Keijo Ruohonen

NONCOMMUTATIVE RECURRENCES

Tampere 1987
Keijo Ruohonen*

NONCOMMUTATIVE RECURRENCES

*Tampere University of Technology
PL 527
SF–33101 TAMPERE
FINLAND
NONCOMMUTATIVE RECURRENCES

Keijo Ruohonen
Institute of Mathematics
Tampere University of Technology
SF-33101 Tampere, Finland

1. Introduction

Linear recurrences have a well-developed and old theory, see e.g. [M1]. Commutative groups may be considered as modules and hence their recurrences share many of the properties of linear recurrences. This is largely true for commutative semigroups, too, as far as they can be embedded in groups.

Recurrences in noncommutative semigroups and groups have received a steady but far less organized interest. For an overview of the older developments and a nice example of the kind of research they started, and a start for a transitive literature search, see [D1].

Recent theoretical study of developmental biology using the so-called Lindenmayer systems introduced and investigated many concepts (such as recurrence systems, locally catenative sequences, DOL systems and HDOL systems) which are of central interest in a theory of noncommutative recurrences, see e.g. [HR] and [RS]. In almost all cases the underlying algebraic structure is that of a free monoid. In [JM], [J1], [D2] and [D3] also free groups are investigated.

Of the more recent application areas of noncommutative recurrences we would like to mention symbolic semantics of algorithms ([Ho],[Ga]), and representation and investigation of space-filling curves, fractals and "graftals" ([D2],[D3],[SiSu]), especially in computer graphics ([Sm],[SQ]).

Experience shows that recurrent noncommutative sequences crop up variously disguised in many unsuspected places and hunting them is fun. Suffice it to mention [Ro], [Co], [Fr] and Table M of [Da]. See also [DMP].

Our chief aim here is to give a certain basis for the theory and an overview of some main issues interspersed with several new observations. Only some elementary group theory and semigroup theory is assumed.

† This is a second revised version. The first version is from July 1985.
2. Definitions and basics

Formally, a $d$-dimensional recurrence $R$ in a (noncommutative) finitely generated semigroup $H$ consists of $d$ finite (possibly empty) sequences of ordered pairs of positive integers:

$$(p_{i1}, q_{i1}), \ldots, (p_{iu_i}, q_{iu_i}) \quad (i=1, \ldots, d)$$

where

$$1 \leq p_{i1} \leq d, \ldots, 1 \leq p_{iu_i} \leq d \quad (i=1, \ldots, d).$$

The order of the recurrence is

$$k = \max_{1 \leq i \leq d; 1 \leq j \leq u_i} q_{ij}.$$  

The recurrence defines an infinite sequence of elements of $H^d$

$$\bar{\omega}_0, \bar{\omega}_1, \ldots,$$

given the initial values $\bar{\omega}_0, \ldots, \bar{\omega}_{k-1}$, as follows. Denote by $\omega_n^{(i)}$ the $i^{th}$ component of $\bar{\omega}_n$. Then

$$\omega_n = \omega_{n-q_{i1}}^{(p_{i1})} \ldots \omega_{n-q_{iu_i}}^{(p_{iu_i})} \omega_{n-k} \quad (i=1, \ldots, d; n \geq k).$$

Similarly, a $d$-dimensional recurrence $R$ in a (noncommutative) finitely generated group $G$ consists of $d$ finite (possibly empty) sequences of ordered triples of integers:

$$(p_{i1}, q_{i1}, r_{i1}), \ldots, (p_{iu_i}, q_{iu_i}, r_{iu_i}) \quad (i=1, \ldots, d)$$

where the $p_{ij}$'s, the $q_{ij}$'s and the order $k$ are as above and

$$r_{i1}, \ldots, r_{iu_i} \in \{-1, 1\} \quad (i=1, \ldots, d).$$

Now the sequence $\bar{\omega}_0, \bar{\omega}_1, \ldots$ is defined by
\[ w_n^{(1)} = \left( \begin{array}{c} (p_{i1})_{i=1}^r \cdots (p_{iu})_{i=1}^r \end{array} \right) \]

given \( \tilde{w}_0, \ldots, \tilde{w}_{k-1} \).

The sequence \( \tilde{w}_0, \tilde{w}_1, \ldots \) is called the sequence generated by the recurrence starting from the given initial values. Components of sequences generated by recurrences in \( H \) (resp. in \( G \)) are called recurrent sequences in \( H \) (resp. in \( G \)).

**Theorem 2.1.** Any recurrent sequence can be obtained as a component of a sequence generated by a recurrence of order 1.

**Proof.** We prove the theorem for groups (the proof for semigroups is similar). Consider a recurrence \( R \) as above and the initial values \( \tilde{w}_0, \ldots, \tilde{w}_{k-1} \).

By reordering if necessary we may restrict ourselves to the first component of \( \tilde{w}_0, \tilde{w}_1, \ldots \). We define a new recurrence \( R' \) of dimension \( dk \) and order 1. The finite sequences comprising \( R' \) are the following:

\[
(1,1,1) \]
\[
(2,1,1) \]
\[
\vdots \]
\[
(k-1,1,1) \]
\[
((p_{11}-1)k + q_{11}, 1, r_{11}) , \ldots , ((p_{1u_1}-1)k + q_{1u_1}, 1, r_{1u_1}) \]
\[
((p_{21}-1)k + q_{21}, 1, r_{21}) , \ldots , ((p_{2u_2}-1)k + q_{2u_2}, 1, r_{2u_2}) \]
\[
(k+1,1,1) \]
\[
\vdots \]
\[
((d-1)k - 1,1,1) \]
\[
((p_{d1}-1)k + q_{d1}, 1, r_{d1}) , \ldots , ((p_{du_d}-1)k + q_{du_d}, 1, r_{du_d}) \]
\[
((d-1)k + 1,1,1) \]
\[
((d-1)k + 2,1,1) \]
\[
\vdots \]
\[
(dk-1,1,1) .
\]
The $k$-th component of the sequence generated by $R'$ starting from the initial value:

$$(\omega_k(1), \omega_{k-1}^0, \omega_k(2), \omega_{k-1}^0, \ldots, \omega_k(d), \omega_{k-1}^0)$$

equals the first component of $\bar{\omega}_0, \bar{\omega}_1, \ldots$, as is easily seen.

Closely related to recurrences of order 1 are iterated morphisms. Let $A_m = \{a_1, \ldots, a_m\}$ be an alphabet and denote by $A_m^*$ (resp. $A_m^+$) the free monoid (resp. free semigroup) generated by $A_m$. An **iterated morphism** in $A_m^*$ (resp. in $A_m^+$) is a sequence

$$\text{id}, \delta, \delta^2, \delta^3, \ldots$$

where $\delta$ is an endomorphism on $A_m^*$ (resp. on $A_m^+$); $m$ is the order of the iterated morphism. The **components** of the iterated morphism are the sequences

$$a_i, \delta(a_i), \delta^2(a_i), \delta^3(a_i), \ldots \quad (i=1, \ldots, m).$$

(Here $\delta^n$ denotes the $n$-fold composition of $\delta$ and $\text{id} = \delta^0$ is the identity morphism.)

**Theorem 2.2.** (i) Any recurrent sequence in a semigroup (resp. monoid, group) $H$, obtained as a component of a sequence generated by a recurrence of dimension $d$ and order $k$, equals the termwise morphic image of a (first) component of an iterated morphism of order $dk$ (resp. $dk$, $2dk$) under a morphism $A_{dk}^+ \to H$ (resp. $A_{dk}^* \to H$, $A_{2dk}^* \to H$).

(ii) Any termwise morphic image of a component of an iterated morphism of order $k$ is a recurrent sequence obtained as a component of a sequence generated by a recurrence of dimension $k$ and order 1.

**Proof.** (i) We prove the result only for groups, the proof for semigroups and monoids is quite analogous (and easier). So, consider a recurrence $R$, as above, in a group $G$, and the first component of the sequence generated by it. By Thm. 2.1 and its proof, we may assume that the recurrence is of order 1 and dimension $d' = dk$. Let $A_{2d'} = \{a_1, \ldots, a_{2d'}\}$ be an alphabet and define the endomorphism $\delta$ on $A_{2d'}^*$ by

$$\delta(a_i) = a_{p_{i1} + d'(1-r_{i1})/2} \cdots a_{p_{iu_i} + d'(1-r_{iu_i})/2} \quad (i=1, \ldots, d')$$
and
\[ \delta(a'_i + i) = a_{p_{i1}} + d'(1 + r_{i1})/2 \quad \cdots \quad a_{p_{i1}} + d'(1 + r_{i1})/2 \quad (i=1, \ldots, d'). \]

Further, define the morphism \( h : A_{2d'}^* \to G \) by
\[ h(a_i) = \omega_0^{(i)}, \quad h(a'_i + i) = (\omega_0^{(i)})^{-1} \quad (i=1, \ldots, d'). \]

It is then straightforward to verify that \( \omega_0^{(1)}, \omega_1^{(1)}, \ldots \) is the termwise image of the first component of the iterated morphism \( \text{id}, \delta, \delta^2, \ldots \) under \( h \).

(ii) Let \( \delta \) be an endomorphism on \( A_m^* \) (resp. on \( A_m^+ \)) and
\[ \delta(a_i) = a_{p_{i1}} \cdots a_{p_{i1}} \quad (i=1, \ldots, m) \]
where \( a_{p_{i1}}, \ldots, a_{p_{i1}} \in A_m \quad (i=1, \ldots, m) \). Then the recurrence
\[ (p_{i1}, 1), \ldots, (p_{i1}, 1) \quad (i=1, \ldots, m) \]
with the initial value \((a_1, \ldots, a_m)\) generates the components of the iterated morphism \( \text{id}, \delta, \delta^2, \ldots \). Mapping by a morphism then gives the result. \( \square \)

**Note 2.1.** Should the semigroup (resp. monoid, group) \( H \) be commutative, then we could define our iterated morphisms on the free commutative semigroup (resp. free commutative monoid) generated by \( A_{d_k} \) (resp. \( A_{d_k}, A_{2d_k} \)). Thm. 2.2 would then hold true with this modification as well.

The following theorem gives some easy to prove termwise closure results for recurrent sequences.

**Theorem 2.3.** (i) If \( \omega_0, \omega_1, \ldots \) is a recurrent sequence in a semigroup (resp. group) \( H \) and \( h : H \to H' \) is a morphism then \( h(\omega_0), h(\omega_1), \ldots \) is a recurrent sequence in \( H' \).

