The Berlekamp–Massey Algorithm and Combinatorics

Ulrich Tamm
Department of Computer Science
University of Chemnitz, 09107 Chemnitz, Germany
tamm@informatik.tu-chemnitz.de

I. Introduction

A Hankel matrix (or persymmetric matrix)

$$A_n = \begin{pmatrix} c_0 & c_1 & c_2 & \cdots & c_{n-1} \\ c_1 & c_2 & c_3 & \cdots & c_n \\ c_2 & c_3 & c_4 & \cdots & c_{n+1} \\ \vdots & \vdots & \vdots & & \vdots \\ c_{n-1} & c_n & c_{n+1} & \cdots & c_{2n-2} \end{pmatrix}. \tag{1.1}$$

is a matrix (a_{ij}) in which for every r the entries on the diagonal $i + j = r$ are the same, i.e., $a_{i,r-i} = c_r$ for some c_r. For a sequence $c_0, c_1, c_2, \dots$ of real numbers we also consider the collection of Hankel matrices $A_n^{(k)}$, $k = 0, 1, \dots$, $n = 1, 2, \dots$, where

$$A_n^{(k)} = \begin{pmatrix} c_k & c_{k+1} & c_{k+2} & \cdots & c_{k+n-1} \\ c_{k+1} & c_{k+2} & c_{k+3} & \cdots & c_{k+n} \\ c_{k+2} & c_{k+3} & c_{k+4} & \cdots & c_{k+n+1} \\ \vdots & \vdots & \vdots & & \vdots \\ c_{k+n-1} & c_{k+n} & c_{k+n+1} & \cdots & c_{k+2n-2} \end{pmatrix}. \tag{1.2}$$

We shall further denote the determinant of a Hankel matrix (1.2) by

$$d_n^{(k)} = \det(A_n^{(k)}). \tag{1.3}$$

In Coding Theory, Hankel matrices play a central role in decoding of BCH codes, especially in the Berlekamp - Massey algorithm. Their connection to orthogonal polynomials often yields useful applications in Combinatorics: Hankel determinants enumerate certain families of weighted paths, Catalan – like numbers often are sequences important in combinatorial enumeration, and, as a recent application, orthogonal polynomials turned out to be an important tool in the proof of the alternating sign matrix conjecture.

The framework for studying combinatorial applications of Hankel matrices and further aspects of orthogonal polynomials was set up by Viennot [23]. Of special interest (cf. [6]) are determinants of Hankel matrices consisting of Catalan numbers $\frac{1}{2m+1}\binom{2m+1}{m}$, namely for the sequence $c_m = \frac{1}{2m+1}\binom{2m+1}{m}$, $m = 0, 1, \dots$ it is

$$d_n^{(0)} = d_n^{(1)} = 1, \qquad d_n^{(k)} = \prod_{1 \le i \le j \le k-1} \frac{i+j+2n}{i+j} \qquad \text{for } k \ge 2, n \ge 1. \tag{1.4}$$

In Section II we shall study Hankel matrices whose entries are defined as generalized Catalan numbers $c_m = \frac{1}{3m+1}\binom{3m+1}{m}$. In this case we could show that

$$d_n^{(0)} = \prod_{j=0}^{n-1} \frac{(3j+1)(6j)!(2j)!}{(4j+1)!(4j)!}, \qquad d_n^{(1)} = \prod_{j=1}^{n} \frac{\binom{6j-2}{2j}}{2\binom{4j-1}{2j}}. \tag{1.6}$$

These numbers are of special interest, since they coincide with two Mills – Robbins – Rumsey determinants, which arise in the enumeration of alternating sign matrices.

Let us recall some properties of Hankel matrices. Of special importance is the equation

$$\begin{pmatrix} c_0 & c_1 & c_2 & \dots & c_{n-1} \\ c_1 & c_2 & c_3 & \dots & c_n \\ c_2 & c_3 & c_4 & \dots & c_{n+1} \\ \vdots & \vdots & \vdots & & \vdots \\ c_{n-1} & c_n & c_{n+1} & \dots & c_{2n-2} \end{pmatrix} \cdot \begin{pmatrix} a_{n,0} \\ a_{n,1} \\ a_{n,2} \\ \vdots \\ a_{n,n-1} \end{pmatrix} = \begin{pmatrix} -c_n \\ -c_{n+1} \\ -c_{n+2} \\ \vdots \\ -c_{2n-1} \end{pmatrix}. \tag{1.7}$$

