ROMAN KÖNIG

Reduction algorithms for some classes of aperiodic monoids


<http://www.numdam.org/item?id=ITA_1985__19_3_233_0>
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 $A$-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 monôides finis $A$-triviaux et qui fournit un algorithme pour dénier 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 $\mathfrak{g}$-trivial syntactic monoid. In 1978 [1] and 1976 [2] his ideas have been modified to yield a characterization of those languages with an $A$-trivial syntactic monoid.

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

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

(*) Received in February 1984, revised in September 1984.

(1) Institut für Mathematische Maschinen und Datenverarbeitung I Martensstraße 3, D-8520 Erlangen, FRG.
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 $R \lor L$ and $Ap$, 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 $R$-trivial, $L$-trivial and $J$-trivial monoids respectively. We first recall some definitions and facts:

**Définition 1.1**: Let $M$ be a monoid. $M$ is called

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

The classes $R$, $L$ and $J$ of all finite $R$-trivial, $L$-trivial and $J$-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. $R$ 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 $R$ iff there is some $k \in \mathbb{N}$ such that $(xy)^k x = (xy)^k$ holds in $M$. Similarly $L$ is ultimately defined by $x(yx)^k = (yx)^k$ and $J$ is ultimately defined by $(xy)^k x = (xy)^k y(xy)^k$. Notice that $J = R \cap L$.

A congruence relation $\rho$ on a monoid $M$ is called fully invariant, if for each endomorphism $f : M \rightarrow M (u, v) \in \rho$ 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 $\Delta_M$, the maximal $\Omega_M$. The subscripts are omitted, if the monoid $M$ is clear from the context. For a finite alphabet $\Sigma$ and a subset $L$ of $\Sigma^*$, the free monoid generated by $\Sigma$, denote by $\sigma_L$ 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 $\Sigma^*/\sigma_L$ 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

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

\[
L_k := \{ (\sigma u, u) \mid (u', \sigma, u') \in R_k \}, \text{ where } u' \text{ denotes the reversal of a word } u \in \Sigma^*.
\]

\( \rho_k (\lambda_k \text{ resp.}) \) denotes the congruence relation on \( \Sigma^* \) generated by \( R_k \) \((L_k \text{ resp.)})\).

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 \( \rho_k \) \((\lambda_k \text{ resp.)})\) (we say \( L \) is \( \rho_k \)-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 \( u, v \in \Sigma^* \neq v \) 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 \( u_1 \ldots u_s \) the following decomposition of \( u\sigma \) as a product of non-empty words:

For every \( i = 1, \ldots, s \), \( u_i \) is the shortest prefix of \( u_1 \ldots u_s \), which contains every letter of \( u_1 \ldots u_s : \alpha(u_i) = \alpha(u_i \ldots u_s) \).

If we assume \( s < k \), then no relation of \( R_k \) can be applied to \( u\sigma \). But \( R_k \) generates \( \rho_k \), so \( s \geq k \) follows. If \( u_1 \ldots u_k \) is not a prefix of \( u \), but \( u_1 \ldots u_k = u\sigma \), 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 \( u\sigma \), \( u_1 \ldots u_k \) has to be a prefix of \( u \) and we obtain a decomposition \( u = u_1 \ldots u_k w \) with

\[
\alpha(u_1) \supseteq \alpha(u_2) \supseteq \ldots \supseteq \alpha(u_{k-1}) \supseteq \alpha(u_k w) \ni \sigma \text{ and } (u\sigma, u) \in R_k \text{ follows}.
\]
LEMMA 1.5: $\rho_k$ and $\lambda_k$ are fully invariant congruence relations on $\Sigma^*$ of finite index.

Proof: Since $\rho_k$ is generated by $R_k$, it is sufficient to prove:

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

Let $f(\sigma) \neq \Lambda$ since otherwise we are done. From $u = u_1 \ldots u_k$ with $\alpha(u_1) \supset \ldots \supset \alpha(u_k) \in \sigma$ follows $\alpha(f(u_1)) \supset \ldots \supset \alpha(f(u_k)) \supset \alpha(f(\sigma))$.

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

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

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

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

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

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

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 $w: \alpha(u) = \alpha(w), w = uw$.

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

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

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

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

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

For the opposite inclusion let $u \in A_{k,\Sigma - \sigma}, v \in A_{k-1,\Sigma}$ 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 $u \notin A_{k,\Sigma - \sigma}$, contrary to our assumption.

If it occurs in $v$ then we have a decomposition

$$w = w_1 w_2 \ldots w_k \tau w', \text{ where } \alpha(w_1) = \alpha(w),$$

$$\alpha(w_1) \supset \ldots \supset \alpha(w_k) \in \tau.$$ 

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

Now $(w_2 \ldots w_k \tau, w_2 \ldots w_k) \in R_{k-1}$, 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) \( M(L) \in R \).