(ii) If \( \omega_0, \omega_1, \ldots \) is a recurrent sequence in a group \( G \) then \( \omega_0^{-1}, \omega_1^{-1}, \ldots \) is also a recurrent sequence in \( G \).

(iii) If \( \omega_0, \omega_1, \ldots \) and \( \omega_0', \omega_1', \ldots \) are recurrent sequences in a semigroup (resp. group) \( H \) then so is \( \omega_0 \omega_0', \omega_1 \omega_1', \ldots \).

(iv) If \( \omega_0, \omega_1, \ldots \) is recurrent in a monoid (resp. group) \( H \) and \( \omega_0', \omega_1', \ldots \) is recurrent in a monoid (resp. group) \( H' \), then \( (\omega_0, \omega_0'), (\omega_1, \omega_1'), \ldots \) is recurrent in \( H \circ H' \).
Proof. (i) and (ii) are immediate from the definitions. We prove (iii) for groups, the proof for semigroups is analogous. Consider the two recurrences

\[(p_{i1}',1,r_{i1}'), \ldots, (p_{iu}',1,r_{iu}') \quad (i=1, \ldots, d_1)\]

and

\[(q_{i1}',1,s_{i1}'), \ldots, (q_{iv}',1,s_{iv}') \quad (i=1, \ldots, d_2)\]

and the first components of the sequences \(\bar{\omega}_0, \bar{\omega}_1, \ldots\) and \(\bar{\tau}_0, \bar{\tau}_1, \ldots\) they generate starting from the initial values

\[(\omega_0^{(1)}, \ldots, \omega_0^{(d_1)}, \tau_0^{(1)}, \ldots, \tau_0^{(d_2)})\]

respectively. Then the last component of the sequence generated by the recurrence

\[(p_{i1}',1,r_{i1}'), \ldots, (p_{iu}',1,r_{iu}') \quad (i=1, \ldots, d_1)\]

\[(d_1+q_{i1}',1,s_{i1}'), \ldots, (d_1+q_{iv}',1,s_{iv}') \quad (i=1, \ldots, d_2)\]

\[(p_{11}',1,r_{11}'), \ldots, (p_{1u}',1,r_{1u}'), (d_1+q_{11}',1,s_{11}'), \ldots, (d_1+q_{1v}',1,s_{1v}')\]

starting from the initial value

\[(\omega_0^{(1)}, \ldots, \omega_0^{(d_1)}, \tau_0^{(1)}, \ldots, \tau_0^{(d_2)}, \omega_0^{(1)} \tau_0^{(1)})\]

equals \(\omega_0^{(1)} \tau_0^{(1)}, \omega_1^{(1)} \tau_1^{(1)}, \ldots\).

To prove (iv) let \(\omega_0, \omega_1, \ldots\) and \(\omega_0', \omega_1', \ldots\) be recurrent in \(H\) and \(H'\), respectively. Then \((\omega_0',1_H'),(\omega_1',1_H'), \ldots\) and \((1_H,\omega_0'),(1_H,\omega_1'), \ldots\) are recurrent in \(H \circ H'\). \((1_H\text{ and }1_H\text{ are the identity elements of }H\text{ and }H', \text{ respectively.})\) Hence \((\omega_0,\omega_0'),(\omega_1,\omega_1'), \ldots\) is recurrent in \(H \circ H'\), too, by (iii). \(\square\)

Note 2.2. Part (iv) of the theorem does not hold true in semigroups without identities in general. For instance, the sequences \(1,1,1,\ldots\) and \(1,2,2^2,\ldots\) are recurrent in \(\mathbb{N}_+\), as is easily seen, but \((1,1),(1,2),(1,2^2),\ldots\) is not recurrent in \(\mathbb{N}_+^2\). Assume the contrary. Then there is a square matrix \(M\) with nonnegative integer entries and row vectors \(\vec{\pi}_1\) and \(\vec{\pi}_2\) with positive integer entries such that
\[ 1 = \bar{\pi}_1 \cdot M^n \bar{\eta}, \quad 2^n = \bar{\pi}_2 \cdot M^n \bar{\eta} \quad \text{for all } n \geq 0 \]

where \( \bar{\eta} \) is a column vector one entry of which equals 1 others being zeros (cf. Note 2.1). Now there is a positive number \( c \) such that \( \bar{\pi}_2 \leq c \bar{\pi}_1 \) and consequently

\[ 2^n = \bar{\pi}_2 \cdot M^n \bar{\eta} \leq c \bar{\pi}_1 \cdot M^n \bar{\eta} = c, \]

a contradiction. Note that \((1,1),(1,2),(1,2^2),\ldots\) is not recurrent in \( \mathbb{N} \times \mathbb{N} \) either (i.e., we may allow \( \bar{\pi}_2 \) to have zero entries above).

For any sequence \( f_0, f_1, \ldots \) the sequences

\[ f_j, f_{p+j}, f_{2p+j}, f_{3p+j}, \ldots \quad (j=0,\ldots,p-1) \tag{1} \]

form a decomposition of \( f_0, f_1, \ldots \). The sequences (1) are called the composite subsequences of \( f_0, f_1, \ldots \).

For any sequences \( f_{i0}, f_{i1}, f_{i2}, \ldots \) (\( i=1,\ldots,p \)) the sequence

\[ f_{10}, f_{20}, \ldots, f_{p0}, f_{11}, f_{21}, \ldots, f_{p1}, \ldots \]

is the composition of the sequences.

For any sequence \( f_0, f_1, \ldots \) the sequence \( f_1, f_2, \ldots \) is obtained from it by forward translation. Similarly the sequences \( f_{-1}, f_0, f_1, \ldots \), where \( f_{-1} \) is arbitrary, are obtained from \( f_0, f_1, \ldots \) by backward translation.

With respect to these basic sequential operations we have full closure in monoids and groups.

**Theorem 2.4.** (i) Any composite subsequence of a recurrent sequence is also recurrent.

(ii) Any composition of recurrent sequences in a monoid (resp. group) is also recurrent.

(iii) Recurrent sequences are closed under forward and backward translation.

**Proof.** (i) Take the first component of the iterated morphism \( \text{id}, \delta, \delta^2, \ldots \) mapped by the morphism \( h \). Then the first component of the iterated morphism \( \text{id}, \delta^p, \delta^{2p}, \ldots \) mapped by \( h \delta^j \) is recurrent.

(ii) Take the first components of the iterated morphisms \( \text{id}, \delta, \delta^2, \ldots \) over disjoint alphabets \( B_i \) (\( i=1,\ldots,p \)), respectively, mapped by the morphisms
h_i on B_i^\ast, respectively. Take then p isomorphic copies of each of the alphabets:

$$B_i^1 (=B_i), \ldots, B_i^p \quad (i=1, \ldots, p),$$

all of them mutually disjoint, and another disjoint alphabet $C = \{c_1, \ldots, c_p\}$. Let $I_{i\cdot j\cdot k}$ be the isomorphism between $B_i^j$ and $B_i^k$ $(i, j, k=1, \ldots, p)$ and let $b_i^1$ be the first symbol of $B_i$ $(i=1, \ldots, p)$. Define then the endomorphism $\delta$ on $B^\ast$, where

$$B = C \cup \left( \bigcup_{i=1}^{p} \bigcup_{j=1}^{p} B_i^j \right),$$

by

$$\delta(c_i) = c_{i+1} \quad (i=1, \ldots, p-1)$$
$$\delta(c_p) = \delta_1(b_1^1) \cdots \delta_p(b_p^1)$$
$$\delta(b) = I_{i\cdot j\cdot j+1}(b) \text{ if } b \in B_i^j \quad (i=1, \ldots, p; j=1, \ldots, p-1)$$
$$\delta(b) = \delta_i I_{i\cdot i\cdot 1}(b) \text{ if } b \in B_i^p \quad (i=1, \ldots, p).$$

Define further the morphism $\eta$ on $B^\ast$ by

$$\eta(c_i) = h_i(b_1^1) \quad (i=1, \ldots, p)$$
$$\eta(b) = h_i I_{i\cdot i\cdot 1}(b) \text{ if } b \in B_i^i \quad (i=1, \ldots, p)$$
$$\eta(b) = \text{identity} \text{ if } b \in B_i^j \quad (i, j=1, \ldots, p; i \neq j).$$

It is not difficult to see that the image of the first component (corresponding to $c_1$) of the iterated morphism $id, \delta, \delta^2, \ldots$ under $\eta$ equals the desired composition.

(iii) Obviously recurrent sequences are closed under forward translation. To show closure under backward translation let $id, \delta, \delta^2, \ldots$ be an iterated morphism over $A_m = \{a_1, \ldots, a_m\}$ and $h : A_m^\ast + H$ a morphism. Let $a$ be an arbitrary element of $H$ and $c$ a new symbol not in $A_m$. Define the endomorphism $\gamma$ on $(A_m \cup \{c\})^\ast$ by

$$\gamma(c) = a_1$$
$$\gamma(a_1) = \delta(a_1) \quad (i=1, \ldots, m).$$

Define further the morphism $h' : (A_m \cup \{c\})^\ast + H$ by
\[ h'(c) = \alpha \]
\[ h'(a_i) = h(a_i) \quad (i=1, \ldots, m). \]

The first component (corresponding to c) of the iterated morphism \( \text{id}, \gamma, \gamma^2, \ldots \) mapped by \( h' \) then equals an (arbitrary) backward translated sequence. For semigroups without identities the proof is similar. \( \square \)

Note 2.3. Parts (i) and (iii) of the theorem hold true for any (finitely generated) semigroups. Part (ii) does not hold true for semigroups without identities in general. For instance, the sequences 1,1,1,... and 1,2,2^2,... are recurrent in \( \mathbb{N}_+ \), as is easily seen, but the sequence 1,1,1,2,1,2^2,1,... is not. Assume the contrary. Then the \( n^{th} \) term of the sequence can be written as \( \bar{\pi} \bar{M}^n \bar{n} \) where \( \bar{\pi} \in \mathbb{N}_+^k \) (a row vector), \( \bar{M} \in \mathbb{N}_+^{k \times k} \), and \( \bar{n} \in \mathbb{N}^k \), for some \( k \), as is easily seen (cf. Note 2.1). Moreover, \( \bar{\pi} \bar{M}^n \bar{n} \in \mathbb{N}_+^k \) for all \( n \geq 0 \). So we have

\[ 1 = \bar{\pi} \bar{M}^{2n} \bar{n}, \quad 2^n = (\bar{\pi} \bar{M}) \bar{M}^{2n} \bar{n} \quad \text{for all } n \geq 0. \]

This is a contradiction (cf. Note 2.2).

