

$$u(x_1, \dots, x_n, y_1, \dots, y_m) = x_1^{s_1} \dots x_n^{s_n} y_1^{t_1} \dots y_m^{t_m},$$
$$v(x_1, \dots, x_n, y_1, \dots, y_m) = x_1^{s'_1} \dots x_n^{s'_n} y_1^{t'_1} \dots y_m^{t'_m}.$$

LEMMA 1. *If $E' = \emptyset$, then it is decidable whether $E \Vdash P$.*

PROOF: $E \Vdash P$ if and only if there are $w_j = \prod_{i=1}^{n} a_i^{x_{ij}} \in A_n^+$, $j \leqslant m$, such that $u(a_1, \dots, a_n, w_1, \dots, w_m) \xleftrightarrow[E]{*} v(a_1, \dots, a_n, w_1, \dots, w_m)$. But $E' = \emptyset$ implies that for any words $w, w' \in A_n^+$, $w \xleftrightarrow[E]{*} w'$ if and only if $\binom{w}{a_i} = \binom{w'}{a_i}$, for all $a_i \in A_n$. So $E \Vdash P$ if and only if the following linear system with integer unknowns x_{ij} is solvable:

$$(*) \qquad \begin{cases} \sum_{j=1}^{m} T_j x_{ij} = S_i, \quad i = 1, 2, \dots, n; \\ \sum_{i=1}^{n} x_{ij} > 0, \quad j = 1, 2, \dots, m; \\ x_{ij} \geqslant 0, \quad i = 1, 2, \dots, n, \ j = 1, 2, \dots, m' \end{cases}$$

where $T_j = t_j - t'_j$, $S_i = s'_i = s_i$. Without loss of generality, we assume that all $T_j \neq 0$ (because we can delete y_j from P, if $T_j = 0$).

Case (i). There are some T_α, T_β, $1 \leqslant \alpha, \beta \leqslant m$, $T_\alpha > 0$, $T_\beta < 0$. In this case (*) is solvable if and only if $(T_1, T_2, \dots, T_m) \mid S_i$, $1 \leqslant i \leqslant n$. Clearly, (*) is solvable implies $(T_1, T_2, \dots, T_m) \mid S_i$, $1 \leqslant i \leqslant n$. On the other hand, if $(T_1, T_2, \dots, T_m) \mid S_i$, then there are integers α_{ij}, $\sum T_j \alpha_{ij} = S_i$. Let us assume that $T_1 > 0$, $T_m < 0$. Take $\beta_{ij} = -T_m N_{ij} + \alpha_{ij}$, $1 \leqslant j \leqslant m - 1$, $\gamma_i = \alpha_{im} + \sum N_{ij} T_j$. We have

$$\sum_{j<m} T_j \beta_{ij} + T_m \gamma_i = S_i,$$

and if N_{ij} are sufficiently large (in particular, N_{ii}), we have $\beta_{ij} > 0$, $\sum_{j<m} T_j \beta_{ij} > S_i$, then we have $\gamma_i = \left(S_i - \sum_{j<m} T_j \beta_{ij}\right) / T_m > 0$.

Case (ii). $T_j > 0$, $j = 1, 2, \dots, m$. (The case of $T_j < 0$ can be treated similarly.) In this case, any $S_i < 0$ implies (*) is unsolvable. If $S_i \geqslant 0$ for all $i = 1, 2, \dots, n$, any solution of (*) will satisfy $0 \leqslant x_{ij} \leqslant S_i$, so it is decidable whether or not (*) has solutions. ∎

From now on, we assume that $E' \neq \emptyset$. Define

$$Q_E = \min\{q > 0 \mid (a_1^q, a_1^{p+q}) \text{ or } (a_1^{p+q}, a_1^q) \in \rho_1^E \text{ for some } p > 0\},$$

and

$$D_E = (g_{11}, \dots, g_{1k}, g_{21}, \dots, g_{2k}, \dots, g_{L1}, \dots, g_{Lk}),$$

that is D_E is the greatest common divisor of g_{ij}, where $g_{ij} = p_{ij} - p'_{ij}$, $1 \leqslant i \leqslant L$, $1 \leqslant j \leqslant k$.

