RAIRO. INFORMATIQUE THÉORIQUE

ROMAN KÖNIG

Reduction algorithms for some classes of aperiodic monoids

RAIRO. Informatique théorique, tome 19, nº 3 (1985), p. 233-260
<http://www.numdam.org/item?id=ITA_1985__19_3_233_0>

R.A.I.R.O. Informatique théorique/Theoretical Informatics
(vol. 19, nº 3, 1985, p. 233 à 260)

REDUCTION ALGORITHMS FOR SOME CLASSES OF APERIODIC MONOIDS (*)

by Roman KÖNIG ([1])

Communicated by J. BERSTEL

Abstract. — *A class of finite, noetherian and confluent rewrite systems is constructed, which allows the description of the M-variety* **R** *of all finite* $\mathcal{R}$*-trivial monoids and gives a decision procedure for membership in* **R**. *This class with its left-right dual leads to the definition of a new M-variety, which again turns out to be decidable.*

Résumé. — *On définit une classe de systèmes de réécriture finis, noethériens et confluents, qui donne une description de la M-variété* **R** *des monoïdes finis* $\mathcal{R}$*-triviaux et qui fournit un algorithme pour décider l'appartenance à* **R**. *La combinaison de cette classe avec son dual mène à la définition d'une nouvelle M-variété, également décidable.*

INTRODUCTION

In 1972 [7] and 1975 [8], I. Simon characterized the class of languages which have a finite $\mathfrak{J}$-trivial syntactic monoid. In 1978 [1] and 1976 [2] his ideas have been modified to yield a characterization of those languages with an $\mathcal{R}$-trivial syntatic monoid.

This way of proceeding seems unnatural in the following sense : in a semigroup S, $\mathcal{R}$ and $\mathcal{L}$ are defined and then $\mathcal{H}$ and $\mathcal{D}$ are derived by forming $\mathcal{H} = \mathcal{R} \cap \mathcal{L}$ and $\mathcal{D} = \mathcal{R} \vee \mathcal{L}$. Since we are considering finite monoids, $\mathfrak{J} = \mathcal{D}$. Therefore it seems to be desirable to characterize the languages with finite $\mathcal{R}$-trivial syntactic monoid and then to derive a characterization for the languages with finite $\mathfrak{J}$-trivial monoid. This is done in the first chapter of this paper. As a by-product we get a characterization of the *M-variety* $\mathbf{R} \vee \mathbf{L}$, generated by finite $\mathcal{R}$-trivial and $\mathcal{L}$-trivial monoids.

The second chapter gives an effective construction of a reduction system which allows to decide for a given finite monoid M whether $M \in \mathbf{R}$.

(*) Received in February 1984, revised in September 1984.
([1]) Institut für Mathematische Maschinen und Datenverarbeitung I Martensstraβe 3, D-8520 Erlangen, FRG.

0399-0540/85/03 233 28/$ 4,80/

The construction of the irreducible word associated to a given word can be realized by a sequential transducer.

The Semi-Thue-Systems constructed in chapter two are combined in chapter three to define an M-variety between $\mathbf{R} \vee \mathbf{L}$ and $\mathbf{Ap}$, the class of aperiodic monoids, which again turns out to be decidable.

I am indebted to my colleague V. Strehl, to F. Baader and to the referee for useful hints and comments.

1. RIGHT- AND LEFT-TESTABLE LANGUAGES

In this section we present a new description of some congruences which give a characterisation of the class of all $\mathcal{R}$-trivial, $\mathcal{L}$-trivial and $\mathfrak{J}$-trivial monoids respectively. We first recall some definitions and facts :

DÉFINITION 1.1 : *Let M be a monoid. M is called*

$$\mathcal{R}\text{-}trivial, \text{ if } \forall a, b \in M\,(aM = bM \Rightarrow a = b)$$
$$\mathcal{L}\text{-}trivial, \text{ if } \forall a, b \in M\,(Ma = Mb \Rightarrow a = b)$$
$$\mathfrak{J}\text{-}trivail, \text{ if } \forall a, b \in M\,(MaM = MbM \Rightarrow a = b)\,.$$

The classes $\mathbf{R}$, $\mathbf{L}$ and $\mathbf{J}$ of all finite $\mathcal{R}$-trivial, $\mathcal{L}$-trivial and $\mathfrak{J}$-trivial monoids respectively are M-varieties in the sense of Eilenberg [2], that is a class of finite monoids closed under taking submonoids, homomorphic images and finite direct products. $\mathbf{R}$ is ultimately defined by the sequence of equations $(xy)^k x = (xy)^k$ $(k \in \mathbb{N})$. This means : A finite monoid M belongs to $\mathbf{R}$ iff there is some $k \in \mathbb{N}$ such that $(xy)^k x = (xy)^k$ holds in M. Similarly $\mathbf{L}$ is ultimately defined by $x(yx)^k = (yx)^k$ and $\mathbf{J}$ is ultimately defined by $(xy)^k x = (xy)^k = y(xy)^k$. Notice that $\mathbf{J} = \mathbf{R} \cap \mathbf{L}$.

A congruence relation ρ on a monoid M is called fully invariant, if for each endomorphism $f : M \to M$ $(u, v) \in \rho$ implies $(f(u), f(v)) \in \rho$ i.e. $\rho \subseteq f \circ \rho \circ f^{-1}$, where « $\circ$ » denotes relational product. The minimal equivalence relation on M is called Δ_M, the maximal Ω_M. The subscripts are omitted, if the monoid M is clear from the context. For a finite alphabet Σ and a subset L of Σ^*, the free monoid generated by Σ, denote by σ_L the syntactic congruence of L. This is the largest congruence relation with the property

$$\sigma_L \subseteq \pi_L := (L \times L) \cup (\Sigma^* \setminus L) \times (\Sigma^* \setminus L)\,.$$

The quotient monoid Σ^*/σ_L is called the syntactic monoid of L and denoted by $M(L)$.

The length of a word $u \in \Sigma^*$ is denoted by $|u|$.

DEFINITION 1.2 : *For* $w \in \Sigma^*$ *denote by* $\alpha(w)$ *the alphabet of* w, *i.e.*

$$\alpha(w) = \{ \sigma \in \Sigma \mid \exists u, v \in \Sigma^* \ w = u\sigma v \} .$$

For $k \in \mathbb{N}$ *define*

$$R_k := \{ (u\sigma, u) \mid \exists u_1, \dots, u_k \in \Sigma^*, \sigma \in \Sigma \text{ such that } u = u_1 \dots u_k \text{ and } \alpha(u_1) \supseteq \dots \supseteq \alpha(u_k) \ni \sigma \}$$

$L_k := \{ (\sigma u, u) \mid (u^r \sigma, u^r) \in R_k \}$, *where* u^r *denotes the reversal of a word* $u \in \Sigma^*$.
ρ_k (λ_k *resp.*) *denotes the congruence relation on* Σ^* *generated by* R_k (L_k *resp.*).

A language $L \subseteq \Sigma^*$ is called right-testable, (left-testable resp.) if there is some integer k, such that L is a union of some equivalence-classes of ρ_k (λ_k resp.) (we say L is ρ_k-saturated).

From this definition we can immediately see the following facts and their left-right-duals :

Remark 1.3.

(1) $R_{k+1} \subseteq R_k, \rho_{k+1} \subseteq \rho_k \ (k \in \mathbb{N})$.
(2) $(u\sigma, u) \in R_k \Rightarrow \forall w \in \Sigma^* \ (wu\sigma, wu) \in R_k$.
(3) $\rho_0 = \lambda_0 = \Omega$.
(4) For every $u, v \in \Sigma^*$ $u \neq v$ there is a maximal $k \in \mathbb{N}$ such that $(u, v) \in \rho_k$: Indeed $(u, v) \in \rho_0$ but $(u, v) \notin \rho_m$ for $m = 1 + \min(|u|, |v|)$.

The set R_k can be considered as a reduction system, which is evidently noetherian.

LEMMA 1.4 : $R_k = \{ (u\sigma, u) \mid u \in \Sigma^*, \sigma \in \Sigma, (u\sigma, u) \in \rho_k \}$.

Proof: The inclusion from left to right is obvious. Let $(u\sigma, u) \in \rho_k$ and $u_1 \dots u_s$ the following decomposition of $u\sigma$ as a product of non-empty words : For every $i = 1, \dots, s$, u_i is the shortest prefix of $u_i \dots u_s$, which contains every letter of $u_i \dots u_s : \alpha(u_i) = \alpha(u_i \dots u_s)$.

If we assume $s < k$, then no relation of R_k can be applied to $u\sigma$. But R_k generates ρ_k, so $s \geqslant k$ follows. If $u_1 \dots u_k$ is not a prefix of u, but $u_1 \dots u_k = u\sigma$, then $u\sigma$ is a prefix of every word w, which can be derived from $u\sigma$ by relations contained in R_k. Since u is a proper prefix of $u\sigma$, $u_1 \dots u_k$ has to be a prefix of u and we obtain a decomposition $u = u_1 \dots u_k w$ with

$$\alpha(u_1) \supseteq \alpha(u_2) \supseteq \dots \supseteq \alpha(u_{k-1}) \supseteq \alpha(u_k w) \ni \sigma \quad \text{and} \quad (u\sigma, u) \in R_k \text{ follows}.$$

LEMMA 1.5 : *ρ_k and λ_k are fully invariant congruence relations on Σ^* of finite index.*

Proof : Since ρ_k is generated by R_k, it is sufficient to prove :

$$(u\sigma, u) \in R_k\,, \quad f \in \mathrm{End}\,(\Sigma^*) \Rightarrow (f(u\sigma), f(u)) \in \rho_k\,.$$

Let $f(\sigma) \neq \Lambda$ since otherwise we are done. From $u = u_1 \dots u_k$ with $\alpha(u_1) \supseteq \dots \supseteq \alpha(u_k) \ni \sigma$ follows $\alpha(f(u_1)) \supseteq \dots \supseteq \alpha(f(u_k)) \supseteq \alpha(f(\sigma))$.

