The Berlekamp-Massey Algorithm. A Sight from Theory of Pade Approximants and Orthogonal Polynomials

S.B. Gashkov[1]* and I.B. Gashkov[2]**

[1] Department Mechanics and Mathematics
Moscow State University, 119899 Moscow, Russia
gashkov@lsili.ru
[2] Department of Engineering Sciences,Physics and Mathematics,
Karlstad University,651 88 Karlstad, Sweden
Igor.Gachkov@kau.se

Abstract In this paper we interpret the Berlekamp-Massey algorithm (BMA) for synthesis of linear feedback shift register (LFSR) as an algorithm computing Pade approximants for Laurent series over arbitrary field. This interpretation of the BMA is based on a iterated procedure for computing of the sequence of polynomials orthogonal to some sequence of polynomial spaces with scalar product depending on the given Laurent series. It is shown that the BMA is equivalent to the Euclidean algorithm of a conversion of Laurent series in continued fractions.

1 Introduction

Let $f_0, \dots, f_{n-1}, \dots$ be a sequence of elements from arbitrary given field F. The given sequence is generated by the given LFSR iff this sequence satisfies the linear recurrence relation of order m, $\sum_{i=0}^{m} f_{i+k} q_i = 0, k = 0, 1, 2, \dots$ with the initial values $f_0, \dots, f_{m-1}$, where $Q(x) = \sum_{i=0}^{m} q_i x^i, q_m = 1$ is the characteristic polynomial of the given LFSR. (see [1].) The reciprocal characteristic polynomial $Q^*(x) = x^m Q(1/x)$ is called the feedback polynomial of the given LFSR. Denote by $L_n(f)$ the least degree of the polynomial Λ_n generating the sequence $f_0, \dots, f_{n-1}$. The number $L_n(f)$ is called *the linear complexity* of the sequences $f_0, \dots, f_{n-1}$. ([1].) The sequence $L_1(f), \dots L_n(f)$ is called *the linear complexity profile* of the sequence $f_0, \dots, f_{n-1}$. J. L. Massey [2] interpreted the Berlekamp algorithm [3] as the algorithm computing of the linear complexity profile for the given sequence and generating the corresponding sequence of the characteristic polynomials. (see [1].) Berlekamp's variant of the BMA is equivalent to the variant of the Euclidean algorithm (EA) given for BCH codes decoding ([4].) In [5], [6] was investigated connections between the BMA and continued fractions.

* The research of first author was support by The Russian Found of Fundamental Investigations, projects 02-01-10142, 00985 and by the grant Sc.Sch. 1807.2003.1
** The research of second author was support by The Royal Swedish Academy of Sciences

M. Bubak et al. (Eds.): ICCS 2004, LNCS 3037, pp. 561–564, 2004.

In [7] was given the matrix generalization of the BMA. This generalization was used in [8] in the proof of the equivalence the BMA and the EA for decoding of BCH codes. We interpret the BMA from the point of view of theory of Pade approximants and orthogonal polynomials.

2 Pade Approximants for Laurent Series, Continued Fractions, Linear Complexity, and BMA

Any expression $z^n(c_0 + c_1/z + c_2/z^2 + \dots),\ c_0 \neq 0$, with any integer n and coefficients $c_i \in F$ is called *a formal Laurent series.* The set $F((1/z))$ of all Laurent series forms the field with respect to the sum and product operation (see [9]). Any series $f(z)$ with null integral part may be expanded in continued fraction

$$f(z) = \cfrac{1}{a_1(z) + \cfrac{1}{a_2(z) + \cfrac{1}{a_3(z) + \dots}}}.$$

The proper fraction formed the first n levels of a given continued fraction, is called a $n-$th convergent to a given continued fraction and is denoted by τ_n. The numerator P_n and the denominator Q_n of the τ_n are calculated by the recurrent formulas $Q_n = a_n Q_{n-1} + Q_{n-2}, Q_1 = 1, Q_0 = 0,\ P_n = a_n P_{n-1} + P_{n-2}, P_1 = a_1, P_0 = 1$. (see [9].) The polynomials Q_n and P_n have degrees $s_n - 1$ and s_n , where $s_n = d_1 + \dots + d_n, s_0 = 0,\ d_n = \deg a_n$. We consider only Laurent series $f(z) = \sum_{i=0}^{\infty} f_i z^{-i-1}$ with null integral part. It is known