3. Minimal dimension

Consider a recurrent sequence, defined as a component of a sequence generated by a recurrence + initial values. There are always infinitely many recurrences which could be used to define the recurrent sequence. The smallest of their dimensions is called the \textbf{minimal dimension} of the sequence.

In the case of commutative groups minimal dimension is trivial:

**Theorem 3.1.** The minimal dimension of a recurrent sequence in a commutative group is 1.

**Proof.** It suffices to consider the case of the free commutative group \( \mathbb{Z}^m \) and show that an "iterated matrix" \( I, M, M^2, \ldots \) satisfies a recurrence of dimension 1 (cf. Note 2.1). But this, of course, follows from the Cayley-Hamilton Theorem. \( \square \)

We note in passing, as a consequence of Thm. 3.1, that any recurrent
sequence in a free monoid satisfies a "nonhomogeneous recurrence" of dimension 1 containing a "variable forcing term" formed of commutators in a metabelian group (see below). (The sequence of the "forcing terms" is, unfortunately not recurrent in the commutator subgroup because this is infinitely generated.) This simple result is akin to several "representations" of free finitely generated monoids by infinitely generated commutative structures; see [R1], [J1], [J2], [Oc] and also the generalized Parikh mappings of [Ka] (which actually appear already in Sect. 5 of [R2]).

Recurrent sequences in commutative semigroups in general can have any minimal dimension. This is true already for \( \mathbb{N} \) as we will now show. For this purpose we first define the digraph associated with a recurrence. Let \( R \) be a recurrence as in the beginning of Sect. 2. Then the digraph is \((V,E)\) where \( V = \{1,\ldots,d\} \) and

\[
E = \{ (i,j) \mid \text{One of the numbers } p_{j_1}^{1}, \ldots, p_{j_d} \text{ is } i. \}.
\]

The label of the directed edge \((i,j)\) is the number of times \( i \) occurs among \( p_{j_1}, \ldots, p_{j_d} \).

**Theorem 3.2.** For any positive integer \( k \) there are recurrent sequences in \( \mathbb{N} \) (and hence in any free monoid) having minimal dimension \( k \).

**Proof.** In a recurrent sequence \( \omega_0, \omega_1, \ldots \) in \( \mathbb{N} \), \( \omega_n \) is an exponential polynomial of \( n \) (see e.g. [Mi]). We say that the sequence is of degree \( t \) if there is a polynomial \( P(n) \) of degree \( t \) such that \( \omega_n < P(n) \) for \( n = 0,1,\ldots \) and, for each polynomial \( Q(n) \) of degree \( t-1 \) or less, \( \omega_n > Q(n) \) for some natural number \( n \). Sequences having a degree are called polynomially bounded.

Consider then a polynomially bounded recurrent sequence of degree \( t \) in \( \mathbb{N} \) having minimal dimension \( d \). Let

\[(p_{i_1}^{1}, q_{i_1}^{1}), \ldots, (p_{i_d}^{1}, q_{i_d}^{1}) \quad (i=1,\ldots,d)\]

be a recurrence of dimension \( d \) such that the first component of the sequence \( \vec{\omega}_0, \vec{\omega}_1, \ldots \) generated be the recurrence (starting from some initial values) equals \( \omega_0, \omega_1, \ldots \). Since \( d \) is minimal it follows that each vertex \( 2, \ldots, d \) is connected to 1 in the digraph associated with the recurrence. This implies that all components of \( \vec{\omega}_0, \vec{\omega}_1, \ldots \) have degrees less than or equal to \( t \), as is easily seen. By Berstel's Theorem (Thm. II.10.1 in [SaSc]) we know that the components of a proper decomposition of \( \vec{\omega}_0, \vec{\omega}_1, \ldots \) are polynomials of \( n \).
We show that \( t \leq d - 1 \) using induction on \( d \). The case \( d = 1 \) is clear. So let us assume (induction hypothesis) that the degree of a polynomially bounded recurrent sequence of minimal dimension \( d < \ell \) is always at most \( d - 1 \). Consider a polynomially bounded recurrent sequence \( \omega_0, \omega_1, \ldots \) of minimal dimension \( \ell \geq 2 \) in \( \mathbb{N} \). Assume, contrary to our claim, that its degree is \( t \geq \ell \). Let the recurrence of dimension \( \ell \) defining \( \omega_0, \omega_1, \ldots \) be as above. By Thm. 2.4(i) and its proof we may assume that the components of \( \bar{\omega}_0, \bar{\omega}_1, \ldots \) (the sequence generated by the recurrence) are polynomials of \( n \), say \( P_1(n), \ldots, P_\ell(n) \). The maximum degree of these polynomials is \( t \) and \( P_1(n) = \omega_n \) has this degree. If more than one of the numbers

\[
P_{11}, \ldots, P_{1u_1}
\]
equals 1, then \( \omega_0, \omega_1, \ldots \) cannot possibly be polynomially bounded. On the other hand, by the induction hypothesis, one of the numbers, say \( P_{11} \), must equal 1, otherwise there are polynomials of degree \( t \) among \( P_2(n), \ldots, P_\ell(n) \) and we can reduce their minimal dimension to \( \ell - 1 \) or less. The minimal dimension of those polynomials \( P_j(n) \), if any, which are of degree less than \( t \), is at most \( \ell - 1 \) because \( j \) cannot be connected to \( i \) in the digraph associated with the recurrence unless \( P_j(n) \) has degree less than \( t \). Hence, by the induction hypothesis, they are at most of degree \( \ell - 2 \leq t - 2 \). Now

\[
P_1(n) = P_1(n-q_{11}) + \sum_{j=2}^{u_1} P_{1j}(n-q_{1j})
\]
so that the polynomials

\[
P_{11}(n), \ldots, P_{1u_1}(n),
\]
if any, are of degree less than \( t - 2 \). But the degree of \( P_1(n) - P_1(n-q_{11}) \) is \( t - 1 \geq 1 \) so that \( u_1 \geq 2 \) and one of the polynomials has degree \( t - 1 \), a contradiction.

It remains to be shown that there are in \( \mathbb{N} \) recurrent sequences of arbitrary degree. Using the binomial identity

\[
\sum_{j=0}^{k} \binom{k+j-1}{k} = \binom{k+n}{k+1}
\]
it is easy to show that the recurrence
\[(1,1)\]
\[(2,1), (1,1)\]
\[(3,1), (2,1)\]
\[\vdots\]
\[(d,1), (d-1,1)\]

with the initial value \((1,0,\ldots,0)\) defines a recurrent sequence of degree \(d-1\) in \(\mathbb{N}\). \[\square\]

Occasionally the semigroup can be embedded in a commutative group and Thm. 3.1 becomes available. (This embeddability property is decidable for finitely defined commutative semigroups, see e.g. [Bi].)

In the absence of inverses or commutativity the problem of the minimal dimension of a recurrent sequence seems to be very difficult. For instance, no algorithm is known even for obtaining the minimal dimension of a recurrent sequence in \(\mathbb{N}\) (see p. 173 of [RS]). Another wide open special case of this problem is the so-called LC problem, see Sect. 6. We do not know either, whether recurrent sequences in groups can have arbitrarily high minimal dimension.

It is not difficult to see that there are recurrent sequences in a free monoid whose minimal dimension exceeds 1 even when embedded in a free group (cf. [JM]). As is well known, free monoids can be embedded in (free) metabelian groups, too. For instance, the monoid \(A_{10}^{\times}\) can be embedded in the (non-free) multiplicative metabelian group generated by the matrices

\[
\begin{pmatrix}
1 & i \\
0 & 10
\end{pmatrix}
\quad (i=0,\ldots,9)
\]

(or, equivalently, in the group generated by the affine functions \(10x+i\) \((i=0,\ldots,9)\) or by the functions \(\frac{x}{1x+10}\) \((i=0,\ldots,9)\)) in an obvious way, and hence in the free metabelian group generated by \(A_{10}\), as well.

Can all recurrent sequences in free monoids be embedded in groups in such a way that their minimal dimension becomes 1? We do not know the answer. Some choices for the group can be ruled out, however. For instance, the recurrent sequence

\[ab, a^2b^2, \ldots, a^n b^n, \ldots\]

does not have minimal dimension 1 in the free metabelian group generated by
\{a, b\} even though it can be embedded in it. This can be seen as follows. Assume the contrary. Then the sequence
\[
\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}^{-1}, \ldots, \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}^{2^n} \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}^{-2^n}, \ldots
\]
that is
\[
\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}, \ldots, \begin{bmatrix} 1 & 2^{-2^n} \\ 0 & 1 \end{bmatrix}, \ldots
\]
satisfies a recurrence of dimension 1 in the metabelian group generated by the matrices
\[
\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}.
\]
Now
\[
\begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & s \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & s+t \\ 0 & 1 \end{bmatrix}
\]
so that the sequence
\[
\frac{1}{2}, \frac{3}{4}, \ldots, 2^{-2^n} - 1, \ldots
\]
then satisfies a recurrence of dimension 1 in \( \mathbb{Z} \). But \( 2^{-2^n} - 1 \) is not an exponential polynomial in \( n \), a contradiction (see e.g. [Mi]).

This example also shows that not all recurrent sequences in the metabelian groups generated by the sets of matrices
\[
\{ \begin{bmatrix} 1 & i \\ 0 & u \end{bmatrix} \mid i = 0, \ldots, u-1 \}
\]
have minimal dimension 1.

The minimal dimension of the sequence \( ab, a^2 b^2, \ldots, a^n b^2, \ldots \) in the free (metabelian) group generated by \( \{a, b\} \) is actually 2 because it can be defined by the recurrence
\[
(2, 1, 1), (1, 1, 1), (2, 1, -1), (1, 1, 1)
\]
\[
(2, 1, 1), (2, 1, 1)
\]
starting from the initial value \( (ab, a) \). It is also not too difficult to
see that its minimal dimension in \( \{a,b\}^* \) is 3.

