RAIRO-Theor. Inf. Appl. **42** (2008) 361–374
DOI: 10.1051/ita:2007037

Available online at:
www.rairo-ita.org

D0L SEQUENCE EQUIVALENCE IS IN *P* FOR FIXED ALPHABETS

Keijo Ruohonen[1]

Abstract. A new algorithm is presented for the D0L sequence equivalence problem which, when the alphabets are fixed, works in time polynomial in the rest of the input data. The algorithm uses a polynomial encoding of words and certain well-known properties of $\mathbb{Z}$-rational sequences.

Mathematics Subject Classification. 68Q45.

1. Introduction

The *D0L sequence equivalence problem* is the following. Given a finite alphabet Σ, endomorphisms δ_1 and δ_2 on Σ^*, and words $\omega_1, \omega_2 \in \Sigma^*$, decide whether or not the sequences $(\delta_1^n(\omega_1))_{n=0}^{\infty}$ and $(\delta_2^n(\omega_2))_{n=0}^{\infty}$ are the same. While such sequences have appeared here and there before, they became quite well-known in the 1970s as sequences generated by certain Lindenmayer systems. (In L systems terminology the relevant data is gathered as $(\Sigma, \delta_i, \omega_i)$ and called a D0L system. Theory of L systems is widely discussed in [19,20].)

The first algorithm for solving the problem was given by Čulik II and Friš [5]. Later several algorithms of different types have been presented, see *e.g.* [6,7,11,21,22]. The complexity of all these algorithms is prohibitively high. Ehrenfeucht and Rozenberg gave an upper bound in [8] and another upper bound is obtained in [21] but these are both extremely large. An explicit upper bound was recently obtained in [24], even for the more general HD0L sequence equivalence problem. It is much smaller than the ones in [8,21] but still nonpolynomial for fixed alphabets. Existence of even smaller bounds has been suspected long, though. Indeed, the well-known "$2n$ conjecture" says that to check the equivalence it suffices to do this for the $2m$ first terms of the sequences where m is the

Keywords and phrases. D0L system, equivalence problem, polynomial-time algorithm.

[1] Institute of Mathematics, Tampere University of Technology, 33101 Tampere, Finland; keijo.ruohonen@tut.fi

Article published by EDP Sciences

cardinality of Σ. So far the conjecture has been proved only for the case $m = 2$ (see [16]). Obviously this conjecture — or any similar conjecture with a bound depending on m only — would, if true, imply that the equivalence problem is in P for any fixed m. Honkala has recently shown that in many special cases such bounds do in fact exist, see [12–15].

If just existence of an algorithm is of interest, then it is perhaps fair to say that it follows almost trivially from certain elementary properties of metabelian groups (as pointed out in [22], following an idea in [1]). This remains true also for the more general HDT0L sequence equivalence problem. It is even possible to use this approach and well-known methods for finding Gröbner bases to get an implementable algorithm for the problem (see [23]). Basically one then tests initial terms of the sequences trying to find a basis, and stopping is quaranteed by Hilbert's Basissatz[1]. Worst-case complexity of this algorithm is thus difficult to estimate and probably quite high. It does seem to work fairly well for small and moderate size instances of the D0L sequence equivalence problem, though.

In view of all this, it is odd that no truly nontrivial examples of equivalent D0L sequences seem to be known. Indeed, in all examples we have seen equivalence can be shown by fairly simple *ad hoc* methods. This and the difficulty in getting fast algorithms for the equivalence problem might be seen as indicating that such nontrivial examples exist but they are very rare and very large.

We show here that an algorithm exists for the D0L sequence equivalence problem which is polynomial-time in any fixed alphabets. We use a polynomial representation of words, as in [23,24]. As in [24] we derive a linear recurrence formula for D0L sequences in this representation, but in a different way to obtain easier complexity considerations. We do not give an explicit polynomial time bound as it would be quite large and depend on the sizes of the alphabets in a complicated way. Our algorithm is implementable in a computer algebra system but probably inferior to the one in [23].

2. $\mathbb{Z}$-rational sequences. A brief overview

We will need certain properties of $\mathbb{Z}$-rational sequences. We give here a very brief overview without proofs. $\mathbb{Z}$-rational sequences — as coefficient sequences of $\mathbb{Z}$-rational formal power series — are widely discussed *e.g.* in [3,25].

A $\mathbb{Z}$-*rational sequence* is a sequence $(f_n)_{n=0}^{\infty}$ satisfying a linear homogeneous recurrence with constant coefficients (LHRCC in short)

$$f_n = c_1 f_{n-1} + c_2 f_{n-2} + \ldots + c_k f_{n-k} \quad \text{for} \quad n \geq k$$

where the coefficients $c_1, c_2, \ldots, c_k$ and the initial values $f_0, f_1, \ldots, f_{k-1}$ are integers. k is the *order* of the LHRCC. The *characteristic polynomial* of the LHRCC is the monic polynomial

$$\chi(r) = r^k - c_1 r^{k-1} - \ldots - c_{k-1} r - c_k \in \mathbb{Z}[r].$$

[1] In fact, existence of an algorithm is also easily proved directly from the Basissatz, see [11].

The roots of χ are the *characteristic roots* of the LHRCC. (We exclude the trivial case where $k = 0$.)

$\mathbb{Z}$-rational sequences $(f_n)_{n=0}^{\infty}$ can be identified with integer sequences having a *matrix representation, i.e.*, a representation of the form

$$f_n = \mathbf{e}\mathbf{M}^n\mathbf{d}^{\mathsf{T}} \quad (n \geq 0)$$

where, for some k, $\mathbf{e}$ and $\mathbf{d}$ are k-vectors with integer entries and $\mathbf{M}$ is a $k \times k$-matrix with integer entries. (Our vectors will be row vectors.) Indeed, a matrix representation corresponding to the LHRCC is obtained using the companion matrix of its characteristic polynomial. On the other hand, an LHRCC corresponding to a matrix representation is obtained from the characteristic polynomial of the matrix $\mathbf{M}$ *via* the Cayley–Hamilton theorem. Note that in the resulting LHRCC the coefficients satisfy $c_{k-n_0+1} = \ldots = c_k = 0$ and $c_{k-n_0} \neq 0$ where n_0 is the multiplicity of zero as an eigenvalue of $\mathbf{M}$.

