Some applications of the Euclidean algorithm

Adhemar Bultheel and Marc Van Barel
K.U. Leuven, Dept. Computing Science, Celestijnenlaan 200A, B-3001 Leuven (Belgium)

Abstract We describe some applications of the Euclidean algorithm in modern computational problems like Padé approximation, iterative solution of linear systems, eigenvalue problems, orthogonal polynomials, coding theory etc.

Keywords: Euclidean algorithm, Lanczos method, linear algebra, approximation.

1 EUCLIDEAN ALGORITHM

Euclidean domain: The Euclidean Algorithm (EA) can be traced back to the theorems 1 and 2 of book 7 of the Elements of Euclid, written ca 300 BC, but it is still today of great practical importance in many modern applications, as we want to illustrate in this paper. It computes a GCD of $r, s \in D$, a Euclidean domain as follows. Set $r_{-1} = s$ and $r_0 = r$, and compute $r_k = r_{k-2} \bmod r_{k-1}$ until $r_k = 0$. Then $r_{k-1} = GCD(s, r)$. At every step of the EA we can introduce units (invertible elements from D) x_k and c_k and use $GCD(s_k, r_k) = GCD(s_k x_k, r_k c_k)$ to meet some normalization condition.

EEA and continued fractions: Denote $s_k = r_{k-1}$, then one step of the EA corresponds to the relation $s_{k-1}/r_{k-1} = q_k + r_k/s_k$, or, introducing the units x_k and c_k, we have

$$[s_k \; r_k] = [s_{k-1} \; r_{k-1}]V_k; \quad V_k = \begin{bmatrix} 0 & 1 \\ 1 & -q_k \end{bmatrix} \begin{bmatrix} x_k & 0 \\ 0 & c_k \end{bmatrix} \equiv \begin{bmatrix} y_k & c_k \\ x_k & a_k \end{bmatrix}$$

where $a_k = -q_k c_k$, $y_k = 0$ and $q_k =$ quotient of s_{k-1}/r_{k-1}. Introducing some V_0 with $x_0 = c_0 = 0$ and y_0 and a_0 some units to normalize the given elements s and r as $s_0 = sy_0$ and $r_0 = ra_0$, we arrive after a small manipulation at a continued fraction corresponding to the expansion

$$-\frac{r}{s} = \frac{y_0}{a_0}\left(\frac{c_1\rfloor}{\lceil a_1} + x_1\frac{c_2\rfloor}{\lceil a_2} + \cdots + x_{k-1}\frac{c_k\rfloor}{\lceil a_k} + x_k\frac{r_k\rfloor}{\lceil s_k}\right).$$

Truncating this after k terms, we shall get a rational approximation for the left hand side of the form c_{0k}/a_{0k}. The recurrence for the numerators and denominators of the approximants as well as for the tails (residuals) is

$$G_k = G_{-1}\underbrace{V_0V_1\ldots V_k}_{V_{0k}} = \begin{bmatrix} y_{0k} & c_{0k} \\ x_{0k} & a_{0k} \\ s_k & r_k \end{bmatrix}; \quad G_{-1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ s & r \end{bmatrix}.$$

This extended recurrence is known as the Extended EA (EEA) [1, 37, 9].

Rational approximation: If we are interested in the rational approximations, then it doesn't matter whether the algorithm will end or not. One of the first applications of this idea is the approximation of a real number by rational numbers. When $r, s \in \mathbb{R}$, then the EEA as described above, taking integer quotients, will generate a sequence of rational numbers approximating $-r/s$. An interesting geometric interpretation of the number theoretic problem can be found in [11] which also includes the multi-dimensional generalization of this problem and the relation with the solution of Diophantine equations.

A similar extension can be imagined for the set of formal Laurent series $D = \mathbb{F}_-\langle z\rangle$ over a field $\mathbb{F}$ having only finitely many terms with positive exponents and where the quotient is the polynomial part of the ratio. Mutatis mutandis, this can be adapted for the formal Laurent series $\mathbb{F}_+\langle z\rangle$ with only finitely many negative exponents.

Complexity, reliability and stability: The computational complexity of the EEA is well known for example for polynomials of degree n, it requires $O(n^2)$ operations (multiplications, additions) to find their GCD. However, it is explained in detail at several places (e.g., [9]) how this can be reduced to $O(n \log_2^2 n)$ when an appropriate divide an conquer technique is applied in conjunction with FFT. On special architectures, the speed can be increased even further. For example, a systolic implementation is discussed in [10].

When the EEA is applied to e.g. Laurent series $\mathbb{F}_-\langle z\rangle$, the successive quotients are of degree 1 or larger. When they all have degree 1, we call it a generic situation. The EEA deals quite naturally with the non-generic situation as well. In many applications however, where the connection with the EEA is not that obvious, great effort has been put in the design of algorithms to deal with breakdown or near-breakdown of the algorithm for a non-generic situation. The point we want to make here is that once the connection with the EEA is made, the adaptation of the algorithm to the non-generic situation, avoiding exact breakdown (reliability) and near-breakdown (stability) is rather obvious.