We want to mention finally two questions related to finding minimal dimensions. First, given a recurrent sequence \( \omega_0, \omega_1, \ldots \), does there exist a number \( k \) and a \( k \)-place function \( f \) such that

\[
\omega_n = f(\omega_{n-1}, \ldots, \omega_{n-k}) \quad \text{for all } n \geq k
\]

Of course, we would like \( f \) to be recursive, too. The answer is positive for commutative groups (and semigroups embeddable in them), by Thm. 3.1. It is also positive for free monoids. This can be seen as follows. Let \( \omega_0, \omega_1, \ldots \) be an arbitrary recurrent sequence in \( A^\infty_m \). If the sequence is periodic, then the case is clear, so we assume that it is not periodic. Denote by \( l_0, l_1, \ldots \) the sequence of the lengths of the words \( \omega_0, \omega_1, \ldots \). Being a termwise morphic image of \( \omega_0, \omega_1, \ldots \), the sequence \( l_0, l_1, \ldots \) is recurrent in \( \mathbb{N} \), and of minimal dimension 1 in \( \mathbb{Z} \), with order \( k \), say. Since \( l_0, l_1, \ldots \) is nonperiodic, too, there is a \( k \)-place (recursive) function \( g \) such that

\[
n = g(l_n, l_{n+1}, \ldots, l_{n+k-1}) \quad (n=0, 1, \ldots),
\]

and our claim follows. We do not know whether a similar result holds true for free groups or metabelian groups.

Our second question stems from the following observation. If a recurrent sequence \( \omega_0, \omega_1, \ldots \) in a semigroup (resp. monoid, group) has minimal dimension 1 then the subsemigroup (resp. submonoid, subgroup) generated by \( \{\omega_0, \omega_1, \ldots\} \) is finitely generated. (The converse, of course, does not hold true in general.) This leads to two problems:

1. Is the subsemigroup (resp. submonoid, subgroup) generated by \( \{\omega_0, \omega_1, \ldots\} \) finitely generated?

2. If so, find a finite basis for it.

The decidability of (1) is open in free monoids, free commutative monoids and free groups. Indeed the decidability would imply that of the LC problem (see Sect. 6) which is an open question in all these. The case of commutative groups is trivial (see Thm. 3.1 and its proof).

Submonoids of \( \mathbb{N} \) are finitely generated, as is easily seen, so that (1) is trivial in \( \mathbb{N} \). It is not difficult to see that (2) can be effectively solved in
Let \( \omega_0, \omega_1, \ldots \) be a recurrent sequence in \( \mathbb{N} \). The case \( \omega_0 = \omega_1 = \cdots = 0 \) is trivial, so let \( t_0 \) be the smallest nonzero term in \( \omega_0, \omega_1, \ldots \). Find then the smallest nonzero representatives (among \( \omega_0, \omega_1, \ldots \)) of the residue classes modulo \( t_0 \) represented by \( \omega_0, \omega_1, \ldots \). These evidently form the desired basis, and can be found effectively (e.g. by a judicious use of Berstel's Theorem (Thm. II.10.1 in [SaSo])).

Decidability of question (1) and effective solvability of (2) remain open in metabelian groups (other than commutative groups), too. On the other hand, in a metabelian group, the normal subgroup generated by \( \{\omega_0, \omega_1, \ldots\} \) is finitely generated and a generator set can be found effectively (see the proof of Thm. 4.1).

4. **Equivalence of recurrent sequences**

In this section we consider only semigroups and groups with decidable word problems. Indeed, by a solution of the equivalence problem for recurrent sequences we mean its reduction to the word problem. Clearly, in a semigroup or group with an undecidable word problem, equivalence of recurrent sequences is also undecidable.

For commutative groups (and semigroups that can be embedded in a commutative group) the equivalence of recurrent sequences is easily decided: Take two such sequences \( \omega_0, \omega_1, \ldots \) and \( \omega_0', \omega_1', \ldots \). Then, by Thm. 2.3, \( \omega_0^{-1} \omega_0' \omega_1^{-1} \omega_1', \ldots \) is also recurrent and, by Thm. 3.1, has minimal dimension 1, and so on. The algorithm obtained in this way is reasonably effective and easy to use in most cases.

For other semigroups and groups the situation is much worse. For free monoids the first algorithms were developed only quite recently. Three such algorithms are known: those in [CK], [R3] and [R4]. All of these algorithms are specialized and complicated, and (as far as known estimates indicate) of very high complexity. The only known "explicit" upper estimate for the complexity can be developed for the algorithm in [R4], and it is not even primitive recursive. Yet there are also indications to the direction that the problem might even have polynomial complexity for fixed order and dimension (see the discussion in [R3]).

There are ways of extending these algorithms into groups. The algorithm of [R3] (and possibly that of [R4] as well, see Sect. 7) extends to metabelian groups.
Theorem 4.1. Equivalence is decidable for recurrent sequences in metabelian groups (and hence in free monoids as well).

Proof. Take two recurrent sequences in a metabelian group $G$: $\omega_0, \omega_1, \ldots$ and $\omega_0', \omega_1', \ldots$. Let the corresponding iterated morphisms be $\text{id}, \delta, \delta^2, \ldots$ and $\text{id}', \delta', (\delta')^2, \ldots$ and let the morphisms mapping the first components $\alpha_0, \alpha_1, \ldots$ and $\alpha_0', \alpha_1', \ldots$ of these into $G$ be $h$ and $h'$ (see Thm. 2.2). We may assume that $\delta$ and $\delta'$ are defined over disjoint alphabets $A$ and $B$, respectively.

Take then the free monoid $(A \cup B)^*$ and embed it in the free metabelian group $M$ generated by $A \cup B$ (see the previous section). Then the sequence $\alpha_0^{r_0} \alpha_1^{r_1} \alpha_2^{r_2} \ldots$ is a recurrent sequence in $M$ (cf. Thm. 2.3). Let $\delta''$ be the common extension of $\delta$ and $\delta'$ onto $M$. Then obviously $\delta'' (\alpha_0^{r_0} \alpha_1^{r_1} \alpha_2^{r_2} \ldots) = (\alpha_0^{r_0} \alpha_1^{r_1} \alpha_2^{r_2} \ldots n_{n+1})^{r_{n+1}} (n=0, 1, \ldots)$. Denote by $N_n$ the normal subgroup of $M$ generated by $\{\alpha_0^{r_0} \alpha_1^{r_1} \alpha_2^{r_2} \ldots n_{n+1})^{r_{n+1}} \}$ (n=0, 1, ...). The sequence $N_0, N_1, \ldots$ then satisfies the ascending chain condition, as is well known (see e.g. [Ha]). On the other hand, if

$$\alpha_0^{r_0} \alpha_1^{r_1} \alpha_2^{r_2} \ldots \in N_{n_{n+1}}$$

then application of $\delta''$ reveals that

$$\alpha_0^{r_0} \alpha_1^{r_1} \alpha_2^{r_2} \ldots \in N_{n_{n+1}}$$

Thus, a number $n_0$ exists, and it can be found by group-theoretic enumeration.

Let then $N_0$ be the normal subgroup of $G$ generated by $\{w_0^{(w_0')}^{-1}, \ldots, w_n^{(w_n')}^{-1} \}$ (n=0, 1, ...) and let $h''$ be the common extension of $h$ and $h'$ onto $M$. An application of $h''$ shows that

$$w_0^{(w_0')}^{-1} \in N_{n_{n+1}}$$

Thus if

$$w_0^{(w_0')}^{-1} = \ldots = w_{n_{n+1}}^{(w_{n_{n+1}}')}^{-1} = \text{identity},$$

then the recurrent sequences $\omega_0, \omega_1, \ldots$ and $\omega_0', \omega_1', \ldots$ are the same. $\square$

We do not know of any estimates of the number $n_0$ in the above proof. So, the complexity of the algorithm remains open. Anyway, the group-theoretic enumeration is rather costly.

The approach of [CK] generalizes into free groups.
Theorem 4.2. Equivalence is decidable for recurrent sequences in free groups (and hence again in free monoids).

Proof. Consider a finitely generated free group $G_1$. Every subset $S$ of $G_1$ has a test set $F$, i.e., a finite set $F \subseteq S$ such that, for a finitely generated free group $G_2$, and every pair $h_1, h_2$ of morphisms $G_1 \rightarrow G_2$,

$$h_1(u) = h_2(u) \text{ for all } u \in S \iff h_1(u) = h_2(u) \text{ for all } u \in F.$$ 

This follows easily using a matrix representation for $G_2$ and Hilbert's Basis Theorem (see Note 6.2 and also [dLR]).

Take then two recurrent sequences $\omega_0, \omega_1, \ldots$ and $\omega'_0, \omega'_1, \ldots$ in a free group $G_2$. Let the corresponding iterated morphisms be $id, \delta, \delta^2, \ldots$ and $id', \delta', (\delta')^2, \ldots$ and let the morphisms mapping the first components $\alpha_0, \alpha_1, \ldots$ and $\beta_0, \beta_1, \ldots$ of these into $G_2$ be $h$ and $h'$, respectively (see Thm. 2.2). We may assume that $\delta$ and $\delta'$ are defined over disjoint alphabets $A$ and $B$, respectively.

Consider then the free monoid $(A \cup B)^*$ and embed it in the free group $G_1$ generated by $A \cup B$. Then the sequence $\alpha_0 \beta_0, \alpha_1 \beta_1, \ldots$ is recurrent in $(A \cup B)^*$ and in $G_1$. Let $h_1$ and $h_2$ be the morphisms $G_1 \rightarrow G_2$ defined by

$$h_1(a) = \begin{cases} h(a), & \text{if } a \in A \\ \text{identity, if } a \in B \end{cases}$$

(for $a \in A \cup B$)

$$h_2(a) = \begin{cases} h'(a), & \text{if } a \in A \\ \text{identity, if } a \in B \end{cases}$$

(for $a \in A \cup B$).

As noted, all subsets of $G_1$ have test sets. In particular $\{\alpha_0 \beta_0, \alpha_1 \beta_1, \ldots\}$ has a test set $F$ in $G_1$. We may assume that $F$ is of the form

$$F = \{\alpha_0^{n_0}, \ldots, \alpha_{n_0}^{n_0} \}$$

for some $n_0$. Now, obviously the sequences $\omega_0, \omega_1, \ldots$ and $\omega'_0, \omega'_1, \ldots$ are the same if and only if $h_1$ and $h_2$ agree on $\{\alpha_0 \beta_0, \alpha_1 \beta_1, \ldots\}$, that is, if and only if $h_1$ and $h_2$ agree on $F$.

The remaining problem is to show that $F$ can be found effectively. Let $\delta''$ be the common extension of $\delta$ and $\delta'$ onto $G_1$. Since $\delta''(\alpha^{n \beta')} = \alpha_{n+1}^{n+1}$ ($n=0,1,\ldots$), any set $\{\alpha_0^{n_0}, \ldots, \alpha_k^{n_k}\}$ which is a test for $\{\alpha_0^{n_0}, \ldots, \alpha_{k+1}^{n_{k+1}}\}$ is also a test set for $\{\alpha_0^{n_0}, \alpha_1^{n_1}, \ldots\}$. But it is decidable whether or not a finite set $F_1$ is a test set for another finite set $F_2 \supseteq F_1$ in $G_1$ because the universal theory of finitely generated free groups is decidable (see [Ma]).

