A matrix Euclidean algorithm for minimal partial realization

Marc Van Barel
Adhemar Bultheel

Katholieke Universiteit Leuven
Department of Computer Science
Celestijnenlaan 200 A
B-3030 Leuven (Heverlee)
Belgium

RUNNING TITLE : A matrix Euclidean algorithm

Submitted as a synopsis of a talk held at the
International Conference on Linear Algebra and Applications
September 28-30, 1987
Universidad Politécnica de Valencia
Valencia, Spain.

A matrix Euclidean algorithm for minimal partial realization.

Marc Van Barel and Adhemar Bultheel

Abstract

Given the Markov parameters of $M(z) = T(z)^{-1}Q(z)$, with $P(z) \in K^{p\times m}[z]$ and $Q(z) \in K^{m\times m}[z]$ polynomial matrices over some field K, the algorithm we shall describe will compute right minimal partial realizations of these parameters. It can also be used to compute a greatest common left divisor of $T(z)$ and $Q(z)$.

1. Introduction

In report [10] we looked at an extension of the Berlekamp-Massey algorithm. The Berlekamp-Massey algorithm [3,4,9] solves the minimal partial realization problem for scalar sequences of Markov parameters. The matrix case is solved by an algorithm described by Dickinson, Morf and Kailath [5] and Anderson, Brasch and Lopresti [1]. Our version is algorithm A of section 12 in report [10]. In [2] Antoulas also gives an algorithm to solve the matrix case such that the solution is in the form of a matrix continued fraction. He calls his algorithm a matrix algorithm of Euclides while it is in fact a matrix Berlekamp-Massey algorithm. In [12] we related our algorithm A to the one of Antoulas.

The algorithm of Euclides is well known for finding the greatest common divisor of two (scalar) polynomials. But the algorithm has other useful applications such as the solution of the scalar minimal partial realization problem. The solution is given in the form of a continued fraction but in contrast with the matrix continued fraction of Antoulas each convergent has another structure i.e. the next convergent has more states than the previous one or the degree of the denominator polynomial of the convergent increases. To compute that part of the continued fraction that determines the next convergent the algorithm of Euclides uses more than one Markov parameter in contrast with the algorithm of Antoulas which uses just one matrix Markov parameter at each step. What we want to give in the next section is an algorithm that constructs a matrix continued fraction such that the next convergent of the continued fraction has another structure than the previous one thus maintaining as much detail as possible.

2. A matrix Euclidean algorithm

Throughout this text we shall freely use the definitions and notations of [10]. As in [11] we shall take the shift parameter $k = -1$, which corresponds to the classical minimal partial realization problem.
We recall the following: Given the $p \times m$ Markov parameters $M_1, M_2, M_3, \cdots \in K^{p\times m}$ (K an arbitrary field), consider polynomial vectors $a(z) = \sum_{i=0}^{\alpha} a_i z^i$, $a_\alpha \neq 0$ which solve

$$\begin{bmatrix} M_1 & M_2 & \cdots & M_{\alpha+1} \\ M_2 & M_3 & \cdots & \vdots \\ \vdots & \vdots & & \\ M_{n+1-\alpha} & & \cdots & M_{n+1} \\ M_{n+2-\alpha} & & \cdots & M_{n+2} \\ \vdots & & & \vdots \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_\alpha \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ r_1 \\ r_2 \\ \vdots \end{bmatrix}, \quad \alpha \leqslant n$$

$r_1 \in K^p$ possibly nonzero is called the residual and $r_1, r_2, \cdots$ is called the residual sequence. n is the level and all solutions of this system are denoted as $S(n,\alpha)$. Introduce the operators R and RS by $Ra = r_1$ and $RSa = [r_1^T r_2^T \cdots]^T$. The residual series is denoted by $RSa(z) = \sum_{i=1}^{\infty} r_i z^{-n+\alpha-i}$. The notion of degree will be extended to series in z^{-1} to mean the largest exponent of z with a nonzero coefficient. Thus the degree of $RSa(z)$ above is $-n+\alpha-1$ if $r_1 \neq 0$. We shall use the notation $dRSa$ to denote the degree of $RSa(z)$ and we shall also refer

to it as the degree of the corresponding residual sequence. We call it residual degree for short. Solution vectors $a_1^n(z), \ldots, a_m^n(z)$ of level n are solutions found on level n of lowest possible degree and with linear independent highest degree coefficients. Auxiliary vectors are solution vectors of level $< n$ whose residuals span the space $\{R[S(l,\alpha)], l = 1,2,\ldots,n-1; \alpha = 0,1,2,\ldots,l\}$ of residuals. An auxiliary vector or a solution vector is said to have potential degree π (w.r.t. level n) if it is a solution vector of degree $\pi - j$ for level $n-j$ for some j, $j = 0,1,\ldots,\pi$.
If the solution vectors of level n are assembled as the columns of a $m \times m$ matrix $A(z)$, then $A(z)$ is the right denominator of a minimal partial realization of order n for the given Markov sequence.

