Mathematical Notes, vol. 79, no. 1, 2006, pp. 41–54.
Translated from Matematicheskie Zametki, vol. 79, no. 1, 2006, pp. 45–59.

Berlekamp–Massey Algorithm, Continued Fractions, Padé Approximations, and Orthogonal Polynomials

S. B. Gashkov and I. B. Gashkov

Received February 16, 2005

Abstract—The Berlekamp–Massey algorithm (further, the BMA) is interpreted as an algorithm for constructing Padé approximations to the Laurent series over an arbitrary field with singularity at infinity. It is shown that the BMA is an iterative procedure for constructing the sequence of polynomials orthogonal to the corresponding space of polynomials with respect to the inner product determined by the given series. The BMA is used to expand the exponential in continued fractions and calculate its Padé approximations.

Key words: *Berlekamp–Massey algorithm, Padé approximations, continued fraction, orthogonal polynomial, Laurent series, Euclid's algorithm.*

1. INTRODUCTION

Suppose we are given a sequence $f_0, \dots, f_{n-1}, \dots$ of elements of an arbitrary field F. It is well known (see [1, 2]) that such a sequence can be generated by a linear feedback shift register (LFSR), given the initial conditions $f_0, \dots, f_{m-1}$ and the linear recurrence relations

$$f_k q_0 + f_{k+1} q_1 + \dots + f_{k+m} q_m = 0, \qquad k = 0, 1, 2, \dots,$$

where

$$Q(x) = q_m x^m + q_{m-1} x^{m-1} + \dots + q_0, \qquad q_m = 1,$$

is the feedback polynomial of the LFSR. This definition differs from the standard one in that the feedback polynomial is replaced by its reciprocal polynomial.

In the case of the field $GF(2)$, the LFSR with feedback polynomial $Q(x)$ is a linear automaton consisting of $m+1$ registers, with the tap on the ith register multiplied by the coefficient q_i; all these taps are summed modulo 2 and the result is input to the first register (see [2]).

Let $L_n(f)$ be the least degree of the polynomial Λ_n generating the sequence $f_0, \dots, f_{n-1}$. It is called (see [1]) the *linear complexity* of the sequence $f_0, \dots, f_{n-1}$, while the sequence $\{L_n(f)\}$ is called the *profile of linear complexity* of the sequence $\{f_n\}$. Massey [3] interpreted Berlekamp's algorithm [4] as an algorithm for calculating the linear complexity of the sequence $f_0, \dots, f_{n-1}$ and of the LFSR (generating it) with feedback polynomial of minimal degree (see also [1, 2]).

The BMA has various applications [1–4]. It is well known [5] that the BMA is equivalent, in a certain sense, to the version of Euclid's algorithm for BCH decoding proposed in [6] (see [2]). The relation between the BMA and the continued fractions was studied in numerous works (see [7–10]).

In this paper, we propose an interpretation of the BMA based on theory of Padé approximations and orthogonal polynomials.

2. LAURENT SERIES, PADÉ APPROXIMATIONS, AND CONTINUED FRACTIONS

An expression of the form

$$z^n\left(c_0+\frac{c_1}{z}+\frac{c_2}{z^2}+\cdots\right),\qquad c_0\neq 0,$$

for any integer n, with coefficients c_i belonging to F, is called a *formal Laurent series.* On the set $F((1/z))$ of all Laurent series, the operations of addition and multiplication are defined in the standard way; under these operations, this set forms a field. (see [11]). Further, we shall only consider Laurent series with zero integral part, i.e., series of the form $f(z)=f_0/z+f_1/z^2+\cdots$. Such series can be expanded (see [11]) in continued fractions

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

The fraction formed by the first n levels of the continued fraction for $f(z)$ is called the *nth convergent* and denoted by τ_n.