If $f(\sigma) = \sigma_1 \dots \sigma_s$ $(\sigma_i \in \Sigma, i = 1, \dots, s)$ then $f(u\sigma) = f(u_1) \dots f(u_k).\sigma_1 \dots \sigma_s$ and from $\alpha(f(u_k)) \ni \sigma_i$ for each $i = 1, .., s$ we obtain $(f(u\sigma), f(u)) \in \rho_k$.

Let $A_{k,\Sigma}$ be the set of all irreducible words over Σ relative to R_k. Then

(I) $\qquad A_{0,\Sigma} = \{ \Lambda \}$ for all finite alphabets Σ

(II) $\qquad A_{k,\phi} = \{ \Lambda \}$ for all $k \in \mathbb{N}$

From (I), (II) and the following proposition we deduce by induction that ρ_k has finite index. The left-right-dual proves the lemma for λ_k.

PROPOSITION 1.6 : $A_{k,\Sigma} = \{ \Lambda \} \cup \bigcup_{\sigma \in \Sigma} A_{k,\Sigma \setminus \sigma}.\sigma.A_{k-1,\Sigma}$ *for all* $k > 0$, $\Sigma \neq \varnothing$.

Proof : We prove the inclusion from left to right : Let $w \in A_{k,\Sigma} \setminus \{ \Lambda \}$ and u the shortest prefix of w, which contains every letter of w : $\alpha(u) = \alpha(w)$, $w = uv$.

Since u is shortest possible, $u = u'\sigma$ with $\sigma \notin \alpha(u')$.

Since w is irreducible, $u' \in A_{k,\Sigma \setminus \sigma}$.

If we had $v \notin A_{k-1,\Sigma}$, then v would be reducible.

This means $v = v_1 v_2 \dots v_{k-1} \tau v'$ $(\tau \in \Sigma, v' \in \Sigma^*)$ and $\alpha(v_1) \supseteq \dots \supseteq \alpha(v_{k-1}) \ni \tau$.

Since $\alpha(u) = \alpha(w)$ we have $\alpha(u) \supseteq \alpha(v_1) \supseteq \dots \supseteq \alpha(v_{k-1}) \ni \tau$ and w is reducible, contradicting our assumption, thus $v \in A_{k-1,\Sigma}$.

For the opposite inclusion let $u \in A_{k,\Sigma \setminus \sigma}$, $v \in A_{k-1,\Sigma}$ and suppose $w = u\sigma v \notin A_{k,\Sigma}$.

Since w is reducible, *a* letter of w can be removed. $\sigma \notin \alpha(u)$, thus this letter either occurs in u or in v. If it occurs in u, then $u \notin A_{k,\Sigma \setminus \sigma}$ contrary to our assumption.

If it occurs in v then we have a decomposition

$$w = w_1 w_2 \dots w_k \tau w'\,, \quad \text{where} \quad \alpha(w_1) = \alpha(w)\,,$$
$$\alpha(w_1) \supseteq \dots \supseteq \alpha(w_k) \ni \tau\,.$$

Since $\alpha(w_1) = \alpha(u)$, u is shorter than w_1 or $u = w_1$.

Now $(w_2 \dots w_k \tau, w_2 \dots w_k) \in R_{k-1}$, hence $v \notin A_{k-1,\Sigma}$.

PROPOSITION 1.7 : *The following propositions are equivalent for* $L \subseteq \Sigma^*$:

a) *L is right-testable.*

b) $M(L) \in \mathbf{R}$.

Proof: Let L be right-testable, i.e. L is ρ_k-saturated for some $k \in \mathbb{N}$. Then $\rho_k \subseteq \pi_L$ and since ρ_k is a congruence relation, $\rho_k \subseteq \sigma_L$. Since ρ_k is fully invariant, each relation in Σ^*/ρ_k is a law in Σ^*/ρ_k. Obviously for $\sigma, \tau \in \Sigma$ we have $((\sigma\tau)^k \sigma, (\sigma\tau)^k) \in \rho_k$, and therefore

$$(xy)^k x = (xy)^k$$

holds in Σ^*/ρ_k. (If Σ consists of one letter σ only then

$$\Sigma^*/\rho_k \cong A_{k,\Sigma} = \{ \Lambda, \sigma, \sigma^2, ..., \sigma^k \}$$

with multiplication $\sigma^i \sigma^j = \sigma^{\min(k,i+j)}$, which is clearly an $\mathcal{R}$-trivial monoid). Since $(xy)^k x = (xy)^k$ ultimately defines $\mathbf{R}$, $\Sigma^*/\rho_k \in \mathbf{R}$ and $\rho_k \subseteq \sigma_L$ implies

$$M(L) \in \mathbf{R}$$

Now let $L \subseteq \Sigma^*$ and $M(L) \in \mathbf{R}$.

To prove that L is right-testable we have to show : $\rho_k \subseteq \pi_L$ for some $k \in \mathbb{N}$.

To conclude this, it is sufficient to show :

$$R_k \subseteq \sigma_L \quad \text{for some} \quad k \in \mathbb{N} .$$

Let $| M(L) | = k + 1$ and $(u\sigma, u) \in R_k$. We set $\pi := \sigma_L$ for convenience.

$$(u\sigma, u) \in R_k \text{ means : } u = u_1 \ldots u_k, \alpha(u_1) \supseteq \ldots \supseteq \alpha(u_k) \ni \sigma .$$

Consider the sequence of words

$$w_0 = \Lambda, w_1 = u_1, w_2 = u_1 u_2, ..., w_k = u_1 \ldots u_k, w_{k+1} = u_1 \ldots u_k \sigma .$$

Since $| M(L) | = k + 1$ one can find $i, j \in \{ 0, ..., k + 1 \}$ such that $i < j$ and $(w_i, w_j) \in \pi$.

If $i = k$, then $w_i = u$, $w_j = u\sigma$ and nothing is to be done.

If $i < k$: it suffices to show :

$$(*) \quad \forall \tau \in \alpha(u_{i+1}) \quad (w_i, w_i \tau) \in \pi .$$

Then we have the conclusion

$$\begin{aligned} & (w_i, w_i \sigma) \in \pi && \text{for all } \sigma \in \alpha(u_{i+1}) \\ \Rightarrow & (w_i\tau, w_i \sigma\tau) \in \pi && \text{(since } \pi \text{ is a congruence relation)} \\ \Rightarrow & (w_i, w_i \sigma\tau) \in \pi && \end{aligned}$$

Since $\alpha(u_{i+1}) \supseteq \alpha(u_{i+2}) \supseteq \ldots \supseteq \alpha(u_k) \ni \sigma$ we infer

$$(w_i, w_k) \in \pi$$
$$(w_i, w_{k+1}) \in \pi$$

and we obtain $(w_k, w_{k+1}) = (u, u\sigma) \in \pi$.

To show (*) denote $[w]_\pi$ by $\overline{w}$ and $M(L)$ by M and let $\tau \in \alpha(u_{i+1})$. Then

$$w_{i+1} = w_i\, v\tau v' \,(v, v' \in \Sigma^*)\,.$$

Now

$$\overline{w}_i\, M \supseteq \overline{w_i\, v}\, M \supseteq \overline{w_i\, v\tau}\, M \supseteq \overline{w}_j\, M\,.$$

Since $\overline{w}_i = \overline{w}_j$ we have equality everywhere in the line above. But $M \in \mathbf{R}$ so we get

$$\overline{w}_i = \overline{w_i\, v} = \overline{w_i\, v\tau}$$

from where we conclude

$$\overline{w}_i = \overline{w_i\, \tau}, \text{ i.e. } (w_i, w_i\, \tau) \in \sigma_L\,.$$

Combining theorem 1.7 and its left-right-dual we obtain :

THEOREM 1.8 : *The following propositions are equivalent for* $L \subseteq \Sigma^*$ *:*
a) *L is* $\rho_k \vee \lambda_k$*-saturated for some* $k \in \mathbb{N}$.
b) $M(L) \in \mathbf{J}$.

Proof : Let L be $\rho_k \vee \lambda_k$-saturated, i.e

$$\rho_k \vee \lambda_k \subseteq \sigma_L\,.$$

Then $\rho_k \subseteq \sigma_L$, $\lambda_k \subseteq \sigma_L$, and therefore

$$M(L) \in \mathbf{R} \cap \mathbf{L} = \mathbf{J}\,.$$

Now let $M(L) \in \mathbf{R} \cap \mathbf{L}$. There are $r, l \in \mathbb{N}$ such that $\rho_r \subseteq \sigma_L$, $\lambda_l \subseteq \sigma_L$.
Then for $k = \max(r, l)$ we have $\rho_k \vee \lambda_k \subseteq \sigma_L$.

THEOREM 1.9 : *The following propositions are equivalent for* $L \subseteq \Sigma^*$.
a) *L is* $\rho_k \cap \lambda_k$*-saturated.*
b) $M(L) \in \mathbf{R} \vee \mathbf{L}$.

Proof : Let $\rho_k \cap \lambda_k \subseteq \sigma_L$. This means Σ^*/σ_L is a homomorphic image of a subdirect product of Σ^*/ρ_k and Σ^*/λ_k. Since $\Sigma^*/\rho_k \in \mathbf{R}$, $\Sigma^*/\lambda_k \in \mathbf{L}$, we obtain

$$M(L) \in \mathbf{R} \vee \mathbf{L}\,.$$

Now let $M(L) \in \mathbf{R} \vee \mathbf{L}$. There are finite alphabets Γ, Θ and congruence relations γ on Γ^*, θ on Θ^* such that for some $k \in \mathbb{N}$

$$\rho_{k,\Gamma} \subseteq \gamma$$
$$\lambda_{k,\Theta} \subseteq \theta$$

and

$$\begin{array}{l} \Gamma^*/\gamma \times \Theta^*/\theta \\ \uparrow \\ \cdot \twoheadrightarrow M(L) \end{array}$$

We can assume $\Gamma \cap \Theta = \varnothing$.