Using matrix representations it is easy to see that if $(f_n)_{n=0}^{\infty}$ and $(g_n)_{n=0}^{\infty}$ are $\mathbb{Z}$-rational sequences satisfying LHRCCs of orders k_1 and k_2 then $(f_n \pm g_n)_{n=0}^{\infty}$ and $(f_n g_n)_{n=0}^{\infty}$ are $\mathbb{Z}$-rational sequences satisfying LHRCCs of orders $k_1 + k_2$ and $k_1 k_2$, respectively. (Just take the direct sums and the Kronecker products of the matrices and the vectors.) Moreover, $(f_n)_{n=0}^{\infty}$ and $(g_n)_{n=0}^{\infty}$ both satisfy the same LHRCC of order $k_1 + k_2$. Thus, to check whether the two sequences are the same, it suffices to check the first $k_1 + k_2$ terms.

A *p-decomposition* of a $\mathbb{Z}$-rational sequence $(f_n)_{n=0}^{\infty}$, satisfying an LHRCC of order k, is the collection of sequences

$$(f_{pn+j})_{n=0}^{\infty} \quad (j = k, \ldots, k + p - 1).$$

(Note that the first k terms of $(f_n)_{n=0}^{\infty}$ are excluded in order to get rid of possible initial values that do not affect later terms.) The sequences $(f_{pn+j})_{n=0}^{\infty}$ are the *components* of the p-decomposition and, as is easily seen using a matrix representation, they are $\mathbb{Z}$-rational sequences satisfying the same LHRCC of order at most k and not having zero as its characteristic root.

We then turn to properties concerning the zero terms in a $\mathbb{Z}$-rational sequence $(f_n)_{n=0}^{\infty}$. A fundamental result is

Theorem 2.1 (Skolem–Mahler–Lech)**.** *If the $\mathbb{Z}$-rational sequence $(f_n)_{n=0}^{\infty}$ contains zero terms, then there exist nonnegative integers $a_1, \ldots, a_N$ and $b_1, \ldots, b_N$ such that*

$$\{n \mid f_n = 0\} = \{a_j n + b_j \mid n \geq 0 \text{ and } j = 1, \ldots, N\}.$$

Moreover, each nonzero a_j divides the lcm C of the orders of those primitive roots of unity which can be expressed as ratios of two characteristic roots.

The theorem was first proved using p-adic methods (see *e.g.* [17]), an elementary proof was later obtained by Hansel [10], see also [9]. The latter part of the theorem is an easy consequence of the first part. Berstel and Mignotte [2] showed that

Lemma 2.2. $C \leq e^{2k\sqrt{3 \ln k}}$.

This of course implies that it is decidable whether or not a $\mathbb{Z}$-rational sequence has infinitely many zero terms. On the other hand, it is a famous open problem whether it is decidable if a $\mathbb{Z}$-rational sequence has a zero term. The problem is known to be NP-hard (see [4]), and decidable in the special case $k \leq 5$ (see [9]).

We say that a $\mathbb{Z}$-rational sequence has the *finite-zeros property* if it either is identically zero or has only finitely many zero terms. It may be noted that an upper bound is known for the number of zero terms, if finite, which depends only on k (and is triply exponential in k, see [26]).

Lemma 2.3. *The components of a p-decomposition of $(f_n)_{n=0}^{\infty}$ where C divides p have the finite-zeros property.*

Proof. This follows from the Skolem–Mahler–Lech theorem. The components cannot have only finitely many nonzero terms as is seen by applying the LHRCC backwards. □

Suppose then that we have two doubly indexed collections of $\mathbb{Z}$-rational sequences,

$$(f_n^{(l,i)})_{n=0}^{\infty} \quad (l = 1, \ldots L \text{ and } i = 1, \ldots, M)$$

and

$$(g_n^{(l,i)})_{n=0}^{\infty} \quad (l = 1, \ldots, L \text{ and } i = 1, \ldots, M),$$

all sequences satisfying the same LHRCC of order k. We denote

$$\mathbf{f}_n^{(l)} = (f_n^{(l,1)}, \ldots, f_n^{(l,M)}) \quad \text{and} \quad \mathbf{g}_n^{(l)} = (g_n^{(l,1)}, \ldots, g_n^{(l,M)}) \quad (l = 1, \ldots, L).$$

Then the sequence $(F_n)_{n=0}^{\infty}$ where

$$F_n = \sum_{l=1}^{L} \|\mathbf{f}_n^{(l)} - \mathbf{g}_n^{(l)}\|^2$$

satisfies an LHRCC of order k^2. By Lemmas 2.2 and 2.3, components of the K-decomposition of the sequence $(F_n)_{n=0}^{\infty}$ where

$$K = \left\lfloor e^{2k^2\sqrt{6\ln k}} \right\rfloor !$$

will then have the finite-zeros property. Thus the finite-zeros property of $(F_n)_{n=0}^{\infty}$ can be forced by a decomposition depending only on the order k.

Lemma 2.4. *If, for the K-decomposition above and the j*th *components, there is an infinite sequence $\sigma_1, \sigma_2, \ldots$ of L-permutations such that*

$$\mathbf{f}_{Kn+j}^{(l)} = \mathbf{g}_{Kn+j}^{(\sigma_n(l))} \quad (n \geq 0 \text{ and } l = 1, \ldots, L)$$

then

$$\mathbf{f}_{Kn+j}^{(l)} = \mathbf{g}_{Kn+j}^{(\sigma(l))} \quad (n \geq 0 \text{ and } l = 1, \ldots, L)$$

for some (single) L-permutation σ.