2 APPROXIMATION OF FORMAL SERIES

One possible application is the approximation of formal Laurent series. Suppose we work in $\mathbb{F}_-\langle z\rangle$ as explained in section 1. The successive rational approximants for $f = -r/s$ (suppose for simplicity that $s = -1$, so that $f = r$) satisfy $f - c_{0k}/a_{0k} = r_k/a_{0k}$. When the "quotients" have $\deg a_k(z) = \alpha_k$, then it can be shown that for a strictly proper f: $\deg c_{0k} < \deg a_{0k} = \alpha_{0k} = \alpha_1 + \cdots + \alpha_k$ and $\deg (r_k/a_{0k}) = -2\alpha_{0k} - \alpha_{k+1}$ with $\alpha_{k+1} \geq 1$. Comparing the degrees of freedom in the approximant ($2\alpha_{0k}$) and the number of interpolation conditions that are met, we see that we have solved here a Padé approximation problem at infinity [4]. When f is the transfer function of a linear system, then the approximant is the one of minimal (McMillan) degree which fits the first $2\alpha_{0k}$ coefficients. This is known as a solution of the minimal partial realization (MPR) problem [36]. In this context, the EEA is closely related to the Berlekamp-Massey algorithm, which was first designed for shift register synthesis of linear predictive codes. The numbers α_{0k} are known as Kronecker indices. The numbers α_k did not seem to have received a standard name. We shall call them Euclidean indices.

Similarly, the rational approximants produced by the EEA for the ratio of two elements from $\mathbb{F}_+\langle z\rangle$ are convergents of a continued fraction which is known as a P-fraction, a name due to Arne Magnus [39]. The P stands for principal part (plus constant term) which is indeed what is meant by the quotient here. The approximants are known as Padé approximants (at the origin, but this is what is usually meant by Padé approximation). One of the earlier papers to explicitly recognize the EA as a method for computing Padé approximants is [42].

In the literature of Padé approximation, the notion of Padé table is a convenient concept to formulate certain results. The table is a two dimensional array which contains in the entry (i, j) a Padé approximant with numerator degree i and denominator degree j. In general the Padé table consists of square blocks of size 1 or larger. The entries in one block are all equal. A block of size > 1 is called singular. A Padé table with singular blocks is called non-normal. The EA computes Padé approximants on diagonals of the table thereby jumping from block to block.

3 LINEAR ALGEBRA AND ORTHOGONAL POLYNOMIALS

The interpolation conditions for the MPR problem in a linearized form can be written as a Hankel system of equations. Suppose we denote by bold face letters the vertical matrices containing the coefficients of series or polynomials, then the condition that for $f(z) \in \mathbb{F}_-\langle z\rangle$, $\deg a_{0k}(z) \leq \alpha_{0k}$ there should exist a polynomial $c_{0k}(z)$ of degree $< \alpha_{0k}$ such that $\deg r_k < -\alpha_{0k}$ with $r_k(z) = f(z)a_{0k}(z) - c_{0k}(z)$, can be written as $H\mathbf{a}_{0k} = \mathbf{r}_k$ with $H = H(f)$ the Hankel matrix with symbol f. With the down shift matrix Z we can define blocks $A_{\cdot k} = [\mathbf{a}_{0k}|Z\mathbf{a}_{0k}|\ldots|Z^{\alpha_{k+1}-1}\mathbf{a}_{0k}]$ and the upper triangular block matrix $A = [A_{\cdot 0}|A_{\cdot 1}|\ldots]$. It turns out that $HA = R$ (R block lower triangular) and $A^THA = D$ with D block diagonal.

This relation can be interpreted in two different ways: (1) as a block triangular factorization of H^{-1} and, (2) as a block orthogonality relation for the polynomials a_{0k} with respect to the moment matrix H. By block orthogonality we mean that a polynomial in a block is orthogonal to all the polynomials in previous blocks, but it may not be orthogonal to all the polynomials in the same block (See e.g. [15]). The matrix H is not necessarily positive definite or strongly regular (some of its leading submatrices may be singular). In fact the sizes of the blocks in the decomposition correspond to the number of consecutive leading submatrices that are singular. In terms of Padé approximation, this corresponds to a part of the diagonal path passing through a singular block of the Padé table.

The orthogonal polynomials satisfy the recurrence relation $a_{0k}(z) = a_{0,k-2}(z)x_{k-1}c_k + a_{0,k-1}(z)a_k(z)$ which follows immediately from the EEA. As before, the x_{k-1} and c_k are units and $a_k(z) = -q_k(z)c_k$ is the "quotient" of $s_{k-1}(z)$ and $r_{k-1}(z)$. It represents a generalization of the 3-term recurrence relation for classical orthogonal polynomials. This recurrence relation can again be written as the matrix relation $ZA = AT$, with T a block tridiagonal which is also a sparse upper Hessenberg matrix. It generalizes the Jacobi matrix from the theory of orthogonal polynomials. An equivalent formulation of the previous relation is $A^TH(zf)A = DT = J$ with J a symmetric block tridiagonal. For a discussion of these matters see for example [22, 31, 33, 16].