The homomorphism

$$(\Gamma \cup \Theta)^* \xrightarrow{(f_1, f_2)} \Gamma^*/\gamma \times \Theta^*/\theta$$

defined by

$$\sigma \xrightarrow{f_1} \begin{cases} \sigma, & \text{if} \quad \sigma \in \Gamma \\ \Lambda, & \text{if} \quad \sigma \in \Theta \end{cases}$$

$$\sigma \xrightarrow{f_2} \begin{cases} \sigma, & \text{if} \quad \sigma \in \Theta \\ \Lambda, & \text{if} \quad \sigma \in \Gamma \end{cases}$$

has surjective projections and thus for

$$\gamma' = f_1 \circ \gamma \circ f_1^{-1}$$
$$\theta' = f_2 \circ \theta \circ f_2^{-1}$$
$$X = \Gamma \cup \Theta$$

we have

$$X^*/\gamma' \cap \theta' \cong \Gamma^*/\gamma \times \Theta^*/\theta$$

and since ρ_k and λ_k are fully invariant we obtain

$$\rho_{k,X} \subseteq f_1 \circ \rho_{k,\Gamma} \circ f_1^{-1} \subseteq f_1 \circ \gamma \circ f_1^{-1} \subseteq \gamma'$$
$$\lambda_{k,X} \subseteq f_2 \circ \lambda_{k,\Theta} \circ f_2^{-1} \subseteq f_2 \circ \theta \circ f_2^{-1} \subseteq \theta'$$

and

$$\rho_{k,X} \cap \lambda_{k,X} \subseteq \gamma' \cap \theta' \text{ follows}.$$

There are a congruence relation β on X^* such that $X^*/\beta \simeq M(L)$ and $\gamma' \cap \theta' \subseteq \beta$ and $f : \Sigma^* \to X^*$ making

$$\begin{array}{ccc} \Sigma^* & \to & X^* \\ \downarrow & & \downarrow \\ M(L) & \cong & X^*/\beta \end{array}$$

commutative. Now

$$\sigma_L = f\circ\beta\circ f^{-1} \supseteq f\circ(\rho_{k,X}\cap\lambda_{k,X})\circ f^{-1} \supseteq$$
$$\supseteq f\circ\rho_{k,X}\circ f^{-1}\cap f\circ\lambda_{k,X}\circ f^{-1} \supseteq \rho_{k,\Sigma}\cap\lambda_{k,\Sigma}\,.$$

COROLLARY 1.10 : *Let $M = \Sigma^*/\rho$ be a finite monoid.*

(1) $$M\in\mathbf{R}\Leftrightarrow\exists k \quad \rho_k\subseteq\rho$$

(2) $$M\in\mathbf{L}\Leftrightarrow\exists k \quad \lambda_k\subseteq\rho$$

(3) $$M\in\mathbf{J}\Leftrightarrow\exists k \quad \rho_k\vee\lambda_k\subseteq\rho$$

(4) $$M\in\mathbf{R}\vee\mathbf{L}\Leftrightarrow\exists k\ \rho_k\cap\lambda_k\subseteq\rho\,.$$

2. SOME COMBINATORIAL PROPERTIES OF ρ_k AND λ_k

The congruence relations ρ_k and λ_k have some nice combinatorial properties, which allow a very detailed description of the monoid Σ^*/ρ_k. The most important of these is :

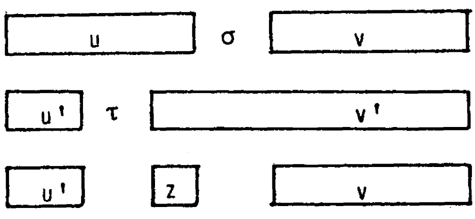
LEMMA 2.1 : *Every ρ_k-class has a unique shortest representative.*

Proof : Two words $u, v\in\Sigma^*$ which are reducible to the same R_k-irreducible word $w\in\Sigma^*$ are obviously ρ_k-equivalent.

For the opposite direction we prove by induction on k : R_k is a confluent Semi-Thue-System.

For $k = 0$ we have $R_k = \{(\sigma, \Lambda)\mid\sigma\in\Sigma\}$, which is obviously confluent.

Let $k\geqslant 1$, $w = u\sigma v = u'\tau v'$ and $(u\sigma, u)\in R_k$, $(u'\tau, u')\in R_k$. We may assume that u' is a prefix of u and thus we have the following situation.



We want to prove

$$(uv, u'zv)\in\rho_k \quad\text{and}\quad (u'v', u'zv)\in\rho_k\,.$$

Since $u = u'\tau z$ and $(u'\tau, u')\in R_k$ we have

$$(u, u'z)\in\rho_k \quad\text{and}\quad (uv, u'zv)\in\rho_k\,.$$

To see the second relation let u_0 be the shortest prefix of u which contains every letter of u.

If $u'\tau$ is a prefix of u_0, then the decomposition $u = u_1 \ldots u_k$ with $(A)\ \alpha(u_1) \supseteq \ldots \supseteq \alpha(u_k) \ni \sigma$ can be converted into a decomposition of $u'z$ because $u' = u'_1 \ldots u'_k$ with $\alpha(u'_1) \supseteq \cdots \supseteq \alpha(u'_k)\quad \tau$ and so cancelling this occurrence of τ does not effect the inclusions of (A).

If $u'\tau$ is not a prefix of u_0, then u_0 is a prefix of $u'\tau$ and since $(u'\tau, u') \in R_k$, u_0 is a prefix of u'.

$$u = u_0 v_0$$
$$u' = u_0 v'_0 .$$

Now we have $(v_0 \sigma, v_0) \in R_{k-1}$, $(v'_0 \tau, v'_0) \in R_{k-1}$.

By hypothesis we have

$$(v'_0 z\sigma, v'_0 z) \in R_{k-1}$$

from where we get

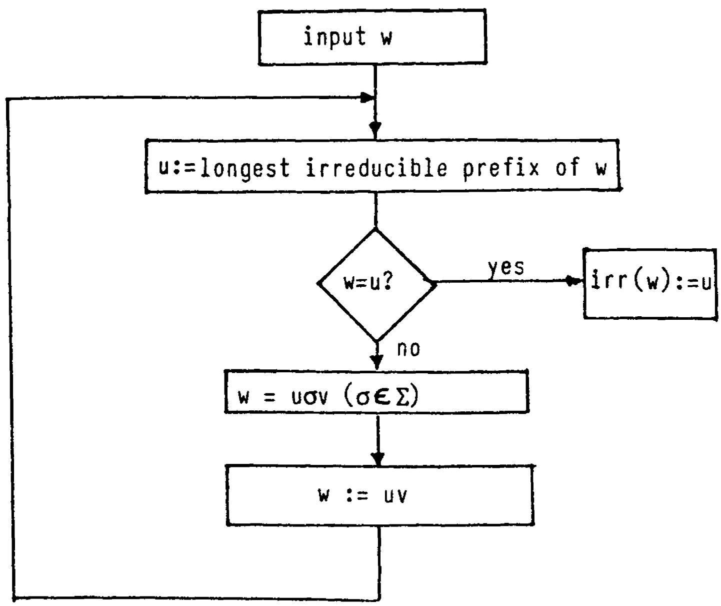
$$(u_0 v'_0 z\sigma, u_0 v'_0 z) \in R_k$$

and

$$(u'v', u'zv) \in \rho_k .$$

Remark 2.2

(1) Since the order, in which the reduction steps of R_k are applied, is immaterial, we can do it from left to right by applying the leftmost possible reduction recursively until the resulting word is reduced. This yields an algorithm for the construction of the shortest representative irr (w) of a given $w \in \Sigma^*$ and thus a decision procedure for the word problem in Σ^*/ρ_k :

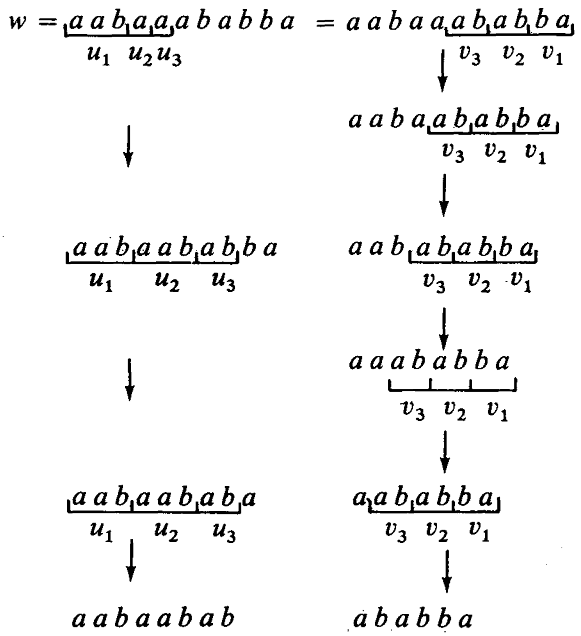


(2) The considerations under (1) show the significance of knowing the set of all irreducible words over Σ relative to R_k.

(3) The set $A_{k,\Sigma}$ of all irreducible words over Σ is a tree; every prefix of an irreducible word is irreducible.

(4) From (1) a decision procedure for the word problem in $\Sigma^*/\rho_k \cap \lambda_k$ is easily derived.

Examples 2.3 : $k = 3$



w ρ_3-reduces to *aabaabab* and λ_3-reduces to *ababba*. In each step the word $u_1\,u_2\,u_3$ is the maximal λ_3-reduced prefix and $v_3\,v_2\,v_1$ is the maximal λ_3-reduced suffix.