Lemma 2. *For any $w, w' \in A_n^+$, $w \xleftrightarrow[E]{*} w'$ implies $\binom{w}{a_i} - \binom{w'}{a_i} = 0 \mod D_E$, $1 \leqslant i \leqslant n$.*

Proof: It is enough to prove that $\binom{w}{a_i} - \binom{w'}{a_i} = 0 \mod D_E$, $1 \leqslant i \leqslant n$, for all $(w, w') \in \rho_n^E$. Let $f \equiv g \in E'$, $f = x_1^{p_{s1}} \dots x_k^{p_{sk}}$, $g = x_1^{p'_{s1}} \dots x_k^{p'_{sk}}$. Then $\varphi \colon V^+ \to A_n^+$ is a homomorphism, $\varphi(f) = w$, $\varphi(g) = w'$, and $\binom{\varphi(x_j)}{a_i} = \alpha_{ij}$, $j = 1, 2, \dots, k$. We have

$$\binom{w}{a_i} - \binom{w'}{a_i} = \sum_{j=1}^{k} (p_{sj} - p'_{sj})\alpha_{ij} = 0 \pmod{D_E}.$$

∎

Lemma 3. $E \Vdash x^{Q_E} \equiv x^{Q_E + D_E}$.

Proof: Let $D_E = \sum \beta_{ij} g_{ij}$ and $M = \max\{1, 1 - \beta_{ij} \ (1 \leqslant i \leqslant L, 1 \leqslant j \leqslant k)\}$. We have

$$(*) \qquad D_E = \sum (M + \beta_{ij}) g_{ij} - \sum M g_{ij}.$$

Because $M \geqslant 1$, $M + \beta_{ij} \geqslant 1$, for any sufficiently large number N,

$$a_1^N \xleftrightarrow[E]{*} a_1^{N + D_E},$$

because we can find an implication chain corresponding to equation (*). Assume $\left(a_1^{Q_E}, a_1^{Q_E + p}\right) \in \rho_n^E$, we have

$$a_1^{Q_E} \xleftrightarrow[E]{*} a_1^{Q_E + Np} \xleftrightarrow[E]{*} a_1^{Q_E + Np + D_E} \xleftrightarrow[E]{*} a_1^{Q_E + D_E}.$$

∎

For convenience, we write $w_1 \Leftrightarrow w_2$ if for some (w, w') or $(w', w) \in \rho_n^E$, $\binom{w_1}{a_i} - \binom{w}{a_i} = \binom{w_2}{a_i} - \binom{w'}{a_i}$, $i = 1, 2, \dots, n$, and $\binom{w_1}{a_i} \neq \binom{w_2}{a_i}$ for some $a_i \in A_n$. Note $w_1 \leftrightarrow w_2$ implies $w_1 \xleftrightarrow[E]{*} w_2$. On the other hand, $w_1 \xleftrightarrow[E]{*} w_2$ implies either

(i) $\binom{w_1}{a_i} = \binom{w_2}{a_i}$, $1 \leqslant i \leqslant n$; or

(ii) for some $z_1, z_2, \dots, z_s \in A_n^+$, $w_1 = z_1$, $w_2 = z_s$, $z_i \Leftrightarrow z_{i+1}$, $i \leqslant s - 1$.

Now, let $N = \max\{k, Q_E\}$. For a word $a_1^{k_1} a_2^{k_2} \dots a_n^{k_n} \in A_n^+$, construct sets $B_i(w)$, $C_i(w)$, and functions $F_i^w \colon A_n \to \{0, 1\}$ iteratively.