If the matrices $A_n^{(0)}$ are nonsingular for all n, then (cf. [4], p. 246) the polynomials

$$t_j(x) := x^j + a_{j,j-1}x^{j-1} + a_{j,j-2}x^{j-2} + \dots a_{j,1}x + a_{j,0} \tag{1.8}$$

form a sequence of monic orthogonal polynomials with respect to the linear operator T mapping x^l to its moment $T(x^l) = c_l$ for all l, i. e.

$$T(t_j(x) \cdot t_m(x)) = 0 \text{ for } j \neq m, \tag{1.9}$$

$$\text{or equivalently,} \qquad T(x^m \cdot t_j(x)) = 0 \text{ for } m = 0, \dots, j-1. \tag{1.10}$$

In Section III we shall study matrices $L_n = (l(m,j))_{m,j=0,1,\dots,n-1}$ defined by

$$l(m,j) = T(x^m \cdot t_j(x)). \tag{1.11}$$

By (1.10) these matrices are lower triangular. The recursion for Catalan – like numbers, as defined by Aigner [1], can be derived via matrices L_n with determinant 1. Further, the Lanczos algorithm yields a factorization $L_n = A_n \cdot U_n^t$, where A_n is a nonsingular Hankel matrix as in (1.1), L_n is defined by (1.11) and

$$U_n = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ a_{1,0} & 1 & 0 & \dots & 0 & 0 \\ a_{2,0} & a_{2,1} & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ a_{n-1,0} & a_{n-1,1} & a_{n-2,2} & \dots & a_{n-1,n-2} & 1 \end{pmatrix}. \tag{1.12}$$

is the triangular matrix whose entries are the coefficients of the polynomials $t_j(x)$.

In Section III we further shall discuss the Berlekamp – Massey algorithm, where Hankel matrices of syndromes resulting after the transmission of a code word over a noisy channel have to be studied. Via the matrix L_n defined by (1.11) it will be shown that the Berlekamp – Massey algorithm applied to Hankel matrices with real entries can be used to compute the coefficients in the corresponding orthogonal polynomials. In this case all Hankel matrices A_n under consideration are nonsingular.

Hankel matrices come into play when the power series

$$F(x) = c_0 + c_1 x + c_2 x^2 + \dots \tag{1.13}$$

is expressed as a continued fraction. If the Hankel determinants $d_n^{(0)}$ and $d_n^{(1)}$ are different from 0 for all n, the so–called S–fraction expansion of $\frac{1}{x}F(\frac{1}{x})$ has the form

$$\frac{1}{x}F(\frac{1}{x}) = \cfrac{c_0}{x - \cfrac{q_1}{1 - \cfrac{e_1}{x - \cfrac{q_2}{1 - \cfrac{e_2}{x - \dots}}}}} \tag{1.14}$$

where for $n \geq 1$ (cf. [16], p. 304)

$$q_n = \frac{d_n^{(1)} \cdot d_{n-1}^{(0)}}{d_{n-1}^{(1)} \cdot d_n^{(0)}}, \qquad e_n = \frac{d_{n+1}^{(0)} \cdot d_{n-1}^{(1)}}{d_n^{(0)} \cdot d_n^{(1)}}. \tag{1.15}$$

(1.14) can be transformed to the J–fraction

$$\cfrac{c_0}{x - \alpha_1 - \cfrac{\beta_1}{x - \alpha_2 - \cfrac{\beta_2}{x - \alpha_3 - \cfrac{\beta_3}{x - \alpha_4 - \dots}}}} \tag{1.16}$$

with $\alpha_1 = q_1$, and $\alpha_{j+1} = q_{j+1} + e_j$, $\beta_j = q_j e_j$ for $j \geq 1$. (cf. [16], p.375).
For the notion of S– and J– fraction (S stands for Stieltjes, J for Jacobi) we refer to the standard book by Perron [16]. We follow here the (q_n, e_n)–notation of Rutishauser [20]. (1.16) was used by Flajolet ([7]) to study combinatorial aspects of continued fractions, especially, he gave an interpretation of the coefficients in the continued fractions expansion in terms of weighted lattice paths.