The set $A_{k,\Sigma}$ of all ρ_k-irreducible words over Σ is contained in

$$\{\Lambda\} \cup \bigcup_{\sigma\in\Sigma} A_{k,\Sigma\setminus\sigma}.\sigma.A_{k-1,\Sigma}$$

by proposition 1.6. The following lemma gives a recursive construction of $A_{k,\Sigma}$ as a disjoint union of simpler sets.

LEMMA 2.4 : *For $k \in \mathbb{N}$ and a finite alphabet Σ define*

$$D_{k,\Sigma} = \{ u \in A_{k,\Sigma} \mid \alpha(u) = \Sigma \},$$

then

$$D_{k,\phi} = \{ \Lambda \}, \quad D_{0,\Sigma} = \varnothing \, (k \geqslant 0, \Sigma \neq \varnothing)$$

and

$$D_{k,\Sigma} = \bigcup_{\sigma \in \Sigma} \left(D_{k,\Sigma \sim \sigma} \cdot \sigma \cdot \bigcup_{\Sigma' \subseteq \Sigma} D_{k-1,\Sigma'} \right) (\Sigma \neq \varnothing, k \geqslant 1)$$

and all unions are disjoint.

Proof:

(1) If $\Sigma \neq \Sigma'$, then $D_{k,\Sigma} \cap D_{k,\Sigma'} = \varnothing (k \geqslant 0)$.

(2) $A_{k,\Sigma} = \bigcup_{\Sigma' \subseteq \Sigma} D_{k,\Sigma'}$ is a disjoint union for all $k \geqslant 0$.

(3) Let $w \in D_{k,\Sigma}$ and u the shortest prefix of w with $\alpha(u) = \alpha(w) = \Sigma$. As in the proof of proposition 1.6 we have $w = uv$, $u = u' \sigma$ with

$$\sigma \in \Sigma, u' \in D_{k,\Sigma \sim \sigma} \quad \text{and} \quad v \in A_{k-1,\Sigma} \text{ and so}$$

$$D_{k,\Sigma} \subseteq \bigcup_{\sigma \in \Sigma} (D_{k,\Sigma \sim \sigma} . \sigma . A_{k-1,\Sigma}) \text{ follows .}$$

The opposite inclusion follows as in proposition 1.6 if one additionally notes that if $u \in D_{k,\Sigma \sim \sigma}$, $v \in A_{k-1,\Sigma}$, then $\alpha(u\sigma v) = \Sigma$. From (2) follows the desired formula and from (1) follows the disjointness.

$$\text{Let } a_{k,n} := | A_{k,\Sigma} | \quad \text{for an } n\text{-letter alphabet } \Sigma, k \geqslant 0$$

$$\text{and } d_{k,n} := \frac{| D_{k,\Sigma} |}{n\,!} \quad \text{for an } n\text{-letter alphabet } \Sigma, k \geqslant 0 \,.$$

Since permuting the letters of Σ preserves reducedness,

$$| D_{k,\Sigma} | \text{ is divisible by } n\,! \text{ if } \Sigma \text{ consists of } n \text{ letters .}$$

COROLLARY 2.5 :

(1) $d_{1,n} = 1 = d_{k,0} \, (k \geqslant 0, n \geqslant 0), d_{0,n} = 0 \, (n > 0)$.

(2) $d_{k,n} = d_{k,n-1} \cdot \sum_{r \leqslant n} (n)_r \, d_{k-1,r} \, (k > 0, n > 0)$

(3) $a_{k,n} = \dfrac{d_{k+1,n}}{d_{k+1,n-1}} \quad (k \geqslant 0, n > 0)$

where $(n)_r$ *denotes falling factorials* :

$$(n)_r = n.(n-1).....(n-r+1) \,.$$

Proof : To see (1), observe that

$$D_{k,\phi} = \{ \Lambda \} \; (k \geqslant 0), \; D_{0,\Sigma} = \varnothing \; (\Sigma \neq \varnothing)$$

and if $\Sigma = \{ \sigma_1, \ldots, \sigma_n \}$, then

$$D_{1,\Sigma} = \{ \sigma_{p(1)} \ldots \sigma_{p(n)} \mid p \in S_n \} .$$

(2) The lemma implies for $k \geqslant 1$, $n > 0$

$$n \,!\, d_{k,n} = n.(n-1)\,!\, d_{k,n-1} \cdot \sum_{r \leqslant n} \binom{n}{r} r \,!\, d_{k-1,r} ,$$

from which (2) follows.

(3) From the proof of the lemma follows

$$a_{k,n} = \sum_{r \leqslant n} \binom{n}{r} r \,!\, d_{k,r}$$

$$= \sum_{r \leqslant n} (n)_r \, d_{k,r} = \frac{d_{k+1,n}}{d_{k+1,n-1}} .$$

Calculation of the first of these numbers gives the tables :

$d_{k,n}$	$k \rightarrow$ 0	1	2	3	4	5	6	7	8
n 0	1	1	1	1	1	1	1	1	1
1	0	1	2	3	4	5	6	7	8
2	0	1	10	75	628	6325	75966	1063615	17017960
3	0	1	160	77025	290519080				
4	0	1	10400						
5	0	1	3390400						

$a_{k,n}$	0	1	2	3	4	5	6	7
0	1	1	1	1	1	1	1	1
1	1	2	3	4	5	6	7	8
2	1	5	25	157	1265	12661	151945	2127245
3	1	16	1027	462610				
4	1	65	253569					
5	1	326	408105811					
6	1	1957						
7	1	13700						
8	1	109601						
9	1	986410						

To give an example, let $k = 2$, $\Sigma = \{ a, b \}$. Since $d_{2,2} = 10$, $d_{2,1} = 2$, $d_{2,0} = 1$

Λ

a, a^2

$ab, aab, aba, aaba, abb, aabb, abab, aabab, abba, aabba$

is a complete list of types of reduced words for $\rho_{2,\Sigma}$. A list for $A_{2,\Sigma}$ is obtained by applying the permutation (a, b) to the letters of each word.

LEMMA 2.6 : *Let* $l_{k,n} := \max \{ | w | : w \in A_{k,\Sigma'} | \Sigma | = n \}$

and $$Q_{k,\Sigma} = \{ w \in A_{k,\Sigma} : w | = l_{k,n}, n = | \Sigma | \} .$$

Then

$$Q_{0,\Sigma} = \{ \Lambda \}, \quad Q_{k,\phi} = \{ \Lambda \} \text{ and for } k \geqslant 1, \quad \Sigma \neq \emptyset$$

$$Q_{k,\Sigma} = \bigcup_{\sigma \in \Sigma} Q_{k,\Sigma \sim \sigma} . \sigma . Q_{k-1,\Sigma}$$

$$Q_{k,\Sigma} = \bigcup_{(\sigma_1, \ldots, \sigma_k) \in \Sigma^k} Q_{k,\Sigma \sim \sigma_1} . \sigma_1 . Q_{k-1,\Sigma \sim \sigma_2} . \sigma_2 . \ldots . Q_{1,\Sigma \sim \sigma_k} \sigma_k .$$

Moreover

$$l_{k,n} = \binom{n+k}{k} - 1 \qquad (k \geqslant 0, n \geqslant 0) .$$

Proof: Let $w \in Q_{k,\Sigma}$, $k \geqslant 1$, $\Sigma \neq \emptyset$.

Then $w = u\sigma v$ with $u \in D_{k,\Sigma \sim \sigma}$, $v \in A_{k-1,\Sigma}$.

If $u \notin Q_{k,\Sigma \sim \sigma}$, then an arbitrary $u' \in Q_{k,\Sigma \sim \sigma}$ gives a word $w' = u' \sigma v$ with $| w' | > | w |$. If $v \notin Q_{k-1,\Sigma}$ then each $v' \in Q_{k-1,\Sigma}$ gives a word $w' = u\sigma v'$ with $| w' | > | w |$. Since the opposite inclusion is obvious, the first equation is established.

The second equation follows by recursive application of the first.

The third formula is true for $k = 0$ and all n and for $n = 0$ and all k. The first equation implies for the lengths :

$$l_{k,n} = l_{k,n-1} + 1 + l_{k-1,n} .$$

Assuming the formula to be true for all indices with sum $\leqslant k + n - 1$ we get

$$l_{k,n} = \binom{n+k-1}{k} + \binom{n+k-1}{k-1} - 1 = \binom{n+k}{k} - 1 .$$

The number $l_{k,n}$ is the depth of the tree of minimal representatives of $\rho_{k,\Sigma}$ ($|\Sigma| = n$). It also allows to give an upper bound for a finite generating system for ρ_k :

COROLLARY 2.7 : *There is a generating system for* $\rho_{k,\Sigma}$ *with at most* $n^{\binom{n+k}{k}}$ *elements if* $|\Sigma| = n$.

Proof : Following remark 2.2 shows that

$$\{ (u\sigma, u) \mid u \in A_{k,\Sigma}, u\sigma \notin A_{k,\Sigma}, \sigma \in \Sigma \}$$

is a generating system for ρ_k. Since $A_{k,\Sigma}$ is a tree, the cardinality of the set

$$\{ u \in A_{k,\Sigma} \mid u\sigma \notin A_{k,\Sigma} \}$$

is at most $n^{l_{k,n}}$. Since there are n choices for $\sigma \in \Sigma$ one has at most

$$n^{l_{k,n}+1} = n^{\binom{n+k}{k}} \text{ pairs in the generating system .}$$

Next we study the set of idempotents in Σ^*/ρ_k.