4 ITERATIVE SOLUTION OF LINEAR SYSTEMS OF EQUATIONS

During the last five years an enormous effort has been done to develop and apply the previous theory in the context of the iterative solution of linear systems with so called Krylov subspace methods. The Lanczos algorithm has long been believed to be only numerically acceptable for Hermitean positive definite systems because of the numerical difficulties one may expect when the algorithm is applied in a non-generic situation when some numbers become zero or nearly zero. However, as in previous situations, the EEA may also here bring a solution to overcome such a breakdown whenever possible (curable breakdown).

Suppose we want to solve the system $Mx = b$. The size of the matrix M is m. The residual is $r = b - Mx$. For some starting vector x_0, successive approximants x_k are

obtained by a conjugate direction method minimizing the residual norm. It turns out that the residuals $r_k = b - Mx_k$ are elements from the Krylov subspaces $\mathcal{K}_k(r_0, M) = \text{span}\{r_0, Mr_0, \ldots, M^k r_0\}$. More precisely, there exists a polynomial $\varphi_k(z)$ of degree k and $\varphi_k(0) = 1$ such that $r_k = \varphi_k(M)r_0$. Let us first suppose that M is symmetric. Then minimizing $\|r_k\|^2 = r_k^T r_k$ is equivalent to minimizing $\|\varphi_k\|_H^2$ where the latter norm is taken with respect to the Hankel moment matrix $H = H(f)$ where $f(z) = \sum f_k z^{-k}$ and $f_k = r_0^T M^{k-1} r_0$. The comonic polynomial of minimal norm is an orthogonal one, hence we get the orthogonality relations $\varphi_k \perp \varphi_l$ for $k \neq l$ with respect to the metric H or equivalently $r_k \perp r_l$ in the metric I. Thus in principle we can perform the iterations of the Lanczos algorithm whenever we can construct the orthogonal polynomials φ_k.

The problem of breakdown occurs when the Hankel matrix $H = H(f)$ is not strongly regular, which can happen when M is not positive definite. But we are then in a situation where we have to construct formal orthogonal polynomials with respect to an indefinite Hankel moment matrix, and this problem has been treated in the previous section.

The previous formulas can be translated into the present terminology as follows. First we consider for $n < m$ the matrix $Y_n = [y_0|y_1|\ldots|y_n]$ where $y_0 = r_0$ and $y_k = My_{k-1}$ for $n \geq k \geq 1$. Then, by definition, the leading submatrix of size $n+1$ of H is given by $H_n = Y_n^T Y_n$. The Krylov space is the column space of Y_n and the problem is to construct an orthogonal basis for this space. We have to find an upper triangular matrix A_n such that the columns of $\hat{Y}_n = Y_n A_n$ are orthogonal vectors, or in the presence of singular blocks, they should be block orthogonal vectors. The matrix A_n is a submatrix of the matrix A we had in the previous section and which can be constructed recursively from the data f or equivalently from the matrix Y_n by the EEA. The orthogonality means that $\hat{Y}_n^T \hat{Y}_n = A_n^T H_n A_n = D_n$ with D_n block diagonal. Moreover we have that $\hat{Y}_n M \hat{Y}_n = A_n^T H_n(zf) A_n = D_n T_n = J_n$ is a block tridiagonal matrix. Note that in the block case, the index n refers to the number of blocks, rather than the number of columns.

At first sight, the case of a non symmetric matrix M, can not be treated by the EA because the matrix with entries $r_0(M^T)^i M^j r_0$ is not Hankel anymore. One possibility is to construct orthogonal polynomials for a general moment matrix, but this is computationally less efficient because the Jacobi matrix will then not be tridiagonal or block tridiagonal, but it will be a full upper Hessenberg matrix. Algorithms of this type belong to the class of Arnoldi-like algorithms. However, it is still possible, with substantially less computational effort to generate a Hankel matrix as before. Indeed, we consider two Krylov subspaces: the one generated by the vectors y_i and another one $\mathcal{K}_n(r_0, M^T)$, which is spanned by the columns of $Z_n = [z_0|z_1|\ldots|z_n]$ with $z_0 = r_0$ and $z_k = M^T z_{k-1}$. Clearly, the matrix $H_n = H_n(f) = Z_n^T Y_n$ is again Hankel with symbol $f(z) = z_0^T(zI - M)^{-1} y_0$. Applying the EA as before to get the upper triangular factor A_n, leads to the fact that $\hat{Z}_n = Z_n A_n$ and $\hat{Y}_n = Y_n A_n$ satisfy a block biorthogonality condition $\hat{Z}_n^T \hat{Y}_n = A_n^T H_n A_n = D_n$. For a survey of recent developments see [26, 33, 16].