(1.9) results from the quality of the approximation to $\frac{1}{x}F(\frac{1}{x})$ by quotients of polynomials $\frac{p_j(x)}{t_j(x)}$ with $t_j(x)$ defined under (1.8). The polynomials $t_j(x)$ hence obey the three – term recurrence

$$t_j(x) = (x - \alpha_j)t_{j-1}(x) - \beta_{j-1} \cdot t_{j-2}(x), \qquad t_0(x) = 1, \qquad t_1(x) = x - \alpha_1, \tag{1.17}$$

$$\text{with } \alpha_1 = q_1 \text{ and } \alpha_{j+1} = q_{j+1} + e_j, \qquad \beta_j = q_j e_j \text{ for } j \geq 1. \tag{1.18}$$

II. Hankel Determinants And Alternating Sign Matrices

The generating function

$$C(x) = \sum_{m=0}^{\infty} \frac{1}{3m+1} \binom{3m+1}{m} x^m \tag{2.1}$$

fulfills the functional equation $C(x) = 1 + x \cdot C(x)^3$, from which immediately follows that

$$\frac{1}{C(x)} = 1 - x \cdot C(x)^2. \tag{2.2}$$

Lattice path enumeration allows to derive the following identity.

Lemma 2.1:

$$\left(\sum_{m=0}^{\infty}\binom{3m}{m}x^m\right)\cdot\left(\sum_{m=0}^{\infty}\frac{1}{3m+1}\binom{3m+1}{m}x^m\right)=\sum_{m=0}^{\infty}\binom{3m+1}{m}x^m. \tag{2.3}$$

Theorem 2.1: For $m=0,1,2\dots$ let denote $c_m=\frac{1}{3m+1}\binom{3m+1}{m}$. Then

$$\begin{pmatrix} c_0 & c_1 & c_2 & \dots & c_{n-1}\\ c_1 & c_2 & c_3 & \dots & c_n\\ c_2 & c_3 & c_4 & \dots & c_{n+1}\\ \vdots & \vdots & \vdots & & \vdots\\ c_{n-1} & c_n & c_{n+1} & \dots & c_{2n-2}\end{pmatrix}=\prod_{j=0}^{n-1}\frac{(3j+1)(6j)!(2j)!}{(4j+1)!(4j)!},$$

$$\begin{pmatrix} c_1 & c_2 & c_3 & \dots & c_n\\ c_2 & c_3 & c_4 & \dots & c_{n+1}\\ c_3 & c_4 & c_5 & \dots & c_{n+2}\\ \vdots & \vdots & \vdots & & \vdots\\ c_n & c_{n+1} & c_{n+2} & \dots & c_{2n-1}\end{pmatrix}=\prod_{j=1}^{n}\frac{\binom{6j-2}{2j}}{2\binom{4j-1}{2j}} \tag{2.4}$$

Proof: Observe that

$$\binom{3m}{m}=\frac{\prod_{j=1}^{m}(3j)\prod_{j=0}^{m-1}(3j+1)\prod_{j=0}^{m-1}(3j+2)}{m!\prod_{j=1}^{m}(2j)\prod_{j=0}^{m-1}(2j+1)}=(\frac{27}{4})^m\frac{\prod_{j=0}^{m-1}(\frac{2}{3}+j)\prod_{j=0}^{m-1}(\frac{1}{3}+j)}{m!\prod_{j=0}^{m-1}(\frac{1}{2}+j)}$$

and accordingly

$$\binom{3m+1}{m}=\frac{\prod_{j=1}^{m}(3j)\prod_{j=0}^{m-1}(3j+4)\prod_{j=0}^{m-1}(3j+2)}{m!\prod_{j=1}^{m}(2j)\prod_{j=0}^{m-1}(2j+3)}=(\frac{27}{4})^m\frac{\prod_{j=0}^{m-1}(\frac{2}{3}+j)\prod_{j=0}^{m-1}(\frac{4}{3}+j)}{m!\prod_{j=0}^{m-1}(\frac{3}{2}+j)}.$$