LEMMA 2.8 : *A word* $w \in \Sigma^*$ *is idempotent, i.e.* $(w^2, w) \in \rho_{k,\Sigma}$ *iff*

$$w = u_1 \dots u_k \quad \textit{with} \quad \alpha(u_1) = \cdots = \alpha(u_k) .$$

Proof : If $w = u_1 \dots u_k$ with $\alpha(u_1) = \cdots = \alpha(u_k)$ then for each $\sigma \in \alpha(w)$ one has

$$\alpha(u_1) \supseteq \dots \supseteq \alpha(u_k) \ni \sigma$$

and $(w\sigma, w) \in \rho_k$ follows, which implies

$$(ww, w) \in \rho_k .$$

On the other hand let $(ww, w) \in \rho_k$. Decompose $w = w_1 \dots w_k$, where w_i is the shortest prefix of $w_i \dots w_k$, which contains all the letters of $w_i \dots w_k$. Since $(w^2, w) \in \rho_k$, we have $\alpha(w_1) \supseteq \dots \supseteq \alpha(w_k) \supseteq \alpha(w_1)$, from where the desired equality follows.

COROLLARY 2.9 : *Let* $w \in \Sigma^*$. *Then*

$$(w^2, w) \in \rho_k \Leftrightarrow (w^2, w) \in \lambda_k \Leftrightarrow (w^2, w) \in \rho_k \cap \lambda_k .$$

Remark and Example 2.10 :

a) Denote by $F'_{r,\Sigma}$, $F_{r,\Sigma}$ resp. the set

$$F'_{r,\Sigma} = \{ w \in \Sigma^* \mid (w^2, w) \in \rho_r \}$$

$$F_{r,\Sigma} = \{ w \in \Sigma^* \mid (w^2, w) \in \rho_r, \alpha(w) = \Sigma \} \text{ resp.}$$

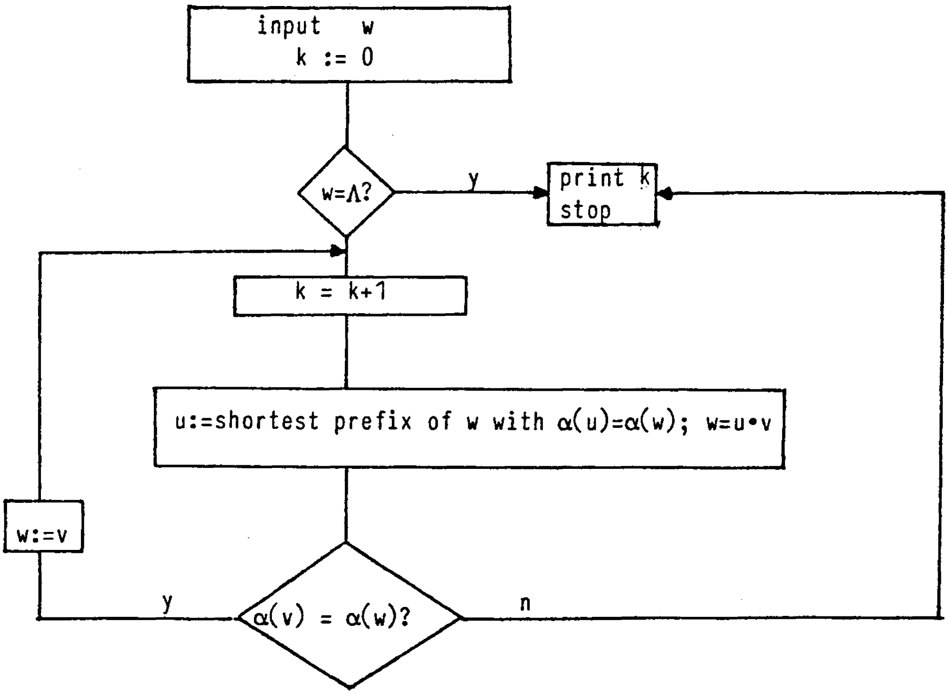
Then obviously $F'_{r,\Sigma} = \bigcup_{\Gamma \subseteq \Sigma} F_{r,\Gamma}$ (disjoint) and

$$\Gamma \subseteq \Sigma \Rightarrow F'_{r,\Gamma} \subseteq F'_{r,\Sigma} .$$

The lemma says :

$$F_{s,\Sigma} \cdot F_{t,\Sigma} = F_{s+t,\Sigma} .$$

b) For each word $w \in \Sigma^* \setminus \{ \Lambda \}$ there is a maximal number $k \in \mathbb{N}$, such that $(w^2, w) \in \rho_k \cap \lambda_k$. k is obtained by the following algorithm :



Let $E_{k,\Sigma} = \{ w \in D_{k,\Sigma} \mid (w^2, w) \in \rho_k \} = D_{k,\Sigma} \cap F_{k,\Sigma}$ the set of ρ_k-reduced idempotents with $\alpha(w) = \Sigma$.

LEMMA 2.11 : $E_{k,\phi} = D_{k,\phi} = \{ \Lambda \} \, (k \geqslant 0)$

$$E_{0,\Sigma} = D_{0,\Sigma} = \varnothing \quad (\Sigma \neq \varnothing)$$

$$E_{k,\Sigma} = \bigcup_{\sigma \in \Sigma} D_{k,\Sigma - \sigma} . \sigma . E_{k-1,\Sigma} \quad (k \geqslant 1, \Sigma \neq \varnothing)$$

Let $e_{k,n} := \dfrac{| E_{k,\Sigma} |}{n\,!}$ *for some* Σ *with* $| \Sigma | = n$.

Then

$$e_{k,0} = 1 \quad (k \geqslant 0)$$

$$e_{0,n} = 0 \quad (n \geqslant 1)$$

$$e_{k,n} = n\,!\, d_{k,n-1}\, e_{k-1,n} \quad (k \geqslant 1, n \geqslant 1) .$$

Proof: Obviously $E_{k,\phi} = \{ \Lambda \}$ for $k \geqslant 0$ and $E_{0,\Sigma} = \varnothing$ for all $\Sigma \neq \varnothing$.

Let $w \in E_{k,\Sigma}$ $(k \geqslant 1, \Sigma \neq \varnothing)$ and u the shortest prefix of w with $\alpha(u) = \alpha(w)$. Then $w = uv$, $u = u' \sigma$ with $u' \in D_{k,\Sigma - \sigma}$ and $v \in E_{k-1,\Sigma}$, since

$$v = v_1 \dots v_{k-1} \quad \text{with} \quad \alpha(v_1) = \cdots = \alpha(v_{k-1}) .$$

For the other inclusion take $u \in D_{k,\Sigma - \sigma}$, $v \in E_{k-1,\Sigma}$.

Since $E_{k,\Sigma} \subseteq D_{k,\Sigma}$ for all k, Σ, we have $u\sigma v \in D_{k,\Sigma}$. Moreover v has a factorisation $v = v_1 \dots v_{k-1}$ with $\alpha(v_1) = \cdots = \alpha(v_{k-1}) = \Sigma$; since $\alpha(u\sigma) = \Sigma$, $u\sigma v \in E_{k,\Sigma}$.

Since evidently the union above is disjoint, we get

$$n\,!\, e_{k,n} = n.(n-1)\,!\, d_{k,n-1} . n\,!\, e_{k-1,n}$$

from where the formula follows.

The first values of $e_{k,n}$ are listed in the following table :

$e_{k,n}$		$k \to$ 0	1	2	3	4	5
n	0	1	1	1	1	1	1
$\downarrow$	1	0	1	1	1	1	1
	2	0	1	4	24	192	1920
	3	0	1	60	25308		
	4	0	1	3840			
	5	0	1				

Remark 2.12

(1) $Q_{k,\Sigma} \subseteq E_{k,\Sigma}$ for all $k \in \mathbb{N}$.

(2) The monoid Σ^*/ρ_k is isomorphic to the set $A_{k,\Sigma}$ together with the operation $u.v = \operatorname{irr}(uv)$, where $\operatorname{irr}(uv)$ is the unique word x in $A_{k,\Sigma}$ with $(x, uv) \in \rho_k$. The algorithm of remark 2.2 does this efficiently.

(3) Each of the subsets $D_{k,\Sigma}(\Gamma \subseteq \Sigma)$ constitutes a subsemigroup of $A_{k,\Sigma}$.

(4) Each of the subsets $E_{k,\Gamma}(\Gamma \subseteq \Sigma)$ is an idempotent subsemigroup. Moreover, $E_{k,\Sigma}$ is a two-sided ideal in $A_{k,\Sigma}$.

(5) $E_{k,\Sigma}$ and $Q_{k,\Sigma}$ are subsemigroups of left-zeroes of $A_{k,\Sigma}$.

Example 2.13 : Let again $k = 2$, $\Sigma = \{ a, b \}$. Then

$$l_{2,2} = \binom{2+2}{2} - 1 = 5$$

$$Q_{k,\Sigma} = \{ aabab, aabba, bbaba, bbaab \}$$

$$E_{k,\Sigma} = Q_{k,\Sigma} \cup \{ abab, abba, baba, baab \} .$$

Remark 2.14

(1) The word-problem in Σ^*/ρ_k can now be solved by the following algorithm :