It is easily verified that, for such an arbitrary series, the sequences of its coefficients satisfies the linear recurrence relations

$$\sum_{i=0}^{m} f_{i+k}q_i=0,\qquad k=0,\dots,n-1, \tag{1}$$

if and only if

$$f(z)Q(z)=P(z)+\frac{c}{z^{n+1}}+\frac{c_{n+2}}{z^{n+2}}+\cdots,\qquad c\in F,\quad \deg P<\deg Q. \tag{2}$$

Condition (2) is equivalent to the condition

$$f(z)-\frac{P(z)}{Q(z)}=\frac{b}{z^{n+1+\deg Q}}+\cdots,\qquad b\in F,\quad \deg P<\deg Q. \tag{3}$$

Therefore, the LFSR with feedback polynomial $Q(z)$ generates the sequence $f_0,\dots,f_{L-1}$ if and only if (2) (or (3)) is satisfied for $n=L-\deg Q$.

It is well known [11] that, for any n, there exists a regular fractions P_n/G_n of degree at most n satisfying this condition. It is also well known [11] that all such fractions are uniquely defined up to a common multiplier both of the numerator and the denominator, which can be canceled. The fraction which is irreducible is called the *nth* (diagonal) *Padé approximation* π_n of the series f. Its numerator P_n and denominator G_n form the *nth Padé pair.* These polynomials are uniquely defined up to a constant factor.

Fractions P/Q of *arbitrary* degree satisfying condition (2) are *not uniquely defined.* If $\pi_n=P_n/G_n$ and the polynomial $Q=G_n$ is the polynomial of least degree $m\le n$ satisfying the condition

$$f(z)Q(z)=P(z)+\frac{c_{n+1}}{z^{n+1}}+\cdots,$$

then relations (1) hold. Therefore, if the degree of the fraction π_n is denoted by Π_n and we choose a polynomial of the same degree G_n so that $\pi_n=P_n/G_n$, then the LFSR with feedback polynomial G_n and initial state of the registers $f_0,\dots,f_{\Pi_n-1}$ will generate the sequence $f_0,\dots,f_{\Pi_n+n-1}$, whence $L_{\Pi_n+n}\le\Pi_n$. It is easy to verify that $L_{\Pi_n+n}=\Pi_n$.

If the degree of the denominator in the nth Padé pair is equal to n, i.e., the Padé pairs are uniquely defined up to a constant factor, then the index n is called *normal*. It is well known [11] that if $n_0 < n_1$ are adjacent normal indices, then

$$f(z) - \pi_{n_0}(z) = c_{n_0+n_1} z^{-n_0-n_1} + \cdots, \qquad c_{n_0+n_1} \neq 0,$$

i.e., the exact order of tangency of $\pi_{n_0}(z)$ to the series $f(z)$ is equal to n_0+n_1, and all the π_k for $n_1 > k > n_0$ are equal to π_{n_0}. Hence, for $n_1 > k \geq n_0$,

$$f(z)G_{n_0}(z) - P_{n_0}(z) = G_{n_0}(z)(c_{n_0+n_1} z^{-n_0-n_1} + \cdots) = e_{n_1} z^{-n_1} + \cdots = b_k z^{-k-1} + \cdots$$

for some b_k, possibly zero. Therefore, the following assertion is valid.

Lemma 1. *For $n_0 \leq k < n_1$, the following equalities hold*:

$$G_k = G_{n_0}, \qquad n_0 = \Pi_{n_0} = \Pi_k = L_{k+\Pi_k} = L_{k+n_0}.$$

Let us prove the following assertion.