5 EIGENVALUE PROBLEM AND LINEAR SYSTEMS

Let us consider a linear system which can be described by the state space equations

$$\begin{aligned} x_{k+1} &= Ax_k + Bu_k, & A &\in \mathbb{F}^{n\times n}, B \in \mathbb{F}^{n\times 1} \\ y_{k+1} &= C^T x_{k+1}, & C &\in \mathbb{F}^{n\times 1} \end{aligned}$$

The vector x_k is the state, u_k is the input and y_k is the output. The triple (A, B, C) is called a state space realization of the system. When the number n (dimension of the state

space) is the smallest possible one to describe the input-output behaviour of the system, the realization is called minimal.

After taking z-transforms (e.g., $u(z) = \sum u_k z^{-k}$), we obtain $y(z) = f(z)u(z)$ with transfer function $f(z) = C^T(zI - A)^{-1}B$. The coefficients in its expansion at ∞, i.e., $f_k = C^T A^{k-1} B$ are called Markov parameters, and the sequence (f_k) is called the impulse response. Thus the MPR problem is to match a certain number of Markov parameters by constructing a rational transfer function of the smallest possible degree. It is a Padé approximation problem at infinity for the transfer function of the system.

The matrix $\mathcal{O} = [C\ A^TC\ (A^T)^2C\ \ldots]^T$ is called the observability matrix and $\mathcal{R} = [B\ AB\ A^2B\ \ldots]$ is called the reachability matrix. The system is called reachable when $\mathcal{R}$ has full rank, i.e., $n = \operatorname{rank}\mathcal{R}$ and it is called observable when $\mathcal{O}$ has full rank, i.e., when $n = \operatorname{rank}\mathcal{O}$. When $n = \operatorname{rank}\mathcal{R} = \operatorname{rank}\mathcal{O} = \operatorname{rank}\mathcal{O}\mathcal{R}$, then the realization is minimal. Note that $H = \mathcal{O}\mathcal{R}$ is the same as the Hankel matrix $H(f)$, hence $\operatorname{rank} H(f) = \deg f$, if f is reduced.

To see that the Lanczos algorithm can also help in reducing the eigenvalue problem for the matrix M to a simpler one, suppose that n refers to the block index such that D_n is regular. Then note that from (notation of previous section) $\hat{Z}_n^T\hat{Y}_n = D_n$ and hence $\hat{Z}_n^T = D_n\hat{Y}_n^{-1}$, it follows from $\hat{Z}_n^T M\hat{Y}_n = D_nT_n$ that $\hat{Y}_n^{-1}M\hat{Y}_n = T_n$. This means that M is similar to T_n and thus it has the same eigenvalues. Since T_n is much simpler, being a sparse block tridiagonal, its eigenvalues are easily obtained. Since the finite dimensional analog of $ZA = AT$ reads $F(a_{0,n+1})A_n = A_nT_n$, where $F(a_{0,n+1})$ represents the Frobenius matrix for the polynomial $a_{0,n+1}(z)$, also $T_n = A_n^{-1}F(a_{0,n+1})A_n$ and thus it follows that the eigenvalues of M are eigenvalues of T_n and therefore zeros of $a_{0,n+1}(z)$.

All this is true when there is some $\alpha_{0,n+1}$ which is equal to m, the size of the matrix M. This need not be true in general. First note that the input for the EA is essentially $f(z) = z_0^T(zI - M)^{-1}y_0$. The triple (M, y_0, z_0) is a state space realization for f. But if it is not minimal, then M may contain a larger spectrum than can be obtained as poles from f. The EA or Lanczos algorithm will end because $\alpha_{0,n+1} = r = \deg f < m$. It will thus be impossible to recover the whole spectrum of M from f. The Lanczos algorithm will have a breakdown, which can not be cured by the principles of the EA. Note that nonminimality is no problem in the solution of systems, since this breakdown indicates that f is approximated exactly and the residual will be zero. For the eigenvalue problem however, it turns out that there are two possibilities to be considered. Define $r_y = \operatorname{rank} Y_\infty = \dim \mathcal{K}_\infty(y_0, M)$ and $r_z = \operatorname{rank} Z_\infty = \dim \mathcal{K}_\infty(z_0, M^T)$, then either (A) or (B) will happen.
(A) $m > r = \min\{r_y, r_z\}$, then the system is reachable or observable, and we can recover the spectrum of M restricted to the reachability space (that is $\mathcal{K}_\infty(z_0, M^T)$ = the column space of Z_∞) or the observability space (that is $\mathcal{K}_\infty(y_0, M)$ = the column space of Y_∞).
(B) $r < \min\{r_y, r_z\}$, then the starting vectors y_0 and/or z_0 were chosen inadequately so that they do not have components along a basis for the maximal Jordan block that can be associated with each eigenvalue of M. The algorithm is trapped in a smaller dimensional space and only the spectral information of M restricted to these smaller spaces will be recovered. See [33, 44, 16].