(*a*) Generate $A_{k,\Sigma}$

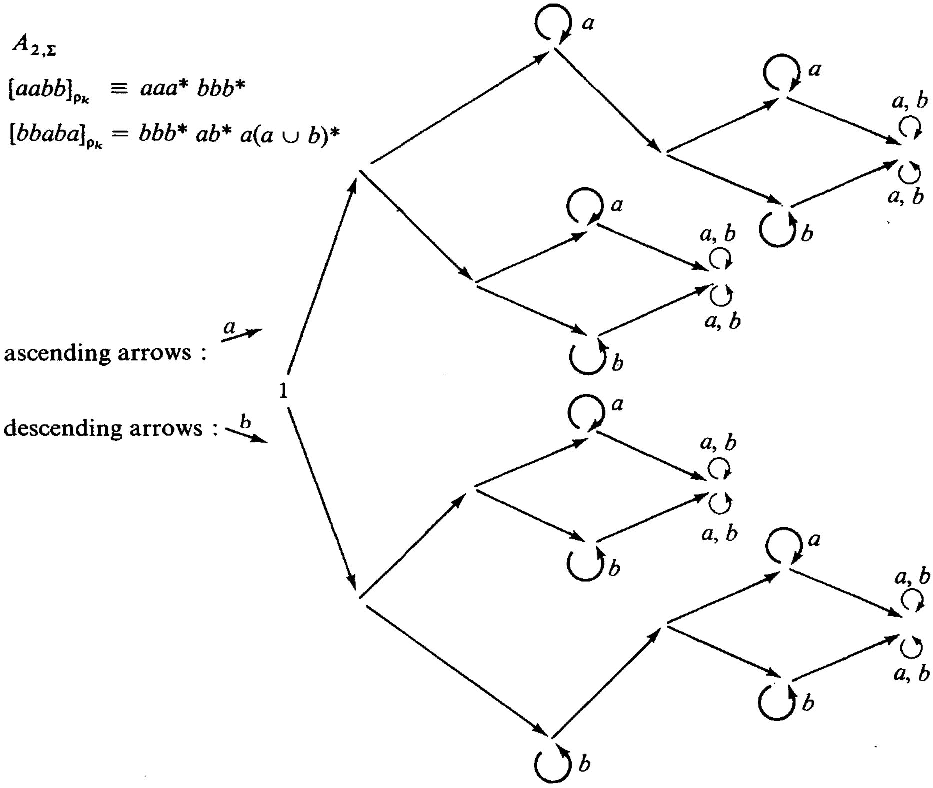
(*b*) Consider $A_{k,\Sigma}$ as a Σ-automaton with state-set $A_{k,\Sigma}$ and operations

$$u.\sigma = \begin{cases} u\sigma, & \text{if } u\sigma \in A_{k,\Sigma} \\ u & \text{if } u\sigma \notin A_{k,\Sigma} \end{cases}$$

where $u \in A_{k,\Sigma}$, $\sigma \in \Sigma$

(*c*) Two words $v, w \in \Sigma^*$ are ρ_k-equivalent, iff $\Lambda.v = \Lambda.w$ in this automaton.

(2) This automaton also gives a possibility to describe the equivalence class of a word w by a regular expression : Consider again the case $\Sigma = \{ a, b \}$, $k = 2$. Then Σ^*/ρ_k is the following graph :



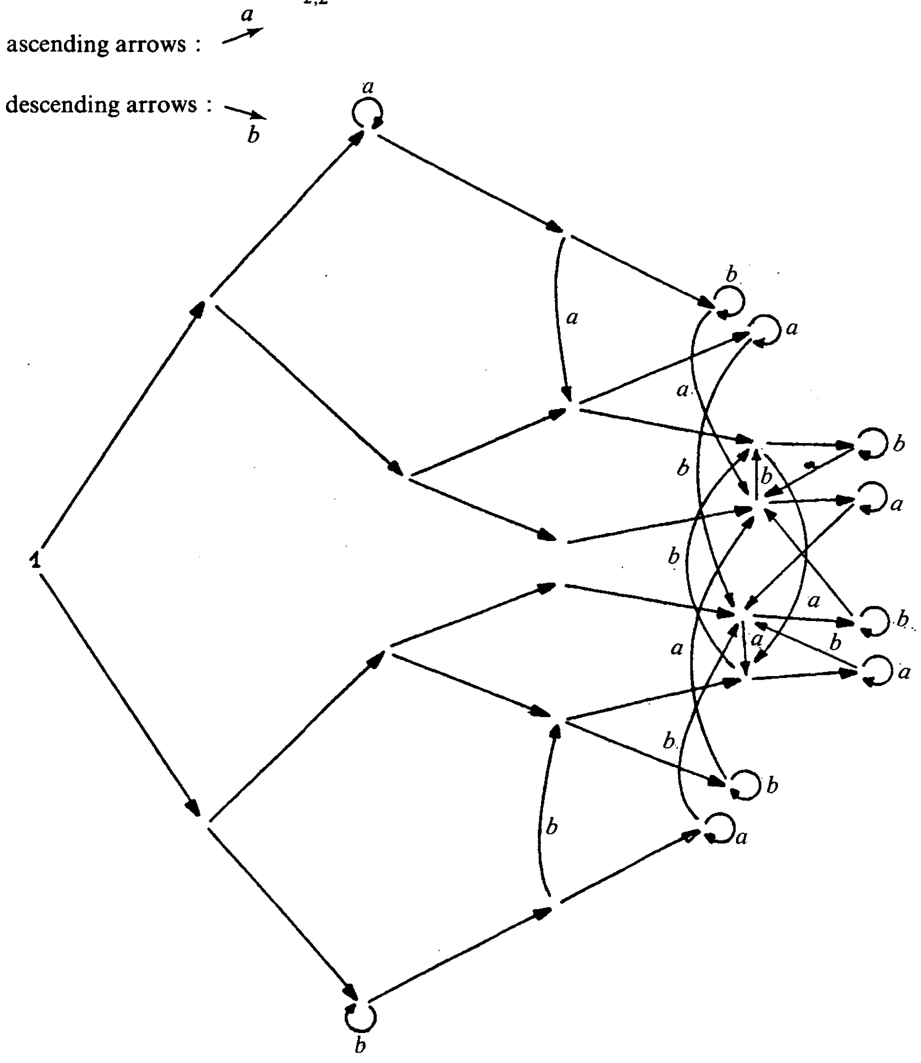
(3) If we add the following output function to this automaton

$$u * \sigma = \begin{cases} \Lambda, & \text{if} \quad u.\sigma = u \\ \sigma, & \text{if} \quad u.\sigma = u\sigma \end{cases}$$

we obtain a sequential transducer which realizes the function $f : \Sigma^* \to \Sigma^*$ which associates to every word $u \in \Sigma^*$ its shortest representative irr(u). This shows that f is a sequential function.

(4) Analogously Σ^*/λ_k is presented by the following graph :

$B_{2,\Sigma}$



Note that $A_{k,\Sigma}$ and $B_{k,\Sigma}$ are anti-isomorphic by the mapping $w \mapsto w^r$.

The previous considerations allow to give a decision procedure for membership in **R**

THEOREM 2.16 : *Let M be a monoid of cardinality m with generating system $\Sigma \subseteq M$. The following properties are equivalent :*

(1) $M \in \mathbf{R}$

(2) $u \in A_{m,\Sigma}$, $u\sigma \notin A_{m,\Sigma} (\sigma \in \Sigma) \Rightarrow u\sigma = u$ in M

(3) For $k := \left\lceil \frac{m-1}{2} \right\rceil$ and every $x, y \in M \quad \{ 1 \}$ $(xy)^k x = (xy)^k$ or $(yx)^k y = (yx)^k$ in M.

Proof : (1) $\Leftrightarrow$ (2) follows from corollary 1.10, since ρ_m is generated by $\{ (u\sigma, u) \mid u \in A_{m,\Sigma}, u\sigma \notin A_{m,\Sigma}, \sigma \in \Sigma \}$ (Remark 2.2).

(3) $\Rightarrow$ (1) : Let $a, b \in M$, $(a, b) \in \mathscr{R}$. There are $x, y \in M$ such that $ax = b$, $by = a$. If $x = 1$ or $y = 1$ then $a = b$. Hence let $x, y \in M \quad \{ 1 \}$. If $(xy)^k x = (xy)^k$ then $b = byx = b(yx)^{k+1} = by(xy)^k x = b(yx)^k y = by = a$. Similarly if $(yx)^k y = (yx)^k$ we obtain $a = b$; hence $M \in \mathbf{R}$.

(1) $\Rightarrow$ (3) : Choose x and y arbitrarily in $M \setminus \{ 1 \}$ and consider the sequence

$$1, x, xy, xyx, (xy)^2, (xy)^2 x, \ldots, (xy)^k x .$$

This sequence of $2k + 2$ elements in M must contain two members, which are identical.

Case 1 : $\exists s, t \leqslant k, s < t$

$$(xy)^s x = (xy)^t x$$

Now
$$(xy)^t x = (xy)^t . x$$
$$(xy)^t \quad = (xy)^s x . y (xy)^{t-s-1}$$

and $((xy)^t x, (xy)^t) \in \mathscr{R}$. Since $M \in \mathbf{R}$, $(xy)^t x = (xy)^t$,

and $(xy)^k x = (xy)^k$ follows.

Case 2 : $\exists s, t \leqslant k, s < t$

$$(xy)^s = (xy)^t .$$

Right-multiplication with x gives case 1.

Case 3 : $\exists s, t \leqslant k, s \leqslant t$

$$(xy)^s = (xy)^t x$$

if $s = t$, we are done. Otherwise

$$(xy)^t x = (xy)^t . x$$
$$(xy)^t \quad = (xy)^s (xy)^{t-s}$$
$$= (xy)^t x . (xy)^{t-s}$$

and we obtain $((xy)^t x, (xy)^t) \in \mathcal{R}$. The rest follows as in case 1.

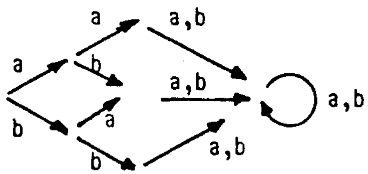
Case 4 : $\exists s, t \leqslant k, s < t$

$$(xy)^s x = (xy)^t .$$

Left multiplication by y gives, similarly as in case 3, $((yx)^t y, (yx)^t) \in \mathcal{R}$. To decide membership in **R**, we have now two possibilities :

— Generate $A_{k,\Sigma}$ and test property (2)
— Test property (3).

Example 2.17 : Let the monoid M be given by



It is obvious, that $u \in A_{3,\Sigma}$, $u\sigma \notin A_{3,\Sigma} \Rightarrow u\sigma = u$ in M for $\sigma \in \Sigma = \{ a, b \}$. If, however, the monoid M is given by a multiplication table, it may be more efficient to test property (3).

We call an M-Variety **W** decidable, if for every finite monoid M it is decidable whether $M \in \mathbf{W}$. It is clear, that $\mathbf{V} \cap \mathbf{W}$ is decidable, if **V** and **W** are decidable.