Then with (2.2) and (2.3) we have the representation

$$D(x):=1-x\cdot C(x)^2=\frac{\sum_{m=0}^{\infty}\binom{3m}{m}x^m}{\sum_{m=0}^{\infty}\binom{3m+1}{m}x^m}=\frac{F(\alpha,\beta,\gamma,y)}{F(\alpha,\beta+1,\gamma+1,y)},$$

which is the quotient of two hypergeometric series, where

$$F(\alpha,\beta,\gamma,y)=1+\frac{\alpha\beta}{\gamma}y+\frac{\alpha(\alpha+1)\beta(\beta+1)}{2!\cdot\gamma(\gamma+1)}y^2+\frac{\alpha(\alpha+1)(\alpha+2)\beta(\beta+1)(\beta+2)}{3!\cdot\gamma(\gamma+1)(\gamma+2)}y^2+\dots$$

with the parameter choice $\alpha=\frac{2}{3},\quad \beta=\frac{1}{3},\quad \gamma=\frac{1}{2},\quad y=\frac{27}{4}x.$
For quotients of such hypergeometric series the continued fractions expansion as in (1.14) was found by Gauss (see [16], p. 311). Namely for $n=1,2,\dots$ it is

$$e_n=\frac{(\alpha+n)(\gamma-\beta+n)}{(\gamma+2n)(\gamma+2n+1)},\qquad q_n=\frac{(\beta+n)(\gamma-\alpha+n)}{(\gamma+2n-1)(\gamma+2n)}.$$

Some further elementary calculations – carried out exactly in [22] – finally yield the formula in the theorem. (q.e.d.)

Let us finally discuss the connection to the Mills – Robbins – Rumsey determinants

$$T_n(x,\mu) = \det\left(\sum_{t=0}^{2n-2}\binom{i+\mu}{t-i}\binom{j}{2j-t}x^{2j-t}\right)_{i,j=0,\dots,n-1}, \tag{2.6}$$

where μ is a nonnegative integer (discussed e. g. in [15]). For $\mu = 0,1$ it is $T_n(1,\mu) = d_n^{(\mu)}$ - the Hankel determinants in (2.4). Stanley [21] conjectured $T_n(1,1)$ to be the generating function for alternating sign matrices invariant under a reflection about a vertical axis (cf. also [15]. This has recently been proved by Kuperberg [10].

An *alternating sign matrix* is a square matrix with entries from $\{0,1,-1\}$ such that i) the entries in each row and column sum up to 1, ii) the nonzero entries in each row and column alternate in sign. An example is

$$\begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & -1 & 1 & 0 \\ 1 & -1 & 1 & -1 & 1 \\ 0 & 1 & -1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

The alternating sign matrix conjecture concerns the total number of $n \times n$ alternating sign matrices, which was conjectured by Mills, Robbins, and Rumsey to be $\prod_{j=0}^{n-1}\frac{(3j+1)!}{(n+j)!}$. The problem was open for fifteen years until it was finally settled by Zeilberger [25]. The development of ideas is described in Bressoud's book [4]. There are deep relations to Statistical Mechanics, since the configuration of water molecules in "square ice" can be described by an alternating sign matrix.

Recently, it has been discovered [19] that the formula for the total number of alternating sign matrices also arises as a Hankel determinant where the entries in the matrix are the coefficients of the generating function $\frac{1-(1-9x)^{1/3}}{3x}$. An appropriate combinatorial interpretation of these numbers might yield a new and simpler proof of the alternating sign matrix conjecture.

III. Catalan – like Numbers and the Berlekamp – Massey Algorithm

In this section we shall study two – dimensional arrays $l(m,j)$, $m,j = 0,1,2,\dots$ and the matrices $L_n = (l(m,j))_{m,j=0,1,\dots,n-1}$ defined by

$$l(m,j) = T(x^m \cdot t_j(x)), \tag{3.1}$$

where T is the linear operator defined under (1.9). Application of the three–term–recurrence

$$t_j(x) = (x-\alpha_j)t_{j-1}(x) - \beta_{j-1}t_{j-2}(x)$$

(cf. (1.17)) and the linearity of T yield the recursion

$$l(m,j) = l(m-1,j+1) + \alpha_{j+1}l(m-1,j) + \beta_j l(m-1,j-1) \tag{3.2}$$

with initial values $l(m,0) = c_m$, $l(0,j) = 0$ for $j \neq 0$ (and $\beta_0 = 0$, of course). Especially,

$$l(m,m) = c_0\beta_1\beta_2\cdots\beta_m, \quad l(m+1,m) = c_0\beta_1\beta_2\cdots\beta_m(\alpha_1+\alpha_2+\ldots+\alpha_{m+1}) \tag{3.3}$$

We shall point out two connections of the matrices L_n to Combinatorics and Coding Theory. Namely, for the case that $\beta_j = 1$ for all j the matrices L_n occur in the derivation of Catalan

– like numbers as defined by Aigner in [1]. They also can be determined in order to find the factorization $L_n = A_n \cdot U_n^t$, where A_n is a nonsingular Hankel matrix of the form (1.1) and U_n is the matrix (1.12) with the coefficients of the orthogonal polynomials in (1.8). Via formula (3.3) the Berlekamp – Massey algorithm can be applied to find the parameters α_j and β_j in the three – term recurrence of the orthogonal polynomials (1.8).