(i) Construct

$$B_0(w) = \{w\} = \{a_1^{k_1} a_2^{k_2} \dots a_n^{k_n}\}.$$

$$F_0^w(a_j) = \begin{cases} 1, & \text{if } k_j \geqslant N \\ 0, & \text{otherwise;} \end{cases}$$

$$C_0(w) = \{a_1^{p_1} a_2^{p_2} \dots a_n^{p_n} \mid p_j = \min\{k_j, N\}, j \leqslant n\}.$$

https://doi.org/10.1017/S0004972700015288 Published online by Cambridge University Press

(ii) For any $i > 0$, construct

$$B_1(w) = \{a_1^{m_1} a_2^{m_2} \dots a_n^{m_n} \mid a_1^{m_1} a_2^{m_2} \dots a_n^{m_n} \Leftrightarrow w', \text{ for some } w' \in C_{i-1}(w)\},$$

$$F_1^w(a_j) = \begin{cases} 1, & \text{if } F_{i-1}^w(a_j) = 1 \text{ or } m_j \geqslant N \text{ for some} \\ & a_1^{m_1} a_2^{m_2} \dots a_n^{m_n} \in B_1(w) \\ 0, & \text{otherwise;} \end{cases}$$

$$C_i(w) = \{a_1^{p_1} a_2^{p_2} \dots a_n^{p_n} \mid \text{for some } a_1^{m_1} a_2^{m_2} \dots a_n^{m_n} \in B_1(w), p_j = \min\{N, m_j\}, j \leqslant n\}$$
$$\cup \{a_1^{p_1} a_2^{p_2} \dots a_n^{p_n} \mid \text{for some } a_1^{m_1} a_2^{m_2} \dots a_n^{m_n} \in B_i(w), p_j = F_i^w(a_j)N + (1 - F_i^w(a_j))m_j\}$$
$$\cup C_{i-1}(w).$$

Lemma 4. *The following statements are true:*

(i) $C_i(w) \subseteq C_{i+1}(w)$, $i \geqslant 0$;

(ii) $C_i(w) \subseteq \{a_1^{m_1} a_2^{m_2} \dots a_n^{m_n} \mid m_j \leqslant N, j = 1, 2, \dots, n\}$;

(iii) $C_i(w) = C_{i+1}(w)$ *implies* $C_i(w) = C_{i+p}(w)$ *and* $F_{i+1}^w = F_{i+p}^w$, *for any* $p > 0$.

Proof: Self-evident. ∎

Let i be the number such that $C_i(w) = C_{i+1}(w)$, define

$$F^w = F_{i+1}^w;$$
$$C(w) = \{a_1^{m_1} a_2^{m_2} \dots a_n^{m_n} \mid \text{for some } a_1^{q_1} a_2^{q_2} \dots a_n^{q_n} \in C_i(w), m_j = F^w(a_j)N + (1 - F^w(a_j))q_j\}.$$

Lemma 5. *For any* $i \geqslant 0$

(i) $F_i^w(a_j) = 1$ *implies* $w \overset{*}{\underset{E}{\longleftrightarrow}} w a_j^{D_E}$;

(ii) *for any* $a_1^{p_1} a_2^{p_2} \dots a_n^{p_n} \in C_i(w)$, *there is* $a_1^{q_1} a_2^{q_2} \dots a_n^{q_n} \in A_n^+$, *where* $q_k = p_k$ *if* $F_i^w(a_k) = 0$, *otherwise* $q_k \geqslant N$, $k = 1, 2, \dots, n$, *and* $w \overset{*}{\underset{E}{\longleftrightarrow}} a_1^{q_1} a_2^{q_2} \dots a_n^{q_n}$.

Proof: We prove this lemma by induction. For $i = 0$, it is clearly true. Now assume it is true for $i - 1$. If $F_i^w(a_j) = 1$ and $F_{i-1}^w(a_j) = 1$, then $w \overset{*}{\underset{E}{\longleftrightarrow}} w a_j^{D_E}$, by inductive assumption. If $F_i^w(a_j) = 1$ but $F_{i-1}^w(a_j) = 0$, then there are $a_1^{m_1} a_2^{m_2} \dots a_n^{m_n} \in B_i(w)$, $a_1^{h_1} a_2^{h_2} \dots a_n^{h_n} \in C_{i-1}(w)$, $a_1^{m_1} a_w^{m_2} \dots a_n^{m_n} \Longleftrightarrow a_1^{h_1} a_2^{h_2} \dots a_n^{h_n}$, $m_j \geqslant N$. By

https://doi.org/10.1017/S0004972700015288 Published online by Cambridge University Press