**Proof:** Let \( L \) be right-testable, i.e. \( L \) is \( \rho_k \)-saturated for some \( k \in \mathbb{N} \). Then \( \rho_k \subseteq \pi_L \) and since \( \rho_k \) is a congruence relation, \( \rho_k \subseteq \sigma_L \). Since \( \rho_k \) is fully invariant, each relation in \( \Sigma^*/\rho_k \) is a law in \( \Sigma^*/\rho_k \). 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 \( \Sigma^*/\rho_k \). (If \( \Sigma \) consists of one letter \( \sigma \) 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 \( R \)-trivial monoid).

Since \( (xy)^k x = (xy)^k \) ultimately defines \( R \), \( \Sigma^*/\rho_k \in R \) and \( \rho_k \subseteq \sigma_L \) implies

\[
M(L) \in R
\]

Now let \( L \subseteq \Sigma^* \) and \( M(L) \in R \).

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.

\[
(u \sigma, u) \in R_k \quad \text{means} \quad u = u_1 ... u_k, \alpha(u_1) \supseteq ... \supseteq \alpha(u_k) \ni \sigma.
\]

Consider the sequence of words

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

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 :

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

Then we have the conclusion

\[
(w_p, w_i \sigma) \in \pi \quad \text{for all} \quad \sigma \in \alpha(u_{i+1})
\]

\[
\Rightarrow (w_i \tau, w_i \sigma \tau) \in \pi \quad \text{(since} \pi \text{is a congruence relation)}
\]

\[
\Rightarrow (w_p, w_i \sigma \tau) \in \pi
\]
Since \( \alpha(u_{i+1}) \supseteq \alpha(u_{i+2}) \supseteq \ldots \supseteq \alpha(u_k) \supseteq \sigma \) we infer

\[
(w_p, w_k) \in \pi \\
(w_p, w_{k+1}) \in \pi
\]

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

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

\[
w_{i+1} = w_i \nu \nu' (v, v' \in \Sigma^*)
\]

Now

\[
\bar{w}_i M \supseteq \bar{w}_i v M \supseteq \bar{w}_i \nu \tau M \supseteq \bar{w}_j M.
\]

Since \(\bar{w}_i = \bar{w}_j\) we have equality everywhere in the line above. But \(M \in R\) so we get

\[
\bar{w}_i = \bar{w}_i \nu = \bar{w}_i \nu \tau
\]

from where we conclude

\[
\bar{w}_i = \bar{w}_i \tau, \text{ i.e. } (w_p, w_i \tau) \in \sigma_L.
\]

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) \(M(L) \in J\).

**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

\[
M(L) \in R \cap L = J.
\]

Now let \(M(L) \in R \cap L\). 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) \(M(L) \in R \lor L\).

**Proof**: Let \(\rho_k \cap \lambda_k \subseteq \sigma_L\). This means \(\Sigma^*/\sigma_L\) is a homomorphic image of a subdirect product of \(\Sigma^*/\rho_k\) and \(\Sigma^*/\lambda_k\). Since \(\Sigma^*/\rho_k \in R, \Sigma^*/\lambda_k \in L\), we obtain

\[
M(L) \in R \lor L.
\]
Now let $M(L) \in \mathbb{R} \vee L$. There are finite alphabets $\Gamma$, $\Theta$ and congruence relations $\gamma$ on $\Gamma^*$, $\theta$ on $\Theta^*$ such that for some $k \in \mathbb{N}$
\[
\rho_{k,\Gamma} \leq \gamma \\
\lambda_{k,\Theta} \leq \theta
\]
and
\[
\Gamma^*/\gamma \times \Theta^*/\theta \xrightarrow{\pi_1} M(L)
\]
We can assume $\Gamma \cap \Theta = \emptyset$.

The homomorphism
\[
(\Gamma \cup \Theta)^* \xrightarrow{(f_1,f_2)} \Gamma^*/\gamma \times \Theta^*/\theta
\]
defined by
\[
\sigma f_1 \begin{cases} 
\sigma, & \text{if } \sigma \in \Gamma \\
\Lambda, & \text{if } \sigma \in \Theta
\end{cases} \\
\sigma f_2 \begin{cases} 
\sigma, & \text{if } \sigma \in \Theta \\
\Lambda, & \text{if } \sigma \in \Gamma
\end{cases}
\]
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 $\rho_k$ and $\lambda_k$ are fully invariant we obtain
\[
\rho_{k,X} \leq f_1 \circ \rho_{k,\Gamma} \circ f_1^{-1} \leq f_1 \circ \gamma \circ f_1^{-1} \leq \gamma' \\
\lambda_{k,X} \leq f_2 \circ \lambda_{k,\Theta} \circ f_2^{-1} \leq f_2 \circ \theta \circ f_2^{-1} \leq \theta'
\]
and
\[
\rho_{k,X} \cap \lambda_{k,X} \leq \gamma' \cap \theta' \text{ follows .}
\]