In view of corollary 1.10 (3) we see that a finite monoid M belongs to **J** iff there are a natural k and an alphabet Σ such that $M \simeq \Sigma^*/\rho$ for some congruence relation ρ and $R_k \cup L_k \subseteq \rho$.

Unfortunately the union of the reduction systems for ρ_k and λ_k does not give a confluent Semi-Thue-System :

$$\text{Let} \quad \Sigma = \{ a, b \}, \quad k = 2, \quad w = ababa .$$

abab and *baba* are both $\rho_2 \vee \lambda_2$-equivalent to w and irreducible.

On the other hand the word problem for $\rho_k \cap \lambda_k$ is decidable. Note that by corollary 1.10 (4) the sequence $\rho_k \cap \lambda_k$ defines $\mathbf{R} \vee \mathbf{L}$.

In [1], the M-variety **R** is characterized by the sequence ${}_n\sim_R$ of congruence relations on Σ^* defined in the following way : Put

$${}_n\sim \; := \{ (u, v) \mid \forall w \in \Sigma^n \; u \in w \sqcup\!\sqcup \Sigma^* \Leftrightarrow v \in w \sqcup\!\sqcup \Sigma^* \} .$$

and

${}_n\sim_R \; := \{ (u, v) \mid$ for every prefix a of u there is a prefix b of v such that $a \; {}_n\sim b$ and for every prefix b of v there is a prefix a of u such that $a \; {}_n\sim b \}$

Although $_n\sim_R$ and ρ_n are defined in completely different ways, we can prove : $_n\sim_R = \rho_n$ for every natural n.

For this purpose consider the algorithm which produces for every word $w \in \Sigma^*$ the shortest representative $\chi_n(w)$ of its $_n\sim_R$-class, described in [1], p. 11.

It is clear from this algorithm that $_n\sim_R$ is generated by the set

$$\{ (u\sigma, u) \mid u \in \Sigma^*, \sigma \in \Sigma, u\sigma \ {}_n\!\sim u \} = {}_n{-}_R \, .$$

Lemma 3 of [8] states that $u\sigma \ {}_n{-}_R \ u$ iff $(u\sigma, u) \in R_n$ and $_n\sim_R = \rho_n$ follows.

3. COMMON GENERALIZATION OF ρ_k AND λ_k

In the definition of ρ_k a letter within a word w may be removed, if some condition for the part of w, occurring to the left of this letter, is true. Since λ_k is just the left-right-dual of ρ_k, a corresponding property holds for λ_k. Therefore the following generalization is very natural :

DEFINITION 3.1 : *For $r, l \in \mathbb{N}$ and a finite alphabet Σ define*

$$M_{r,l} = \{ (u\sigma v, uv) \mid (u\sigma, u) \in R_r, (\sigma v, v) \in L_1 \}$$

$\mu_{r,l} = \overline{M_{r,l}}$, *the congruence relation on Σ^* generated by $M_{r,l}$.*

Facts 3.2 :

(1) $\mu_{r,0} = \rho_r$

$\mu_{0,l} = \lambda_l$.

(2) $M_{r+1,l} \subseteq M_{r,l}$; $\mu_{r+1,l} \subseteq \mu_{r,l}$

$M_{r,l+1} \subseteq M_{r,l}$; $\mu_{r,l+1} \subseteq \mu_{r,l}$.

(3) $\mu_{r,l} \subseteq \rho_r \cap \lambda_l$.

(4) $(u\sigma v, uv) \in M_{r,l}$

$\Rightarrow (xu\sigma vy, xuvy) \in M_{r,l}$ for all $x, y \in \Sigma^*$.

LEMMA 3.3 : *$\mu_{r,l}$ is a fully invariant congruence relation with finite index.*

Proof : An argument very similar as in the proof of lemma 1.5 shows that $\mu_{r,l}$ is fully invariant. Let $A_r(B_l, C_{r,l}$ resp.) be the set of irreducible words over Σ relative to $\rho_r(\lambda_l, \mu_{r,l}$ resp.) and $w \in C_{r,l}$. Thus for each $\sigma \in \alpha(w)$, we have

$$w = u_0 \, \sigma v_0 \Rightarrow (u_0 \, \sigma, u_0) \notin R_r \quad \text{or} \quad (\sigma v_0, v_0) \notin L_l \, .$$

Let $\sigma_1, ..., \sigma_s$ be the sequence of letters of w, for which $w = u_i \, \sigma_i \, v_i$ and

$(u_i\, \sigma_i, u_i) \notin R_r$ $(i = 1, \ldots, s)$ and $\tau_1, \ldots, \tau_t$ the sequence of letters of w, for which

$$w = u'_i\, \tau_i\, v'_i \quad \text{and} \quad (\tau_i\, v'_i, v'_i) \notin L_l\,.$$

Now we have $\sigma_1 \ldots\ldots \sigma_s \in A_r$ since $(u\tau, u) \in R_r$ and $(u\tau\sigma, u\tau) \notin R_r$ imply $(u\sigma, u) \notin R_r$. A similar argument shows $\tau_1 \ldots\ldots \tau_t \in B_l$.

Let $A, B \subseteq \Sigma^*$, $\Sigma' = \{ \sigma' \mid \sigma \in \Sigma \}$, $\Sigma'' = \{ \sigma'' \mid \sigma \in \Sigma \}$

$$B' = \{ \sigma'_1 \ldots \sigma'_n \mid b = \sigma_1 \ldots \sigma_n \in B \}$$

$$\begin{array}{l} (\Sigma \cup \Sigma')^* \xrightarrow{g} \Sigma^* \quad g : \begin{array}{l} \sigma \mapsto \sigma \\ \sigma' \mapsto \sigma \end{array}, \\ \quad \downarrow f \\ (\Sigma \cup \Sigma')^* / \sigma\tau' = \tau'\sigma \end{array}$$

f the natural epimorphism, then the shuffle of A and B is

$$A \sqcup\!\sqcup B := g(f^{-1}\, f(A.B')) \quad [2]\,,$$

and for

$$\begin{array}{l} (\Sigma \cup \Sigma' \cup \Sigma'')^* \xrightarrow{k} \Sigma^* \quad k : \begin{array}{l} \sigma \mapsto \sigma \\ \sigma' \mapsto \sigma \\ \sigma'' \mapsto \sigma \end{array} \\ \quad \downarrow h \\ (\Sigma \cup \Sigma' \cup \Sigma'')^* \Big/ \begin{array}{l} \sigma\tau' = \tau'\sigma \\ \sigma\sigma' = \sigma'' \end{array} \end{array}$$

h the natural epimorphism, we define the amalgamated shuffle

$$A \,\dot{\sqcup\!\sqcup}\, B := k(h^{-1}\, h(A.B'))\,.$$

The amalgamated shuffle is also known as the infiltration product [5] or simply as shuffle [6].

From the consideration above we conclude that $C_{r,l} \subseteq A_r \,\dot{\sqcup\!\sqcup}\, B_l$ and since A_r, B_l are finite, this shows that $\mu_{r,l}$ has finite index.

That $A_r \sqcup\!\sqcup B_l$ is not sufficient to contain $C_{r,l}$ is shown by the following example, which is due to F. Baader (personal communication).

Let $\Sigma = \{ a, b \}$, $r = l = 2$. Then $aaabaaa \in C_{2,2}$, but for all $x, y \in \Sigma^*$ such that $aaabaaa \in x \sqcup\!\sqcup y$ we have $x \notin A_2$ or $y \notin B_2$.

The next theorem shows that $C_{r,l}$ in fact is a system of shortest representatives for $\mu_{r,l}$.

THEOREM 3.4 : *Each $\mu_{r,l}$-class has a unique shortest representative.*

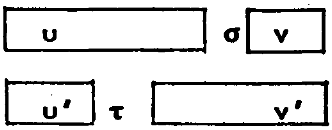
Proof : We show that again $M_{r,l}$ is a confluent Semi-Thue-System.

Let $w \in \Sigma^*$ be arbitrary, $w = u\sigma v = u'\tau v'$ and

$$(u\sigma, u) \in R_r,\ (\sigma v, v) \in L_l,\ (u'\tau, u') \in R_r,\ (\tau v', v') \in L_l\,.$$

This means : $(u\sigma v, uv) \in M_{r,l}$ and $(u' \tau v', u' v') \in M_{r,l}$.

We have to show : uv and $u' v'$ have a common descendent.
Let us suppose u' is a prefix of u :



$$uv = u' \tau u'' v$$

$$u'v' = u' u'' \sigma v$$

From $(u' \tau, u') \in \rho_r$ we derive

$$(u' \tau u'', u' u'') \in \rho_r ,$$
$$(u' u'' \sigma, u' \tau u'' \sigma) \in \rho_r$$
$$u' u'' \sigma = u\sigma$$
$$(u\sigma, u) \in \rho_r$$
$$u = u' \tau u''$$
$$(u' \tau u'', u' u'') \in \rho_r .$$

The chain implies $(u' u'' \sigma, u' u'') \in \rho_r$. Since $(\sigma v, v) \in \lambda_l$, together with lemma 1.4 we obtain $(u' u'' \sigma v, u' u'' v) \in M_{r,l}$.

Similarly from $(\sigma v, v) \in \lambda_l$ we derive $(u'' \sigma v, u'' v) \in \lambda_l$,

$$(\tau u'' v, \tau u'' \sigma v) \in \lambda_l$$
$$\tau u'' \sigma v = \tau v'$$
$$(\tau v', v') \in \lambda_l$$
$$v' = u'' \sigma v$$
$$(u'' \sigma v, u'' v) \in \lambda_l$$

and obtain $(\tau u'' v, u'' v) \in L_l$. Since $(u' \tau, u') \in R_r$ we also have $(u' \tau u'' v, u' u'' v) \in M_{r,l}$ and $u' u'' v$ is a common descendent of uv and $u' v'$.