Proof. Assume there is such a sequence of L-permutations. Some L-permutation σ must then occur infinitely many times in the sequence. The lemma now follows because the sequence $(G_n)_{n=0}^{\infty}$ where

$$G_n = \sum_{l=1}^{L} \|\mathbf{f}_n^{(l)} - \mathbf{g}_n^{(\sigma(l))}\|^2$$

also satisfies an LHRCC of order k^2 and components of its K-decomposition have the finite-zeros property by Lemma 2.3. □

3. Polynomial representation of words and morphisms

Consider an alphabet $\Sigma = \{a_1, \ldots, a_m\}$. We denote by $[w]$ the canonical image of a word $w \in \Sigma^*$ in the free commutative monoid generated by Σ, identified with $\mathbb{N}^m$.

The so-called *Magnus representation* μ for the word monoid Σ^* is the faithful polynomial-matrix-representation given by

$$a_i \rightleftharpoons \mu(a_i) = \begin{pmatrix} 1 & 0 \\ x_i & u_i \end{pmatrix} \quad (i = 1, \ldots, m)$$

where $x_1, \ldots, x_m$ (collectively denoted by $\mathbf{x}$) and $u_1, \ldots, u_m$ (collectively denoted by $\mathbf{u}$) are different polynomial variates, see [18][2]. Representation of a word $w \in \Sigma^*$ is then of the form

$$w \rightleftharpoons \mu(w) = \begin{pmatrix} 1 & 0 \\ p(\mathbf{x}, \mathbf{u}) & \mathbf{u}^{\boldsymbol{\alpha}} \end{pmatrix}$$

where $\boldsymbol{\alpha}$ is the multi-index $(\alpha_1, \ldots, \alpha_m) = [w]$ and

$$p(\mathbf{x}, \mathbf{u}) = \sum_{i=1}^{m} p_i(\mathbf{u}) x_i \quad \text{and} \quad \mathbf{u}^{\boldsymbol{\alpha}} = u_1^{\alpha_1} \ldots u_m^{\alpha_m}.$$

Here $p_i(\mathbf{u})$ and $\mathbf{u}^{\boldsymbol{\alpha}}$ are polynomials with integer coefficients. Catenation of words is represented by matrix multiplication:

$$\begin{pmatrix} 1 & 0 \\ q(\mathbf{x}, \mathbf{u}) & \mathbf{u}^{\boldsymbol{\beta}} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ r(\mathbf{x}, \mathbf{u}) & \mathbf{u}^{\boldsymbol{\gamma}} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ q(\mathbf{x}, \mathbf{u}) + \mathbf{u}^{\boldsymbol{\beta}} r(\mathbf{x}, \mathbf{u}) & \mathbf{u}^{\boldsymbol{\beta}+\boldsymbol{\gamma}} \end{pmatrix}.$$

The empty word is thus represented by the identity matrix.

The following properties of the representation $\mu(w)$ are easily proved by induction.

- The total degree of each of the polynomials $p_1(\mathbf{u}), \ldots, p_m(\mathbf{u})$ is less than $\alpha_1 + \cdots + \alpha_m$ (the total degree of $\mathbf{u}^{\boldsymbol{\alpha}}$).
- Nonzero coefficients of the polynomials $p_1(\mathbf{u}), \ldots, p_m(\mathbf{u})$ are all $= 1$.

[2]Originally Magnus representation was applied to finitely generated free metabelian groups.

- The grand total number of terms in the polynomials $p_1(\mathbf{u}), \ldots, p_m(\mathbf{u})$ equals the length of the word w.

We will consider polynomials of the form $\sum_{i=1}^{m} p_i(\mathbf{u})x_i$, such as those appearing as lower left elements in the matrices, as elements of the free $\mathbb{Z}[\mathbf{u}]$-module $\mathcal{M}$ generated by $x_1, \ldots, x_m$ or as elements of the vector space $\mathcal{V}$ over $\mathbb{Z}(\mathbf{u})$ (the quotient field of $\mathbb{Z}[\mathbf{u}]$) generated by $x_1, \ldots, x_m$. We will mostly use the customary vectorial notation:

$$\mathbf{p}(\mathbf{u}) = (p_1(\mathbf{u}), \ldots, p_m(\mathbf{u})).$$

For a polynomial $p(\mathbf{u}) \in \mathbb{Z}[\mathbf{u}]$ we will need its representation in the so-called *unitary form*

$$p(\mathbf{u}) = \sum_{l=1}^{L^+} \mathbf{u}^{\boldsymbol{\alpha}_l^+} - \sum_{l=1}^{L^-} \mathbf{u}^{\boldsymbol{\alpha}_l^-}.$$

This representation is not unique, and $p(\mathbf{u})$ is the zero polynomial exactly when, for some L, $L^+ = L^- = L$ and there is an L-permutation σ such that $\boldsymbol{\alpha}_l^+ = \boldsymbol{\alpha}_{\sigma(l)}^-$ $(l = 1, \ldots, L)$. (On the other hand, unitary representation of a nonzero polynomial with the least possible number of terms is unique.)

Consider then an endomorphism δ on Σ^*. We denote by $[\delta]$ the endomorphism on $\mathbb{N}^m$ induced by δ under the canonical morphism. We identify $[\delta]$ with an $m \times m$-matrix whence

$$[\delta(w)] = [w][\delta].$$

Further, we denote

$$\mu(\delta(a_i)) = \begin{pmatrix} 1 & 0 \\ r_i(\mathbf{x}, \mathbf{u}) & \mathbf{u}^{\boldsymbol{\alpha}_i} \end{pmatrix} \quad (i = 1, \ldots, m).$$

The endomorphism δ thus induces two mappings. First, the endomorphism d on $\mathbb{Z}[\mathbf{u}]$ defined by

$$d(u_i) = \mathbf{u}^{\boldsymbol{\alpha}_i} = \mathbf{u}^{[\delta(a_i)]} \quad (i = 1, \ldots, m),$$

and second the additive mapping $D : \mathcal{M} \longrightarrow \mathcal{M}$ given by

$$D\left(\sum_{i=1}^{m} p_i(\mathbf{u})x_i\right) = \sum_{i=1}^{m} d(p_i(\mathbf{u}))r_i(\mathbf{x}, \mathbf{u}) \quad (i = 1, \ldots, m).$$