inductive assumption, there are $a_1^{f_1}a_2^{f_2}\dots a_n^{f_n} \in A_n^+$, $a_1^{f_1}a_2^{f_2}\dots a_n^{f_n} \overset{*}{\underset{E}{\longleftrightarrow}} w$, $f_j = h_j$, but $f_k \geqslant h_k$ for all $k \neq j$. Now we have

$$\begin{aligned} w &\overset{*}{\underset{E}{\longleftrightarrow}} a_1^{f_1}a_2^{f_2}\dots a_j^{h_j}\dots a_n^{f_n} \\ &\overset{*}{\underset{E}{\longleftrightarrow}} a_1^{m_1'}a_2^{m_2'}\dots a_j^{m_j}\dots a_n^{m_n'} \qquad (\text{where } m_k' = f_k - h_k + m_k) \\ &\overset{*}{\underset{E}{\longleftrightarrow}} a_1^{m_1'}a_2^{m_2'}\dots a_j^{m_j+D_E}\dots a_n^{m_n'} \qquad (\text{by Lemma 3}) \\ &\overset{*}{\underset{E}{\longleftrightarrow}} \left(a_1^{m_1'}a_2^{m_2'}\dots a_j^{m_j}\dots a_n^{m_n'}\right)a_j^{D_E} \\ &\overset{*}{\underset{E}{\longleftrightarrow}} wa_j^{D_E}. \end{aligned}$$

Now take $a_1^{p_1}\dots a_n^{p_n} \in C_i(w)$ if $a_1^{p_1}\dots a_n^{p_n} \in C_{i-1}(w)$, then by the inductive assumption and since $w \overset{*}{\underset{E}{\longleftrightarrow}} wa_j^{D_E}$ for all j with $F_i^w(a_j)$, we know there is $a_1^{q_1}\dots a_n^{q_n} \in A_n^+$, where $q_k = p_k$ if $F_i^w(a_k) = 0$, and $q_k \geqslant N$, if $F_i^w(a_k) = 0$, $k = 1, 2, \dots, n$, and $w \overset{*}{\underset{E}{\longleftrightarrow}} a_1^{q_1}\dots a_n^{q_n}$. If $a_1^{p_1}\dots a_n^{p_n} \notin C_{i-1}(w)$, let $a_1^{m_1}\dots a_n^{m_n} \in B_i(w)$, $a_1^{h_1}\dots a_n^{h_n} \in C_{i-1}(w)$, $a_1^{f_1}\dots a_n^{f_n} \in A_n^+$, such that

(i) $p_j = m_j$, if $F_i^w(a_j) = 0$;
(ii) $a_1^{h_1}\dots a_n^{h_n} \Longleftrightarrow a_1^{m_1}\dots a_n^{m_n}$
(iii) $x \overset{*}{\underset{E}{\longleftrightarrow}} a_1^{f_1}\dots a_n^{f_n}$, and $f_j \geqslant N$ if $F_{i-1}^w(a_j) = 1$, otherwise $f_j = h_j$, $j = 1, 2, \dots, n$.

Then we have

$$\begin{aligned} w &\overset{*}{\underset{E}{\longleftrightarrow}} a_1^{g_1}\dots a_n^{g_n} \qquad (\text{by (iii)}) \\ &\overset{*}{\underset{E}{\longleftrightarrow}} a_1^{m_1'}\dots a_n^{m_n'}, \qquad (\text{by (ii)}) \end{aligned}$$

where $m_j' = m_j + (g_j - h_j)$. Because $w \overset{*}{\underset{E}{\longleftrightarrow}} wa_j^{D_E}$ where $F_i^w(a_j) = 1$, letting $M > N/D_E$, we have

$$w \overset{*}{\underset{E}{\longleftrightarrow}} a_1^{q_1}\dots a_n^{q_n},$$

where $q_j = m_j' + MD_E > N$, if $F_i^w(a_j) = 1$, otherwise $q_j = m_j' = m_j = p_j$. ∎

Lemma 6. *Let $w = a_1^{p_1}\dots a_n^{p_n}$. If there is $w' = a_1^{q_1}\dots a_n^{q_n} \in A_n^+$, such that $w \overset{*}{\underset{E}{\longleftrightarrow}} w'$ and $q_j \geqslant N$, then $F^w(a_j) = 1$.*