Aigner in [1] introduced Catalan – like numbers and considered Hankel determinants consisting of these numbers. For positive reals a and s Catalan – like numbers $C_m^{(a,s)}$ are defined as entries $b(m,0)$ in a two – dimensional array $b(m,j)$, $m = 0,1,2,\ldots$, $j = 0,1,\ldots,m$, with initial conditions $b(m,m) = 1$ for all $m = 0,1,2,\ldots$, $b(0,j) = 0$ for $j > 0$, and recursion

$$\begin{aligned} b(m,0) &= a \cdot b(m-1,0) + b(m-1,1), \\ b(m,j) &= b(m-1,j-1) + s \cdot b(m-1,j) + b(m-1,j+1) \text{ for } j = 1,\ldots,m. \end{aligned} \tag{3.4}$$

The matrices $B_n = (b(m,j))_{m,j=0,\ldots,n-1}$, obtained from this array, have the property that $B_n \cdot B_n^t$ is a Hankel matrix with determinant 1. In the example below the binomial coefficients $\binom{2m+1}{m}$ arise as $C_m^{(3,2)}$.

$$\begin{array}{ccccc} 1 \\ 3 & 1 \\ 10 & 5 & 1 \\ 35 & 21 & 7 & 1 \\ 126 & 84 & 36 & 9 & 1 \end{array}$$

In [1] it is further shown that $C_m^{(1,1)}$ are the Motzkin numbers, $C_m^{(2,2)}$ are the Catalan numbers and $C_m^{(3,3)}$ are restricted hexagonal numbers.

Important for the decoding of BCH codes is also a decomposition of the Hankel matrix $A_n = V_n D_n V_n^t$ as a product of a Vandermonde matrix V_n, its transpose V_n^t and the diagonal matrix D_n. Here the parameters in the Vandermonde matrix are essentially the roots of the polynomial $t_n(x)$. This decomposition was already discovered by Baron Gaspard Riche de Prony [18] (rather known as the leading engineer in the construction of the Pont de la Concorde in Paris and as project head of the group producing the logarithmic and trigonometric tables from 1792 - 1801).

Via (3.3) the parameters r_j in the Berlekamp – Massey algorithm presented below will be explained in terms of the three – term recurrence of the orthogonal polynomials related to the Hankel matrices A_n.

Peterson [17] and Gorenstein and Zierler [8] presented an algorithm for the decoding of BCH codes. The most time–consuming task is the inversion of a Hankel matrix A_n as in (1.1), in which the entries c_i are syndromes resulting after the transmission of a codeword over a noisy channel. Matrix inversion, which takes $O(n^3)$ steps was proposed to solve equation (1.7). Berlekamp found a way to determine the $a_{n,j}$ in (1.7) in $O(n^2)$ steps. His approach was to determine them as coefficients of a polynomial $u(x)$ which is found as appropriate solution of the “key equation”

$$F(x)u(x) = q(x) \bmod x^{2t+1}.$$

Here the coefficients $c_0, \ldots, c_{2t}$ up to degree $2t$ of $F(x)$ can be calculated from the received word. Further, the roots of $u(x)$ yield the locations of the errors (and also determine $q(x)$). Motivated by the application in Coding Theory one is interested in finding polynomials of minimum possible degree fulfilling the key equation. This key equation is solved by iteratively calculating solutions $(q_k(x), u_k(x))$ to $F(x)u_k(x) = q_k(x) \bmod z^{k+1}$, $k = 0, \ldots, 2t$.

The algorithm is presented by Berlekamp in [2]. Massey [13] made a slight simplification of Berlekamp's algorithm and derived it as a problem in the design of linear feedback shift registers (cf. also [3], p. 180).