Because we want to construct a matrix continued fraction à la Antoulas, that is as simple as possible but whose convergents solve minimal partial realization problems of increasing orders, we construct solution vectors such that they can be used at as much further levels as possible. To find these solution vectors, we use the fact that we know all vectors of $S(n,\alpha)$. It was shown in [12] that a basis for them is given by the solution vectors and auxiliary vectors (possibly shifted) of that level. More precisely $a(z) \in S(n,\alpha)$ has the form

$$a(z) = \sum_{l=1}^{m} \sum_{d=\alpha_l}^{\alpha} \nu_{l,d} z^{d-\alpha_l} a_l^n(z) + \sum_{i=1}^{s} \sum_{j=\pi_i}^{\min(n,\alpha)} \mu_{i,j} z^{j-\pi_i} x_i(z) \tag{1}$$

where $a_1^n(z), \ldots, a_m^n(z)$ are the solution vectors of degrees $\alpha_1 \leqslant \alpha_2 \leqslant \cdots \leqslant \alpha_m$ and $x_i(z)$, $i = 1,2,\ldots,s$ are the auxiliary vectors of potential degrees $\pi_1, \pi_2, \ldots, \pi_s$ for level n.
Using formula (1), we want to transform the solution vectors a_i^n, making them solution vectors of levels as deep as possible, i.e. with least possible residual degree. In doing so we can use a_i^n not only at level n but possibly also at deeper levels.
E.g. starting from a basis for $S(0,0)$ consisting of m linearly independent constant vectors $a_1^0, \ldots, a_m^0 \in K^m$, in step D.1.1. of the algorithm D below, we only need to consider combinations of the form

$$a_i' = a_i^0 + \sum_{k=1}^{i-1} \gamma_{i,k} a_k^0.$$

More generally, in step D.2.4.1., we are given m solution vectors $a_1^{n+1}, a_2^{n+2}, \ldots, a_m^{n+1}$ of degrees $\alpha_1 \leqslant \alpha_2 \leqslant \cdots \leqslant \alpha_m$. By considering combinations of the form

$$a_i^{n+1} + \sum_{l=1}^{i-1} \sum_{d=\alpha_l}^{\alpha_l} \nu_{l,d} z^{d-\alpha_l} a_l^{n+1} + \sum_{k=1}^{s} \sum_{j=\pi_k}^{\alpha_l} \mu_{k,j} z^{j-\pi_k} x_k \tag{2}$$

where x_k are the auxiliary vectors of potential degree π_k, we shall find m solution vectors with linear independent highest degree coefficients and with residual degrees as small as possible without increasing their degrees.

Algorithm D we are going to describe now is an adaptation of algorithm A given in section 12 of [10] or its reformulation given in section 2.3 of [11]. The latter relates it to a matrix continued fraction as in [2]. More details and some examples can be found in [13].
Some comments on the notation used: For successive levels $n = 0,1,2,\ldots$, the solution vectors are computed (D.2.1.) and then, using formula (1), their residual degrees are made as small as possible (D.2.4.). Each time several matrices are updated: The numerator matrices (NM), the denominator matrices (DM) and the residual matrices (RSM). At all time $M(z)DM(z) - NM(z) = RSM(z)$. Also information about degrees and potential degrees (vector dM) is updated. Each matrix has two parts : The A-part which refers to the auxiliary vectors and the S-part which refers to the solution vectors. All transformations of these matrices can be described in terms of elementary operations applied to the columns, i.e. multiplications from the right with elementary matrices E which have the following meaning (see [11])
$E_i(a)$ = unit matrix with column i multiplied by a
E_{ij} = unit matrix with column i and column j interchanged

$E_{ij}(a)$ = unit matrix with column j replaced by column j plus a times column i.

All these transformations are collected in unimodular transformation matrices V_i (D.2.5.) where i refers to the level. They contain all the information to construct a matrix continued fraction whose convergents are the successive minimal partial realizations.