There are a congruence relation $\beta$ on $X^*$ such that $X^*/\beta \simeq M(L)$ and $\gamma' \cap \theta' \leq \beta$ and $f : \Sigma^* \rightarrow X^*$ making
\[
\begin{array}{ccc}
\Sigma^* & \rightarrow & X^* \\
\downarrow & & \downarrow \\
M(L) & \cong & X^*/\beta
\end{array}
\]
vol. 19, no 3, 1985
commutative. Now
\[ \sigma_L = \alpha \beta \sigma^{-1} \cong \alpha \beta (\rho_{k,X} \cap \lambda_{k,X}) \sigma^{-1} \cong \alpha \beta \rho_{k,X} \sigma^{-1} \cap \alpha \beta \lambda_{k,X} \sigma^{-1} \cong \rho_{k,\Sigma} \cap \lambda_{k,\Sigma} . \]

**Corollary 1.10:** Let \( M = \Sigma^*/\rho \) be a finite monoid.

1. \( M \in R \iff \exists k \rho_k \subseteq \rho \)
2. \( M \in L \iff \exists k \lambda_k \subseteq \rho \)
3. \( M \in J \iff \exists k \rho_k \vee \lambda_k \subseteq \rho \)
4. \( M \in R \lor L \iff \exists k \rho_k \cap \lambda_k \subseteq \rho \).

2. SOME COMBINATORIAL PROPERTIES OF \( \rho_k \) AND \( \lambda_k \)

The congruence relations \( \rho_k \) and \( \lambda_k \) have some nice combinatorial properties, which allow a very detailed description of the monoid \( \Sigma^*/\rho_k \). The most important of these is:

**Lemma 2.1:** Every \( \rho_k \)-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 \( \rho_k \)-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 \( k \geq 1 \), \( w = u\sigma v = u' \tau v' \) 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.

\[
\begin{array}{c}
\text{u} \\
\tau \\
\text{z} \\
\text{v} \\
\sigma \\
\end{array}
\]

We want to prove
\[(uw, u'zv) \in \rho_k \quad \text{and} \quad (u'v', u'zv) \in \rho_k . \]

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 \( \alpha(u_1') \supseteq \ldots \supseteq \alpha(u_k') \) \( \tau \) and so cancelling this occurrence of \( \tau \) 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 \( u' \).

\[
\begin{align*}
  u &= u_0 v_0 \\
  u' &= u_0 v'_0 .
\end{align*}
\]

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

\[
(u' v', u' z v) \in \rho_k .
\]

**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 \( \text{irr}(w) \) of a given \( w \in \Sigma^* \) and thus a decision procedure for the word problem in \( \Sigma^*/\rho_k \):

```
input w

w:=longest irreducible prefix of w

w=u? yes irr(w):=u

no w = uσv (σ∈Σ)

w := uv
```

vol. 19, n° 3, 1985
(2) The considerations under (1) show the significance of knowing the set of all irreducible words over $E$ relative to $R_k$.

(3) The set $A_{k,\Sigma}$ of all irreducible words over $\Sigma$ 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: $k = 3$

\[
\begin{align*}
\text{w = } & a a b a a a a b a b b a = a a b a a a b a b b a \\
& u_1 u_2 u_3 \quad \text{v}_3 \quad \text{v}_2 \quad \text{v}_1 \\
\end{align*}
\]

\[
\begin{align*}
& a a b a a b a b b a \\
& u_1 u_2 u_3 \quad \text{v}_3 \quad \text{v}_2 \quad \text{v}_1 \\
& \quad \text{v}_3 \quad \text{v}_2 \quad \text{v}_1 \\
\end{align*}
\]

\[
\begin{align*}
& a a b a a b a b b a \\
& u_1 u_2 u_3 \quad \text{v}_3 \quad \text{v}_2 \quad \text{v}_1 \\
& \quad \text{v}_3 \quad \text{v}_2 \quad \text{v}_1 \\
\end{align*}
\]

\[
\begin{align*}
& a a b a a b a b b a \\
& u_1 u_2 u_3 \quad \text{v}_3 \quad \text{v}_2 \quad \text{v}_1 \\
\end{align*}
\]

\[
\begin{align*}
& a a b a a b a b b a \\
& u_1 u_2 u_3 \quad \text{v}_3 \quad \text{v}_2 \quad \text{v}_1 \\
\end{align*}
\]

\[
\begin{align*}
& a a b a a b a b b a \\
& u_1 u_2 u_3 \quad \text{v}_3 \quad \text{v}_2 \quad \text{v}_1 \\
\end{align*}
\]

\[
\begin{align*}
& a a b a a b a b b a \\
& u_1 u_2 u_3 \quad \text{v}_3 \quad \text{v}_2 \quad \text{v}_1 \\
\end{align*}
\]

\[
\begin{align*}
& a a b a a b a b b a \\
\end{align*}
\]

\[
\begin{align*}
& a b a b a b b a \\
\end{align*}
\]

\[
\begin{align*}
& a b a b a b b a \\
\end{align*}
\]

\[
\begin{align*}
& a b a b a b b a \\
\end{align*}
\]

\[
\begin{align*}
& a b a b a b b a \\
\end{align*}
\]

\[
\begin{align*}
& a b a b a b b a \\
\end{align*}
\]

$w \rho_3$-reduces to $aabaabab$ and $\lambda_3$-reduces to $ababba$. In each step the word $u_1 u_2 u_3$ is the maximal $\lambda_3$-reduced prefix and $v_3 v_2 v_1$ is the maximal $\lambda_3$-reduced suffix.