Proof: If $p_j \geqslant N$, then $F^w(a_j) = F_0^w(a_j) = 1$. Now assume $p_j < N$. If $F^w(a_j) = 0$, let

$$w = z_0 \Longleftrightarrow z_1 \Longleftrightarrow \dots \Longleftrightarrow z_{t-1} \Longleftrightarrow z_t \Longleftrightarrow \dots \Longleftrightarrow z_s = w',$$

where $z_i = a_1^{q_{i1}} \dots a_n^{q_{in}}$, $i \leqslant s$, and $q_{ij} < N$ for all $i \leqslant t-1$, but $q_{tj} \geqslant N$. There are $z_i' \in C_i(w)$, $z_i' = a_1^{p_{i1}} \dots a_n^{p_{in}}$, where $p_{ij} = q_{ij}$ if $F_i^w(a_j) = 0$, otherwise $p_{ij} = N$, $i \leqslant t-1$. Imitate $z_{t-1} \Longleftrightarrow z_t$, we have $z_{t-1}' \Longleftrightarrow a_1^{h_1} \dots a_n^{h_n}$, where $h_j = q_{tj} \geqslant N$. So $F^w(a_j) = 1$. ∎

LEMMA 7. *Let $w = a_1^{m_1} \dots a_n^{m_n}$, $w' = a_1^{q_1} \dots a_n^{q_n}$. If $w \overset{*}{\underset{E}{\longleftrightarrow}} w'$, then there is $a_1^{p_1} \dots a_n^{p_n} \in C(w)$, where $p_j = q_j$ if $F^w(a_j) = 0$, otherwise $p_j = N$.*

PROOF: Let

$$w = z_0 \Longleftrightarrow z_1 \Longleftrightarrow \dots \Longleftrightarrow z_t = w',$$

where $z_i = a_1^{q_{i1}} \dots a_n^{q_{in}}$, $i \leqslant t$. Just as we did in the proof of Lemma 6, take the same $z_i' \in C_i(w)$. So there is $a_1^{p_1} \dots a_n^{p_n} \in C(w)$, where $p_j = N$ if $F^w(a_j) = 1$, otherwise $p_j = q_{ij} = q_j$. ∎

LEMMA 8. *Let $w = a_1^{m_1} \dots a_n^{m_n}$, $w' = a_1^{q_1} \dots a_n^{q_n}$. Then $w \overset{*}{\underset{E}{\longleftrightarrow}} w'$, if and only if*

(i) $m_i - q_i = 0 \pmod{D_E}$, $i \leqslant n$;
(ii) $F^w = F^{w'}$;
(iii) $C(w) \cap C(w') \neq \emptyset$.

PROOF: Clearly, $w \overset{*}{\underset{E}{\longleftrightarrow}} w'$ implies the conditions (i), (ii), and (iii), by Lemma 2, 5, 6, 7. Now assume that (i), (ii) and (iii) are true. For convenience, we assume that $F^w(a_j) = 1$ for all $j \leqslant d$, $F^w(a_j) = 0$ for all $j > d$, where $d \geqslant 0$. (ii) and (iii) imply that there are $w_1 = a_1^{f_1} \dots a_d^{f_d} a_{d+1}^{p_{d+1}} \dots a_n^{p_n}$, $w_2 = a_1^{h_1} \dots a_d^{h_d} a_{d+1}^{p_{d+1}} \dots a_n^{p_n} \in A_n^+$, f_j, $h_j \geqslant N$, and $w \overset{*}{\underset{E}{\longleftrightarrow}} w_1$, $w' \overset{*}{\underset{E}{\longleftrightarrow}} w_w$. For any $j \leqslant d$, $f_j - h_j = (f_j - m_j) + (m_j - q_j) + (q_j - h_j) = 0 \pmod{D_E}$, by (i) and Lemma 2, and therefore $a_j^{f_j} \overset{*}{\underset{E}{\longleftrightarrow}} a_j^{h_j}$, by Lemma 3. Hence $w \overset{*}{\underset{E}{\longleftrightarrow}} w_1 \overset{*}{\underset{E}{\longleftrightarrow}} w_2 \overset{*}{\underset{E}{\longleftrightarrow}} w'$. ∎

Now we state and prove the main result of this paper.