Algorithm D

D.1 {Initialisation}
$NM = [NMA \mid NMS] = [I_p \mid 0] \in K^{p\times(p+m)}[z]$ (numerator matrix)
$DM = [DMA \mid DMS] = [0 \mid I_m] \in K^{m\times(p+m)}[z]$ (denominator matrix)
$RSM = [RSMA \mid RSMS] = [-I_p \mid M(z)] \in K^{p\times(p+m)}[[z^{-1}]]$ (residual matrix)
$dM = [dMA \mid dMS] = [1 \cdots 1 \mid 0 \cdots 0] \in K^{1\times(p+m)}$ (degree matrix)

D.1.1 **For** $i = 2,3,\ldots,m$

D.1.1.1 Search for $a = a_i^0 + \sum_{l=1}^{i-1} \gamma_{i,l} a_l^0$ with $dRSa(z)$ as low as possible

D.1.1.2 Replace $\begin{bmatrix} a_i^0 \\ RSa_i^0 \end{bmatrix}$ by $\begin{bmatrix} a \\ RSa \end{bmatrix}$ in $\begin{bmatrix} DMS \\ RSMS \end{bmatrix}$

D.2 **For** $n = 0,1,2,\cdots$
Suppose we know

$NM = [y_1 \cdots y_p \mid c_1^n \cdots c_m^n]$

$DM = [x_1 \cdots x_p \mid a_1^n \cdots a_m^n]$

$RSM = [RSx_1 \cdots RSx_p \mid RSa_1^n \cdots RSa_m^n]$

$dM = [\pi_1 \cdots \pi_p \mid \alpha_1 \cdots \alpha_m]$

D.2.1 **For** $i = 1,2,\ldots,m$

D.2.1.1 Take Ra_i^n from $RSMS$ (the coefficient of $z^{-n+\alpha_i-1}$)

D.2.1.2 **If** $Ra_i^n = 0$ **then** a_i^{n+1} can be chosen as a_i^n and $V^{(i)} = I_{p+m}$

D.2.1.3 **If** $Ra_i^n \neq 0$ **then**

D.2.1.3.1 Write Ra_i^n as a linear combination of $Rx_1,\ldots,Rx_p$:

$$Ra_i^n = -\sum_{j=1}^{p} \mu_j \, Rx_j$$

D.2.1.3.2 {Update for solution vector a_i^{n+1} based on a_i^n}

D.2.1.3.2.1 Take r to be the index of the auxiliary vector with highest potential degree which is used actively in this linear combination, i.e. with $\mu_r \neq 0$ (note that $\alpha_i < \pi_r$)

D.2.1.3.2.2 Set

$$V^{(i)} = E_{r,p+i}E_{p+i}(\mu_r) \prod_{j\neq r} E_{j,p+i}(\mu_j z^{\pi_r-\pi_j})E_{r,p+i}(z^{\pi_r-\alpha_i})$$

D.2.1.3.2.3 Replace

$$\begin{bmatrix} NM \\ DM \\ RSM \end{bmatrix} \text{ by } \begin{bmatrix} NM \\ DM \\ RSM \end{bmatrix} V^{(i)}$$

D.2.1.3.2.4 {The corresponding interchange of degrees}
Replace dM by $dM \cdot E_{r,p+i}$

D.2.2 {Reordering w.r.t. dMS}
Define the permutation matrix PS such that $dMS.PS$ has its entries in non-decreasing order from left to right and reorder all other entries correspondingly i.e. replace

$$\begin{bmatrix} NMS \\ DMS \\ RSMS \\ dMS \end{bmatrix} \text{ by } \begin{bmatrix} NMS \\ DMS \\ RSMS \\ dMS \end{bmatrix} . PS.$$

D.2.3 {Prepare for the next level}
Increase the entries of dMA by 1

D.2.4 {Using formula (1), we compute now the final solution vectors for level $n+1$}

D.2.4.1 For $i = 1,2, \ldots, m$

D.2.4.1.1 **If** a_i^{n+1} is not a solution vector of level n **then**

D.2.4.1.1.1 Find a linear combination

$$a = a_i^{n+1} + \sum_{l=1}^{i-1} \sum_{d=\alpha_l}^{\alpha_l} \nu_{l,d} z^{d-\alpha_l} a_l^{n+1} + \sum_{k=1}^{p} \sum_{j=\pi_k}^{\alpha_l} \mu_{k,j} z^{j-\pi_k} x_k$$

such that $dRSa$ is as small as possible.
(Note that there may be more than 1 solution).