Theorem 1. *The following statements are equivalent:*

(i) the LFSR with the characteristic polynomial $Q(z)$ generates the sequence $f_0, \dots f_{L-1}$;

(ii) there exist the polynomials P, Q such that

$$f(z)Q(z) = P(z) + \frac{c}{z^{L-\deg Q+1}} + \dots, c \in F,$$

where $\deg P(z) < \deg Q(z)$;

(iii) there exist the polynomials P, Q such that

$$f(z) - \frac{P(z)}{Q(z)} = \frac{b}{z^{L+1}} + \dots, b \in F, \deg P < \deg Q.$$

For any n there exists a unique uncancelled proper fraction $P_n/G_n, \deg G_n \leq n$ such that $f(z)Q_n(z) = P_n(z) + \frac{c}{z^{n+1}} + \dots, c \in F$. (see [9]). This fraction is called $n-$th (diagonal) *Pade approximants* π_n of a number f. It a numerator P_n Suppose $\pi_n = P_n/G_n$ and $Q = G_n$ is the polynomial of minimal degree $m \leq n$ such that $f(z)Q(z) = P(z) + \frac{c_{n+1}}{z^{n+1}} + \dots$; then the sequence $f_0, \dots, f_{n+m-1}$ satisfies the recurrence relation $\sum_{i=0}^{m} f_{i+k} q_i = 0, k = 0, \dots, n-1$. Denote by Π_n degree of the fraction π_n.

Theorem 2. $L_{\Pi_n+n} = \Pi_n$.

If the degree of denominator of $n-$th Pade fraction is equal n, then the index n is called *normal.* If $n_0 < n_1$ there are adjacent normal indexes, then ([9]) for any $k, n_1 > k \geq n_0$, $f(z)G_{n_0}(z) - P_{n_0}(z) = G_{n_0}(z)(cz^{-n_0-n_1} + \dots) = ez^{-n_1} + \dots = bz^{-k-1} + \dots, c, e, b \in F$ and $G_k = G_{n_0}, n_0 = \Pi_{n_0} = \Pi_k = L_{k+\Pi_k} = L_{k+n_0}$. The sequence of normal indexes coincides with the sequence $s_0, s_1, s_2, \dots$ and Pade approximants $\pi_{s_n} = \tau_n = P_n/Q_n$. ([9].) Therefore, for any $k, s_n \leq k < s_{n+1}$, is valid $\pi_k = \pi_{s_n} = \tau_n, G_k = G_{s_n} = Q_n$ and for any sequence $\{f_0, \dots, f_{s_n+k}\}, k = s_n - 1, \dots, s_{n+1} - 2$ the minimal LFSR has the characteristic polynomial Q_n.

Theorem 3. $L_{k+s_n} = s_n,\ s_{n-1} \leq k < s_n$.

From theorem 3 easy follows well known

Theorem 4. *If the LFSR of the complexity $L_k(f)$ generates the sequence $f_0, \dots, f_k$ then $L_{k+1}(f) = L_k(f)$, else $L_{k+1}(f) = \max\{L_k(f), k+1-L_k(f)\}$.*

3 The Interpretation of the BMA in Terms of Orthogonal Polynomials

The following part of the paper *does not assume any knowledge about the BMA* and can be used for a *alternative description* of this algorithm.