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

\[
\{ \Lambda \} \cup \bigcup_{\sigma \in \Sigma} A_{k,\Sigma} \rightarrow \sigma \cdot A_{k-1,\Sigma}
\]

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 $\Sigma$ define

\[
D_{k,\Sigma} = \{ u \in A_{k,\Sigma} | \alpha(u) = \Sigma \},
\]

R.A.I.R.O. Informatique théorique/Theoretical Informatics
then
\[ D_{k,\phi} = \{ \Lambda \} , \quad D_{0,\Sigma} = \emptyset (k \geq 0, \Sigma \neq \emptyset) \]

and
\[ D_{k,\Sigma} = \bigcup_{\sigma \in \Sigma} (D_{k,\Sigma - \sigma} \cdot \sigma \cdot \bigcup_{\Sigma' \subseteq \Sigma} D_{k-1,\Sigma'}) (\Sigma \neq \emptyset, k \geq 1) \]

and all unions are disjoint.

Proof:
(1) If \( \Sigma \neq \Sigma' \), then \( D_{k,\Sigma} \cap D_{k,\Sigma'} = \emptyset(k \geq 0) \).
(2) \( A_{k,\Sigma} = \bigcup_{\Sigma' \subseteq \Sigma} D_{k,\Sigma'} \) is a disjoint union for all \( k \geq 0 \).
(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
\[ \sigma \in \Sigma, u' \in D_{k,\Sigma - \sigma} \quad \text{and} \quad v \in A_{k-1,\Sigma} \text{ and so} \]
\[ D_{k,\Sigma} \subseteq \bigcup_{\sigma \in \Sigma} (D_{k,\Sigma - \sigma} \cdot \sigma \cdot A_{k-1,\Sigma}) \text{ follows}. \]

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

Let \( a_{k,n} := |A_{k,\Sigma}| \) for an \( n \)-letter alphabet \( \Sigma \), \( k \geq 0 \)
and \( d_{k,n} := \frac{|D_{k,\Sigma}|}{n!} \) for an \( n \)-letter alphabet \( \Sigma \), \( k \geq 0 \).

Since permuting the letters of \( \Sigma \) preserves reducedness,
\[ |D_{k,\Sigma}| \text{ is divisible by } n! \text{ if } \Sigma \text{ consists of } n \text{ letters}. \]

**Corollary 2.5:**
(1) \( d_{1,n} = 1 = d_{k,0} (k \geq 0, n \geq 0) \), \( d_{0,n} = 0 (n > 0) \).
(2) \( d_{k,n} = d_{k,n-1} \cdot \sum_{r \leq n} (n)_r \cdot d_{k-1,r} (k > 0, n > 0) \)
(3) \( a_{k,n} = \frac{d_{k+1,n}}{d_{k+1,n-1}} (k \geq 0, n > 0) \)

where \( (n)_r \) denotes falling factorials:
\[ (n)_r = n \cdot (n - 1) \cdot \ldots \cdot (n - r + 1) \, . \]
Proof: To see (1), observe that
\[ D_{k,\Phi} = \{ \Lambda \} \quad (k \geq 0), \quad D_{0,\Sigma} = \emptyset \quad (\Sigma \neq \emptyset) \]
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 \( k \geq 1, n > 0 \)
\[ n! \cdot d_{k,n} = n! \cdot (n - 1)! \cdot d_{k,n-1} \cdot \sum_{r \leq n} \binom{n}{r} r! \cdot d_{k-1,r}, \]
from which (2) follows.

(3) From the proof of the lemma follows
\[ a_{k,n} = \sum_{r \leq n} \binom{n}{r} r! \cdot d_{k,r} \]
\[ = \sum_{r \leq n} (n)_r \cdot d_{k,r} = \frac{d_{k+1,n}}{d_{k+1,n-1}}. \]

Calculation of the first of these numbers gives the tables:

<table>
<thead>
<tr>
<th>( d_{k,n} )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>( n )</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>1</td>
<td>10</td>
<td>75</td>
<td>628</td>
<td>6325</td>
<td>75966</td>
<td>1063615</td>
<td>17017960</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>1</td>
<td>160</td>
<td>77025</td>
<td>290519080</td>
<td>1063615</td>
<td>17017960</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>1</td>
<td>10400</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>1</td>
<td>3390400</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( a_{k,n} )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>5</td>
<td>25</td>
<td>157</td>
<td>1265</td>
<td>12661</td>
<td>151945</td>
<td>2127245</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>16</td>
<td>1027</td>
<td>462610</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>65</td>
<td>253569</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>326</td>
<td>40810581</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>1957</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>13700</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>109601</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>986410</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
To give an example, let $k = 2$, $\Sigma = \{ a, b \}$. Since $d_{2,2} = 10$, $d_{2,1} = 2$, $d_{2,0} = 1$

\[ \Lambda \]
\[ a, a^2 \]
 \[ \text{ab, aab, aba, aaba, abb, aabb, abab, aabab, abba, aabba} \]

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

\[ Q_{0,\Sigma} = \{ \Lambda \}, \quad Q_{k,\Phi} = \{ \Lambda \} \text{ and for } k \geq 1, \quad \Sigma \neq \emptyset \]
\[ Q_{k,\Sigma} = \bigcup_{\sigma \in \Sigma} Q_{k,\Sigma-\sigma \cdot \sigma} Q_{k-1,\Sigma} \]
\[ Q_{k,\Sigma} = \bigcup_{(\sigma_1, \ldots, \sigma_k) \in \Sigma^k} Q_{k,\Sigma-\sigma_1 \cdot \sigma_2 \cdot \sigma_2 \cdots \sigma_{k-1,\Sigma-\sigma_k} \sigma_k} . \]

Moreover

\[ l_{k,n} = \binom{n+k}{k} - 1 \quad (k \geq 0, n \geq 0) . \]

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

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

If $u \notin Q_{k,\Sigma-\sigma}$, then an arbitrary $u' \in Q_{k,\Sigma-\sigma}$ 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 $\leq k + n - 1$ 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 \( \rho_k \):

**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 \( \rho_k \). 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

\[
n^{l_{k,n}+1} = n\binom{n+k}{k}
\]

pairs in the generating system.

Next we study the set of idempotents in \( \Sigma^*/\rho_k \).

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

\[
w = u_1 \ldots u_k \quad \text{with} \quad \alpha(u_1) = \ldots = \alpha(u_k).
\]

**Proof**: If \( w = u_1 \ldots u_k \) with \( \alpha(u_1) = \ldots = \alpha(u_k) \) then for each \( \sigma \in \alpha(w) \) one has

\[
\alpha(u_1) \supseteq \ldots \supseteq \alpha(u_k) \ni \sigma.
\]

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 \( w = w_1 \ldots w_k \), where \( w_i \) is the shortest prefix of \( w_i \ldots w_k \), which contains all the letters of \( w_i \ldots w_k \). Since \((w^2, w) \in \rho_k\), we have \( \alpha(w_1) \supseteq \ldots \supseteq \alpha(w_k) \supseteq \alpha(w_1) \), from where the desired equality follows.

**Corollary 2.9**: Let \( w \in \Sigma^* \). Then

\[
(w^2, w) \in \rho_k \iff (w^2, w) \in \lambda_k \iff (w^2, w) \in \rho_k \cap \lambda_k.
\]
Remark and Example 2.10:

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

$$F_{r, \Sigma} = \{ w \in \Sigma^* | (w^2, w) \in \rho_r \}$$

$$F_{r, \Sigma} = \{ w \in \Sigma^* | (w^2, w) \in \rho_r, \alpha(w) = \Sigma \}$$

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

vol. 19, no 3, 1985
Lemma 2.11: \( E_{k,\phi} = D_{k,\phi} = \{ \Lambda \} (k \geq 0) \)

\[ E_{0,\Sigma} = D_{0,\Sigma} = \emptyset \quad (\Sigma \neq \emptyset) \]

\[ E_{k,\Sigma} = \bigcup_{\sigma \in \Sigma} D_{k,\Sigma - \sigma} \cdot E_{k-1,\Sigma} \quad (k \geq 1, \Sigma \neq \emptyset) \]

Let \( e_{k,n} := \frac{|E_{k,\Sigma}|}{n!} \) for some \( \Sigma \) with \( |\Sigma| = n \).

Then

\[
\begin{align*}
  e_{k,0} &= 1 \quad (k \geq 0) \\
  e_{0,n} &= 0 \quad (n \geq 1) \\
  e_{k,n} &= n! \cdot d_{k,n-1} \cdot e_{k-1,n} \quad (k \geq 1, n \geq 1).
\end{align*}
\]

Proof: Obviously \( E_{k,\phi} = \{ \Lambda \} \) for \( k \geq 0 \) and \( E_{0,\Sigma} = \emptyset \) for all \( \Sigma \neq \emptyset \).

Let \( w \in E_{k,\Sigma} \) \( (k \geq 1, \Sigma \neq \emptyset) \) 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

\[
v = v_1 \ldots v_{k-1} \quad \text{with} \quad \alpha(v_1) = \cdots = \alpha(v_{k-1}).\]

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 \( k, \Sigma \), we have \( u \sigma v \in D_{k,\Sigma} \). Moreover \( v \) has a factorisation \( v = v_1 \ldots v_{k-1} \) 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

\[
n! e_{k,n} = n \cdot (n - 1)! \cdot d_{k,n-1} \cdot n! e_{k-1,n}
\]

from where the formula follows.