Thus $d(\mathbf{u}^{\boldsymbol{\alpha}}) = \mathbf{u}^{\boldsymbol{\alpha}[\delta]}$. The latter mapping can be given in a matrix-vector-form

$$D(\mathbf{p}(\mathbf{u})) = d(\mathbf{p}(\mathbf{u}))\mathbf{R}(\mathbf{u})$$

where $\mathbf{R}(\mathbf{u}) = (r_{ij}(\mathbf{u}))$ is the $m \times m$-matrix given by

$$r_i(\mathbf{x}, \mathbf{u}) = \sum_{j=1}^{m} r_{ij}(\mathbf{u})x_j \quad (i = 1, \ldots, m).$$

Note that, while D is not a module morphism, it does behave in a similar way because, for $q(\mathbf{u}) \in \mathbb{Z}[\mathbf{u}]$,

$$D(q(\mathbf{u})\mathbf{p}(\mathbf{u})) = d(q(\mathbf{u}))D(\mathbf{p}(\mathbf{u})).$$

Note also that δ does not induce a mapping on $\mathbb{Z}(\mathbf{u})$ unless $[\delta]$ is nonsingular — a rather restrictive assumption, implying *e.g.* that δ is injective — which is why we need to work in both $\mathcal{V}$ and $\mathcal{M}$.

4. Polynomial representation of D0L sequences

Take a D0L system $G = (\Sigma, \delta, \omega)$ with alphabet Σ of cardinality m, endomorphism δ on Σ^* and $\omega \in \Sigma^*$. We will exclude the (simple) case where $\delta^n(\omega)$ equals the empty word for some n.

Magnus representation of the sequence $(\delta^n(\omega))_{n=0}^{\infty}$ generated by the system gives

$$\mu(\delta^n(\omega)) = \begin{pmatrix} 1 & 0 \\ s_n(\mathbf{x}, \mathbf{u}) & \mathbf{u}^{\boldsymbol{\beta}_n} \end{pmatrix} \quad (n \geq 0).$$

As the sequence $(\mathbf{u}^{\boldsymbol{\beta}_n})_{n=0}^{\infty}$ is easily handled (see the next section and note that $\boldsymbol{\beta}_n = [\omega][\delta]^n$) we will take a closer look at the sequence $(s_n(\mathbf{x}, \mathbf{u}))_{n=0}^{\infty}$ or, in vectorial notation, $(\mathbf{s}_n(\mathbf{u}))_{n=0}^{\infty}$. (Note that we have $\mathbf{s}_n(\mathbf{u}) \neq \mathbf{0}$ for $n \geq 0$.) We use the notation in the previous section.

The following simple observation is crucial for our constructs:

Lemma 4.1. *Let n_0 be the multiplicity of zero as an eigenvalue of $[\delta]$. If for a polynomial $p(\mathbf{u}) \in \mathbb{Z}[\mathbf{u}]$ we have $d^{n_1}(p(\mathbf{u})) = 0$ for some $n_1 \geq 0$ then $d^n(p(\mathbf{u})) = 0$ for all $n \geq \min\{n_0, n_1\}$.*

Proof. Assume $d^{n_1}(p(\mathbf{u})) = 0$ for some $n_1 \geq 0$ and take a unitary representation for $p(\mathbf{u})$:

$$p(\mathbf{u}) = \sum_{l=1}^{L^+} \mathbf{u}^{\boldsymbol{\alpha}_l^+} - \sum_{l=1}^{L^-} \mathbf{u}^{\boldsymbol{\alpha}_l^-}.$$

Since

$$d^n(p(\mathbf{u})) = \sum_{l=1}^{L^+} \mathbf{u}^{\boldsymbol{\alpha}_l^+ [\delta]^n} - \sum_{l=1}^{L^-} \mathbf{u}^{\boldsymbol{\alpha}_l^- [\delta]^n}$$

we must have $L^+ = L^- = L$ and there is an L-permutation σ such that

$$(\boldsymbol{\alpha}_l^+ - \boldsymbol{\alpha}_{\sigma(l)}^-)[\delta]^{n_1} = \mathbf{0} \quad (l = 1, \ldots, L).$$

It follows immediately that

$$(\boldsymbol{\alpha}_l^+ - \boldsymbol{\alpha}_{\sigma(l)}^-)[\delta]^n = \mathbf{0} \quad (n \geq n_1 \text{ and } l = 1, \ldots, L).$$

Each sequence $((\boldsymbol{\alpha}_l^+ - \boldsymbol{\alpha}_{\sigma(l)}^-)[\delta]^n)_{n=0}^\infty$ however satisfies the LHRCC given by the Cayley–Hamilton theorem applied to $[\delta]$. Applying this LHRCC backwards then proves the claim. □

We note next that we have a recursion giving $\mathbf{s}_n(\mathbf{u})$ in terms of $\mathbf{s}_{n-1}(\mathbf{u})$:

$$\mathbf{s}_n(\mathbf{u}) = D(\mathbf{s}_{n-1}(\mathbf{u})) = d(\mathbf{s}_{n-1}(\mathbf{u}))\mathbf{R}(\mathbf{u}).$$

This is not very useful as such, and we will derive a linear homogeneous recurrence with nonconstant coefficients for the sequence $(\mathbf{s}_n(\mathbf{u}))_{n=0}^\infty$ taking the terms as elements of the vector space $\mathcal{V}$, possibly ignoring a number of initial terms. For this purpose, for $n = 0, 1, \ldots$, define t_n to be the largest number such that the vectors $\mathbf{s}_n(\mathbf{u}), \ldots, \mathbf{s}_{n+t_n-1}(\mathbf{u})$ are linearly independent. Since $\mathbf{s}_n(\mathbf{u}) \neq \mathbf{0}$, we have $1 \leq t_n \leq m$. A basic property of these numbers is

Lemma 4.2. *Either* $t_{n+1} = t_n$ *or* $t_{n+1} = t_n - 1$ $(n \geq 0)$.