6 CODING THEORY

Another classical application of the Euclidean algorithm can be found in the theory of error correcting codes, more precisely Goppa codes. Two examples are BCH codes and Reed-Solomon codes. A comprehensive treatment of the subject can be found in [41].

The Berlekamp and Massey algorithm (BMA) [8, 40], was first developed in this context to find linear feedback shift register realizations for the associated system. In a sense, this is equivalent to the Euclidean algorithm. It requires inner products though, hence it is a layer adjoining variant [13] of the EA and therefore less suited for parallel implementation. See also [23, 24] for generalizations of the BMA to multi-sequences.

7 MATRIX AND OTHER GENERALIZATIONS

Most of the previous notions concerning the EA can be generalized to the $q \times p$ dimensional situation. There are several possibilities for generalizing all the scalar notions and what might be understood by a EA for this situation is not uniquely defined.

Linear systems: The theory of linear systems was probably the first place where matrix generalizations of the previous theory were developed. The concept of state space is remarkably easy to adapt to systems with multiple inputs and multiple outputs. In the realization triple (A, B, C) one should assume that $B \in \mathbb{F}^{n\times p}$ and $C \in \mathbb{F}^{n\times q}$ where p is the dimension of the input vector u_k and q is the dimension of the output vector y_k. The transfer function becomes a matrix rational function of size $q \times p$. There are several possibilities to write a rational matrix function as the "ratio" of two polynomial matrices. For example $f(z) = s(z)^{-1}r(z)$ with s and r polynomial $r \in \mathbb{F}^{q\times p}[z]$ and $s \in \mathbb{F}^{q\times q}[z]$ is a left description. The Hankel matrix $H(f)$ is replaced by a block Hankel matrix with $q \times p$ blocks.

Greatest common divisor: The definition of greatest common left divisor (GCLD) for matrix polynomials can be found in [36, p.376-378]. You can also find there a theorem saying that g is a GCLD of s and r when there exists a unimodular matrix V such that $[s\ r]V = [g\ 0]$. A unimodular matrix is a polynomial matrix whose inverse is again a polynomial matrix. Thus the matrix version of the EEA will, exactly like in the scalar case, start from G_{-1} and generate successively $G_k = G_{k-1}V_k$ until after a finite number of steps one has $[s_n\ r_n]$ with $r_n = 0$. The matrices V_k are a composition of elementary Gaussian-type elimination matrices involving powers of z off the diagonal. Their description can be found in [48] for the MPR problem and in [14] for the matrix Padé problem. On a more theoretical basis, the same ideas are found in [3]. Predecessors are [21] and [2].

Approximation of series: When the previous algorithm is used for matrix polynomials s and r, then it will end after a finite number of steps. In general it may be applied to matrix Laurent series and then it may never stop, but at every stage, the approximants $c_{0k}a_{0k}^{-1}$ are matrix versions of the Padé approximants at ∞ or at 0 of the rational matrix function $f = -s^{-1}r$. Again we refer to the papers mentioned above for the details. See also [29].

Matrix continued fractions: We can also associate with the matrices V_k an elementary step of a matrix continued fraction. However, in the scalar case, the left top element y_k was zero. In the matrix case, this will no longer hold. This implies that the matrix generalization of the continued fraction will not only continue the division steps in the denominator, but it will also show a continuing division in the numerator. More precisely, the convergents of the continued fraction on the right in the expansion

$$-s^{-1}r = \left[y_0\left(c_1 + y_1\frac{c_2 + y_2\frac{\cdots}{\cdots}}{a_2 + x_2\frac{\cdots}{\cdots}}\right)\right]\left[a_0\left(a_1 + x_1\frac{c_2 + y_2\frac{\cdots}{\cdots}}{a_2 + x_2\frac{\cdots}{\cdots}}\right)\right]^{-1}; \quad \text{where } \frac{a}{b} = ab^{-1}$$

are the successive approximants.

Multi-point interpolation: Until now, we only mentioned rational approximation with interpolation conditions at 0 or ∞. Of course, it would not be difficult to replace the indeterminate z by $x - \alpha$ which would result in a Laurent series in the neighborhood of α, or one could consider simultaneous approximation of two series: one at 0 and one at ∞ or even at more points, giving multi-point rational approximations. The technicalities are of course more involved, but basically the same. Whether the reader is still prepared to call this a variant of the Euclidean algorithm is of course a matter of taste.

By now multipoint and matrix versions have been considered [51, 5, 7, 50, 49]. The block structure of some these problems has been discussed recently [32, 6].

8 DUALITY

As en example of the previous generalizations, we mention the vector valued Padé approximation problem, which has a longer history. We use this context to bring a remarkable duality to the foreground. There are two types of problems that were already considered by Hermite.

