On Solutions of Linear Functional Systems

Sergei A. Abramov*
Computer Center of the
Russian Academy of Science
Vavilova 40, Moscow 117967, Russia
abramov@ccas.ru

Manuel Bronstein
INRIA – Projet CAFÉ
2004, Route des Lucioles, B.P. 93
F-06902 Sophia Antipolis Cedex, France
Manuel.Bronstein@sophia.inria.fr

ABSTRACT

We describe a new direct algorithm for transforming a linear system of recurrences into an equivalent one with nonsingular leading or trailing matrix. Our algorithm, which is an improvement to the EG elimination method [2], uses only elementary linear algebra operations (ranks, kernels and determinants) to produce an equation satisfied by the degrees of the solutions with finite support. As a consequence, we can bound and compute the polynomial and rational solutions of very general linear functional systems such as systems of differential or (q–)difference equations.

1. INTRODUCTION

Let K be a field of characteristic 0 and $K[x]$ a ring of univariate polynomials over K. Using formal power series with respect to suitable bases and the induced recurrences for their coefficients, we introduced in [5] an algorithm for computing all the solutions in $K[x]$ of homogeneous and inhomogeneous functional equations of the form $Ly = 0$ or $Ly = f$ for a large class of K–linear maps $L : K[x] \to K[x]$. That algorithm was applicable in particular to linear ordinary differential, difference and q–difference equations with coefficients in $K[x]$. In this paper, we generalize that algorithm to a similar class of K–linear maps $L : K[x]^m \to K[x]^r$. As a consequence, we obtain direct algorithms for solving systems of linear ordinary differential, difference and q–difference equations, as well as mixed differential/q–difference equations. Our algorithm, which is based on constructing and transforming a linear recurrence system induced by the initial functional system, solves the following problems:

(a) Transform a linear recurrence system into an equivalent one with nonsingular leading or trailing matrix.

(b) Compute the formal power series solutions of a linear functional system with polynomial coefficients.

(c) Compute the polynomial solutions of a linear functional system with polynomial coefficients.

(d) Compute the Laurent series solutions of a linear functional system with polynomial coefficients.

Since the rational solutions of a differential system of the form $Y'(x) = A(x)Y(x)$ have their poles among the poles of $A(x)$, points (c) and (d) imply that we can compute all the rational solutions of such systems. In combination with direct algorithms for bounding the denominators of solutions, we can also compute all the rational solutions of difference and q–difference systems of the form $Y(x+1) = A(x)Y(x)$ or $Y(qx) = A(x)Y(x)$ (see Section 8).

Our contribution consists in an improvement to the EG–elimination method [2] for solving problem (a) above, which is an important component of several computer algebra algorithms besides solving problems (b), (c) and (d). We neither uncouple the systems nor compute superirreducible forms as in [3, 7], but only rely on elementary linear algebra operations that can be performed using efficient modular methods. Our algorithm, which is complete whenever the functional system is not underdetermined, has been implemented both in the Σ^{it} library[1] and in D. Khmelnov's `LinearFunctionalSystems`[2] package.

2. INDUCED RECURRENCE SYSTEMS

The algorithm of [5] was based on transforming a K–linear map $L : K[x] \to K[x]$ into a recurrence satisfied by the coefficients, with respect to a suitable basis that depends on L, of a formal power series solution of $Ly = 0$. That transformation was formalized in [6] where it was shown to be an isomorphism between certain K–algebras of linear operators acting on polynomials and sequences. We briefly recall its definition and key properties, referring to [6] for the proofs and additional details. Let $\mathcal{B} = \langle P_n \rangle_{n \geq 0}$ be a persistent sequence of polynomials, *i.e.* a sequence in $K[x]$ satisfying:

P1. $\deg P_n = n$ for $n \geq 0$,

P2. $P_n \mid P_m$ for $0 \leq n < m$.

*Supported by a grant from the French–Russian Liapunov Institute, Project No 98–03 and by a grant from the Russian Foundation for Basic Research, Project No 01–01–00047.

[1] `http://www.inria.fr/cafe/Manuel.Bronstein/sumit/`

[2] To be included in an upcoming release of MAPLE.

ISSAC 2001, UWO, Canada

Note that P1 implies that $\mathcal{B}$ is a basis of $K[x]$. Let $K[[\mathcal{B}]]$ be the K–algebra of formal power series of the form $\sum_{n\geq 0} c_n P_n$ where $c_n \in K$. Since $K[x]$ can be naturally embedded into $K[[\mathcal{B}]]$ we view it as a subalgebra of $K[[\mathcal{B}]]$. Let $K^{\mathbb{Z}}$ be the K–algebra of two–way infinite sequences with entries in K and $\kappa : K[[\mathcal{B}]] \to K^{\mathbb{Z}}$ be the mapping sending $\sum_{n\geq 0} c_n P_n$ to its coefficient sequence $c = \langle c_n \rangle_{n\in\mathbb{Z}}$, extended by taking $c_n = 0$ for $n < 0$.

We say that an endomorphism $L \in \mathrm{End}_K(K[x])$ is *compatible with $\mathcal{B}$* if there are $A, B \in \mathbb{N}$ and elements $\alpha_{i,n} \in K$ for all $n \geq 0$ and $-A \leq i \leq B$ such that

$$LP_n = \sum_{i=-A}^{B} \alpha_{i,n}\ P_{n+i} \qquad (1)$$

with $P_k = 0$ for $k < 0$. The set of the endomorphisms of $K[x]$ compatible with $\mathcal{B}$ is a K–algebra, which we denote $\mathrm{End}_{\mathcal{B}}(K[x])$. It follows from (1) that every $L \in \mathrm{End}_{\mathcal{B}}(K[x])$ can be extended to a K–algebra endomorphism of $K[[\mathcal{B}]]$ by linearity.