THEOREM 9. *Let E and P be as described before, $E' \neq \emptyset$. It is decidable whether $E \Vdash P$.*

PROOF: $w = a_1^{s_1} \dots a_n^{s_n}$, $w' = a_1^{s_1'} \dots a_n^{s_n'}$. We can assume $F^{w'}(a_j) = 1$ if and only if $j \leqslant p$, for some $p \geqslant 0$. We need to consider three cases.

(i) All t_j and $t_j' = 0$. In this case, P reduces to an identity, and $E \Vdash P$ if and only if $w \overset{*}{\underset{E}{\longleftrightarrow}} w'$. By Lemma 8, this is decidable.

(ii) Some $t_j' > 0$, and some $t_j > 0$. In this case, $E \Vdash P$ if and only if $(D_E, T_1, T_2, \dots, T_m) \mid S_i$, $i = 1, 2, \dots, n$, where $T_j = t_j - t_j'$, $S_i = s_i - s_i$. Becasue there are $w_1, \ldots, w_m \in A_n^+$, such that

$$u(a_1, \ldots, a_n, w_1, \ldots, w_m) \overset{*}{\underset{E}{\longleftrightarrow}} v(a_1, \ldots, a_n, w_1, \ldots, w_m),$$

the following system with integer unknowns x_{ij} is solvable:

$$(***) \qquad S_i + \sum T_j x_{ij} = 0 \pmod{D_E}, \quad i = 1, 2, \ldots, n;$$

and this in turn implies $(D_E, T_1, T_2, \ldots, T_m) \mid S_i$, $i = 1, 2, \ldots, n$. On the other hand, $(D_E, T_1, T_2, \ldots, T_m) \mid S_i$ means (***) is solvable, and if x_{ij}, $i \leqslant n$, $j \leqslant m$, is a solution, then $MD_E + x_{ij}$, $i \leqslant n$, $j \leqslant m$, is also a solution, for any $M > 0$. Therefore, there exist $w_1, \ldots, w_m \in A_n^+$, such that

$$\begin{gathered} \binom{u}{a_j} > N, \quad \binom{v}{a_j} > N, \\ \binom{u}{a_j} - \binom{v}{a_j} = 0 \pmod{D_E}, \\ j = 1, 2, \ldots, n; \end{gathered}$$

where $u = u(a_1, \ldots, a_n, w_1, \ldots, w_m)$, $v = v(a_1, \ldots, a_n, w_1, \ldots, w_m)$. Let

$$X = a_1^{h_1} \ldots a_n^{h_n}, \quad Y = a_1^{f_1} \ldots a_n^{f_n},$$

where $h_j = \binom{u}{a_j}$, $f_j = \binom{v}{a_j}$, $j \leqslant n$. We have

$$u \overset{*}{\underset{E}{\longleftrightarrow}} X \overset{*}{\underset{E}{\longleftrightarrow}} Y \overset{*}{\underset{E}{\longleftrightarrow}} v.$$

(iii) All $t'_j = 0$, but some $t_j > 0$. We can assume that all $t_j > 0$. In this case, it is not difficult to see that $E \Vdash P$ if and only if

(a) $F^w \leqslant F^{w'}$ (that is $F^w(a_j) = 0$ for all $j > p$);

(b) $(t_1, t_2, \ldots, t_m, D_E) \mid s - s'$, $i \leqslant p$;

(c) for some $a_1^{f_1} \ldots a_n^{f_n} \in C(w')$, there exist $x_{ij} \geqslant 0$, such that $s_i + \sum_{j=1}^{m} t_j x_{ij} = f_i$, $i \geqslant P + 1$;

so it is also decidable. ∎

References

[1] B. Benninghofen, S. Kemmerich and M.M. Richter, *Systems of reductions* (Springer-Verlag, Berlin, Heidelberg, New York, 1987).

Monash University
Clayton, Victoria 3168
Australia