A sequence of shift registers $(\ell_j, u_j(x))$, $j = 1, \ldots, 2n-2$ is constructed, where ℓ_j denotes the length (the degree of u_j) and

$$u_j(x) = b_{j,j}x^j + b_{j,j-1}x^{j-1} + \ldots + b_{j,1}x + 1.$$

the feedback–connection polynomial of the j–th shift register. The Berlekamp – Massey algorithm works over any field and will iteratively compute the polynomials $u_j(x)$ as follows using a second sequence of polynomials $v_j(x)$.

Berlekamp – Massey Algorithm: Let $u_0(x) = 1, v_0(x) = 1$ and $\ell_0 = 0$. Then for $j = 1, \ldots, 2n-2$ set

$$r_j = \sum_{t=0}^{\ell_j} b_{j-1,t}c_{j-1-t}, \tag{3.5}$$

$$\ell_j = \delta_j(j - \ell_{j-1}) + (1 - \delta_j)\ell_{j-1}, \tag{3.6}$$

$$\begin{pmatrix} u_j(x) \\ v_j(x) \end{pmatrix} = \begin{pmatrix} 1 & -r_jx \\ \delta_j \cdot 1/r_j & (1-\delta_j)x \end{pmatrix} \cdot \begin{pmatrix} u_{j-1}(x) \\ v_{j-1}(x) \end{pmatrix}, \tag{3.7}$$

where

$$\delta_j = \begin{cases} 1 & \text{if } r_j \neq 0 \text{ and } 2\ell_{j-1} \leq j-1 \\ 0 & \text{otherwise} \end{cases}. \tag{3.8}$$

The relation of Berlekamp's algorithm to continued fraction techniques was pointed out by Mills [14] and thoroughly studied by Welch and Scholtz [24].

Several authors (e. g. [11], p. 156) state that the proof of the above recurrence is quite complicated or that there is need for a transparent explanation. We shall see now that the analysis is much simpler for the case that all principle submatrices of the Hankel matrix A_n are nonsingular. As a useful application, then the r_j's yield the parameters from the three – term recurrence of the underlying polynomials.

So, let us assume from now on that all principal submatrices A_i, $i \leq n$ of the Hankel matrix A_n are nonsingular. For this case, Imamura and Yoshida [9] demonstrated that $\ell_j = \ell_{j-1} = \frac{j}{2}$ for even j and $\ell_j = j - \ell_{j-1} = \frac{j+1}{2}$ for odd j such that δ_j is 1 if j is odd and 0 if j is even ($\frac{q_{2j}(x)}{u_{2j}(x)}$ then are the convergents to $F(x)$).

This means that there are only two possible recursions for $u_j(x)$ depending on the parity of j, namely

$$u_{2j}(x) = u_{2j-1}(x) - \frac{r_{2j}}{r_{2j-1}} x u_{2j-2}(x), \quad u_{2j-1}(x) = u_{2j-2}(x) - \frac{r_{2j-1}}{r_{2j-3}} x^2 u_{2j-4}(x).$$

So the algorithm is simplified in (3.6) and we obtain the recursion

$$\begin{pmatrix} u_{2j}(x) \\ v_{2j}(x) \end{pmatrix} = \begin{pmatrix} 1 - \frac{r_{2j}}{r_{2j-1}} x & -r_{2j-1} x \\ \frac{1}{r_{2j-1}} x & 0 \end{pmatrix} \cdot \begin{pmatrix} u_{2j-2}(x) \\ v_{2j-2}(x) \end{pmatrix}. \tag{3.9}$$

By the above considerations we have the following three–term recurrence for $u_{2j}(x)$ (and also for $q_{2j}(x)$ with different initial values).

$$u_{2j}(x) = (1 - \frac{r_{2j}}{r_{2j-1}} x) u_{2j-2}(x) - \frac{r_{2j-1}}{r_{2j-3}} x^2 u_{2j-4}(x).$$

Since the Berlekamp - Massey algorithm determines the solution of equation (1.7) it must be

$$x^j \cdot u_{2j}(\frac{1}{x}) = t_j(x).$$

as under (1.8). This is consistent with (1.17) where we consider the function $F(\frac{1}{x})$ instead of $F(x)$. By the previous considerations, for $t_j(x)$, we have the recurrence

$$t_j(x) = (x - \frac{r_{2j}}{r_{2j-1}}) t_{j-1}(x) - \frac{r_{2j-1}}{r_{2j-3}} t_{j-2}(x) \tag{3.10}$$

Equation (3.10) now allows to give a simple interpretation of the calculations in the single steps carried out in the course of the Berlekamp – Massey algorithm for the special case that all principle submatrices of the Hankel matrix A_n are nonsingular.