Remark 3.5 : The proof of lemma 3.3 shows :

$$A_r . B_l \subseteq C_{r,l} \subseteq A_r \,\dot{\sqcup\!\sqcup}\, B_l .$$

The inclusions are strict in general.

For $r = 2$, $l = 2$ we have

$aaba \in A_2$, $abab \in B_2$, thus
$aaabab ab \in A_2 \;\dot{\sqcup\!\sqcup}\; B_2$, but
aaababab is reducible to *aababab* in $\mu_{2,2}$.

For $r = 1$, $l = 1$ we have $A_1 . B_1 \neq C_{1,1}$, e.g. $aabb \in C_{1,1} \quad A_1 . B_1$.

Example 3.6 :

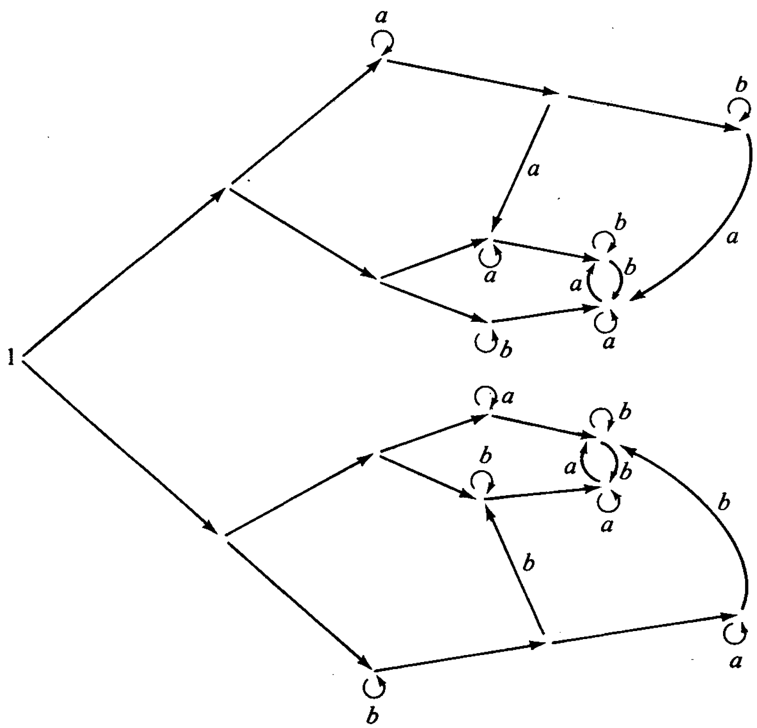
$$C_{11} \subseteq A_1 \;\dot{\sqcup\!\sqcup}\; B_1 , \quad \Sigma = \{ a, b \}$$

$$A_1 = \{ \Lambda, a, b, ab, ba \} , \quad B_1 = \{ \Lambda, a, b, ab, ba \} = A_1$$

$$A_1 \sqcup\!\sqcup B_1 = \{ \Lambda, a, b, a^2, ab, ba, b^2, aab, aba, baa, bab, abb, bba, abab, aabb, abba, bbaa, baab, baba \}$$

$$= C_{1,1} \text{ (in this case)} .$$

Thus the monoid Σ^*/μ_{11} is isomorphic to



Similarly as in remark 2.14 this monoid also presents an automaton deciding the word problem in Σ^*/μ_{11} and describing the equivalence classes by regular expressions.

The function $g : \Sigma^* \to \Sigma^*$ associating to every word $u \in \Sigma^*$ its shortest representative irr (u) with respect to $\mu_{r,l}$ is realized by the following bimachine (see [0] for the definition of a bimachine) :

Take A_r and B_l as state sets and next-state functions

$$u.\sigma = \begin{cases} u\sigma, & \text{if} \quad u\sigma \in A_r \\ u, & \text{if} \quad u\sigma \notin A_r \end{cases} \quad (\sigma \in \Sigma, u \in A_r)$$

and

$$\sigma.v = \begin{cases} \sigma v, & \text{if} \quad \sigma v \in B_l \\ v, & \text{if} \quad \sigma v \notin B_l \end{cases} \quad (\sigma \in \Sigma, v \in B_l).$$

The output function γ is defined as

$$\gamma(u, \sigma, v) = \begin{cases} \sigma, & \text{if} \quad u\sigma \in A_r \quad \text{or} \quad \sigma v \in B_l \\ \Lambda, & \text{else}. \end{cases}$$

This bimachine produces for every input $u \in \Sigma^*$ the output irr $(u) = \gamma(\Lambda, u, \Lambda)$.

COROLLARY 3.7 : *For arbitrary $r, l \geqslant 0$ the monoid $\Sigma^*/\mu_{r,l}$ has a decidable word problem.*

Let **V** denote the following class of monoids :

$$M \in \mathbf{V} \Leftrightarrow M \cong \Sigma^*/\rho \quad \text{for some finite alphabet } \Sigma \text{ and there is some}$$
$$k \in \mathbb{N} \quad \text{such that} \quad \mu_{kk} \subseteq \rho.$$

Then **V** is an M-variety ([4]) and we have :

PROPOSITION 3.8 :

$$\mathbf{R} \vee \mathbf{L} \subseteq \mathbf{V} \subseteq \mathbf{Ap}.$$

Proof : $\mathbf{R} \vee \mathbf{L} \subseteq \mathbf{V}$, since $\mu_{kk} \subseteq \rho_k \cap \lambda_k$.
For $\sigma \in \Sigma$ we have $(\sigma^{2k+1}, \sigma^{2k}) \in \mu_{kk}$.
Since μ_{kk} is fully invariant, $x^{2k+1} = x^{2k}$ is an equation which holds in Σ^*/μ_{kk}.
This shows $\mathbf{V} \subseteq \mathbf{Ap}$.

THEOREM 3.9 : **V** *is decidable.*

Proof: Let $M \simeq \Sigma^*/\rho$ and $|M| = r$. We show :

$$M \in \mathbf{V} \quad \text{iff} \quad \mu_{r,r} \subseteq \rho.$$

The implication from right to left being trivial, we suppose $M \in \mathbf{V}$, which means $\rho \supseteq \mu_{k,k}$ for some $k \in \mathbb{N}$. We can choose $k \leqslant r$: Let $(u\sigma v, uv) \in M_{r,r}$, i.e. $u = u_1 \dots u_r$, $v = v_r \dots v_1$ such that

$$(*) \quad \alpha(u_1) \supseteq \dots \supseteq \alpha(u_r) \ni \sigma \in \alpha(v_r) \subseteq \dots \subseteq \alpha(v_1).$$

Considering the sequences $u_0 = 1, u_1, u_1 u_2, \dots, u_1 \dots u_r$ and $v_r \dots v_1$, $v_{r-1} \dots v_1, \dots, v_1$, $v_0 = 1$ we can find i, j, h, l such that $0 \leqslant i < j \leqslant r$ and $0 \leqslant h < l \leqslant r$ and $u_0 u_1 \dots u_i = u_0 u_1 \dots u_i u_{i+1} \dots u_j$ and

$$v_h v_{h-1} \dots v_0 = v_l v_{l-1} \dots v_{h+1} v_h \dots v_0 .$$

The inclusions (*) imply :

$$((u_{i+1} \dots u_j)^k u_{j+1} \dots u_r \sigma v_r \dots v_{l+1}(v_l \dots v_{h+1})^k ,$$
$$(u_{i+1} \dots u_j)^k u_{j+1} \dots u_r v_r \dots v_{l+1}(v_l \dots v_{h+1})^k) \in \mu_{kk}$$

and since $\mu_{kk} \subseteq \rho$ we have in M :

$$\begin{aligned} uv &= u_0 \dots u_i(u_{i+1} \dots u_j) u_{j+1} \dots u_r v_r \dots v_{l+1}(v_l \dots v_{h+1}) v_h \dots v_0 \\ &= u_0 \dots u_i(u_{i+1} \dots u_j)^k u_{j+1} \dots u_r v_r \dots u_{l+1}(v_l \dots v_{h+1})^k v_h \dots v_0 \\ &= u_0 \dots u_i(u_{i+1} \dots u_j)^k u_{j+1} \dots u_r \sigma v_r \dots v_{l+1}(v_l \dots v_{h+1})^k v_h \dots v_0 \\ &= u\sigma v . \end{aligned}$$

Therefore $(u\sigma v, uv) \in \rho$ and we obtain

$$\mu_{rr} \subseteq \rho .$$

There are some open questions concerning the M-Variety $\mathbf{V}$:

1) Find a sequence of equations which ultimately defines $\mathbf{V}$.
2) Find other algebraic characterisations of $\mathbf{V}$.
3) Is $\mathbf{R} \vee \mathbf{L} \neq \mathbf{V}$?
4) Characterize those L with $M(L) \in \mathbf{V}$.

REFERENCES

[0] J. Berstel, *Transductions and Context-free Languages*. Teubner, 1979.

[1] J. A. Brzozowski, F. E. Fich, *Languages of $\mathcal{R}$-trivial Monoids*. Res. Rep. CS-78-32, Waterloo, 1978.

[2] S. Eilenberg, *Automata, Languages and Machines*. Vol. B, Academic Press, 1979.

[3] F. E. Fich, *Languages of $\mathcal{R}$-trivial and Related Monoids*. Res. Rep. CS-79-18, Waterloo, 1979.

[4] R. König, *Beiträge zur algebraischen Theorie der formalen Sprachen*. Dissertation, Erlangen, 1983.

[5] M. Lothaire, *Combinatorics on words*. Addison-Wesley, 1983.

[6] R. C. Lyndon, *On Burnside's Problem*. Trans. AMS 77, 1954.

[7] I. Simon, *Hierarchies of Events with Dot-Depth One*. Ph. D. thesis, Waterloo, 1972.

[8] I. Simon, *Piecewise testable events*. LNCS 33, Springer Berlin 1975, 214-222.