Theorem 1. *The profile of linear complexity and the sequence of normal indices s_n, $n = 1, 2, \dots$, are related by*

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

Proof. It is well known [11] that the sequence of normal indices coincides with the sequence of degrees $s_0, s_1, s_2, \dots$ of the denominators of the convergents and

$$f(z) - \tau_m(z) = \frac{c_m}{z^{s_m+s_{m+1}}}, \qquad c_m \neq 0, \tag{4}$$

i.e., the Padé approximation is $\pi_{s_n} = \tau_n = P_n/Q_n$. For $s_n \leq k < s_{n+1}$, Lemma 1 implies $\pi_k = \tau_n$, $G_k = Q_n$; hence

$$\sum_{i=0}^{s_n} f_{i+k} q_{n,i} = 0, \quad k = 0, \dots, s_{n+1}-2, \qquad \sum_{i=0}^{s_n} f_{i+k} q_{n,i} \neq 0, \quad k = s_{n+1}-1,$$

where $Q_n(z) = q_{n,s_n} z^{s_n} + \cdots + q_{n,0}$. In other words, the LFSR with polynomial $Q_n(z)$ generates the sequence $\{f_0, \dots, f_m\}$ for $m = s_n + s_{n+1} - 2$, but does not generate it for $m = s_n + s_{n+1} - 1$. Since, for $s_{n+1} > k \geq s_n$, we have $s_n = L_{k+s_n}$, it follows that, for any sequence $\{f_0, \dots, f_{s_n+k}\}$, $k = s_n - 1, \dots, s_{n+1} - 2$, its minimal LFSR has feedback polynomial equal to Q_n. The definition of a normal index implies the uniqueness (up to a constant factor) of a polynomial $G_{s_n} = Q_n$ of degree s_n such that, for some regular fraction,

$$f(z) - \frac{P_n(z)}{Q_n(z)} = \frac{c_n}{z^{2s_n+1}}.$$

Hence there exists a unique LFSR of complexity s_n generating the sequence $\{f_0, \dots, f_{2s_n-1}\}$, and its feedback polynomial is equal to the polynomial Q_n up to a constant factor. Such a shift register generates all the sequences $\{f_0, \dots, f_{s_n+k}\}$, $k = s_n, \dots, s_{n+1} - 2$. In particular, $L_{k+s_n} = s_n$, $k = s_n, \dots, s_{n+1} - 1$. The upper bounds in the theorem follow from the equalities proved above.

Let us prove the lower bounds by contradiction. Assume that, for some k, $s_n + s_{n-1} \leq k < 2s_n$, the inequality $L_k < s_n$ holds. Then, for some polynomials P, Q, condition (2) holds for $n = k - \deg Q$, $\deg Q < s_n$. For $m = n - 1$, it follows from relation (4) that

$$f(z)Q_{n-1}(z) = P_{n-1}(z) + \frac{d}{z^{s_n}} + \cdots, \qquad d \neq 0.$$

Multiplying the first of the equalities by Q_{n-1}, the second by Q, and subtracting the second from the first, we obtain

$$\begin{aligned} Q_{n-1}P(z) - QP_{n-1}(z) &= Q_{n-1}(z)\left(\frac{b}{z^{k+1-\deg Q - s_{n-1}}} + \cdots\right) - Q(z)\left(\frac{d}{z^{s_n}} + \cdots\right) \\ &= \left(\frac{b}{z^{k+1-s_{n-1}-\deg Q}} + \cdots\right) - \left(\frac{d}{z^{s_n-\deg Q}} + \cdots\right) \\ &= \frac{d}{z^{s_n-\deg Q}} + \cdots = \frac{e}{z^1} + \cdots, \end{aligned}$$

because $d \neq 0$ and $s_n - \deg Q < k+1-s_{n-1}-\deg Q$. We have a polynomial on the left and a nonzero Laurent series on the right; thus, we have obtained a contradiction. The theorem is now proved. □

Combining the equalities proved above, we see that $L_k = s_n$ for $s_{n-1} + s_n \le k < s_{n+1} + s_n$.

To prove (in the standard way) that the BMA is well defined, we shall use the following theorem [1, 2].