There is the problem of finding polynomials $p_0, \ldots, p_n$ with certain bounds $\delta_0, \ldots, \delta_n$ on their degrees such that they approximate given power series $f_0, \ldots, f_n$ up to a certain order in the sense that $\sum_0^n p_k(z) f_k(z) = O(z^\omega)$ ($\omega = \sum_k \delta_k + n$ at least). This is known as the Padé-Hermite approximation problem.

On the other hand, there is the problem of simultaneous Padé approximation where polynomials $q_0, \ldots, q_n$ are to be found such that for given series $f_1, \ldots, f_n$ and given integer ω, it holds that $f_k(z)q_0(z) - f_0(z)q_k(z) = O(z^\omega)$ and $\deg q_k \leq \omega - \delta_k$.

There is an intimate relation between the two problems. Solving one problem is equivalent to solving the other. For a discussion of the general duality principle in vector Padé-Hermite problems, see [19, 38].

9 LOOK-AHEAD STRATEGIES

The latest successes that were obtained in this circle of problems is a breakthrough in improving the numerical stability of this type of algorithms. This is the problem we mentioned before of how to make the algorithms deal with near-breakdown, and not just with exact breakdown.

Taylor was probably the first to propose a look-ahead strategy in the context of the Lanczos algorithm, see [47, 45]. These papers coined the term look-ahead. See also [12, 25, 27, 28]. The same idea has been implemented for the related problems that were discussed in this survey, like for example Padé approximation [32], the solution of Hankel [43, 18] and Toeplitz systems [54, 35, 34] and in general rational (matrix) interpolation problems [52].

The EA gives a reliable algorithm because it jumps over the singular blocks in the Padé table, or in terms of Hankel matrices, it skips the singular leading submatrices. Such a singularity is detected by a pivot element being zero. Near-breakdown is detected when this pivot is small resulting in a dramatic loss of accuracy. Thus numerically, it makes more sense not to leap from a nonsingular situation to the next one, but to leap from a well conditioned situation to a well conditioned one. This then results in a stable EEA (SEEA).

Because a well-conditioned situation is a nonsingular one by definition, the transition matrix V_k^s we shall need in a SEEA to jump from one approximant to the next one, will be a product of some of the V_k matrices of the EEA. Therefore, the matrix V_k^s will not

have the same simple form as a V_k with $y_k = 0$, x_k and c_k units and only a_k polynomial. In general V_k^s will have polynomial entries in all 4 places, but it will still be unimodular.

The same idea of grouping together several steps of the simple EEA was already used in the superfast versions of the EEA. Suppose we need N steps of a classical EEA to reach a solution, then the divide and conquer strategy grouped the product $V_1 \dots V_N$ as $V_{1n} V_{n+1,N}$ where $n = \lfloor N/2 \rfloor$. In terms of Padé approximation, this means that to have an approximant of degree $\alpha_{0,N+1}$ of $f = -s^{-1}r$, we may compute a degree $\alpha_{0,n+1}$ approximant for f and a degree $\alpha_{0,N+1} - \alpha_{0,n+1}$ approximant for the tail of the continued fraction. These two can then be combined to give the desired approximant. By applying this strategy recursively, the superfast algorithms emerge.

In the previous discussion, a leap from a well conditioned point to a well conditioned point was always supposed to be on a path that is normally followed by the EEA, thus on a diagonal path. By introducing shift parameters [50, 49] this extends to any parallel diagonal. By changing the number of interpolation conditions as well as the degree conditions, one can walk in principle from any sonsingular (well conditioned) point to any other nonsingular (well conditioned) point in the interpolation table. The idea is that the solution to an interpolation problem can be written as a system of homogeneous linear equations. The space of all the solutions for this problem is a submodule which is generated as polynomial multiples of some basis of polynomial vectors.

10 CONCLUDING REMARKS

In these applications, the farther we are away from the simple scalar case, the more difficult it will be to recognise the Euclidean algorithm. If one is prepared to push this a little further, one could design Lanczos type algorithms for Toeplitz matrices or even general matrices [17] or algorithms for quasi-Hankel or Toeplitz matrices or structured matrices in general (e.g., [46, 38]).

Another important challenge for future research is to see how time-variant system theory can be applied to the circle of ideas we have proposed here. In time-variant systems, the matrices A, B and C also depend on k. See [30, 53, 20].

Acknowledgement: This research was supported by the National Fund for Scientific Research (NFWO), project Lanczos, grant #2.0042.93.

References

[1] A.V. Aho, J.E. Hopcroft, and J.D. Ullman. *The design and analysis of computer algorithms.* Addison Wesley, Reading, Mass., 1974.

[2] B.M. Anderson, F.M. Brasch, and P.V. Lopresti. The sequential construction of minimal partial realizations from finite input-output data. *SIAM J. Control*, 13(3):552–571, May 1975.