Let $Pol(n)$ be the space of polynomials of degree less than n over a field F. For the given sequence $\{f_0, \dots, f_{n-1}\}$ over a field F we consider the linear functional $l_f(P) = \sum_{i=0}^{n-1} f_i p_i, P(z) = \sum\limits_{i=0}^{n-1} p_i z^i$. over the space $Pol(n)$. On the space $Pol(n)$ may be defined the scalar product $(P, Q) = (P, Q)_f$ of polynomials P, Q by equality $(P, Q) = l_f(PQ)$. Obviously is valid the identity $(P, Q) = (PQ, 1)$. Following [9], we rewrite the equalities $\sum_{i=0}^{m} f_{i+k} q_i = 0, k = 0, \dots, s-1$, where $Q(z) = \sum_{i=0}^{m} q_i z^i, q_m = 1$, as the equalities $(Q(z), z^k) = 0, k = 0, \dots, s-1$, where (P, Q) is the scalar product of polynomials P, Q. Orthogonality of vectors is denoted by the symbol $\perp$. Therefore, the system of equalities $(Q_n(z), z^k) = 0, k = 0, \dots, s_n - 1$ is equivalent to the relation $Q_n(z) \perp Pol_{s_n}$. Hence $Q_n \perp Q_{n-1}$ and the sequence of polynomials $Q_n(z) = \sum_{i=0}^{s_n} q_{n,i} z^i$, is uniquely determined by the mentioned above condition of the orthogonality.

Suppose that we have computed the polynomial Q_n by the given sequence $f_0, \dots, f_{2s_n-1}$. It is valid $\Lambda_{2s_n} = Q_n$. Computing $(Q_n(z), z^k) = \sum_{i=0}^{m} f_{i+k} q_{n,i}, m = s_n, k = m, m+1, \dots$ we find minimal k such that $(Q_n(z), z^k) \neq 0$. Hence, we can find s_{n+1}, because $k = s_{n+1} - 1$. Since the polynomial $Q_n(z)$ satisfies the condition $\sum_{i=0}^{s_n} f_{i+k} q_{n,i} = 0, k = 0, \dots, s_{n+1} - 2$, then the LFSR with the characteristic polynomial Q_n generates any sequence $f_0, \dots, f_k$, where $k = 2s_n, \dots, s_n + s_{n+1} - 2$. Therefore, we have $\Lambda_k = Q_n, k = 2s_n, \dots, s_n + s_{n+1} - 1$. Further, we find $d_{n+1} = s_{n+1} - s_n$. Let's look for the polynomial Q_{n+1} in the form $a_{n+1}(z)Q_n(z) + Q_{n-1}(z)$, where $\deg a_{n+1} = d_{n+1}$. The polynomial Q_{n+1} is uniquely determined (with an exactitude up to a constant factor) by the condition $Q_{n+1} \perp Pol_{s_{n+1}}$. By the induction hypothesis $Q_n \perp Pol_{s_{n+1}-1}$, but the polynomial Q_n is not orthogonal to the space $Pol_{s_{n+1}}$. Hence, $(Q_n(z), z^{s_{n+1}-1}) = \Delta_{s_n+s_{n+1}-1} \neq 0$. Since $a_{n+1}(z)z^k \in Pol_{s_{n+1}-1}, z^k \in Pol_{s_n-1}$, we see that for any polynomial a_{n+1} of degree d_{n+1} $a_{n+1}(z)Q_n(z) + Q_{n-1}(z) \perp Pol_{s_n-1}$. To choose the polynomial a_{n+1} such that the polynomial $a_{n+1}(z)Q_n(z) + Q_{n-1}(z)$ is orthogonal to the space generated by the monomials $z^{s_n-1}, \dots, z^{s_{n+1}-1}$, we need next condition. The projections of the polynomials $a_{n+1}(z)Q_n(z)$ and $Q_{n-1}(z)$ on this space are opposite, i.e. $(a_{n+1}(z)Q_n(z), z^k) = -(Q_{n-1}(z), z^k), k = s_n - 1, \dots, s_{n+1} - 1$. These equalities concerning coefficients of the polynomial a_{n+1} determine the system of linear equations with a triangular matrix. This system may be solved by the following iterated algorithm.