Theorem 2. *For any k, either $L_{k+1}(f) = L_k(f)$, where f_k is the next tap on the* LFSR *of complexity $L_k(f)$ generating the sequence $f_0, \dots, f_{k-1}$, or $L_{k+1}(f) = \max\{L_k(f), k+1-L_k(f)\}$.*

Proof. The proof is easily obtained from the equalities $L_k = s_n$, $s_{n-1} + s_n \le k < s_{n+1} + s_n$. Indeed, it suffices to verify that, for $k = s_{n+1} + s_n - 1$, we have

$$L_{k+1} = s_{n+1} = k+1-s_n = k+1-L_k > L_k,$$

for $s_{n-1} + s_n \le k < 2s_n$, we have

$$L_{k+1} = s_n = L_k \ge k+1-s_n = k+1-L_k,$$

and, for $2s_n \le k < s_n + s_{n+1}$, for any sequence $\{f_0, \dots, f_{k-1}\}$ the minimal LFSR generating it has feedback polynomial equal to Q_n. □

3. THE BERLEKAMP–MASSEY ALGORITHM (BMA)

Let us show that the BMA simultaneously calculates both the elements $a_n(z)$ of the continued fraction in the case of an arbitrary series $f(z)$ and the sequence $Q_n = a_nQ_{n-1} + Q_{n-2}$, $Q_1 = a_1$, $Q_0 = 1$ of the denominators of its convergents (the Padé fractions). It also calculates the sequence of feedback polynomials Λ_n generating of the first n terms of the sequence $f_0, \dots, f_{n-1}, \dots$.

Let us present the standard description of the operation of the BMA (see [2]). By the induction hypothesis, for $i \le k$ there exists a LFSR with polynomial Λ_i generating the sequence $f_0, \dots, f_{i-1}$ and such that if $i < k$ and $f_i \neq f_{i+1}$, then $L_{i+1}(f) = \max\{L_i(f), i+1-L_i(f)\}$, and, otherwise, $\Lambda_{i+1} = \Lambda_i$. The induction base is established by the equalities $i = 1$, $L_0(f) = 0$, $\Lambda_1(x) = 1 + x$.

Suppose that m is the largest index satisfying $L_m(f) < L_{m+1}(f)$; then we put $s = L_{m+1}(f)$, $r = L_m(f)$. By the induction hypothesis, it follows from the relations

$$s = L_k(f) = \cdots = L_{m+1}(f) > L_m(f) = r$$

that $s = \max(r, m+1-r) = m+1-r$, because if $s = r$, then $L_{m+1}(f) = L_m(f)$, which cannot be true. Suppose that

$$\Lambda_i = c^{(i)}_{L_i(f)} x^{L_i(f)} + \cdots + c^{(i)}_1 x + c^{(i)}_0, \qquad c^{(i)}_0 = 1, \quad i = 1, \dots, k;$$

then, by definition,

$$\sum_{i=1}^{s} c_i^{(k)} f_{j-i} = \begin{bmatrix} f_j & \text{for } j = s, \dots, k-1, \\ a_k & \text{for } j = k \end{bmatrix}$$

and, similarly,

$$\sum_{i=1}^{r} c_i^{(m)} f_{j-i} = \begin{bmatrix} f_j & \text{for } j = r, \dots, m-1, \\ t_m & \text{for } j = m \end{bmatrix}$$

for some $t_m \ne a_m$, because $f_{m+1} \ne f_m$ by the choice of m. Setting $\mu_m = t_m - a_m \ne 0$, in accordance with the BMA, we define the polynomial

$$\Lambda_{k+1}(x) = \Lambda_k(x) + b_k \mu_m^{-1} x^{k-m} \Lambda_m(x)$$

of degree

$$\begin{aligned} \max(\deg \Lambda_k, \deg \Lambda_m + k - m) &= \max(s, r + k - m) = \max(s, (k+1) - (m+1-r)) \\ &= \max(s, (k+1) - s) = d. \end{aligned}$$

This polynomial generates the sequence $f_0, \dots, f_k$.