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

<table>
<thead>
<tr>
<th>( e_{k,n} )</th>
<th>( k \rightarrow )</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
</tr>
<tr>
<td>( n )</td>
<td>0</td>
</tr>
<tr>
<td>( \downarrow )</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>5</td>
</tr>
</tbody>
</table>

R.A.I.R.O. Informatique théorique/Theoretical Informatics
Remark 2.12

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

2. The monoid \( \Sigma^*/\rho_k \) is isomorphic to the set \( A_{k,\Sigma} \) together with the operation \( u \cdot v = \text{irr}(uv) \), where \( \text{irr}(uv) \) 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 \( \Sigma^*/\rho_k \) can now be solved by the following algorithm:
   (a) Generate \( A_{k,\Sigma} \)
   (b) Consider \( A_{k,\Sigma} \) as a \( \Sigma \)-automaton with state-set \( A_{k,\Sigma} \) and operations

\[
u \cdot \sigma = \begin{cases} u\sigma, & \text{if } u\sigma \in A_{k,\Sigma} \\ u & \text{if } u\sigma \notin A_{k,\Sigma} \end{cases}
\]

where \( u \in A_{k,\Sigma}, \sigma \in \Sigma \)
   (c) Two words \( v, w \in \Sigma^* \) are \( \rho_k \)-equivalent, iff \( \Lambda \cdot v = \Lambda \cdot w \) 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 \( \Sigma^*/\rho_k \) is the following graph:
(3) If we add the following output function to this automaton

\[ u \ast \sigma = \begin{cases} \Lambda, & \text{if } u.\sigma = u \\ \sigma, & \text{if } u.\sigma = u\sigma \end{cases} \]

we obtain a sequential transducer which realizes the function \( f : \Sigma^* \to \Sigma^* \) which associates to every word \( u \in \Sigma^* \) its shortest representative \( \text{irr}(u) \). This shows that \( f \) is a sequential function.
(4) Analogously $\Sigma^*/\lambda_k$ is presented by the following graph:

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

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

vol. 19, n° 3, 1985
Theorem 2.16: Let $M$ be a monoid of cardinality $m$ with generating system $\Sigma \subseteq M$. The following properties are equivalent:

1. $M \in \mathbb{R}$
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 $x, y \in M$ \{ 1 \} $(xy)^k x = (xy)^k$ or $(yx)^k y = (yx)^k$ in $M$.

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

(3) $\Rightarrow$ (1): Let $a, b \in M$, $(a, b) \in \mathbb{R}$. There are $x, y \in M$ such that $ax = b$, $by = a$. If $x = 1$ or $y = 1$ then $a = b$. Hence let $x, y \in M \setminus \{ 1 \}$. 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 $M \in \mathbb{R}$.

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

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

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

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

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

Now

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

and

$$((xy)^t x, (xy)^t) \in \mathbb{R}. \text{ Since } M \in \mathbb{R}, (xy)^t x = (xy)^t,$$

and

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

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

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

Right-multiplication with $x$ gives case 1.

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

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

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

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

$$(xy)^t = (xy)^t (xy)^{-s}$$

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

R.A.I.R.O. Informatique théorique/Theoretical Informatics
and we obtain \(((xy)^t, x, (xy)^t) \in \mathcal{R}\). The rest follows as in case 1.

**Case 4** : \( \exists s, t \leq k, s < t \)

\[(xy)^s x = (xy)^t \].

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

![Diagram](attachment:image.png)

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 \( M \in W \). It is clear, that \( V \cap W \) 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 \( \Sigma \) such that \( M \cong \Sigma^*/\rho \) for some congruence relation \( \rho \) and \( R_k \cup L_k \subseteq \rho \).

Unfortunately the union of the reduction systems for \( \rho_k \) and \( \lambda_k \) does not give a confluent Semi-Thue-System:

Let \( \Sigma = \{ a, b \}, \ k = 2, \ w = ababa \).

\( abab \) and \( baba \) are both \( \rho_2 \lor \lambda_2 \)-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 \( R_k \lor L_k \).

In [1], the \( M \)-variety \( R \) is characterized by the sequence \( n \sim_R \) of congruence relations on \( \Sigma^* \) defined in the following way: Put

\[ n \sim := \{ (u, v) \mid \forall w \in \Sigma^n \ u \in w \quad \Sigma^* \Leftrightarrow v \in w \ 1 \Sigma^* \} \].

and

\[ n \sim_R := \{ (u, v) \mid \text{for every prefix } a \text{ of } u \text{ there is a prefix } b \text{ of } v \text{ such that } a \sim b \text{ and for every prefix } b \text{ of } v \text{ there is a prefix } a \text{ of } u \text{ such that } a \sim b \} \].

vol. 19, n° 3, 1985
Although \( n \sim R \) and \( \rho_n \) are defined in completely different ways, we can prove:

\[ n \sim R = \rho_n \text{ for every natural } n. \]

For this purpose consider the algorithm which produces for every word \( w \in \Sigma^* \) the shortest representative \( x_n(w) \) 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 \( u\sigma_n \sim R u \) iff \( (u\sigma, u) \in R_n \) and \( n \sim R = \rho_n \) follows.