Let now $\phi : K^{\mathbb{Z}} \to K^{\mathbb{Z}}$ be the shift given by $\phi(a) = b$ where $b(n) = a(n+1)$ for $n \in \mathbb{Z}$. Let $\mathcal{E}$ be the K–algebra of recurrence operators of the form $R = \sum_{i=s}^{r} a_i(n)\phi^i$ with $r, s \in \mathbb{Z}$ and $a_i \in K^{\mathbb{Z}}$ for $s \leq i \leq r$. If $a_s \neq 0 \neq a_r$, then we write $r = \deg_\phi(R)$ and $s = \nu_\phi(R)$. The product in R is the composition of operators, and is given by $\phi \cdot a = \phi(a) \cdot \phi$ for any $a \in K^{\mathbb{Z}}$. Define $\mathcal{R}_{\mathcal{B}} : \mathrm{End}_{\mathcal{B}}(K[x]) \to \mathcal{E}$ by

$$\mathcal{R}_{\mathcal{B}} L = \sum_{i=-B}^{A} \alpha_{-i,n+i}\phi^i$$

where A, B and the $\alpha_{i,n}$ are given by (1).

THEOREM 1 ([6]). *$\mathcal{R}_{\mathcal{B}}$ is an isomorphism of K–algebras between $\mathrm{End}_{\mathcal{B}}(K[x])$ and $\mathcal{E}$.*

As a consequence, if $\mathrm{End}_{\mathcal{B}}(K[x])$ contains a skew–polynomial ring $K[x][\theta_1, \ldots, \theta_m]$, then $\mathcal{R}_{\mathcal{B}}$ is uniquely determined on it by $\mathcal{R}_{\mathcal{B}} x$ and $\mathcal{R}_{\mathcal{B}}\theta_1, \ldots, \mathcal{R}_{\mathcal{B}}\theta_m$. For example, $K[x][d/dx, \sigma_q]$, where σ_q is the automorphism of $K[x]$ over K that maps x to qx for a given $q \in K$, is compatible with the power basis $\mathcal{P} = \langle x^n \rangle_{n\geq 0}$ and $\mathcal{R}_{\mathcal{P}}$ is given on $K[x][d/dx, \sigma_q]$ by $\mathcal{R}_{\mathcal{P}}(x) = \phi^{-1}$, $\mathcal{R}_{\mathcal{P}}(d/dx) = (n+1)\phi$ and $\mathcal{R}_{\mathcal{P}}(\sigma_q) = q^n$. It follows that $\mathcal{R}_{\mathcal{P}}$ maps $K[x][d/dx, \sigma_q]$ into $K[n, q^n][\phi, \phi^{-1}]$. Another common example is the ring of linear ordinary difference operators $K[x][\sigma]$, where σ is the automorphism of $K[x]$ over K that maps x to $x+1$. That ring is compatible with either the binomial coefficient basis $\langle \binom{x}{n} \rangle_{n\geq 0}$ or the descending factorial basis $\langle x^{\underline{n}} \rangle_{n\geq 0}$, and is mapped by $\mathcal{R}$ into $K[n][\phi, \phi^{-1}]$ with either one.

THEOREM 2 ([6]). *For any $L \in \mathrm{End}_{\mathcal{B}}(K[x])$ and any $y \in K[[\mathcal{B}]]$, $\kappa L y = (\mathcal{R}_{\mathcal{B}} L)(\kappa y)$.*

Theorem 2 reduces finding the solutions $y \in K[x]$ of $Ly = f$ to finding the solutions $z \in K^{\mathbb{Z}}$ with finite support of $(\mathcal{R}_{\mathcal{B}} L)z = \kappa f$. When L is a linear ordinary differential, difference or q–difference equation, $\mathcal{R}_{\mathcal{B}} L$ is in $K[n][\phi, \phi^{-1}]$ or $K[q^n][\phi, \phi^{-1}]$. Therefore, an upper bound on the support of solutions with finite support can be obtained as a zero of the trailing coefficient of $\mathcal{R}_{\mathcal{B}} L$. Once that bound is known, the recurrence $\mathcal{R}_{\mathcal{B}} L$ can be used to produce formal series solutions of $Ly = f$ and the polynomial solutions are found by equating enough terms above the degree bound to 0. This is essentially the algorithm described in [5] and we now proceed to generalize it to functional systems of the form:

$$\begin{pmatrix} L_{11} & \ldots & L_{1m} \\ L_{21} & \ldots & L_{2m} \\ \vdots & & \vdots \\ L_{r1} & \ldots & L_{rm} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix} = \begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_r \end{pmatrix} \qquad (2)$$

where $L_{ij} \in \mathrm{End}_{\mathcal{B}}(K[x])$ for $1 \leq i \leq r$ and $1 \leq j \leq m$. Applying κ to row i of (2) and using Theorem 2 and the K–linearity of κ, we have

$$\kappa\left(\sum_{j=1}^{m} L_{ij} y_j\right) = \sum_{j=1}^{m} \kappa(L_{ij} y_j) = \sum_{j=1}^{m} (\mathcal{R}_{\mathcal{B}} L_{ij})(\kappa y_j)\,.$$

Applying κ and $\mathcal{R}_{\mathcal{B}}$ pointwise to vectors and matrices, this proves:

THEOREM 3. *For any matrix L with entries in $\mathrm{End}_{\mathcal{B}}(K[x])$ and any $Y \in K[[\mathcal{B}]]^m$, $\kappa L Y = (\mathcal{R}_{\mathcal{B}} L)(\kappa Y)$.*