[3] A.C. Antoulas. On recursiveness and related topics in linear systems. *IEEE Trans Automatic Control*, AC-31:1121–1134, 1986.

[4] G.A. Baker, Jr. and P.R. Graves-Morris. *Padé Approximants. Part I: Basic Theory*, volume 13 of *Encyclopedia of mathematics and its applications.* Addison-Wesley Publishing Co., Reading, 1981.

[5] B. Beckermann. *Zur Interpolation mit polynomialen Linearkombinationen beliebiger Funktionen.* PhD thesis, Universität Hannover, 1989.

[6] B. Beckermann, J. Gilewicz, and V. Kaliaguine. On the definition and normality of a general table of simultaneous Padé approximants. Technical Report CPT-92/P.2686, CNRS Luminy, France, 1992.

[7] B. Beckermann and G. Labahn. A uniform approach for Hermite-Padé and simultaneous Padé approximants and their matrix-type generalizations. *Numer. Alg.*, 3(1-4):45–54, 1992.
[8] E.R. Berlekamp. *Algebraic coding theory.* McGraw-Hill, New York, 1968.
[9] R.P. Brent, F.G. Gustavson, and D.Y.Y. Yun. Fast solution of Toeplitz systems of equations and computation of Padé approximants. *J. Algorithms*, 1:259–295, 1980.
[10] R.P. Brent and H.T. Kung. Systolic VLSI arrays for polynomial GCD computation. *IEEE Trans. on computers*, C-33(8):731–736, 1984.
[11] A.J. Brentjes. *Multi-dimensional continued fraction algorithms*, volume 145. Mathematical Centre, Amsterdam, The Netherlands, 1981.
[12] C. Brezinski, M. Redivo Zaglia, and H. Sadok. Avoiding breakdown and near-breakdown in Lanczos type algorithms. *Numerical Algorithms*, 1(3):261–284, 1991. Addendum, vol. 2(2):133-136, 1992.
[13] A.M. Bruckstein and T. Kailath. Inverse scattering for discrete transmission-line models. *SIAM Review*, 29(3):359–389, 1987.
[14] A. Bultheel and M. Van Barel. A matrix Euclidean algorithm and the matrix minimal Padé approximation problem. In C. Brezinski, editor, *Continued fractions and Padé approximants*, pages 11–51. North-Holland, 1990.
[15] A. Bultheel and M. Van Barel. Formal orthogonal polynomials and rational approximation for arbitrary bilinear forms. Technical Report TW163, Department of Computer Science, K.U. Leuven, December 1992.
[16] A. Bultheel and M. Van Barel. Euclid, Padé and Lanczos, another golden braid. Technical Report TW188, Department of Computer Science, K.U. Leuven, April 1993.
[17] A. Bultheel and M. Van Barel. Linear algebra, rational approximation and orthogonal polynomials, 1993. (In preparation).
[18] S. Cabay and R. Meleshko. A weakly stable algorithm for Padé approximants and the inversion of Hankel matrices. *SIAM J. Matrix Anal. Appl.*, 14:735–765, 1993.
[19] G. De Samblanx. Vektor Padé-Hermite benaderingen (Vector Padé-Hermite approximation). Master's thesis, K.U. Leuven, Dept. Computing Sci., 1993. (In Dutch).
[20] P. Dewilde, M.A. Kaashoek, and M. Verhaegen, editors. *Challenges of a generalized, non-stationary system theory.* Essays of the Dutch Academy of Arts and Sciences. Dutch Acad. Arts Sci., Amsterdam, 1993.
[21] B.W. Dickinson, M. Morf, and T. Kailath. A minimal realization algorithm for matrix sequences. *IEEE Trans. Autom. Control*, AC-19:31–38, 1974.
[22] A. Draux. *Polynômes orthogonaux formels – applications*, volume 974 of *Lecture Notes Mathematics.* Springer-Verlag, Berlin, 1983.
[23] Gui-Liang Feng and K.K. Tzeng. A generalized Euclidean algorithm for multisequence shift-register synthesis. *IEEE Trans. Information Theory*, 35(3):584–594, 1989.
[24] Gui-Liang Feng and K.K. Tzeng. A generalization of the Berlekamp-Massey algorithm for multisequence shift-register synthesis with applications to decoding cyclic codes. *IEEE Trans. Information Theory*, 37(5):1274–1287, 1991.
[25] R.W. Freund. The look-ahead Lanczos process for large nonsymmetric matrices and related algorithms. In M.S. Moonen, G. Golub, and B.L.R. De Moor, editors, *Linear algebra for large scale and real-time applications*, volume 232 of *NATO-ASI series E: Applied Sciences*, pages 137–163. Kluwer Acad. Publ., Dordrecht, 1993.
[26] R.W. Freund, G.H. Golub, and N.M. Nachtigal. Iterative solution of linear systems. *Acta Numerica*, 1:57–100, 1992.
[27] R.W. Freund, M.H. Gutknecht, and N.M. Nachtigal. An implementation of the look-ahead Lanczos algorithm for non-Hermitian matrices, Part I. *SIAM J. Sci. Stat. Comp.*, 14(1):137–158, 1993.
[28] R.W. Freund and N.M. Nachtigal. An implementation of the look-ahead Lanczos algorithm for non-Hermitian matrices, Part II. Technical Report 90.46, RIACS, NASA Ames Research Center, Moffet Field, 1990.