### 3. COMMON GENERALIZATION OF \( \rho_k \) AND \( \lambda_k \)

In the definition of \( \rho_k \) 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 \( \lambda_k \) is just the left-right-dual of \( \rho_k \), a corresponding property holds for \( \lambda_k \). Therefore the following generalization is very natural:

**Definition 3.1:** For \( r, l \in \mathbb{N} \) and a finite alphabet \( \Sigma \) define

\[ M_{r,l} = \{ (u\sigma v, uw) \mid (u\sigma, u) \in R_r, (\sigma v, v) \in L_l \} \]

\[ \mu_{r,l} = \overline{M_{r,l}}, \text{ the congruence relation on } \Sigma^* \text{ generated by } M_{r,l}. \]

**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. \( (u\sigma v, uv) \in M_{r,l} \)
   \[ (xu\sigma uy, xuy) \in M_{r,l} \text{ for all } x, y \in \Sigma^*. \]

**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 \( A_r(B_p, C_{r,l} \text{ resp.}) \) be the set of irreducible words over \( \Sigma \) relative to \( \rho_r(\lambda_p, \mu_{r,l} \text{ resp.}) \) and \( w \in C_{r,l} \). Thus for each \( \sigma \in \alpha(w) \), we have

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

Let \( \sigma_1, \ldots, \sigma_s \) be the sequence of letters of \( w \), for which \( w = u_i \sigma_i v_i \) and
(u_1, \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

\[ w = u'_1 \tau_1 v'_1 \text{ and } (\tau_i v'_i, v'_i) \notin L_1. \]

Now we have \sigma_1, \ldots, \sigma_s \in A_r since \((u_\tau, u) \in R_r \text{ and } (u\tau \sigma, u) \notin R_r\) imply \((u \sigma, u) \notin R_r\). A similar argument shows \tau_1, \ldots, \tau_t \in B_t.

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

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

\[
\begin{align*}
(S \cup \Sigma')^* & \xrightarrow{g} \Sigma^* \xrightarrow{\sigma \mapsto \sigma'} \Sigma' \\
(S \cup \Sigma')^*/\sigma \tau' &= \tau' \sigma
\end{align*}
\]

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

\[
\begin{align*}
A \bullet B := g(f^{-1} f(A.B')) & [2],
\end{align*}
\]

and for

\[
\begin{align*}
(S \cup \Sigma' \cup \Sigma'')^* & \xrightarrow{k} \Sigma^* \xrightarrow{\sigma \mapsto \sigma'} \Sigma' \xrightarrow{\sigma'' \mapsto \sigma''} \Sigma'' \\
(S \cup \Sigma' \cup \Sigma'')^*/\sigma \tau' &= \tau' \sigma \xrightarrow{\sigma \sigma' = \sigma''}
\end{align*}
\]

\(h\) the natural epimorphism, we define the amalgamated shuffle

\[
\begin{align*}
A \bullet B := k(h^{-1} h(A.B')).
\end{align*}
\]

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

From the consideration above we conclude that \(C_{r,t} \subseteq A_r \bullet B_t\) and since \(A_r, B_t\) are finite, this shows that \(\mu_{r,t}\) has finite index.

That \(A_r \bullet B_t\) is not sufficient to contain \(C_{r,t}\) is shown by the following example, which is due to F. Baader (personal communication).

Let \(\Sigma = \{ a, b \}, r = l = 2\). Then \(aaabaaa \in \Sigma_{2,2}\), but for all \(x, y \in \Sigma^*\) such that \(aaabaaa \in x \bullet y\) we have \(x \notin A_2\) or \(y \notin B_2\).

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

**Theorem 3.4:** Each \(\mu_{r,t}\)-class has a unique shortest representative.

**Proof:** We show that again \(M_{r,t}\) is a confluent Semi-Thue-System.

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

\[(u \sigma, u) \in R_r, (\sigma v, v) \in L_\rho, (u' \tau, u') \in R_r, (\tau v', v') \in L_1.\]

vol. 19, n° 3, 1985
This means: \((uw, uv) \in M_{r,l}\) and \((u' v', u' v') \in M_{r,l}\).