Unfortunately, we do not know whether or not the method of proof of Thm. 4.1.
is applicable to free groups. Were it so then equivalence would be decidable for all groups (with a decidable word problem).

If one is interested in the equivalence of two sequences generated by recurrences, the situation is no different. Indeed, these two equivalence problems are essentially of the same complexity. This can be seen as follows. Quite obviously, an algorithm for deciding equivalence of two recurrent sequences gives an algorithm for deciding equivalence of sequences generated by recurrences. Suppose then that the equivalence of two recurrent sequences is to be decided. Take the two corresponding recurrences (+ initial values) and combine them, as in the proof of Thm. 2.3(iii), to obtain a recurrence which defines both of the recurrent sequences. Finally take this combined recurrence and the recurrence obtained from it by interchanging the finite sequences corresponding to the recurrent sequences in question, and decide the equivalence of the sequences generated by the two recurrences.

We then turn to some consequences of decidability of equivalence of recurrent sequences. Consider a fixed recurrent sequence $\omega_0, \omega_1, \ldots$ in a free monoid, containing infinitely many terms different from the identity. We may obviously assume that when defining the recurrent sequence using a recurrence (+ initial values), say, as the first component of the sequence it generates, the digraph associated with the recurrence (see the previous section) does not contain vertices unconnected to 1. Without restricting generality we may also assume that no component of the sequence generated by the recurrence consists of identities only, by removing the corresponding finite sequences from the recurrence, if necessary. N.B. that both assumptions may be achieved without increasing dimension.

**Theorem 4.3.** If we restrict ourselves to recurrences of order not exceeding a given number, then there is an algorithm for finding the minimal dimension of a recurrent sequence in a free monoid.

**Proof.** The case where the sequence contains only finitely many terms different from the identity is not too difficult and can be detected effectively. We leave the details to the reader.

So we have the case mentioned above. By Thm. 2.1 we have an upper bound $D$ on the dimension of the recurrence without violating the bound on its order. (Note that the recurrent sequence may be defined by a recurrence of "too high order.") After the assumptions made we have only finitely many possible recurrences + initial values to examine and these can be found effectively, as is seen by considering the digraphs. The key observation is that the digraphs as-
sociated with these recurrences cannot have arbitrarily high labels of edges and similarly that the initial values cannot be arbitrarily long since in the digraphs associated with recurrences of minimal dimension there are paths of length at most D from any vertex to 1 and the order is bounded. Not all of these possible recurrences + initial values actually define the recurrent sequence in question but by Thm. 4.1 (or by Thm. 4.2) we can sort out those which do, and then find the smallest of their dimensions. □

Note 4.1. Thm. 4.1 and Thm. 4.2 also give us a semialgorithm for finding out minimal dimensions in metabelian groups, free groups and free monoids, i.e., a procedure which, when given a recurrent sequence in terms of a recurrence (of dimension d) + initial values,

(i) eventually produces a recurrence of lower dimension defining the sequence when it is possible, and

(ii) takes infinitely many steps otherwise.

(Another way of putting this is to say that the set of those recurrences (+ initial values) in a metabelian group, free group or a free monoid which define the recurrent sequence and are of dimension lower than that of the input recurrence, is recursively enumerable.) The semialgorithm simply enumerates all recurrences + initial values with dimension smaller than d and checks equivalence by Thm. 4.1 or by Thm. 4.2. For many related problems there are similar semialgorithms which are more or less trivial. This is so e.g. for checking whether the minimal dimension of a recurrence in \( \mathbb{N} \) equals 1 (this semialgorithm checks divisibility of polynomials, cf. Lemma 1.1 in [R2]), and for the LC problem (see Sect. 6).

5. Generalizations

Concerning generalizations of the kind of recurrences defined in Sect. 2 we note first that they are "closed under forcing", i.e., adding recurrent sequences as "forcing terms" in the recurrences. To be more specific, recurrent sequences defined by the forced recurrences can be defined by "usual" recurrences as well. This is rather obvious since the forcing terms can be considered as components generated by a recurrence of higher dimension.
A genuine generalization can be obtained by adding "morphism coefficients." A recurrence with morphism coefficients in a semigroup $H$ is a finite sequence of finite (possibly empty) sequences of ordered triples:

$$(p_{i1}, q_{i1}, e_{i1}), \ldots, (p_{i\mu}, q_{i\mu}, e_{i\mu}) \quad (i=1, \ldots, d)$$

where the $p_{ij}$'s and the $q_{ij}$'s are as in Sect. 2 and the $e_{ij}$'s are endomorphisms on $H$. Components of the sequence generated by this recurrence satisfy

$$\omega_n^{(i)} = e_{i1}(\omega_{n-q_{i1}}) \ldots e_{i\mu}(\omega_{n-q_{i\mu}}) \quad (i=1, \ldots, d; n \geq k)$$

(see Sect. 2). For groups the definitions are analogous. Thm. 2.1 holds true for recurrent sequences defined by recurrences with morphism coefficients, too, as is easily seen.

It is now possible to allow infinitely generated semigroups and groups with a genuine effect. Since the recurrent sequences obtained in this way may be rather unwieldy, we allow only finitely generated semigroups and groups here.

For commutative monoids and groups recurrent sequences defined by recurrences with morphism coefficients can be defined by "usual" recurrences as well, and there is no generalization. We show this for monoids (for groups the proof is analogous). It suffices to consider free monoids only. So, assume that $\omega_n^{(1)}$ is the first component of a sequence $\omega_n, \omega_1, \ldots$ generated by a recurrence of dimension $d$ and order $1$, with morphism coefficients, in $\mathbb{N}^k$. If we identify the terms $\omega_n$ as elements $\vec{\omega}_n$ of $\mathbb{N}^{dk}$ in the natural way, then the sequence $\vec{\omega}_0, \vec{\omega}_1, \ldots$ satisfies a "matrix recurrence" $\vec{\omega}_{n+1} = M \vec{\omega}_n (n=0, 1, \ldots)$ where $M \in \mathbb{N}^{dk \times dk}$, as is easily seen. Hence $\vec{\omega}_0, \vec{\omega}_1, \ldots$ satisfies a generalized recurrence $(1, 1, e)$ in $\mathbb{N}^{dk}$. But then $\vec{\omega}_0, \vec{\omega}_1, \ldots$ is recurrent in $\mathbb{N}^{dk}$ (by Thm. 2.2) whence $\omega_n^{(1)}, \omega_1^{(1)}, \ldots$ is recurrent in $\mathbb{N}^k$.

Not all recurrent sequences defined by recurrences with morphism coefficients in a free commutative semigroup can be defined by "usual" recurrences. Obviously, in $\mathbb{N}_+$ no generalization is obtained. But already in $\mathbb{N}^2 - \{0\}$, the sequence

$$(1, 0), (0, 1), (1, 0), (0, 2), (1, 0), (0, 2^2), (1, 0), \ldots$$

generated by the generalized recurrence $(1, 2, e)$, where the endomorphism $e$ is defined by $e((1, 0)) = (1, 0)$ and $e((0, 1)) = (0, 2)$, is not recurrent. (Were it recurrent in $\mathbb{N}^2 - \{0\}$, then the sequence $1, 1, 1, 2, 1, 2^2, 1, \ldots$ would be recurrent in $\mathbb{N}_+$, a contradiction; cf. Note 2.3.)
It is also the case that not all recurrent sequences defined by recurrences with morphism coefficients in a free noncommutative monoid can be defined by "usual" recurrences. So, in this case a genuine generalization is obtained, too. A simple example is the sequence defined as the first component of the sequence generated by the recurrence \( (1,1,e),(1,1,e) \) in \( \{a,b\}^* \), where \( e \) is given by \( e(a) = a^3 \), \( e(b) = b \), starting from the initial value \( ba \). The sequence in question is then obviously

\[
(1) \quad ba, (ba^3)^2, \ldots, (ba^3)^2^n, \ldots .
\]

We will show that this sequence is not recurrent in \( \{a,b\}^* \). Assume the contrary and let \( \delta : A^*_m \rightarrow A^*_m \) and \( h : A^*_m \rightarrow \{a,b\}^* \) be the corresponding morphisms, given by Thm. 2.2(i).

Denote by \( \text{alph}(w) \) the set of the symbols occurring in the word \( w \in A^*_m \). There is a number \( k \) such that \( \text{alph}(\delta^k(w)) = \text{alph}(\delta^{2k}(w)) \) for all \( w \in A^*_m \) (and \( k \geq 0 \)). If \( k > 1 \) we replace \( \delta \) by \( \delta^k \) and the sequence (1) by its (first) composite subsequence (see Sect. 2). We may thus assume that \( \text{alph}(\delta(w)) = \text{alph}(\delta^{2k}(w)) \) for all \( w \in A^*_m \). Denote then

\[
B_1 = \{ a \in A_m \mid \text{h} \circ \delta(a) \neq \text{identity} \}
\]

and \( B_2 = A_m - B_1 \). Of course \( B_1 \) is nonempty. We now replace \( h \) by \( h \circ \delta \). The symbols of \( B_2 \) (if any) can now be removed without changing our sequence. So we assume that \( \delta \) is an endomorphism on \( B_1^* \) and \( h \) is a morphism \( B_1^* \rightarrow \{a,b\}^* \). As a result \( \delta \) and \( h \) are identity-free. But then our sequence

\[
(ba^3)^2, (ba^3)^2^2, \ldots, (ba^3)^2^n, \ldots ,
\]

cannot be generated because the number of \( b \)'s cannot grow.

There is a particularly simple recurrence with morphism coefficients, namely \( (1,1,e) \). Sequences generated by such recurrences (in free monoids) are sometimes called DOL sequences (see e.g. [RS]), and they are recurrent (by Thm. 2.2(ii)). The famous LC problem or the local catenativity problem for DOL sequences is the problem of deciding whether or not a DOL sequence has minimal dimension 1. Some aspects of this problem are discussed in the next section.