Therefore, finding the solutions $Y \in K[x]^m$ of $LY = F$ for a given $F \in K[x]^r$ is reduced to finding the solutions $Z \in \left(K^{\mathbb{Z}}\right)^m$ with finite support of $(\mathcal{R}_{\mathcal{B}} L)Z = \kappa F$, the latter being a linear recurrence system for Z, which can be seen as a sequence of vectors in K^m. We remark that the original equations do not have to be all of the same type, it is sufficient that their operators all lie in $\mathrm{End}_{\mathcal{B}}(K[x])$ for some basis $\mathcal{B}$. For example, systems of mixed differential/q–difference equations are in the scope of Theorem 3 since $K[x][d/dx, \sigma_q] \subset \mathrm{End}_{\mathcal{P}}(K[x])$ where $\mathcal{P}$ is the power basis.

EXAMPLE 1. *Consider the mixed differential/q–difference system:*

$$\begin{pmatrix} Y_1'(2x) \\ 3077 Y_2'(x) \end{pmatrix} = \begin{pmatrix} 80x^3 + 32x^2 & x^4 - 1 \\ p(x) & q(x) \end{pmatrix} \begin{pmatrix} Y_1(x) \\ Y_2(x) \end{pmatrix} \qquad (3)$$

where

$$p(x) = 988480x^3 + 1037712x^2 + 196928x$$

and

$$q(x) = 12356x^4 + 8029x^3 - 750x^2 + 300x - 120\,.$$

In operator notation, it becomes

$$\begin{pmatrix} QD - 80x^3 - 32x^2 & 1 - x^4 \\ -p(x) & 3077D - q(x) \end{pmatrix} \begin{pmatrix} Y_1 \\ Y_2 \end{pmatrix} = 0$$

where D is d/dx and Q is the automorphism of $\mathbb{Q}(x)$ over $\mathbb{Q}$ that maps x to $2x$. Using $\mathcal{R}_{\mathcal{P}}$ where $\mathcal{P}$ is the power basis, the induced recurrence system is then

$$\begin{pmatrix} f(\phi) & 1 - \phi^{-4} \\ -p(\phi^{-1}) & 3077(n+1)\phi - q(\phi^{-1}) \end{pmatrix} \begin{pmatrix} Z_1 \\ Z_2 \end{pmatrix} = 0 \qquad (4)$$

where

$$f(\phi) = 2^n(n+1)\phi - 80\phi^{-3} - 32\phi^{-2}\,.$$

3. SOLUTIONS WITH FINITE SUPPORT

We now look for solutions $Z \in (K^m)^{\mathbb{Z}}$ with finite support of $(\mathcal{R}_{\mathcal{B}} L)Z = \kappa F$, which we write as

$$\begin{pmatrix} R_{11} & \dots & R_{1m} \\ R_{21} & \dots & R_{2m} \\ \vdots & & \vdots \\ R_{r1} & \dots & R_{rm} \end{pmatrix} Z = G \tag{5}$$

where $G \in K[[\mathcal{B}]]$ is κF for a given $F \in K[x]^m$ and $R_{ij} = \mathcal{R}_{\mathcal{B}} L_{ij}$ for some L_{ij} in $\mathrm{End}_{\mathcal{B}}(K[x])$. Letting M_k be the matrix of sequences whose $(i,j)^{\text{th}}$ entry is the coefficient of ϕ^k in R_{ij}, the system (5) is equivalent to $\left(\sum_{k=s}^{t} M_k(n)\phi^k\right)Z = G$, *i.e.*

$$\sum_{k=s}^{t} M_k(n) Z_{n+k} = G(n) \quad \text{for all } n \in \mathbb{Z} \tag{6}$$

where $s \le t \in \mathbb{Z}$ and we can assume without loss of generality that M_s and M_t are not identically 0. We have the following generalization of Theorem 1 of [5]:

THEOREM 4. *Let L be an $r \times m$ matrix with entries in $End_{\mathcal{B}}(K[x])$, $F \in K[x]^r$, $Y \in K[x]^m$ be nonzero and $N = \max_i(\deg(Y_i))$. If $LY = F$ then either $N \le s + \max_i(\deg(F_i))$ or $Ker(M_s(N-s)) \neq 0$, where M_s is as in (6).*

PROOF. Let $N = \max_i(\deg(Y_i))$, $Z = \kappa Y$ and $G = \kappa F$. Then $Z_N \neq 0$ and $Z_n = 0$ for $n > N$, so equation (6) for $n = N - s$ becomes $M_s(N-s)Z_N = G(N-s)$. If $N > s + \max_i(\deg(F_i))$, then $G(N-s) = 0$, which implies that $Z_N \in \mathrm{Ker}(M_s(N-s))$. $\square$

For Theorem 4 to yield degree bounds for the polynomial solutions of (2), the set $\{n \in \mathbb{Z} \text{ s.t. } \mathrm{Ker}(M_s(n)) \neq 0\}$ must be finite and computable. This implies in particular that $r \ge m$ in (2) and that the L_{ij}'s are all mapped by $\mathcal{R}_{\mathcal{B}}$ into $A[\phi, \phi^{-1}]$ for some *suitable* subalgebra A of $K^{\mathbb{Z}}$. By suitable, we mean that given a nonzero $p \in A$, the set $Z(p) = \{n \in \mathbb{Z} \text{ s.t. } p(n) = 0\}$ is finite and can be computed. This hypothesis is satisfied by the classical equation types as seen in the examples following Theorem 1: $A = K[n]$ when the L_{ij}'s are either all differential operators or all difference operators, $A = K[q^n]$ when the L_{ij}'s are q–difference operators, and $A = K[n, q^n]$ when the L_{ij}'s are mixed differential/q–difference operators. When K is a finitely generated extension of the rational numbers, $K[n]$ is suitable, and [4] describes algorithms showing that $K[q^n]$ and $K[n, q^n]$ are suitable whenever q is not a root of unity.