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

\[
\begin{array}{c}
\text{u} \\
\sigma \\
\text{v} \\
\end{array}
\quad
\begin{array}{c}
\text{u}' \\
\tau \\
\text{v}' \\
\end{array}
\]

\[uv = u' \tau u'' \sigma v\]
\[u'v' = u'u''\sigma v\]

From \((u' \tau, u') \in \rho\), we derive

\[
\begin{align*}
(u' \tau u'', u' u'') & \in \rho_r, \\
(u' u'' \sigma, u' \tau u'' \sigma) & \in \rho_r, \\
u' u'' \sigma & = u \sigma, \\
(u \sigma, u) & \in \rho_r, \\
u & = u' \tau u'' \\
(u' \tau u'', u' u'') & \in \rho_r.
\end{align*}
\]

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

Similarly from \((\sigma v, v) \in \lambda_t\) we derive \((u'' \sigma v, u'' v) \in \lambda_\eta\),

\[
\begin{align*}
(\tau u'' v, \tau u'' \sigma v) & \in \lambda_t, \\
\tau u'' \sigma v & = \tau v', \\
(\tau v', v') & \in \lambda_t, \\
v' & = u'' \sigma v, \\
(u'' \sigma v, u'' v) & \in \lambda_t
\end{align*}
\]

and obtain \((\tau u'' v, u'' v) \in L_t\). Since \((u' \tau, u') \in R_t\) 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:

\[A_r, B_t \subseteq C_{r,l} \subseteq A_r \perp B_t.\]

The inclusions are strict in general.
For $r = 2, l = 2$ we have

$$aaba \in A_2, \ abab \in B_2,$$

thus

$$aaaababab \in A_2 \sqcup B_2,$$ but

$$aaaababab$$

is reducible to $aababab$ in $\mu_{2,2}$.

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

**Example 3.6**:

$$\Sigma_{1,1} \subseteq A_1 \sqcup B_1, \ \Sigma = \{ a, b \}$$

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

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

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

Thus the monoid $\Sigma^*/\mu_{1,1}$ is isomorphic to
Similarly as in remark 2.14 this monoid also presents an automaton deciding
the word problem in $\Sigma^*/\mu_{11}$ and describing the equivalence classes by regular
expressions.

The function $g : \Sigma^* \to \Sigma^*$ associating to every word $u \in \Sigma^*$ its shortest
representative $\text{irr}(u)$ with respect to $\mu_{r,1}$ is realized by the following bimachine
(see [0] for the definition of a bimachine):

Take $A_r$ and $B_i$ as state sets and next-state functions

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

and

$$\sigma.v = \begin{cases} \sigma v, & \text{if } \sigma v \in B_i \\ v, & \text{if } \sigma v \notin B_i \end{cases}$$

The output function $\gamma$ is defined as

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

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

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

Let $V$ denote the following class of monoids:

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

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

**Proposition 3.8:**

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

**Proof**: $R \vee L \subseteq V$, since $\mu_{kk} \subseteq \rho_{k} \cap \lambda_{k}$.

For $\sigma \in \Sigma$ we have $(\sigma^{2k+1}, \sigma^{2k}) \in \mu_{kk}$.

Since $\mu_{kk}$ is fully invariant, $x^{2k+1} = x^{2k}$ is an equation which holds in
$\Sigma^*/\mu_{kk}$.

This shows $V \subseteq \text{Ap}$.

**Theorem 3.9**: $V$ is decidable.

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

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

R.A.I.R.O. Informatique théorique/Theoretical Informatics
The implication from right to left being trivial, we suppose $M \in V$, which means $\rho \supseteq \mu_{kk}$ for some $k \in \mathbb{N}$. We can choose $k \leq r$: Let $(u \sigma v, uv) \in M_{r,r}$, i.e. $u = u_1 \ldots u_r$, $v = v_r \ldots v_1$ such that

(*) $\alpha(u_1) \supseteq \ldots \supseteq \alpha(u_r) \supseteq \alpha(v_r) \supseteq \ldots \supseteq \alpha(v_1)$.

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

$$v_h v_{h-1} \ldots v_0 = v_i v_{i-1} \ldots v_{h+1} v_h \ldots v_0.$$ 

The inclusions (*) imply:

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

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

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

$$uv = u_0 \ldots u_i(u_{i+1} \ldots u_j) u_{j+1} \ldots u_r v_r \ldots v_{l+1}(v_l \ldots v_{h+1}) v_h \ldots v_0$$

$$= u_0 \ldots u_i(u_{i+1} \ldots u_j)^k u_{j+1} \ldots u_r v_r \ldots u_{l+1}(v_l \ldots v_{h+1})^k v_h \ldots v_0$$

$$= u_0 \ldots u_i(u_{i+1} \ldots u_j)^k u_{j+1} \ldots u_r \sigma v_r \ldots v_{l+1}(v_l \ldots v_{h+1})^k v_h \ldots v_0$$

$$= u \sigma v.$$ 

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

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

There are some open questions concerning the $M$-Variety $V$:

1) Find a sequence of equations which ultimately defines $V$.

2) Find other algebraic characterisations of $V$.

3) Is $R \vee L \neq V$?

4) Characterize those $L$ with $M(L) \in V$. 

vol. 19, no 3, 1985
REFERENCES