Proof. We show first that the sequence $t_0, t_1, \ldots$ is nonincreasing. If $t_n = m$, then obviously $t_{n+1} \leq t_n$. Consider then the case $t_n < m$. Because the vectors $\mathbf{s}_n(\mathbf{u}), \ldots, \mathbf{s}_{n+t_n}(\mathbf{u})$ are linearly dependent, for each $(t_n+1) \times (t_n+1)$-submatrix $\mathbf{S}(\mathbf{u})$ of the $(t_n+1) \times m$-matrix

$$\begin{pmatrix} \mathbf{s}_n(\mathbf{u}) \\ \vdots \\ \mathbf{s}_{n+t_n}(\mathbf{u}) \end{pmatrix}$$

we have $\det(\mathbf{S}(\mathbf{u})) = 0$. Since then also $\det(d(\mathbf{S}(\mathbf{u}))) = d(\det(\mathbf{S}(\mathbf{u}))) = 0$ it follows that the same is true for the matrix

$$\begin{pmatrix} \mathbf{s}_{n+1}(\mathbf{u}) \\ \vdots \\ \mathbf{s}_{n+t_n+1}(\mathbf{u}) \end{pmatrix} = \begin{pmatrix} d(\mathbf{s}_n(\mathbf{u})) \\ \vdots \\ d(\mathbf{s}_{n+t_n}(\mathbf{u})) \end{pmatrix} \mathbf{R}(\mathbf{u})$$

whence $t_{n+1} \leq t_n$.

Since the vectors $\mathbf{s}_n(\mathbf{u}), \ldots, \mathbf{s}_{n+t_n-1}(\mathbf{u})$ are linearly independent, it is not possible that $t_{n+1} < t_n - 1$. □

By the lemma, within the $m(n_0+m-1)+1$ first terms of the sequence $t_0, t_1, \ldots$ we must have at least $n_0 + m$ consecutive terms of equal value, say

$$t_{n_1} = t_{n_1+1} = \ldots = t_{n_1+n_0+m-1} = t$$

where n_1 is chosen to be the smallest possible. (As above, n_0 denotes the multiplicity of zero as an eigenvalue of $[\delta]$.) Choice of the bound $n_0 + m$ will become clear below. Note that

$$n_1 \leq (m-1)(n_0+m-1).$$

The $t \times m$-matrices

$$\begin{pmatrix} \mathbf{s}_{n_1+i}(\mathbf{u}) \\ \vdots \\ \mathbf{s}_{n+i+t-1}(\mathbf{u}) \end{pmatrix} = \begin{pmatrix} d^i(\mathbf{s}_{n_1}(\mathbf{u})) \\ \vdots \\ d^i(\mathbf{s}_{n_1+t-1}(\mathbf{u})) \end{pmatrix} d^{i-1}(\mathbf{R}(\mathbf{u})) \cdots d(\mathbf{R}(\mathbf{u}))\mathbf{R}(\mathbf{u})$$

$(i = 0, \ldots, n_0)$ will thus all be of the full rank t. It follows that for at least one $t \times t$-submatrix $\mathbf{S}(\mathbf{u})$ of

$$\begin{pmatrix} \mathbf{s}_{n_1}(\mathbf{u}) \\ \vdots \\ \mathbf{s}_{n_1+t-1}(\mathbf{u}) \end{pmatrix}$$

we have

$$d^i(\det(\mathbf{S}(\mathbf{u}))) = \det(d^i(\mathbf{S}(\mathbf{u}))) \neq 0 \quad (i = 0, \ldots, n_0).$$

Applying Lemma 4.1 we see then that in fact

$$d^i(\det(\mathbf{S}(\mathbf{u}))) \neq 0 \quad (i \geq 0).$$

We are now ready to derive the desired linear homogeneous recurrence (with non-constant coefficients) for the sequence $(\mathbf{s}_n(\mathbf{u}))_{n=0}^{\infty}$. Since the vectors $\mathbf{s}_{n_1}(\mathbf{u}), \ldots, \mathbf{s}_{n_1+t-1}(\mathbf{u})$ are linearly independent while $\mathbf{s}_{n_1}(\mathbf{u}), \ldots, \mathbf{s}_{n_1+t}(\mathbf{u})$ are linearly dependent, $\mathbf{s}_{n_1+t}(\mathbf{u})$ is a unique linear combination of $\mathbf{s}_{n_1}(\mathbf{u}), \ldots, \mathbf{s}_{n_1+t-1}(\mathbf{u})$ in $\mathcal{V}$. Solving the system

$$(c_0(\mathbf{u}), \ldots, c_{t-1}(\mathbf{u})) \begin{pmatrix} \mathbf{s}_{n_1}(\mathbf{u}) \\ \vdots \\ \mathbf{s}_{n_1+t-1}(\mathbf{u}) \end{pmatrix} = \mathbf{s}_{n_1+t}(\mathbf{u})$$

for $c_0(\mathbf{u}), \ldots, c_{t-1}(\mathbf{u})$ in $\mathbb{Z}(\mathbf{u})$ using Cramer's rule and the nonsingular submatrix $\mathbf{S}(\mathbf{u})$ we get

$$c_h(\mathbf{u}) = \frac{f_h(\mathbf{u})}{\det(\mathbf{S}(\mathbf{u}))} \quad (h = 0, \ldots, t-1)$$

for some polynomials $f_0(\mathbf{u}), \ldots, f_{t-1}(\mathbf{u}) \in \mathbb{Z}[\mathbf{u}]$. (Note that these polynomials will also be $t \times t$-determinants, formed of elements of $\mathbf{s}_{n_1}(\mathbf{u}), \ldots, \mathbf{s}_{n_1+t}(\mathbf{u})$.) Thus

$$\det(\mathbf{S}(\mathbf{u}))\mathbf{s}_{n_1+t}(\mathbf{u}) = f_{t-1}(\mathbf{u})\mathbf{s}_{n_1+t-1}(\mathbf{u}) + \cdots + f_0(\mathbf{u})\mathbf{s}_{n_1}(\mathbf{u}).$$