Assume from now on that the system (2) satisfies the above hypotheses. If it has a polynomial solution of degree N, then either $N \le s + \max_i(\deg(f_i))$ or $\det(M)(N-s) = 0$ for all nonsingular $m \times m$ submatrices M of M_s. If M_s has rank m, then there is at least one such submatrix, and the suitability hypothesis on A implies that we can find a finite set of candidates for N. Remark that this is always the case for $m = 1$, and we obtain in that case the algorithm of [5].

4. TRANSFORMING THE RECURRENCE

We now describe our improvement to [2] for transforming the recurrence (6) into an equivalent one, but with M_s of rank m. Write R for the matrix on the left hand side of (5).

LEMMA 1. *Suppose that $v^T R = 0$ and $v^T G \neq 0$ for some $v \in (K^{\mathbb{Z}})^r$. Then the systems (5) and (2) are inconsistent.*

PROOF. For any solution Z of (5), we have $0 = v^T RZ = v^T G \neq 0$, so (5) is inconsistent. Let $u = \mathcal{R}_{\mathcal{B}}^{-1} v$, $L = \mathcal{R}_{\mathcal{B}}^{-1} R$ and Y be any solution of $LY = F$ where $\kappa F = G$. By Theorem 1, $v^T R = 0$ implies that $u^T L = 0$, hence that $u^T F = u^T LY = 0$. Applying then κ and Theorem 3 we get $0 = \kappa(u^T F) = \mathcal{R}_{\mathcal{B}}(u^T)\kappa F = v^T G \neq 0$, so (2) is inconsistent. $\square$

Let $d_i(R) = \max_j(\deg_\phi(R_{ij}))$ for each i. Suppose that $\mathrm{rk}(M_s) < m$ and let then $v \in \mathrm{Ker}(M_s{}^T)$ be nonzero and $w = v^T R$. If $w = 0$ and $v^T G \neq 0$, then (5) and (2) are inconsistent by Lemma 1. Otherwise, let $I_v = \{i \text{ s.t. } v_i \neq 0\}$ and $d = \max_{i \in I_v}(d_i(R))$, and choose $i_0 \in I_v$ such that $d_{i_0}(R) = d$. If $w = 0$ and $v^T G = 0$, then let R' be R with row i_0 removed and G' be G with the $i_0{}^{\text{th}}$ entry removed. Finally, if $w \neq 0$, then let R' be R with row i_0 replaced by $(\phi^{-1}w_1, \dots, \phi^{-1}w_m)$ and G' be G with the $i_0{}^{\text{th}}$ entry replaced by $\phi^{-1}(v^T G)$. In both cases, replace $RZ = G$ by $R'Z = G'$ and repeat the above procedure until either M_s has rank m or strictly less than m rows.

By construction, $RZ = G \implies R'Z = G'$ in both cases, so the solutions of (5) appear among the solutions of $R'Z = G'$. We now prove that the above algorithm terminates: since $v^T M_s = 0$, $\nu_\phi(w_j) > s$ for $1 \le j \le m$, so $\nu_\phi(\phi^{-1}w_j) \ge s$, which implies that $\nu_\phi(R'_{ij}) \ge s$ for all i, j. Since $v \in A^r$, $\deg_\phi(w_j) \le d$ for $1 \le j \le m$, so $d_{i_0}(R') < d_{i_0}(R)$, which implies that $\sum_i d_i(R') < \sum_i d_i(R)$. Therefore, replacing $RZ = G$ by $R'Z = G'$, we have decreased either the number of rows of (5) or $\sum_i d_i(R)$. Since $\sum_i d_i(R) \ge rs$, the algorithm must terminate when either M_s has rank m or the system (5) has strictly less than m rows (in which case we fail to produce a degree bound since the system is in fact underdetermined).

EXAMPLE 2. *Continuing Example 1, we rewrite the recurrence system (4) as*

$$\begin{pmatrix} 2^n(n+1) & 0 \\ 0 & 3077(n+1) \end{pmatrix} Z_{n+1} + \begin{pmatrix} 0 & 1 \\ 0 & 120 \end{pmatrix} Z_n$$

$$+ \begin{pmatrix} 0 & 0 \\ -196928 & -300 \end{pmatrix} Z_{n-1} + \begin{pmatrix} -32 & 0 \\ -1037712 & 750 \end{pmatrix} Z_{n-2}$$

$$+ \begin{pmatrix} -80 & 0 \\ -988480 & -8029 \end{pmatrix} Z_{n-3} + \begin{pmatrix} 0 & -1 \\ 0 & -12356 \end{pmatrix} Z_{n-4} = 0$$

The trailing matrix is singular and its left kernel is generated by $v = (12356, -1)^T$. Letting R be the matrix on the left hand side of (4) and replacing its second row by $\phi^{-1}v^T R$, we get the new system

$$\begin{pmatrix} 2^n(n+1) & 0 \\ 0 & 0 \end{pmatrix} Z_{n+1} + \begin{pmatrix} 0 & 1 \\ 12356n2^{n-1} & -3077n \end{pmatrix} Z_n$$

$$+ \begin{pmatrix} 0 & 0 \\ 0 & 12236 \end{pmatrix} Z_{n-1} + \begin{pmatrix} -32 & 0 \\ 196928 & 300 \end{pmatrix} Z_{n-2}$$

$$+ \begin{pmatrix} -80 & 0 \\ 642320 & -750 \end{pmatrix} Z_{n-3} + \begin{pmatrix} 0 & -1 \\ 0 & 8029 \end{pmatrix} Z_{n-4} = 0$$