Finally we will discuss the construction used in the proof of Thm. 4.1 which also utilizes a generalization of our concept of recurrence in a metabelian group. This generalized recurrence is of the "forced type" discussed
in the beginning of this section. It is of dimension 1 but, unfortunately, of unknown order. Sometimes this recurrence is easily obtained by elimination. As an example, consider a recurrent sequence $z_0, z_1, \ldots$ defined by the recurrence

$$(2,1,1), (3,1,1)$$

$$(2,1,1), (2,1,1), (2,1,1), (2,1,1)$$

$$(3,1,1), (3,1,1), (3,1,1)$$

in a group. The recurrence can be written in the form

$$\begin{align*}
   z_{n+1} &= u_n v_n \\
   u_{n+1} &= u_n^4 \\
   v_{n+1} &= (u_n^{-1} z_n)^3
\end{align*}$$

We then give the steps of the elimination process:

1) $$\begin{align*}
   z_{n+1} &= u_n v_n \\
   u_{n+1} &= u_n^4 \\
   v_{n+1} &= (u_n^{-1} z_n)^3
\end{align*}$$

2) $$\begin{align*}
   z_{n+2} &= u_n^4 (u_n^{-1} z_n)^3 = u_n^3 z_n (u_n^{-1} z_n)^2 \\
   u_{n+1} &= u_n^4
\end{align*}$$

3) $$\begin{align*}
   z_{n+2} &= u_n^3 z_n u_n^{-2} u_n z_n u_n^{-1} z_{n+1} = u_n^2 (u_n^{-1} z_n u_n^{-1}) z_{n+1} \\
   u_{n+1} &= u_n^4
\end{align*}$$

4) $$\begin{align*}
   z_{n+2} &= u_n^2 (u_n^{-1} z_n u_n^{-1}) z_{n+1} \\
   u_{n+1} &= (z_n z_n^{-1}) (u_n z_n u_n^{-1})^4
\end{align*}$$

5) $$\begin{align*}
   z_{n+3} &= (z_n z_n^{-1} (u_n z_n u_n^{-1})^4 (u_n^2 z_n u_n^{-2}) (u_n z_n u_n^{-1}) z_{n+1} z_{n+2} u_n^2 u_n^{-1} z_{n+2}
\end{align*}$$
From the generalized recurrence of dimension 1 given by 5) it follows immediately that the normal subgroup generated by \( \{ z_0, z_1, \ldots \} \) is already generated by \( \{ z_0, z_1, z_2 \} \). Note that 2) gives a "usual" recursion of dimension 2 and order 2. Hence any recurrent sequence defined by our recurrence has minimal dimension 1 or 2, i.e. the recurrence is overdimensional.

Elimination always works if we start with a recurrence of dimension 2 and order 1. To see this, consider a recurrence

\[
(p_{11}, 1, r_{11}), \ldots, (p_{1u_1}, 1, r_{1u_1}) \\
(p_{21}, 1, r_{21}), \ldots, (p_{2u_2}, 1, r_{2u_2})
\]

or, written in another form, as above,

\[
\begin{align*}
    z_{n+1} &= x_1 \cdots x_{u_1} \\
    y_{n+1} &= y_1 \cdots y_{u_2}
\end{align*}
\]

where

\[
\begin{align*}
    x_i &= \begin{cases} 
        z_{n}^{r_{1i}}, & \text{if } p_{1i} = 1 \\
        v_{n}^{r_{1i}}, & \text{if } p_{1i} = 2
    \end{cases}, \\
    y_i &= \begin{cases} 
        z_{n}^{r_{2i}}, & \text{if } p_{2i} = 1 \\
        v_{n}^{r_{2i}}, & \text{if } p_{2i} = 2
    \end{cases}
\end{align*}
\]

Using the identity \( ab = aba^{-1}a \) repeatedly we can write

\[
\begin{align*}
    z_{n+1} &= Z_{n} v_{n}^{k} \\
    v_{n+1}^{k} &= V_{n} v_{n}^{k}
\end{align*}
\]

where \( Z_{n} \) and \( V_{n} \) are products of conjugates of \( z_{n} \) and \( z_{n}^{-1} \) (and hence belong to the normal subgroup generated by \( z_{n} \)). We then write

\[
V_{n+1}^{k} = V_{n} (z_{n}^{-1} z_{n+1})^{k}
\]

and finally

\[
z_{n+2} = z_{n+1} V_{n+1}^{k} = z_{n+1} V_{n} (z_{n}^{-1} z_{n+1})^{k}
\]

(This could be used in the proof of Thm. 4.1 but it gives no sharper a result than does Thm. 3.1.)
Sometimes a similar result can be obtained by an appropriate group extension. As an example, consider the metabelian group $M_{10}$ generated by the matrices
\[
\begin{pmatrix}
1 & i \\
0 & 10
\end{pmatrix} \quad (i=0,\ldots,9)
\]
(see Sect. 3). This group is a subgroup of the metabelian group
\[
M = \{ \begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix} \mid x,y \in \mathbb{Q} \text{ and } y \neq 0 \}.
\]
Take then two elements $A$ and $B$ of $M$ with the same trace and either both different from the identity matrix or both equal to the identity matrix. The equation $AX = XB$ then has solutions in $M$, as is easily seen. Consider a recurrent sequence $\omega_0, \omega_1, \ldots$ in $M_{10}$ (or in $M$). It follows from Thm. 3.1 that there exist numbers $k, \ell_1, \ldots, \ell_k$ such that
\[
\text{trace}(\omega_n) = \text{trace}(\omega_{n-1}^{\ell_1} \cdots \omega_{n-k}^{\ell_k}) \quad (n=k,k+1,\ldots).
\]
Now suppose that, for all $n \geq k$, the elements
\[
\omega_n, \omega_n^{\ell_1} \cdots \omega_n^{\ell_k}
\]
are either both equal to the identity matrix or both different from the identity matrix. In this case there are elements $x_{k}, x_{k+1}, \ldots$ of $M$ such that
\[
\omega_n = x_n \omega_{n-1}^{\ell_1} \cdots \omega_{n-k}^{\ell_k} x_n^{-1} \quad (n=k,k+1,\ldots).
\]
I.e., the normal subgroup of $M$ generated by $\{\omega_0, \omega_1, \ldots\}$ is already generated by $\{\omega_0^{\ell_1}, \ldots, \omega_{k-1}^{\ell_k}\}$.

Unfortunately, testing whether the above condition on the elements
\[
\omega_n, \omega_n^{\ell_1} \cdots \omega_n^{\ell_k}
\]
holds seems to be very difficult. (Already testing whether or not the trace of $\omega_n$ (in $M_{10}$) equals 2 for some $n$ is easily seen to be equivalent to a notorious open problem: deciding whether or not there are zeros in recurrent sequences in $\mathbb{Z}$ (see e.g. [SaSo]).) Hence it seems quite difficult to use methods like this in the proof of Thm. 4.1. It is interesting that similar difficulties prevented the construction in [R6] from reaching a satisfactory goal and were overcome in [R4] only by some very elaborate argumentation. See also Sect. 7.
6. The LC problem: Test sets

The LC problem was introduced in the previous section. Very little is known about the problem (an overview is given in [RS]). We present here two of our old results concerning this problem. First, we show that decidability of another well-known problem (open at the time of this writing), namely the regularity problem for the so-called OL languages, implies that of the LC problem. (A. Salomaa conjectured in [Sa] that this regularity problem is undecidable but we feel that the opposite conjecture is more plausible.) Second, we identify a small but nontrivial class of DOL sequences which cannot be locally catenative. Since there is a trivial semialgorithm for the LC problem, such "negative" results are of certain interest.

Note 6.1. In private discussions we learned that these results were probably discovered independently by several persons. (Which may be why they have not been published.) Especially, we would like to thank Prof. G. Rozenberg who kindly gave us a copy of his manuscript (unpublished, undated and untitled) which contains a short proof of what is essentially our Corollary 6.1. Indeed, our original proof of the result was unnecessarily cumbersome and the present proof is largely modelled after that of Rozenberg's.

Let $A^*$ and $B^*$ be finitely generated free monoids. Then a finite substitution $\sigma : A^* \rightarrow 2^B$ is a morphism from $A^*$ into the the monoid of finite subsets of $B^*$. A finite substitution is naturally extended onto the monoid of subsets of $A^*$. If $A = B$, $\sigma$ can be iterated: $id, \sigma, \sigma^2, \ldots$. Such sequences are called iterated finite substitutions on $A^*$. Their components are sequences $\Omega_0, \Omega_1, \ldots$ of finite subsets of $A^*$, and the sets

$$\bigcup_{n=0}^{\infty} \sigma(\Omega_n) = \bigcup_{n=1}^{\infty} \Omega_n$$

are the so-called OL languages generated by $\sigma$.

Theorem 6.1. If it is decidable of a OL language whether or not it is a regular set, then the LC problem is decidable, too.

Proof. Consider the (generalized) recurrence $(1,1,e)$ in $A^*$, where $e$ is an endomorphism on $A^*$ (see the previous section), and an initial value $\omega_0 \in A^*$. The sequence generated by this recurrence + initial value, say $\omega_0, \omega_1, \ldots$, or one of
its forward translations \( \omega_1, \omega_{k+1}, \ldots \) is locally catenative (i.e., has minimal dimension 1) if and only if the submonoid \( S_1 \) of \( A^* \) generated by \( \{\omega_0, \omega_1, \ldots\} \) is a regular subset of \( A^* \), see Thm. 4.1 of [R2]. Actually there is a "degenerate" exception, duly indicated in Sect. 4 of [R2], where the regularity of \( S_1 \) does not imply local catenativity of \( \omega_0, \omega_1, \ldots \) or any of its forward translations. This "degeneracy" is, however, easily detected effectively and does not cause any problems here, see [R2]. (An example is the DOL sequence \( a, ab, ab^2, \ldots, ab^n, \ldots \).)

Suppose then that \( \omega_0, \omega_1, \ldots \) is not one of those degenerate exceptions and that \( S_1 \) is regular. We can then effectively find an \( k \) such that \( \omega_k, \omega_{k+1}, \ldots \) is locally catenative and a 1-dimensional recurrence \((1, q_1), \ldots, (1, q_u)\) for it, as is easily seen. Let the order of the obtained recurrence be \( k \). Obviously, \( \{\omega_0, \ldots, \omega_{k+k-1}\} \) is then a set of generators of \( S_1 \). If \( \omega_0, \omega_1, \ldots \) is locally catenative, it satisfies a 1-dimensional recurrence \((1, q_1'), \ldots, (1, q_u')\) of order \( k' \), say. By iterating the recurrence, if necessary, we may assume that \( k' > k + l \). On the other hand, since \( \omega_{k+k+1}', \ldots, \omega_{k+k-1}' \) (if any) belong to the submonoid of \( A^* \) generated by \( \{\omega_k', \ldots, \omega_{k+k-1}'\} \), we may assume that \( k' - q_i' < k + k - 1 \), i.e., \( q_i' < k' - k - 1 \), \( (i=1, \ldots, u') \). To check whether or not \( \omega_0, \omega_1, \ldots \) is locally catenative, it then suffices to check whether or not any of the terms of \( \omega_{k+k}', \omega_{k+k+1}', \ldots \) belong to the subset \( S_2 \) of \( A^* \) formed by those elements of the monoid \( (S_1) \) generated by \( \{\omega_0, \ldots, \omega_{k+k-1}\} \) which contain at least one generating occurrence of \( \omega_0 \). But, \( S_2 \) obviously is a regular subset of \( A^* \), and it is well-known to be decidable of any DOL sequence and any regular set \( S \) whether or not the sequence contains terms in \( S \); see e.g., [RS]. (This decidability is a special case of a more general decidability result, namely that of emptiness of the so-called ETOL languages, see e.g., [RS]. A particularly transparent explanation for these decidability results is given on p. 243 of [R5].)