Applying now D repeatedly on both sides of the above equation we get the recurrence

$$g_n(\mathbf{u})\mathbf{s}_{n+t}(\mathbf{u}) = g_{n,t-1}(\mathbf{u})\mathbf{s}_{n+t-1}(\mathbf{u}) + \ldots + g_{n,0}(\mathbf{u})\mathbf{s}_n(\mathbf{u}) \quad \text{for } n \geq n_1$$

where $g_{n_1}(\mathbf{u}) = \det(\mathbf{S}(\mathbf{u}))$ and $g_{n_1,h}(\mathbf{u}) = f_h(\mathbf{u})$ and

$$g_{n+1}(\mathbf{u}) = d(g_n(\mathbf{u})) \quad \text{and} \quad g_{n+1,h}(\mathbf{u}) = d(g_{n,h}(\mathbf{u})).$$

As noted, $g_n(\mathbf{u}) \neq 0$ for $n \geq n_1$, meaning that the recurrence is well-defined in $\mathcal{V}$.

Since $\mathbf{s}_n(\mathbf{u}) \neq \mathbf{0}$, it follows, by Lemma 4.1, that for at least one h the coefficient polynomials $g_{n,h}(\mathbf{u})$ on the right hand side must be $\neq 0$ for $n \geq n_1$. In fact, especially

$$g_{n,0}(\mathbf{u}) \neq 0 \quad (n \geq n_1)$$

because otherwise, by Lemma 4.1, we have $g_{n_0+n_1,0}(\mathbf{u}) = 0$ and one the numbers $t_{n_1+1}, \ldots, t_{n_0+n_1+t-1}$ will be less than t, contradicting the bound $n_0 + m$ above.

The recurrence thus obtained is uniquely determined by the sequence $(\mathbf{s}_n(\mathbf{u}))_{n=0}^{\infty}$ in the sense that the rational functions

$$\frac{g_{n,h}(\mathbf{u})}{g_n(\mathbf{u})} \quad (n \geq n_1 \text{ and } h = 0, \ldots, t-1)$$

are unique. This follows immediately from the following lemma since subtracting two such recurrences, leading coefficients divided out and different in the sense mentioned, will give rise to a linear dependence of t consecutive terms in the sequence $(\mathbf{s}_n(\mathbf{u}))_{n=0}^{\infty}$.

Lemma 4.3. *$t_n = t$ for all $n \geq n_1$.*

Proof. We know that $t_{n_1} = t$. Suppose, contrary to what is claimed, that for some $n \geq n_1$ we have $t_n = t$ and $t_{n+1} = t - 1$ (*cf.* Lem. 4.2). Then the vectors $\mathbf{s}_n(\mathbf{u}), \ldots, \mathbf{s}_{n+t-1}(\mathbf{u})$ are linearly independent while $\mathbf{s}_{n+1}(\mathbf{u}), \ldots, \mathbf{s}_{n+t}(\mathbf{u})$ are linearly dependent. It follows that $\mathbf{s}_{n+t}(\mathbf{u})$ is a linear combination of the vectors $\mathbf{s}_{n+1}(\mathbf{u}), \ldots, \mathbf{s}_{n+t-1}(\mathbf{u})$. However, the recurrence formula we obtained implies that $\mathbf{s}_n(\mathbf{u})$ is a linear combination of $\mathbf{s}_{n+1}(\mathbf{u}), \ldots, \mathbf{s}_{n+t}(\mathbf{u})$, and thus of $\mathbf{s}_{n+1}(\mathbf{u}), \ldots, \mathbf{s}_{n+t-1}(\mathbf{u})$ as well, a contradiction. □

The recurrence we have derived is thus the unique recurrence of minimal order for the sequence $(\mathbf{s}_n(\mathbf{u}))_{n=0}^{\infty}$, valid after ignoring n_1 initial terms of the sequence.

Finally we want to point out that if we measure the size of the D0L system $G = (\Sigma, \delta, \omega)$ by, say,

$$|G| = \max_{a \in \Sigma} \{|\delta(a)|, |\omega|\}$$

where vertical bars denote length of word, then, for any fixed m, the above constructs are obviously in polynomial time with respect to $|G|$. Remember also that the nonzero coefficients of the polynomials in $\mathbf{s}_n(\mathbf{u})$ all equal 1, and that the total number of terms in $\mathbf{s}_n(\mathbf{u})$ equals $|\delta^n(\omega)|$. Thus the coefficients as well as the numbers of terms of the polynomials $g_n(\mathbf{u})$ and $g_{n,h}(\mathbf{u})$ are polynomially bounded with respect to $|G|$.

5. The algorithm

As inputs, we have two D0L systems $G_1 = (\Sigma, \delta_1, \omega_1)$ and $G_2 = (\Sigma, \delta_2, \omega_2)$ where the cardinality of Σ is denoted by m. If the sequences of words generated by G_1 and G_2 both contain the empty word, then their equivalence is easily determined in polynomial time. Obviously, if only one of the sequences contains the empty

word then they are not equivalent, and again this is easily detected in polynomial time. We may thus assume that G_1 and G_2 do not generate the empty word. We denote by n_0 the larger of the multiplicities of zero as an eigenvalue of $[\delta_1]$ and $[\delta_2]$. Then $n_0 \leq m-1$ because otherwise at least one of the systems would generate the empty word.

Our algorithm then proceeds as follows.

(1) The first step is to verify that the $2(m-1)^2+m+1$ first terms of the sequences generated by G_1 and G_2 are the same. (This clearly can be done in polynomial time.) If not, then the systems do not generate the same sequence, and we stop.

Equality of this many initial terms of the generated sequences makes it possible to carry out the construct described in the previous section for both D0L systems, taking care of ignored initial terms and guaranteeing equality of initial values of the recurrences obtained. Note especially that it also guarantees that the sequences $([\omega_1][\delta_1]^n)_{n=0}^{\infty}$ and $([\omega_2][\delta_2]^n)_{n=0}^{\infty}$ are identical because they both satisfy the same LHRCC of order $2m$ and $2m \leq 2(m-1)^2+m+1$.