Continuing this process several times eventually yields a recurrence with a nonsingular trailing matrix whose determinant is $2^{n-5}(n-4)-80$ times a positive integer constant. It is easy to find (see for example [4, §4]) that its only positive integer root is $n = 9$, so Theorem 4 implies that $\max(\deg(Y_1), \deg(Y_2)) = 5$ *for any nonzero polynomial solution of (3). Using for example undetermined coefficients, we find that the polynomial solution space of (3) is generated by*

$$Y = \begin{pmatrix} x^5 + x^4 - 1 \\ -80x^4 - 112x^3 - 32x^2 \end{pmatrix}$$

REMARK 1. *The above algorithm can also be used to obtain an equivalent recurrence with M_t of rank m rather than M_s: we simply use a nonzero $v \in Ker({M_t}^T)$ and choose $i_0 \in I_v$ such that $\nu_{i_0}(R)$ is minimal for $i \in I_v$, where $\nu_i(R) = \min_j(\nu_\phi(R_{ij}))$. When $w = v^T R \neq 0$, we replace R_{i_0} by $(\phi w_1, \ldots, \phi w_m)$ and the ${i_0}^{\rm th}$ entry of G by $\phi(v^T G)$. Otherwise we either prove inconsistency of the system or remove R_{i_0} as previously. Since each step either decreases the number of rows or increases $\sum_i \nu_i(R)$, which is bounded above by rt, this process terminates either when M_t has rank m or the system has strictly less than m rows.*

We conclude this section with a note on the solution space of (5) as it evolves through the algorithm. As we have seen, $RZ = G \implies R'Z = G'$ by construction, but the converse does not always hold: if $R'Z = G'$, then it is easy to see that $v_{i_0} R_{i_0} Z = v_{i_0} G_{i_0}$ and $R_i Z = G_i$ for $i \neq i_0$, where R_i and G_i denote the $i^{\rm th}$ row of R and $i^{\rm th}$ entry of G respectively. Viewing $R_{i_0} Z = G_{i_0}$ as an infinite number of linear constraints on the values of the entries of Z, we see that they do not always follow from $v_{i_0} R_{i_0} Z = v_{i_0} G_{i_0}$ because of the possible zeroes of v_{i_0}. Since v_{i_0} is not identically 0, our suitability hypothesis on A implies that the set $Z(v_{i_0}) = \{n \in \mathbb{Z} \text{ s.t. } v_{i_0}(n) = 0\}$ is finite and can be computed. We then have

$$RZ = G \Leftrightarrow \left\{ \begin{array}{l} R'Z = G', \\ \forall n \in Z(v_{i_0}),\ \sum_{k=s}^t M_{k,i_0}(n) Z_{n+k} = G_{i_0}(n) \end{array} \right. \tag{7}$$

where M_{k,i_0} and G_{i_0} denote the ${i_0}^{\rm th}$ row of M_k and ${i_0}^{\rm th}$ entry of G respectively. Keeping the finitely many linear constraints appearing in (7) at each step through the algorithm makes it possible to replace the recurrence system (5) by the one produced by the algorithm when it terminates. While this step is optional when computing degree bounds, it becomes necessary when we use (6) to generate the solution space.

5. VALID INPUTS

Since the above algorithm fails when the number of rows drops below m, we investigate in this section what hypothesis on the initial system guarantees that the algorithm never reaches that situation (and therefore either proves inconsistency or obtains a degree bound). It turns out to be sufficient to require that the original linear system not be underdetermined. We say that a ring S is a *left Ore domain* if S has no zero divisors and if any two nonzero elements of S have a nonzero common left multiple in S.

LEMMA 2. *If the suitable subalgebra A of $K^{\mathbb{Z}}$ is an integral domain, then $A[\phi, \phi^{-1}]$ is a left Ore domain.*

PROOF. The skew–polynomial ring $F[\phi]$ is a left Ore domain [8] where F is the fraction field of A. Since every $a \in A[\phi, \phi^{-1}]$ can be written as $a = \phi^{-s} a'$ where $s \geq 0$ and $a' \in A[\phi]$, it follows that $A[\phi, \phi^{-1}]$ has no zero divisors. Let $a, b \in A[\phi, \phi^{-1}]$, write $a = \phi^{-s} a'$ and $b = \phi^{-t} b'$ where $s, t \geq 0$ and $a', b' \in A[\phi]$, and let $c \in F[\phi]$ be a nonzero left common multiple of a' and b' in $F[\phi]$. Then, $c = a''a' = b''b'$ for some $a'', b'' \in F[\phi]$. Let $d \in A$ be a nonzero common multiple of the denominators of the coefficients of a'' and b''. Then, $dc = da''a' = da''\phi^s a = db''b' = db''\phi^t b$ is a nonzero left common multiple of a and b in $A[\phi]$. □

The next result uses the notion of rank of a module over a left Ore domain [9, §0.9].