All in all, to test local catenativity of DOL sequences it suffices to be able to test regularity of submonoids generated by terms of DOL sequences.

Let then \( c \) be a new symbol and let \( T \) be the submonoid of \((A \cup \{c\})^*\) generated by \( S_1 \cup \{c\} \). Now, \( T \) is a regular subset of \((A \cup \{c\})^*\) if and only if \( S_1 \) is a regular subset of \( A^* \). This follows, first, because \( S_1 \) is a morphic image of \( T \) and mapping by morphisms preserves regularity. Second, \( T \) is obtained from \( S_1 \) by regular operations and hence is regular whenever \( S_1 \) is.

But \( T \) is a 1L language over \( A \cup \{c\} \). The generating finite substitution \( \sigma \) on \((A \cup \{c\})^*\) is defined by

\[
\sigma(c) = \{c, c^2, \omega_0, \text{identity}\}
\]

\[
\sigma(a) = \{e(a)\}, \text{ if } a \in A,
\]
and it is not difficult to see that \( T = \bigcup_{n=1}^{\infty} c^n(c). \)

The regularity problem for OL languages is a notoriously difficult open problem in formal language theory (see e.g. [A1]). By Thm. 6.1, one might do well to try to solve the LC problem first. (It may be noted, too, that the set of finite substitutions generating regular OL languages is recursively enumerable, i.e., there is a (nontrivial) semialgorithm for the regularity problem, see [R5].)

Let us then turn to our second result in this section. An endomorphism \( e \) on a free monoid \( A_m^\star \) is \textit{synchronized within context} \( \ell \) if it is injective and, for all words \( w_1, w_2, w_3 \in A_m^\star \),

\[ w_1 w_2 w_3 \in e(A_m^\star) \quad \text{and} \quad w_2 \in e(A_m^\star) \Rightarrow w_1, w_2 \in e(A_m^\star). \]

**Lemma 6.1.** If an endomorphism \( e \) on \( A_m^\star \) is synchronized within context \( \ell \), then for all words \( w \in A_m^\star \) and all positive integers \( n \)

\[ w^n \in e(A_m^\star) \Rightarrow w \in e(A_m^\star). \]

**Proof.** Suppose \( w^n \in e(A_m^\star) \). Then \( w^n \in e(A_m^\star) \) so that we may replace \( n \) by its multiples and hence assume \( n \) to be arbitrarily large. Suppose then further that \( w \in e(A_m^\star) \). Write \( w^n \) as the unique catenation of words of \( e(A_m^\star) \): \( w^n = u_1 \cdots u_p \) where \( u_1, \ldots, u_p \in e(A_m^\star) \). We may assume that \( p > \ell \). Since \( w \in e(A_m^\star) \) there is an index \( i \) and words \( v \) and \( v' \) such that \( vv' = u_i \), \( w = u_1 \cdots u_{i-1} v, v, v' \not\in \text{identity} \). But then \( w^n = v' u_{i+1} \cdots u_p u_1 \cdots u_{i-1} v \) and, since \( p > \ell, v, v' \in \text{e}(A_m^\star) \). This contradicts the injectivity of \( e \).

It may be noted that it is decidable of an endomorphism \( e \) whether or not it is synchronized within context \( \ell \) for some value of \( \ell \), see Thm. 3.2 of [R2].

**Theorem 6.2.** Let \( e \) be an endomorphism on \( A_m^\star \), synchronized within context \( \ell \), and \( w \) a word of \( A_m^\star \) such that \( w \in e(A_m^\star) \) and \( w \) contains at least \( \ell \) symbols. Then the sequence \( w, e(w), e^2(w), \ldots \) has minimal dimension greater than \( 1 \) in \( A_m^\star \).

**Proof.** Assume the contrary. If the sequence \( w, e(w), e^2(w), \ldots \) satisfies a recurrence of the type \((1, q), \ldots, (1, q)\) (\( k \) copies) for some \( q \) and \( k \), then \( w^k \in e(A_m^\star) \), a contradiction by Lemma 6.1. If the sequence \( w, e(w), e^2(w), \ldots \) satisfies a recurrence of type other than the above one, then, since all words in the sequence contain at least \( \ell \) symbols, we again have \( w^k \in e(A_m^\star) \), for some \( k \geq 1 \), a contradiction.
An endomorphism synchronized within context 1 is called **totally synchronized**.

**Corollary 6.1.** Let $e$ be a totally synchronized endomorphism on $A_m^*$ and $w$ be a word of $A_m^*$. Then the sequence $w, e(w), e^2(w), \ldots$ has minimal dimension 1 if and only if it is periodic.

**Proof.** Suppose $w, e(w), e^2(w), \ldots$ is not periodic. If $w \in e(A_m^*)$ we replace $w$ by a word $w'$ such that $e(w') = w$, and consider the sequence $w', e(w'), e^2(w'), \ldots$. We continue this until we reach a word not in $e(A_m^*)$. (Note that such a word must exist.) Thm. 6.2 is now applicable.

A periodic sequence obviously has minimal dimension 1. \[\square\]

We then return to the area of our first result, viz. regularity problems and finite substitutions. We say that a finite set $F \subseteq L$ is a **universal** (resp. **existential**) test set for the set $L \subseteq A_m^*$ if, for each pair $\sigma, \tau$ of finite substitutions $A_m^* \rightarrow 2^m$,\[
\sigma(w) = \tau(w) \text{ for all } w \in L \iff \sigma(w) = \tau(w) \text{ for all } w \in F
\]
(resp.
\[
\sigma(w) \cap \tau(w) \neq \emptyset \text{ for all } w \in L \iff \sigma(w) \cap \tau(w) \neq \emptyset \text{ for all } w \in F.
\]

It was shown in [La] that not all subsets have universal test sets. We show below that not all subsets have existential test sets. Obviously subsets generating finitely generated submonoids have test sets of both types. Now, if a DOL sequence $\omega_0, \omega_1, \ldots$ is locally catenative, then the submonoid generated by $\{\omega_0, \omega_1, \ldots\}$ is finitely generated and hence $\{\omega_0, \omega_1, \ldots\}$ has test sets of both types. A characterization of those subsets which have both universal and existential test sets may thus contribute to the solution of the LC problem.

Suppose $A$ has more than two symbols and let $c$ and $d$ be different symbols of $A$. Take then a set $L \subseteq A_m^*$ such that

(i) $L$ is infinite,

(ii) each word of $L$ begins with $c$ and ends with $d$, and

(iii) each word of $L$ contains only one occurrence of $c$ and one occurrence of $d$. 

\[\square\]
We claim that \( L \) has no existential test sets. Consider an arbitrary finite automaton \( M \) with alphabet \( C = A - \{c, d\} \), states \( Q \), initial states \( S \), final states \( T \) and transition relation \( \delta \subseteq Q \times C \times Q \). Define the substitutions \( \sigma \) and \( \tau \) on \( A^* \) by

\[
\sigma(c) = \{ cq \mid q \in S \} \\
\sigma(d) = \{ qd \mid q \in T \} \\
\sigma(a) = \{ q_1 a q_2 \mid (q_1, a, q_2) \in \delta \} \text{ for } a \in C \\
\tau(c) = \{c\} \\
\tau(d) = \{ q^2 d \mid q \in T \} \\
\tau(a) = \{ q^2 a \mid (q, a, q') \in \delta \text{ for some } q' \in Q \} \text{ for } a \in C.
\]

Thus \( \sigma \) and \( \tau \) are finite substitutions \( A^* \to 2^{B^*} \) where \( B = A \cup Q \) (and we assume, of course, that \( A \) and \( Q \) are disjoint). Now, \( M \) accepts a word \( w \in C^* \) if and only if \( \sigma(cwd) \cap \tau(cwd) \neq \emptyset \), as is easily seen.

Suppose then, contrary to the claim, that \( L \) has an existential test set \( F \). Denote \( F' = \{ w \mid cwd \in F \} \). Then \( F' \) is a finite set and hence a regular set, recognized by some finite automaton \( M \). Let \( \sigma \) and \( \tau \) be as above. But then the infinite set \( \{ w \mid cwd \in L \} \) is included in \( F' \), a contradiction.

If we restrict ourselves to bounded finite substitutions, i.e., we fix a number \( k \) (the degree) and consider only finite substitutions \( \sigma : A^* \to 2^{2^k} \) such that \( \text{card}(\sigma(a)) \leq k \) for all \( a \in A \), then all sets \( L \subseteq A^* \) have test sets of both types. For universal test sets this was shown in \( [AL] \). The existence of these test sets follows easily from Hilbert's Basis Theorem, once we use a matrix representation for \( B^* \) (as in Sect. 3, 5 and 7).

As an example, let us consider the case where \( k = 2 \) and \( A = B = \{a, b\} \). We identify \( B^* \) as the monoid \( M_2 \) generated by the matrices

\[
\begin{pmatrix}
1 & 0 \\
0 & 10
\end{pmatrix}, \quad 
\begin{pmatrix}
1 & 1 \\
0 & 10
\end{pmatrix},
\]

say, in the obvious way. Suppose that, for two finite substitutions \( \sigma, \tau : A^* \to 2^A \) of degree 2, we want to test whether or not \( \sigma(abba) \cap \tau(abba) \neq \emptyset \).