D.2.4.1.1.2 The previous linear combination is assembled in the unimodular matrix $W^{(i)}$:

$$W^{(i)} = \prod_{l=1}^{i-1} E_{p+l,p+i} \left(\sum_{d=\alpha_l}^{\alpha_l} \nu_{l,d} z^{d-\alpha_l} \right) \cdot \prod_{k=1}^{p} E_{k,p+i} \left(\sum_{j=\pi_k}^{\alpha_l} \mu_{k,j} z^{j-\pi_k} \right)$$

D.2.4.1.1.3 Replace

$$\begin{bmatrix} NM \\ DM \\ RSM \end{bmatrix} \text{ by } \begin{bmatrix} NM \\ DM \\ RSM \end{bmatrix} W^{(i)}$$

D.2.4.1.2 **If** a_i^{n+1} is a solution vector of level n **then** set $W^{(i)} = I_{p+m}$

D.2.5 Define

$$V_{n+1} = \begin{bmatrix} Y_{n+1} & C_{n+1} \\ X_{n+1} & A_{n+1} \end{bmatrix} = V^{(1)} \ldots V^{(m)} . P . W^{(1)} \ldots W^{(m)}$$

with $P = I \oplus PS$.

Notes

1. It is possible that in step D.2.4.1.1.1 there is more than one solution $a(z)$. It is sufficient to take one of them as the new solution vector $a_i(z)$. The solution generated is not unique.
2. Instead of the initializations $NMA = I_p$ and $DMS = I_m$, we could have taken $NMA = Y_0 \in K^{p \times p}$ and $DMS = A_0' \in K^{m \times m}$ to be any nonsingular matrices. If A_0 is the transformation of A_0' as performed in step D.1.1, then we could define

$$V_0 = \begin{bmatrix} Y_0 & C_0 \\ X_0 & A_0 \end{bmatrix} \text{ with}$$

$X_0 = 0_{m,p}$ and $C_0 = 0_{p,m}$, to complete the set of unimodular matrices

$$V_n = \begin{bmatrix} Y_n & C_n \\ X_n & A_n \end{bmatrix} \quad , \quad n = 1,2,\ldots \text{ of step D.2.5.}$$

If you now set

$$V_{0,n} = V_0 V_1 \cdots V_n = V_{0,n-1} V_n = \begin{bmatrix} Y_{0,n} & C_{0,n} \\ X_{0,n} & A_{0,n} \end{bmatrix} = \begin{bmatrix} NMA_n & NMS_n \\ DMA_n & DMS_n \end{bmatrix}$$

then

$$Y_0 \cfrac{\cdots}{C_1+Y_1 \cfrac{\cdots}{\cdots}} \Bigg/ A_1+X_1 \cfrac{\cdots}{\cdots} \Bigg/ A_0$$

has convergents $C_{0,n}A_{0,n}^{-1}$ giving solutions of the minimal partial realization problem at level n, $n = 0,1,2,\cdots$, i.e. of order $N = n$. This was shown in [11].

3. If we only know the first N Markov parameters M_k, $k = 1,\ldots,N$, we cannot compute the complete residual sequence but only some of its elements. Besides the initial zeros, you will only be able to compute $r_1, r_2, \ldots, r_{N-n}$. However the subsequent elements never enter the computations explicitly, so minimal partial realizations of order N can be computed.

4. It can be seen that the matrices NM and DM are never explicitly needed in algorithm D. The only information needed is RSM and the degrees dM. Hence these matrices can be dropped from the algorithm. The algorithm computes the (matrix) continued fraction expansion of the series $M(z)$. If the transformations V_i are performed on the NM and DM matrices, the numerators and denominators of the successive convergents are obtained by the forward evaluation method as new terms in the continued fraction are computed. If these transformations are not explicitly performed, the numerator and denominator can always be recovered by multiplying the V_i matrices.