THEOREM 5. *If the suitable subalgebra A of $K^{\mathbb{Z}}$ is an integral domain and the left module generated over $A[\phi, \phi^{-1}]$ by the rows of the matrix R appearing on the left hand side of (5) has rank m, then the algorithm of Section 4 either proves that (2) is inconsistent, or it terminates with a matrix M_s of rank m.*

PROOF. For a matrix M with entries in $A[\phi, \phi^{-1}]$, we write M_i for the $i^{\rm th}$ row of M and $\mathcal{M}(M)$ for the left module generated by the M_i's over $A[\phi, \phi^{-1}]$. Using the notations of the algorithm, if $v^T R = 0$, then R' is R with the row i_0 removed, so $\mathcal{M}(R')$ is a submodule of $\mathcal{M}(R)$. Otherwise, R' is R with row i_0 replaced by $R'_{i_0} = \sum_i \phi^{-1} v_i R_i \in \mathcal{M}(R)$, so $\mathcal{M}(R')$ is again a submodule of $\mathcal{M}(R)$. Therefore, in both cases the sequence

$$0 \to \mathcal{M}(R') \to \mathcal{M}(R) \to \mathcal{M}(R)/\mathcal{M}(R') \to 0$$

is a short exact sequence of left $A[\phi, \phi^{-1}]$–modules, which implies ([9, Prop. 9.3]) that

$$\mathrm{rk}\mathcal{M}(R) = \mathrm{rk}\mathcal{M}(R') + \mathrm{rk}(\mathcal{M}(R)/\mathcal{M}(R')) .$$

Furthermore, if $v^T R = 0$, then $v_{i_0} R_{i_0} = -\sum_{i \neq i_0} v_i R_i \in \mathcal{M}(R')$. Otherwise,

$$(\phi^{-1} v_{i_0}) R_{i_0} = R'_{i_0} - \sum_{i \neq i_0} \phi^{-1} v_i R_i \in \mathcal{M}(R') .$$

Therefore, in both cases there is a nonzero $a \in A[\phi, \phi^{-1}]$ such that $a R_{i_0} \in \mathcal{M}(R')$. Let $u = t R_{i_0} + \sum_{i \neq i_0} s_i R_i \in \mathcal{M}(R)$ where t and the s_i's are in $A[\phi, \phi^{-1}]$. If $t = 0$, then $u \in \mathcal{M}(R')$. Otherwise, let $t't = a'a$ be a nonzero common left multiple of t and a in $A[\phi, \phi^{-1}]$ (Lemma 2). Then,

$$t'u = t'tR_{i_0} + \sum_{i \neq i_0} t' s_i R_i = a'aR_{i_0} + \sum_{i \neq i_0} t' s_i R_i \in \mathcal{M}(R') .$$

This implies that $\mathcal{M}(R)/\mathcal{M}(R')$ is a torsion module, so it has rank 0 and $\mathrm{rk}\mathcal{M}(R) = \mathrm{rk}\mathcal{M}(R')$. Therefore the rank of $\mathcal{M}(R)$ remains constant throughout the algorithm, so if $\mathrm{rk}\mathcal{M}(R) = m$ when it starts, it cannot produce a matrix with fewer than m rows. □

The rank condition appearing in Theorem 5 is in fact equivalent to requiring that the system (2) not be underdetermined:

COROLLARY 1. *If the suitable subalgebra A of $K^{\mathbb{Z}}$ is an integral domain and the matrix on the left hand side of (2) has m linearly independent rows over ${\mathcal{R}_{\mathcal{B}}}^{-1}(A[\phi, \phi^{-1}])$, then the algorithm of Section 4 either proves that (2) is inconsistent, or it terminates with a matrix M_s of rank m.*

PROOF. Since $\mathcal{R}_{\mathcal{B}}$ is an isomorphism of K–algebras, if there are m linearly independent rows over ${\mathcal{R}_{\mathcal{B}}}^{-1}(A[\phi,\phi^{-1}])$, then their images under $\mathcal{R}_{\mathcal{B}}$ form a linearly independent subset of $\mathcal{M}(R)$ over the fraction field of $A[\phi,\phi^{-1}]$, which implies that the rank of $\mathcal{M}(R)$ is m and Theorem 5 can be applied. $\square$

First order systems of the form

$$\left(\begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_m \end{pmatrix} \theta - B\right) Y = F \tag{8}$$

where $d_1,\dots,d_m \in K[x]$, B is a square matrix with entries in $K[x]$, F is a vector with entries in $K[x]$ and θ is either the derivation d/dx, the shift $\sigma x = x+1$ or the q–shift $\sigma_q x = qx$, satisfy the hypotheses of Corollary 1 whenever $d_1 \dots d_m \neq 0$ [2], so our algorithm always yields a degree bound for such systems.

6. COMPLEXITY AND REFINEMENTS

The algorithm of Section 4 only needs to compute ranks, determinants and nonzero elements of the kernels of matrices with entries in A. When A is a polynomial ring over K, which is the case for differential and (q–)difference equations, we can use modular and probabilistic methods such as [12] for testing whether the rank is m, [1, §7] for determinants and [11] for elements of the kernel. The worst–case complexity of those methods is $c(r+m)\rho^2 d^2$ field operations in K, where ρ is the rank of M_s, d is a bound on the degrees of its entries and c is a positive constant. Since our algorithm loops at most $r(t-s+1)$ times, the complexity of producing the equation for the degree bound is $cr(t-s)(r+m)m^2d^2$ field operations in K. This indicates that it is better not to convert systems of higher–order operators to larger first–order systems. For example, when the recurrence system is produced from a linear differential system of m equations of order ν with polynomial coefficients of degree δ, then $d = \nu$ and $t - s \le \delta + \nu$, so the above complexity becomes $cr(\delta+\nu)(r+m)m^2\nu^2$ or $c(\delta+\nu)\nu^2 m^4$ when the system is square. Remark that it is linear in the degree of the polynomial coefficients because the entries of the matrix coefficients of the recurrences do not depend on that degree.