(2) We then apply the construct explained in the previous section to both D0L systems. Since $n_0 \leq m-1$, we have

$$(m-1)(n_0+m-1) \leq 2(m-1)^2.$$

Sufficiently many initial terms of the D0L sequences being assumed the same, the numbers n_1 and t will therefore be the same for both systems, and $n_1 \leq 2(m-1)^2$. Thus, starting from the D0L systems, two recurrences are derived for $n \geq n_1$, first

$$g_n^{(1)}(\mathbf{u})\mathbf{s}_{n+t}^{(1)}(\mathbf{u}) = g_{n,t-1}^{(1)}(\mathbf{u})\mathbf{s}_{n+t-1}^{(1)}(\mathbf{u}) + \ldots + g_{n,0}^{(1)}(\mathbf{u})\mathbf{s}_n^{(1)}(\mathbf{u})$$

for G_1, and second

$$g_n^{(2)}(\mathbf{u})\mathbf{s}_{n+t}^{(2)}(\mathbf{u}) = g_{n,t-1}^{(2)}(\mathbf{u})\mathbf{s}_{n+t-1}^{(2)}(\mathbf{u}) + \ldots + g_{n,0}^{(2)}(\mathbf{u})\mathbf{s}_n^{(2)}(\mathbf{u})$$

for G_2, such that none of the coefficients $g_n^{(1)}(\mathbf{u}), g_n^{(2)}(\mathbf{u}), g_{n,0}^{(1)}(\mathbf{u}), g_{n,0}^{(2)}(\mathbf{u})$ equals the zero polynomial. Furthermore, the recurrences are unique, in the sense that the rational functions

$$\frac{g_{n,h}^{(1)}(\mathbf{u})}{g_n^{(1)}(\mathbf{u})} \quad \text{and} \quad \frac{g_{n,h}^{(2)}(\mathbf{u})}{g_n^{(2)}(\mathbf{u})}$$

are uniquely determined by the D0L sequences. Should the sequences be equivalent then the above rational functions would have to be equal.

(3) Since now $\mathbf{s}_n^{(1)}(\mathbf{u}) = \mathbf{s}_n^{(2)}(\mathbf{u})$ $(n = n_1, \ldots, n_1+t-1)$, the initial values of the recurrences obtained above are identical. What then remains to be

checked is whether or not

$$\frac{g_{n,h}^{(1)}(\mathbf{u})}{g_n^{(1)}(\mathbf{u})} = \frac{g_{n,h}^{(2)}(\mathbf{u})}{g_n^{(2)}(\mathbf{u})} \quad i.e. \quad g_{n,h}^{(1)}(\mathbf{u})g_n^{(2)}(\mathbf{u}) = g_n^{(1)}(\mathbf{u})g_{n,h}^{(2)}(\mathbf{u})$$

for $n \geq n_1$ and $h = 0, \ldots, t-1$. We first check whether this holds for $n = n_1, \ldots, n_1 + 2m - 1$. If that is not the case then G_1 and G_2 do not generate the same sequence, and we stop. (Note that this could be included in item (1) since, for any $n_2 \geq n_1$, the above equalities will follow for $n = n_1, \ldots, n_2$ if the equality $\delta_1^n(\omega_1) = \delta_2^n(\omega_2)$ holds for $n = n_1, \ldots, n_2+t$.)

(4) To show how the remaining values $n \geq n_1 + 2m$ are dealt with, consider as an example the case $h = 0$. The other cases are of course quite similar, note however the possibility that $g_{n,h}^{(1)}(\mathbf{u}) = 0$ or $g_{n,h}^{(2)}(\mathbf{u}) = 0$, easily dealt with using Lemma 4.1.

We begin by writing the polynomials $g_n^{(1)}(\mathbf{u}), g_n^{(2)}(\mathbf{u}), g_{n,0}^{(1)}(\mathbf{u}), g_{n,0}^{(2)}(\mathbf{u})$ in their unitary forms. This is done first for $n = n_1$ using the least possible numbers of terms, and then applying $[\delta_1]$ and $[\delta_2]$ repeatedly to the multi-indices. Multiplying these unitary representations we then get the unitary representations

$$g_{n,0}^{(1)}(\mathbf{u})g_n^{(2)}(\mathbf{u}) - g_n^{(1)}(\mathbf{u})g_{n,0}^{(2)}(\mathbf{u}) = \sum_{l=1}^{L^+} \mathbf{u}^{\boldsymbol{\alpha}_{l,n}^+} - \sum_{l=1}^{L^-} \mathbf{u}^{\boldsymbol{\alpha}_{l,n}^-} \quad (n \geq n_1).$$

If $L^+ \neq L^-$, the generated D0L sequences are not the same, and we stop. So we may assume that $L^+ = L^- = L$.

(5) The sequences of the multi-indices above are of the form

$$\boldsymbol{\alpha}_{l,n}^{\pm} = \boldsymbol{\beta}_{1,l}^{\pm}[\delta_1]^{n-n_1} + \boldsymbol{\beta}_{2,l}^{\pm}[\delta_2]^{n-n_1} \quad (n \geq n_1)$$

for some integer vectors $\boldsymbol{\beta}_{1,l}^{\pm}$ and $\boldsymbol{\beta}_{2,l}^{\pm}$, and thus they all satisfy the same LHRCC of order $2m$. We take the K-decompositions of these sequences with $k = 2m$ and

$$K = \left\lfloor e^{8m^2\sqrt{6\ln 2m}} \right\rfloor !$$

(see Sect. 2). Lemma 2.4 then becomes applicable (with $M = m$), and we know that either the generated D0L sequences are not the same or then, for each $j = n_1 + 2m, \ldots, n_1 + 2m + K - 1$, there is an N-permutation σ_j such that

$$\boldsymbol{\alpha}_{l,Kn+j}^{+} = \boldsymbol{\alpha}_{\sigma_j(l),Kn+j}^{-} \quad (n \geq 0 \text{ and } l = 1, \ldots, L).$$

(6) Finally we check existence of the permutations σ_j by searching through and testing equivalence of polynomially many sequences satisfying the same LHRCC of order at most $2m$. If all permutations σ_j exist, then the D0L sequences are equivalent, otherwise they are not.