5. When algorithm D is applied to a sequence of scalar Markov parameters ($p = m = 1$) the algorithm reduces to THE scalar algorithm of Euclides. So algorithm D can be seen as a possible generalization of the scalar algorithm of Euclides. The unimodular matrices V_n are in this case :

$$V_n = \begin{bmatrix} y_n(z) & c_n(z) \\ x_n(z) & a_n(z) \end{bmatrix} = \begin{bmatrix} 0 & c_n \\ 1 & a_n(z) \end{bmatrix}$$

where c_n is a constant different from zero such that $a_n(z)$ is a monic polynomial of degree $\geqslant 1$. Because $y_n(z) \equiv 0$ we obtain a scalar continued fraction not going upwards but only going downwards :

$$\cfrac{c_1}{\lfloor a_1(z)} + \cfrac{c_2}{\lfloor a_2(z)} + \cfrac{c_3}{\lfloor a_3(z)} + \cdots$$

For further details see [6,8].

6. The scalar algorithm of Euclides can also be used to compute a greatest common divisor of two polynomials. This property can also be extended to algorithm D. See [2]. Suppose we have a left matrix fraction description : $T(z)^{-1}Q(z)$ and we want to compute a greatest common left divisor of $T(z)$ and $Q(z)$. Starting from the Markov parameters of $T(z)^{-1}Q(z)$ we compute the unimodular matrices $V_0(z), V_1(z), V_2(z), \ldots, V_N(z)$ using algorithm D until we get a minimal realization of these Markov parameters. This means that

$$[T(z)|-Q(z)]V_0(z)V_1(z)V_2(z)\cdots V_N(z) = [T(z)|-Q(z)]\begin{bmatrix} Y_{0,N}(z) & C_{0,N}(z) \\ X_{0,N}(z) & A_{0,N}(z) \end{bmatrix} = [D(z)|0]$$

or $D(z)$ is a greatest common left divisor of $T(z)$ and $Q(z)$ unique upto a right multiplication with a unimodular matrix (See [7,p.376-378]). Note that $T(z)Y_{0,N}(z)-Q(z)X_{0,N}(z) = D(z)$, so the auxiliary vectors and the corresponding numerator vectors form the solutions of this Bezout equation.

3. Conclusion

We have adapted algorithm A of [10] and [11], which gives a solution of the minimal partial realization problem for matrix sequences, to get algorithm D, which can be seen as A generalization of THE scalar algorithm of Euclides (See notes 5 and 6).

4. References

[1] B.M. Anderson, F.M. Brasch Jr., P.V. Lopresti, The sequential construction of minimal partial realizations from finite input-output data, *SIAM J. Control*, 13:552-571 (1975).

[2] A.C. Antoulas, On recursiveness and related topics in linear systems, *IEEE Trans. Automatic Control*, AC-31:1121-1135 (1986).

[3] E.R. Berlekamp, Nonbinary BCH decoding, International symposium on Information Theory, San Remo, Italy (1962).

[4] E.R. Berlekamp, *Algebraic coding theory*, (Chapts. 7 and 10) McGraw-Hill, New York, 1968.

[5] B.W. Dickinson, M. Morf, T. Kailath, A minimal realization algorithm for matrix sequences, *IEEE Trans. Autom. Control*, AC-19:31-38 (1974).

[6] W.B. Gragg, A. Lindquist, On the partial realization problem, *Lin. Alg. Appl.* 50:277-319 (1983).

[7] T. Kailath, *Linear Systems*, Prentice Hall, Englewood Cliffs, N.J.,1980.

[8] R.E. Kalman, On partial realizations, transfer functions and canonical forms, *Acta Polytechnica Scandinavica*, 31:9-32 (1979).

[9] J.L. Massey, Shift register synthesis and BCH decoding, *IEEE Trans. Information Theory*, IT-15:122-127 (1969).

[10] M. Van Barel, A. Bultheel, A minimal partial realization algorithm for MIMO systems, Report TW79, Dept. Computer Science, Katholieke Universiteit Leuven, July 1986, Revised: April 1987.

[11] M. Van Barel, A. Bultheel, A minimal partial realization algorithm for MIMO systems: II. A matrix continued fraction, Report TW91, Dept. Computer Science, Katholieke Universiteit Leuven, June 1987. See also The minimal partial realization problem, matrix continued fractions and matrix transfer functions, submitted for : Proceedings of the MTNS Conference, Arizona Biltman, Phoenix (June 1987).

[12] M. Van Barel, A. Bultheel, A minimal partial realization algorithm for MIMO systems: III. A parametrization of all solutions, Report TW93, Dept. Computer Science, Katholieke Universiteit Leuven, August 1987.

[13] M. Van Barel, A. Bultheel, A minimal partial realization algorithm for MIMO systems: IV. A matrix Euclidean algorithm, Report TW94, Dept. Computer Science, Katholieke Universiteit Leuven, December 1987.