Note that [11] is not guaranteed to return the full kernel, and that its cost increases for each additional kernel element, which is why we used only one nonzero $v \in \mathrm{Ker}({M_s}^T)$ in Section 4. However, if we use algorithms, such as fraction–free Gaussian elimination or the modular method of [10], that can produce several linearly independent elements of $\mathrm{Ker}({M_s}^T)$, then we can use those elements together in order to decrease the number of times our algorithm must loop. Suppose that we have computed a $\nu \times r$ matrix U of rank ν such that $UM_s = 0$. Pick v^T to be any row of U. Then $v^T M_s = 0$, so apply the algorithm of Section 4 using v and suppose that this leads to the transformation or elimination of the $i_0{}^{\text{th}}$ row of M_s. Then, $v_{i_0} \neq 0$, so use fraction–free Gaussian elimination on U to zero out the column i_0 except for v_{i_0}. Removing the row of U corresponding to v, we obtain a new matrix U' of rank $\nu - 1$ whose column i_0 is 0 and such that $U'M_s = 0$. We can repeat this process until all the rows of U have been used.

Additionally, instead of using any row of U, we can try first to find a linear combination v^T of the rows of U that provides the maximal decrease of $\sum_i d_i(R)$: since $UM_s = 0$, we solve $v^T U M_{s+1} = 0$ obtaining a matrix U'' such that $U'' M_{s+1} = U'' M_s = 0$, then solve $v^T U'' M_{s+2} = 0$ and continue as long as there are nonzero solutions for v. This yields a vector v that maximizes k such that $v^T M_s = \dots = v^T M_{s+k} = 0$. We then pick i such that $v_i \neq 0$ and replace row i of U by v^T and use v first in the above algorithm.

7. SOLVING THE RECURRENCE SYSTEM

Once we have a bound $N \ge 0$ for the degree of the solutions $Y \in K[x]^m$ of (1), we can always use the undetermined coefficients method to find all such solutions. However, this method has a cost of cm^3N^3 operations in K for some positive constant c since there are $m(N+1)$ unknown coefficients. Instead, we can get an algorithm whose complexity is linear in N by generalizing the method of [5] to the recurrence (6). Note first that when using the algorithm of Section 4 to make M_t nonsingular rather than M_s (see Remark 1), Theorem 5 and Corollary 1 remain valid, so assuming that their hypotheses hold, we either prove that the system is inconsistent or obtain M_t of rank m. When that is the case, if we have more than m equations, then $\mathrm{Ker}({M_t}^T) \neq 0$, so we can continue this algorithm until we have exactly m equations (this must happen since we cannot increase $\sum_i \nu_i(R)$ beyond rt). Therefore, we are reduced to finding the solutions Z of support contained in $\{0,\dots,N\}$ of a system of the form (6) where the M_k's are square matrices and M_t is nonsingular. In addition the values of the entries of Z must satisfy a finite number of linear constraints of the form (7) that have been produced by the algorithm. Since A is an integral domain and M_t is square and nonsingular, we can use fraction–free gaussian elimination to compute a nonsingular matrix B with entries in A such that BM_t is nonsingular and diagonal. Multiplying (6) by B on the left yields

$$\begin{aligned}\begin{pmatrix} d_1(n) & & \\ & \ddots & \\ & & d_m(n) \end{pmatrix} Z_{n+t} \quad &= \\ B(n)G(n) \quad &- \quad \sum_{k=s}^{t-1} B(n)M_k(n)Z_{n+k}\end{aligned} \tag{9}$$

for all $n \in \mathbb{Z}$, where $d_1,\dots,d_m \in K[x]$ are such that $d_1 \dots d_m$ is not identically 0. Given initial conditions with undetermined coefficients for Z, we use (9) with increasing values of n to express the entries of Z_{n+t} as linear forms in those undetermined coefficients until Z_{N+s+t} has been determined where N is the degree bound. When $d_i(n) = 0$ for some n, we add a new undetermined coefficient for the i^{th} entry of Z_{n+t} and add the linear constraint obtained by equating the i^{th} row of the right hand side of (9) to 0, as well as the linear constraints obtained from specializing (6) at that value of n (since $B(n)$ can be singular — note that $B(n)$ is nonsingular whenever $\prod_i d_i(n) \neq 0$). We then obtain a linear system for the undetermined coefficients by taking all the constraints (7) together with the ones obtained from the zeroes of the d_i's, and extend that system by equating Z_n with $B(n)G(n)$ for $N < n \le N+s+t$ and solve it over K. Its solutions then yield the general polynomial solution of (2).

8. RATIONAL SOLUTIONS

The power basis $\mathcal{P} = \langle x^n \rangle_{n \geq 0}$ can be extended to the basis $\langle x^n \rangle_{n \in \mathbb{Z}}$ of the field of Laurent series $K((x))$, and the definition of compatibility extended by saying that (1) must hold for all $n \in \mathbb{Z}$. Similarly, the map $\kappa : K[[x]] \to K^{\mathbb{Z}}$ can be extended to a map $K((x)) \to K^{\mathbb{Z}}$ by taking the coefficient sequence of the Laurent series, completed on the left by zeroes. Define then $\nu_x : K(x)^* \to \mathbb{Z}$ by $\nu_x(p) = \max\{n \text{ such that } x^n \mid p\}$ and $\nu_x(p/q) = \nu_x(p) - \nu_x(q)$ for $p, q \in K[x] \setminus \{0\}$. In that context, Theorem 2 still holds, and we have the following analogue of Theorem 4.