We have then proved

Theorem 5.1. *There is an algorithm which, for any two given D0L systems* $(\Sigma, \delta_1, \omega)$ *and* $(\Sigma, \delta_2, \omega_2)$ *decides the equivalence of the sequences* $(\delta_1^n(\omega_1))_{n=0}^{\infty}$ *and* $(\delta_2^n(\omega_2))_{n=0}^{\infty}$ *working in polynomial time with respect to*

$$\max_{a\in\Sigma}\{|\delta_1(a)|, |\omega_1|\} \quad \textit{and} \quad \max_{a\in\Sigma}\{|\delta_2(a)|, |\omega_2|\}$$

for any fixed Σ.

6. Discussion

It is immediate that if the size m of the alphabet is not kept fixed, the algorithm described above will be multiply-exponential-time in m, and not that much better than applying the bound obtained in [24]. It remains an open problem whether or not there are algorithms for the D0L sequence equivalence problem singly-exponential-time in m, or even polynomial-time in all input data. An algorithm of the former type does follow from the $2n$-conjecture. Existence of a polynomial-time algorithm on the other hand might mean that there cannot be any "truly nontrivially" equivalent D0L sequences, and sequence equivalence could be decided by some simple testing of the input data.

References

[1] M.H. Albert and J. Lawrence, A proof of Ehrenfeucht's conjecture. *Theoret. Comput. Sci.* **41** (1985) 121–123.

[2] J. Berstel and M. Mignotte, Deux problèmes décidables des suites récurrentes linéaires. *Bull. Soc. Math. France* **104** (1976) 175–184.

[3] J. Berstel and C. Reutenauer, *Rational Series and Their Languages.* Springer-Verlag (1988).

[4] V.D. Blondel and N. Portier, The presence of a zero in an integer linear recurrent sequence is NP-hard to decide. *Linear Algebra Appl.* **351–352** (2002) 91–98.

[5] K. Čulik II and I. Friš, The decidability of the equivalence problem for D0L-systems. *Inform. Control* **35** (1977) 20–39.

[6] K. Čulik II and J. Karhumäki, A new proof for the D0L sequence equivalence problem and its implications, in *The Book of L,* edited by G. Rozenberg and A. Salomaa. Springer-Verlag (1986) 63–74.

[7] A. Ehrenfeucht and G. Rozenberg, Elementary homomorphisms and a solution of the D0L sequence equivalence problem. *Theoret. Comput. Sci.* **7** (1978) 169–183.

[8] A. Ehrenfeucht and G. Rozenberg, On a bound for the D0L sequence equivalence problem. *Theoret. Comput. Sci.* **12** (1980) 339–342.

[9] V. Halava, T. Harju, M. Hirvensalo and J. Karhumäki, Skolem's Problem — On the Border Between Decidability and Undecidability. *TUCS Technical Report No* **683** (2005) (submitted).

[10] G. Hansel, Une démonstration simple du théorème de Skolem-Mahler-Lech. *Theoret. Comput. Sci.* **244** (1986) 91–98.

[11] J. Honkala, A short solution for the HDT0L sequence equivalence problem. *Theoret. Comput. Sci.* **244** (2000) 267–270.

[12] J. Honkala, A polynomial bound for certain cases of the D0L sequence equivalence problem. *Theoret. Comput. Syst.* **34** (2001) 263–272.
[13] J. Honkala, The equivalence problem of polynomially bounded D0L systems — a bound depending only on the size of the alphabet. *Theoret. Comput. Syst.* **36** (2003) 89–103.
[14] J. Honkala, An n^2-bound for the ultimate equivalence problem of certain D0L systems over an n-letter alphabet. *J. Comput. Syst. Sci.* **71** (2005) 506–519.
[15] J. Honkala, A new bound for the D0L sequence equivalence problem. *Acta Inform.* **43** (2007) 419–429.
[16] J. Karhumäki, On the equivalence problem for binary D0L systems. *Inform. Control* **50** (1981) 276–284.
[17] D.J. Lewis, Diophantine equations: p-adic methods, in *Studies in Number Theory*, edited by W.J. LeVeque. *MAA Studies in Mathematics. Vol.* **6** MAA (1969) 25–75.
[18] W. Magnus, On a theorem of Marshall Hall. *Ann. Math.* **40** (1954) 764–768.
[19] G. Rozenberg and A. Salomaa, *The Mathematical Theory of L Systems.* Academic Press (1980).
[20] *Handbook of Formal Languages. Vols.* **1–3**, edited by G. Rozenberg and A. Salomaa. Springer–Verlag (1997).
[21] K. Ruohonen, Test sets for iterated morphisms. *Mathematics Report No* **49**. Tampere University of Technology (1986).
[22] K. Ruohonen, Equivalence problems for regular sets of word morphisms, in *The Book of L,* edited by G. Rozenberg and A. Salomaa. Springer-Verlag (1986) 393–401.
[23] K. Ruohonen, Solving equivalence of recurrent sequences in groups by polynomial manipulation. *Fund. Inform.* **38** (1999) 135–148.
[24] K. Ruohonen, Explicit test sets for iterated morphisms in free monoids and metabelian groups. *Theoret. Comput. Sci.* **330** (2005) 171 –191.
[25] A. Salomaa and M. Soittola, *Automata-Theoretic Aspects of Formal Power Series.* Springer–Verlag (1978).
[26] W.M. Schmidt, The zero multiplicity of linear recurrence sequences. *Acta Math.* **182** (1999) 243–282.

Communicated by J. Karhumäki.
Received August 21, 2006. Accepted September 18, 2007.