Proposition 3.1: Let A_n be a Hankel matrix with real entries such that all principal submatrices A_i, $i = 1, \ldots, n$ are nonsingular and let T be the linear operator mapping $T(x^l) = c_l$ as in (1.9). Then for the parameters r_j obtained via (3.5) it is

$$r_{2j-1} = T(x^{j-1} \cdot t_{j-1}(x)) = c_0 \beta_1 \beta_2 \cdots \beta_{j-1} \quad ,$$

$$r_{2j} = \alpha_j T(x^{j-1} \cdot t_{j-1}(x)) = c_0 \beta_1 \beta_2 \cdots \beta_{j-1} \alpha_j, \tag{3.11}$$

where α_j and $\beta_1, \ldots, \beta_{j-1}$ are the parameters from the three-term recurrence of the orthogonal polynomials $t_i(x)$, $i = 0, \ldots, j$.

Proof: The proposition, of course, follows directly from (3.10), since the three – term recurrence immediately yields the formula for the r_j's. Let us also verify the identities directly. From the considerations under (3.5) to (3.10) it is clear that the degree of u_{2j-2} is $j-1$. Hence in this case $b_{2j-2,j} = b_{2j-2,j+1} = \ldots = b_{2j-2,2j-2} = 0$ in (3.5) and

$$r_{2j-1} = \sum_{t=0}^{j-1} b_{2j-2,t} c_{2j-2-t} = \sum_{t=0}^{j-1} b_{2j-2,t} T(x^{2j-2-t})$$

$$= T\left(\sum_{t=0}^{j-1} b_{2j-2,t} x^{2j-2-t}\right) = T\left(x^{j-1} \sum_{t=0}^{j-1} b_{2j-2,t} x^{j-1-t}\right) = T\left(x^{j-1} \sum_{t=0}^{j-1} b_{2j-2,j-1-t} x^t\right)$$

$$= T\left(x^{j-1}\sum_{t=0}^{j-1} a_{j-1,t}x^t\right) = T(x^{j-1}t_{j-1}(x)) = c_0\beta_1\beta_2\cdots\beta_{j-1}$$

where the last equation follows by (3.3). A similar calculation shows that

$$r_{2j} = T\left(x^j t_{j-1}(x) - \frac{r_{2j-1}}{r_{2j-3}}x^{j-1}t_{j-2}(x)\right) = T\left(x^j t_{j-1}(x) - \beta_{j-1}x^{j-1}t_{j-2}(x)\right)$$

since by the previous calculation $\frac{r_{2j-1}}{r_{2j-3}} = \beta_{j-1}$. So by (3.3) further

$$r_{2j} = c_0\beta_1\beta_2\cdots\beta_{j-1}\left[(\alpha_1+\alpha_2+\ldots+\alpha_j) - (\alpha_1+\alpha_2+\ldots+\alpha_{j-1})\right] = c_0\beta_1\beta_2\cdots\beta_{j-1}\alpha_j.$$

Remarks:

1) Observe that with Proposition 3.1, the Berlekamp – Massey algorithm can be applied to determine the coefficients α_j and β_j from the three – term reccurence of the orthogonal polynomials $t_j(x)$. From the parameters r_{2j-1} obtained by (3.5) in the odd steps of the iteration $\beta_{j-1} = \frac{r_{2j-1}}{r_{2j-3}}$ can be immediately calculated, and in the even steps $\alpha_j = \frac{r_{2j}}{r_{2j-1}}$ is obtained. By (1.15) and (1.19) it is $\beta_{j-1} = \frac{r_{2j-1}}{r_{2j-3}} = \frac{\det(A_j)\det(A_{j-2})}{\det(A_{j-1})^2}$. Hence $r_{2j-1} = \frac{\det(A_j)}{\det(A_{j-1})}$, which means that the Berlekamp – Massey algorithm also yields a fast procedure to compute the determinant of a Hankel matrix.