A step with any number. At $i-$th step we correct the polynomial $Q_{n+1}^{(i-1)}$ iff $\Delta_{s_n+s_{n+1}+i-2} = (Q_{n+1}^{(i-1)}, z^{s_n+i-2}) \neq 0$. Then we look for the $Q_{n+1}^{(i)} = Q_{n+1}^{(i-1)} + cQ_n z^{d_{n+1}-i+1}$ such that $Q_{n+1}^{(i)} \perp z^{s_n+i-2}$. For this goal we search a constant c such that the projections $Q_{n+1}^{(i-1)}, cQ_n z^{d_{n+1}-i+1}$ on the monomial z^{s_n+i-2} are opposite. Hence, $c = -\Delta_{s_n+s_{n+1}+i-2}/\Delta_{s_n+s_{n+1}-1}$. Since $Q_{n+1}^{(i-1)} \perp Pol_{s_n+i-2}$ by the induction hypothesis, we have $Q_{n+1}^{(i-1)} \perp z^{s_n+k}$ for any $k, -1 \leqslant k \leqslant i-3$. Therefore, $(Q_{n+1}^{(i)}, z^{s_n+k}) = (Q_{n+1}^{(i-1)}, z^{s_n+k}) + (cQ_n z^{d_{n+1}-i+1}, z^{s_n+k}) = c(Q_n, z^{s_{n+1}+k+1-i}) = 0$. Since $Q_{n+1}^{(i)} \perp Pol_{s_n+i-1}$, we see that $\Lambda_{s_n+s_{n+1}+i-2} = Q_{n+1}^{(i)}$. **Last step.** Finally, at $d_{n+1}+1-$th step we get the polynomial $Q_{n+1}^{(d_{n+1}+1)} = Q_n a_{n+1} + Q_{n-1}, \deg Q_{n+1}^{(d_{n+1}+1)} = s_{n+1}$, such that $Q_{n+1}^{(d_{n+1}+1)} \perp Pol_{s_n+d_{n+1}} = Pol_{s_{n+1}}$. This polynomial coincides with the polynomial Q_{n+1}. Hence $\Lambda_{2s_{n+1}} = Q_{n+1}$.

References

1. Jungnickel D., *Finite fields. Structure and arithmetic*, Wissenschaftsverlag, Mannheim, Leipzig, Wien, Zurich (1993).
2. Massey J.L., *Feedback Shift Register Synthesis and BCH Decoding*, *IEEE Trans. Inform. Theory*, **IT15** (1969), 122-128.
3. Berlekamp E.R., *Algebraic coding theory*, McGraw Hill (1968).
4. Dornstetter J.L., *On the equivalence between Berlekamp's and Euclid's algorithms*, *IEEE Trans. Inf. Theory* **IT-33**, 3 (1987), 428-431.
5. Cheng U., *On the continued fractions and Berlekamp's Algorithm*, *IEEE Trans. Inf. Theory* **IT-30**, 3 (1984), 541-544.
6. Zongduo Dai, Kencheng Zeng, *Continued fractions and Berlekamp-Massey Algorithm*, *Advances in Cryptology - Auscript-90*, Springer Verlag, Berlin (1990), 24-31.
7. Feng G.-L., Tzeng K.K., *A generalization of the Berlekamp- Massey algorithm for multisequence shift-register sinthesis with applications To decoding cyclic codes*, *IEEE Trans. Inf. Theory* **IT-37**, (Sept.1991), 1274-1287.
8. Agnes E. Heydtmann, J.M.Jensen, *On the equivalence of the Berlekamp-Massey and Euclidean algorithms for decoding*, *IEEE Trans. Inf. Theory* **IT-46**, 7 (2000), 2614-2624.
9. Nikishin E.M., Sorokin V.N. *Rational approximations and Orthogonality*, Moscow, Nauka (1988), AMS, New York (1996).