[29] P.A. Fuhrmann. A matrix Euclidean algorithm and matrix continued fraction expansion. *Systems and Control Letters*, 3:263–271, 1983.

[30] I. Gohberg, editor. *Time-variant systems and interpolation*, volume 56 of *Operator Theory, Advances and Applications*. Birkhäuser Verlag, 1992.

[31] W.B. Gragg and A. Lindquist. On the partial realization problem. *Lin. Alg. Appl.*, 50:277–319, 1983.

[32] M.H. Gutknecht. Block structure and recursiveness in rational interpolation. In E.W. Cheney, C.K. Chui, and L.L. Schumaker, editors, *Approximation Theory VI*, pages 93–130. Academic Press, 1992.

[33] M.H. Gutknecht. A completed theory of the unsymmetric Lanczos process and related algorithms. Part I. *SIAM J. Matrix Anal. Appl.*, 13(2):594–639, 1992.

[34] M.H. Gutknecht. Stable row recurrences for the Padé table and generically superfast lookahead solvers for non-Hermitian Toeplitz systems. *Lin. Alg. Appl.*, 188/189:351–422, 1993.

[35] M.H. Gutknecht and M. Hochbruck. Look-ahead Levinson and Schur algorithms for non-Hermitian Toeplitz systems. Technical Report 93-11, IPS, ETH Zürich, 1993.

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

[37] D.E. Knuth. *The art of computer programming, Vol 2 : Seminumerical algorithms*. Addison Wesley, Reading, Mass., 1969.

[38] G. Labahn. Inversion components of block Hankel-like matrices. *Lin. Alg. Appl.*, 177:7–48, 1992.

[39] A. Magnus. Expansion of power series into P-fractions. *Math. Z.*, 80:209–216, 1962.

[40] J.L. Massey. Shift-register synthesis and BCH decoding. *IEEE Trans. Inf. Theory*, IT-15:122–127, 1969.

[41] R.J. McEliece. *The theory of information and coding: A mathematical framework for communication*, volume 3 of *Encyclopedia of mathematics*. Addison Wesley, Reading, Mass., 1977.

[42] R.J. McEliece and J.B. Shearer. A property of Euclid's algorithm and an application to Padé approximation. *SIAM J. Appl. Math.*, 34:611–616, 1978.

[43] R.J. Meleshko. *A stable algorithm for the computation of Padé approximants*. PhD thesis, Dept. of Computing Sc., Univ. of Alberta, Canada, 1990.

[44] B.N. Parlett. Reduction to tridiagonal form and minimal realizations. *SIAM J. Matr. Anal. Appl.*, 13:567–593, 1992.

[45] B.N. Parlett, D.R. Taylor, and Z.A. Liu. A look-ahead Lanczos algorithm for unsymmetric matrices. *Mathematics of Comp.*, 44(169):105–124, 1985.

[46] A.H. Sayed. *Displacement structure in signal processing and mathematics*. PhD thesis, Stanford University, August 1992.

[47] D.R. Taylor. *Analysis of the look ahead Lanczos algorithm*. PhD thesis, Center for Pure and Applied Mathematics, University of California, Berkeley, 1982.

[48] M. Van Barel and A. Bultheel. A matrix Euclidean algorithm for minimal partial realization. *Linear Algebra Appl.*, 121:674–682, 1989.

[49] M. Van Barel and A. Bultheel. A new approach to the rational interpolation problem: the vector case. *J. Comput. Appl. Math.*, 33(3):331–346, 1990.

[50] M. Van Barel and A. Bultheel. A general module theoretic framework for vector M-Padé and matrix rational interpolation. *Numer. Alg.*, 3:451–461, 1992.

[51] M. Van Barel and A. Bultheel. A new formal approach to the rational interpolation problem. *Numer. Math.*, 62:87–122, 1992.

[52] M. Van Barel and A. Bultheel. The "look-ahead" philosophy applied to matrix rational interpolation problems. In *Proceedings MTNS, Regensburg, Germany, August 1993*, 1993. Submitted.

[53] A.-J. van der Veen. *Time-variant system theory and computational modeling. Realization, approximation and factorization*. PhD thesis, Technical University Delft, The Netherlands, June 1993.

[54] P. Vyvey. Oplossen van niet sterk reguliere Toeplitz stelsels (The solution of non strongly regular Toeplitz systems). Master's thesis, K.U. Leuven, Dept. Computing Sci., 1987. (In Dutch).