THEOREM 6. *Let $\mathcal{P} = \langle x^n \rangle_{n \in \mathbb{Z}}$, L be an $r \times m$ matrix with entries in $End_{\mathcal{P}}(K[x])$, $F \in K(x)^r$, $Y \in K(x)^m$ be nonzero and $N = \min_i(\nu_x(Y_i))$. If $LY = F$ then either $N \geq t + \min_i(\nu_x(F_i))$ or $Ker(M_t(N-t)) \neq 0$, where M_t is as in (6).*

PROOF. Let $N = \min_i(\nu_x(Y_i))$, $Z = \kappa Y$ and $G = \kappa F$. Then $Z_N \neq 0$ and $Z_n = 0$ for $n < N$, so equation (6) for $n = N - t$ becomes $M_t(N-t)Z_N = G(N-t)$. If $N < t + \min_i(\nu_x(F_i))$, then $G(N-t) = 0$, which implies that $Z_N \in \operatorname{Ker}(M_t(N-t))$. $\square$

If M_t has rank m, then Theorem 6 yields a lower bound for $\min_i(\nu_x(Y_i))$, *i.e.* an upper bound on the power of x that divides the denominator of any nonzero rational solution. Otherwise, if the hypotheses of Corollary 1 hold, then, as explained in Remark 1, we can use the algorithm of Section 4 to transform the recurrence until M_t has rank m.

8.1 Differential equations

Suppose that all the L_{ij}'s in the original system (2) are in $K[x][d/dx]$. Given any irreducible $p \in K[x]$, we use the change of variable $X = x - \alpha$ where α is the image of x in $E = K[x]/(p)$ to get a new system with entries in $E[X][d/dX]$. Since $E[X][d/dX]$ is compatible with $\langle X^n \rangle_{n \in \mathbb{Z}}$, applying the above method in $E[X]$, we get an upper bound on the power of p that divides the denominator of any nonzero rational solution of the original system. This means that we can compute all its rational solutions that have their poles in a prescribed finite set. If in addition, the original system is of the form $\sum_{i=0}^{t} A_i Y^{(i)} = F$ where the A_i's are square matrices with entries in $K[x]$, F has entries in $K[x]$ and A_t is diagonal and nonsingular, then any rational solution Y must have its finite poles among the zeroes of the determinant of A_t, so we can use our algorithm at all its irreducible factors to compute all the rational solutions.

8.2 Difference equations

For a difference system of the form $Y(x+1) - AY(x) = F$ where A and F have entries in $K(x)$, we can use either [3] or [13] to compute a universal denominator $d \in K[x]$ such that the denominator of any nonzero rational solution divides d. Replacing Y by Y'/d, we use our algorithm to get the polynomial solutions Y', thereby obtaining all the rational solutions.

8.3 q–Difference equations

Suppose finally that all the L_{ij}'s in the original system (2) are in $K[x][\sigma_q]$, where σ_q is the automorphism of $K[x]$ over K that maps x to qx for a given $q \in K$. Since $K[x][\sigma_q]$ is compatible with $\langle x^n \rangle_{n \in \mathbb{Z}}$, applying the above method yields an upper bound $\gamma \geq 0$ on the power of x that can appear in the denominator of a nonzero rational solution. If in addition, the original system is of the form $Y(qx) - AY(x) = F$, where A and F have entries in $K(x)$, then the algorithm of [3] can be applied to compute a universal denominator $d \in K[x]$ such that the denominator of any nonzero rational solution divides $x^\gamma d$. Replacing Y by $Y'/x^\gamma d$, we use our algorithm to get the polynomial solutions Y', thereby obtaining all the rational solutions.

9. REFERENCES

[1] ABBOTT, J., BRONSTEIN, M., AND MULDERS, T. Fast deterministic computation of determinants of dense matrices. In *Proceedings of ISSAC'99* (1999), S. Dooley, Ed., ACM Press, pp. 197–204.

[2] ABRAMOV, S. EG–eliminations. *Journal of Difference Equations and Applications 5* (1999), 393–433.

[3] ABRAMOV, S., AND BARKATOU, M. Rational solutions of first order difference systems. In *Proceedings of ISSAC'98* (1998), O. Gloor, Ed., ACM Press, pp. 124–131.

[4] ABRAMOV, S., AND BRONSTEIN, M. Hypergeometric dispersion and the orbit problem. In *Proceedings of ISSAC'2000* (2000), C. Traverso, Ed., ACM Press, pp. 8–13.

[5] ABRAMOV, S., BRONSTEIN, M., AND PETKOVŠEK, M. On polynomial solutions of linear operator equations. In *Proceedings of ISSAC'95* (1995), ACM Press, pp. 290–296.

[6] ABRAMOV, S., PETKOVŠEK, M., AND RYABENKO, A. Special formal series solutions of linear operator equations. *Discrete Mathematics 210* (2000), 3–25.

[7] BARKATOU, M. On rational solutions of systems of linear differential equations. *J. Symbolic Computation 28*, 4 and 5 (October/November 1999), 547–568.

[8] BRONSTEIN, M., AND PETKOVŠEK, M. An introduction to pseudo–linear algebra. *Theoretical Computer Science 157* (1996), 3–33.

[9] COHN, P. *Free Rings and their Relations (2nd edition).* Academic Press, London, 1985.

[10] MCCLELLAN, M. The exact solution of systems of linear equations with polynomial coefficients. *Journal of the ACM 20* (1973), 563–588.

[11] MULDERS, T., AND STORJOHANN, A. Rational solutions of singular linear systems. In *Proceedings of ISSAC'2000* (2000), C. Traverso, Ed., ACM Press, pp. 242–249.

[12] SCHWARTZ, J. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM 27* (1980), 701–717.

[13] VAN HOEIJ, M. Rational solutions of linear difference equations. In *Proceedings of ISSAC'98* (1998), O. Gloor, Ed., ACM Press, pp. 120–123.