We take eight variable matrices in \( M_2 \):

\[
X_{ij} = \begin{pmatrix}
1 & X_{ij} \\
0 & Y_{ij}
\end{pmatrix}, \quad U_{ij} = \begin{pmatrix}
1 & U_{ij} \\
0 & V_{ij}
\end{pmatrix} \quad (i, j = 1, 2)
\]

and write all \( 2^8 \) equations \( S = T \) which we get by taking \( S \) from \( E_1 E_2 E_1' \) and \( T \) from \( T_1 T_2 T_1' \) where \( E_i = \{X_{i1}, X_{i2}\} \), \( T_i = \{U_{i1}, U_{i2}\} \) \((i = 1, 2)\). Each such equation
can be written as a polynomial equation in the variables $x_{ij}$, $y_{ij}$, $u_{ij}$ and $v_{ij}$ $(i,j=1,2)$ because

$$
\begin{pmatrix}
1 & t_1 \\
0 & s_1
\end{pmatrix} = 
\begin{pmatrix}
1 & t_2 \\
0 & s_2
\end{pmatrix} \iff (t_1-t_2)^2 + (s_1-s_2)^2 = 0.
$$

So we have a set of polynomial equations $P_1 = 0, \ldots, P_k = 0$ (where $k = 2^8$). If we are interested in existential test sets, we note first that

$$P_1 = 0 \text{ or } P_2 = 0 \text{ or } \cdots \text{ or } P_k = 0 \iff P_1 \cdots P_k = \text{def } \sum_{abba} = 0.$$

In this way we get, for each word $w \in L$, a polynomial $P_w$ in the variables $x_{ij}$, $y_{ij}$, $u_{ij}$ and $v_{ij}$ $(i,j=1,2)$ such that

$$\sigma(w) \cap \tau(w) \neq \emptyset \iff \text{The equation } P_w = 0 \text{ has a solution (corresponding to } \sigma \text{ and } \tau).$$

By Hilbert's Basis Theorem the system $P_w = 0$ $(w \in L)$ of equations has an equivalent finite subsystem.

For universal test sets the proof is quite analogous: We take an $S$ from $S_1 S_2 S_3 S_4$ and consider the $2^4$ equations $S=T$ which we get by taking in turn all $T$'s from $T_1 T_2 T_3 T_4$. These are combined disjunctively to a single polynomial equation, as above. The procedure is repeated for all possible $S$'s. We get a system of polynomial equations for testing whether or not $\sigma(abba) \subseteq \tau(abba)$. A similar system is obtained for the reverse inclusion, and finally for each word of $L$.

The resulting (infinite) system of polynomial equations has an equivalent finite subsystem by HBT, etc.

**Note 6.2.** It is not clear how one should define finite substitutions in free groups (not to speak of metabelian groups). However, morphisms, i.e. 1-bounded finite substitutions, can, of course, be defined. The above proof then carries through, that is, each subset of a finitely generated free group has a test set for morphisms (the types are now the same). Finitely generated free groups have matrix representations, for instance the group generated by

$$
\begin{pmatrix}
1 & 2 \\
0 & 1
\end{pmatrix}, \quad \begin{pmatrix}
1 & 0 \\
2 & 1
\end{pmatrix}
$$

is free.
7. The method of [R6] and [R4]

In this section we have a look at the constructions in [R6] and [R4] which use a generalization of recurrences closely related to that discussed at the end of Sect. 5. So, as an example, consider $A_{10}^*$ and embed it in $M_{10}$ (see Sect. 3 and 5). Take a recurrence of order 1 and dimension $d$ in $A_{10}^*$ (as embeded in $M_{10}$) and the upper right hand entries of the corresponding matrices. It is not difficult to see that for numbers in these entries we have a (numerical) linear recurrence

$$f_{n}^{(i)} = \sum_{j=1}^{d} F_{ij}(n) f_{n-1}^{(j)} \quad (i=1, \ldots, d)$$

where the $F_{ij}$'s are of the form

$$F_{ij}(n) = \sum_{k=1}^{10} p_{ijk}(n)$$

and the sequences $p_{ijk}(1), p_{ijk}(2), \ldots$ are recurrent in $\mathbb{N}$.

It is shown in [R6] that, possibly after an effectively obtainable decomposition and an unspecified number $N$ of forward translations, we may apply the elimination method to obtain

$$F(n)f_{n}^{(1)} = \sum_{j=1}^{d} F_{j}(n) f_{n-j}^{(1)}$$

where $F$ and the $F_{j}$'s are differences of expressions of the form (1), and effectively obtainable. Moreover, (2) is nontrivial, i.e. $F(n) \neq 0$. The problem is that the number $N$ is so far not known to be effectively calculable, only its existence is guaranteed. An algorithm for checking existence of zero terms in recurrent sequences in $\mathbb{Z}$ would give an algorithm for obtaining $N$, but this is a famous open problem, as mentioned in Sect. 5.

Since

$$\begin{bmatrix} 1 & a \\ 0 & 10^y \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 10 \end{bmatrix}^x = \begin{bmatrix} 1 & a10^x \\ 0 & 10^{x+y} \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 \\ 0 & 10 \end{bmatrix}^x \begin{bmatrix} 1 & a \\ 0 & 10^y \end{bmatrix} = \begin{bmatrix} 1 & a \\ 0 & 10^{x+y} \end{bmatrix}$$

$$\begin{bmatrix} 1 & a10^{-y} \\ 0 & 10^x \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & 10^y \end{bmatrix} = \begin{bmatrix} 1 & a+b \\ 0 & 10^{x+y} \end{bmatrix}$$
\[
\begin{pmatrix}
1 & a
\end{pmatrix}^{-1} = \begin{pmatrix}
1 & -10^{-y} a \\
0 & 10^{-y}
\end{pmatrix}
\]

and
\[
\begin{pmatrix}
1 & a10^x \\
0 & 10^y
\end{pmatrix} = \begin{pmatrix}
1 & 0 \\
0 & 10
\end{pmatrix}^{-x} \begin{pmatrix}
1 & a \\
0 & 10^y
\end{pmatrix} \begin{pmatrix}
1 & 0 \\
0 & 10
\end{pmatrix}^x.
\]

(2) implies that the recurrent sequence \(\omega_0, \omega_1, \ldots\) defined by our recurrence (in \(M_{10}\)) satisfies a (nontrivial) recurrence
\[
Z(n)\left(\prod_{i=1}^{k_0} X_{Oi}^{-1}(n) \omega_{n} X_{Oi}(n)\right) \left(\prod_{i=1}^{g_0} Y_{Oi}^{-1}(n) \omega_{n} Y_{Oi}(n)\right) = \left(\prod_{j=1}^{d} \prod_{i=1}^{k_j} X_{ji}^{-1}(n) \omega_{n-j} X_{ji}(n)\right) \left(\prod_{i=1}^{\ell_j} Y_{ji}^{-1}(n) \omega_{n-j} Y_{ji}(n)\right)
\]

where the \(X_{ji}\)'s, the \(Y_{ji}\)'s and \(Z\) are of the form \(\begin{pmatrix} 1 & 0 \\ 0 & 10 \end{pmatrix}^x\).

[R6] and [R4] are concerned with equivalence of recurrent sequences in free monoids and use numerical coding and linear recurrences. The main methods of investigating equivalence of linear recurrent sequences use either

(i) greatest common divisors of linear operators,
(ii) lowest common multiples of linear operators, or
(iii) other operators governing the difference of the sequences whenever such operators are easily obtained.

In [R6] and [R4] we chose (i) (the most elegant approach in many ways). (ii) could be used here also (and actually was used in [R7]). Since we start with linear recurrence systems of order 1, (iii) is possible in [R6] and [R4] (and [R7]), too, and would actually lead to somewhat simpler argumentation: Starting from two linear recurrences
\[
f_n^{(i)} = \sum_{j=1}^{d} F_{ij}(n)f_{n-1}^{(j)} \quad (i=1, \ldots, d)
\]
\[
g_n^{(i)} = \sum_{j=1}^{e} G_{ij}(n)g_{n-1}^{(j)} \quad (i=1, \ldots, e)
\]
we may consider the linear recurrence
\[
\begin{align*}
    f_n^{(i)} &= \sum_{j=1}^{d} F_{ij}(n) f_{n-1}^{(j)} \quad (i=1, \ldots, d) \\
    g_n^{(i)} &= \sum_{j=1}^{e} G_{ij}(n) g_{n-1}^{(j)} \quad (i=1, \ldots, e) \\
    h_n &= f_n^{(1)} - g_n^{(1)}
\end{align*}
\]

in order to investigate the equality of \( f_0^{(1)}, f_1^{(1)}, \ldots \) and \( g_0^{(1)}, g_1^{(1)}, \ldots \), use elimination to obtain a recurrence equation of type (2) for \( h_0, h_1, \ldots \), etc.

8. Inference

As in Sect. 4, we consider here only semigroups and groups with a decidable word problem. Suppose we have a "black box" which gives us terms of a recurrent sequence \( \omega_0, \omega_1, \ldots \), as many as we want. How many terms does one need to infer the underlying recurrence + initial values (or one of them)?

If no additional information about the recurrence is provided, then no finite amount of terms suffices for the inference because recurrent sequences may share arbitrarily many initial terms without being equivalent. This is true even if an upper bound on the order or on the dimension is given, but not both. So let us assume that (at least) upper bounds on order and dimension are provided. By Thm. 2.1 we may assume that the order of the recurrence equals 1 and an upper bound \( d \) on the dimension is given.

It follows from Thm. 3.2 (and its proof) that for commutative groups (and semigroups embeddable in them) a finite number of terms is sufficient for inference: one simply goes through systematically all recurrences of order 1 and dimension not higher that \( d \), and checks whether they define \( \omega_0, \omega_1, \ldots \) using the algorithm for the equivalence problem.

Although we know that equivalence of recurrent sequences is decidable in other cases, too, e.g. in free monoids, free groups and metabelian groups, the inference problem remains open for them in the absence of any further information (in addition to the bound on the dimension, that is). Indeed, as far as our present knowledge goes, it may well be impossible to infer the recurrence on this information alone, no matter how many terms we have available.

What then would be appropriate further information which would make inference possible without making the set of candidates (recurrences + initial values) finite? (Inference among finitely many candidates is obviously possible whenever
equivalence of recurrent sequences can be decided.) One possibility is inference of initial values where we know the recurrence but do not know anything about its initial values. (Somewhat more generally we might know that the recurrence comes from a known finite collection of recurrences.) A closer look at the proofs in Sect. 4 reveals that inference of initial values is possible in free monoids, free groups and metabelian groups.

References


[Co] Cohn, H.: Growth types of Fibonacci and Markoff. Fibonacci Quart. 17 (1979), 178-183


[Da] Davies, O.L. (ed.): The Design and Analysis of Industrial Experiments. Oliver and Boyd (1967)