2) By Proposition 3.1 the identity (3.5) reduces to $\sum_{t=0}^{j} a_{j,t}c_{j+t} = c_0\beta_1\beta_2\cdots\beta_j$ where the $a_{j,t}$ are the coefficients of the polynomial $t_j(x)$, the β_i's are the coefficients in their three – term recurrence and the c_i's are the corresponding moments. For the classical orthogonal polynomials all these parameters are usually known, such that one might also use (3.5) in the Berlekamp – Massey algorithm to derive combinatorial identities.

3) The number wall algorithm due to Conway – also motivated by continued fractions – was recently presented as a cookbook for linear feedback shift registers [12].

References

[1] M. Aigner, "Catalan-like numbers and determinants", *J. Comb. Th. A* 87, 1999, 33-51.

[2] E.R. Berlekamp, *Algebraic Coding Theory*, McGraw–Hill, 1968.

[3] R.E. Blahut, *Theory and Practice of Error Control Codes*, Addison – Wesley, 1984.

[4] D.M. Bressoud, *Proofs and Confirmations*, Cambridge Univ. Press, 1999.

[5] C. Brezinski, *Padé–Type Approximation and General Orthogonal Polynomials*, 1980.

[6] M. Desainte-Catherine and X.G. Viennot, "Enumeration of certain Young tableaux with bounded height", *Combinatoire Énumérative (Montreal 1985)*, Springer , 1986, 58-67.

[7] P. Flajolet, "Combinatorial aspects of continued fractions", *Disc. Math.* 32, 1980, 125-161

[8] D.C. Gorenstein and N. Zierler, "A class of error–correcting codes in p^m symbols", *J. Soc. Indus. Appl. Math.* 9, 1961, 207-214.

[9] K. Imamura and W. Yoshida, “A simple derivation of the Berlekamp – Massey algorithm and some applications”, *IEEE Trans. Inform. Theory* 33, 1987, 146-150.

[10] G. Kuperberg, “Symmetry classes of alternating–sign matrices under one roof”, arXiv math.CO/0008184, 2001.

[11] S. Lin and D.J. Costello, *Error – Control Coding*, Prentice – Hall, 1983.

[12] W.F. Lunnon, “The number-wall algorithm: an LFSR cookbook”, *J. Integer Sequences*, 2001, Article 01.1.1 (electronic).

[13] J.L. Massey, “Shift register synthesis and BCH decoding”, *IEEE Trans. Inform. Theory* 15, 1969, 122-127.

[14] W.H. Mills, “Continued fractions and linear recurrences”, *Math. Comp.* 29, 1975, 173-180

[15] W.H. Mills, D.P. Robbins, and H. Rumsey Jr., “Enumeration of a symmetry class of plane partitions”, *Discrete Math.* 67, 1987, 43-55.

[16] O. Perron, *Die Lehre von den Kettenbrüchen*, Chelsea Publishing Company, 1929.

[17] W.W. Peterson, “Encoding and error–corection procedures for the Bose–Chaudhuri codes”, *Trans. IRE* 6, 1960, 459-470.

[18] G. de Prony, “Essai expérimental et analytique sur les lois de la dilatabilité de fluides élastiques et sur les celles de la force expansive de la vapeur de l’ alcool, à différentes températures”, *J. de l’École Polytechnique* 1, cahier 22, 1795, 24-76.

[19] J. Propp, “The many faces of alternating sign matrices”, *Discr. Math. Theoret. Comp. Sci. Proceedings* AA (DM-CCG), 2001, 43-58.

[20] H. Rutishauser, *Der Quotienten–Differenzen–Algorithmus*, Birkhäuser, 1957.

[21] R.P. Stanley, “A baker’s dozen of conjectures concerning plane partitions”, *Combinatoire Énumérative (Montreal 1985)*, Lect. Notes Math. 1234, 1986, 285-293.

[22] U. Tamm, “Some aspects of Hankel matrices in coding theory and combinatorics”, *Electronic J. Combinatorics* 8, 2001, article # A31 (electronic).

[23] X.G. Viennot, “A combinatorial theory for general orthogonal polynomials with extensions and applications”, *Polynômes Orthogonaux et Applications, Proceedings, Bar – le – Duc*, Springer 1984, 139-157.

[24] L.R. Welch and R.A. Scholtz, “Continued fractions and Berlekamp’s algorithm”, *IEEE Trans. Inform. Theory* 25, 1979, 19-27.

[25] D. Zeilberger, “Proof of the refined alternating sign matrix conjecture”, *New York Journal of Mathematics* 2, 59-68, 1996.