The description of the BMA is complete, but it was assumed in it that the LFSR generates the sequence defined by the linear recurrence relations

$$f_k q_0^* + f_{k-1} q_1^* + \dots + f_{k-m}^* q_m = 0, \qquad k = m, m+1, \dots,$$

where $Q^*(x) = q_m^* x^m + q_{m-1}^* x^{m-1} + \dots + q_0^*$, $q_m^* = 1$, is the feedback polynomial of the LFSR considered. We used *another definition* of the feedback polynomial, namely,

$$Q(x) = q_m x^m + q_{m-1} x^{m-1} + \dots + q_0, \qquad q_m = 1,$$

in which the sequence generated by the LFSR, satisfies the linear recurrence relations

$$f_k q_0 + f_{k+1} q_1 + \dots + f_{k+m} q_m = 0, \qquad k = 0, 1, 2, \dots.$$

The two methods of the definition of the feedback polynomial are related by the equalities

$$q_i^* = q_{m-i}, \qquad i = 0, \dots, m,$$

which imply that the polynomials Q and Q^* are mutually reciprocal, i.e., $Q(x) = x^m Q^*(1/x)$.

Further, let $\{s_n\}$ be the sequence of normal indices; we do not require that the leading coefficient of the polynomials Λ_i be equal to 1. Then the following assertion is valid.

Theorem 3. *For* $k = s_{n+1} + s_n - 1$,

$$\Lambda_{k+1}(x) = c_k x^{d_{n+1}} \Lambda_k(x) + Q_{n-1}(x), \qquad c_k \in F,$$

for $k = s_n + s_{n-1}, \dots, 2s_n - 1$,

$$\Lambda_{k+1}(x) = \Lambda_k(x) + c_k x^{2s_n - 1 - k} Q_{n-1}(x),$$

and for $k = 2s_n, \dots, s_n + s_{n+1} - 2$

$$\Lambda_{k+1} = \Lambda_k.$$

Proof. We can rewrite the relation $\Lambda^*_{k+1}(x) = \Lambda^*_k(x) + b_k\mu_m^{-1}x^{k-m}\Lambda^*_m(x)$ defining the step of the BMA, using reciprocal polynomials:

$$\begin{aligned}\Lambda_{k+1}(x) = x^{L_{k+1}}\Lambda^*_{k+1}\Big(\frac{1}{x}\Big) &= x^{L_{k+1}}\Lambda^*_k\Big(\frac{1}{x}\Big) + b_k\mu_m^{-1}x^{L_{k+1}}x^{m-k}\Lambda^*_m\Big(\frac{1}{x}\Big)\\ &= x^{L_{k+1}-L_k}\Lambda_k(x) + b_k\mu_m^{-1}x^{L_{k+1}-L_m}x^{m-k}\Lambda_m(x).\end{aligned}$$

As proved above, for $s = L_k(f) = \dots = L_{m+1}(f) > L_m(f) = r$, we have

$$s = m+1-r, \qquad L_m(f)+k-m = r+k-m = (k+1)-(m+1-r), = k+1-s = k+1-L_k(f).$$

Hence, for $\Lambda_{k+1} \neq \Lambda_k$, it follows that

$$L_{k+1}(f) = k+1-L_k(f) = L_m(f)+k-m, \qquad L_{k+1}(f) - L_m(f) - k + m = 0.$$

For $k = s_{n+1}+s_n-1$, we obviously have $L_{k+1} = s_{n+1}$, $L_k = s_n$, $L_{k+1}-L_k = s_{n+1}-s_n = d_{n+1}$, $m = s_n+s_{n-1}-1$, $L_m = s_{n-1}$, $\Lambda_m = Q_{n-1}$; therefore,

$$\begin{aligned}\Lambda_{k+1}(x) &= x^{L_{k+1}-L_k}\Lambda_k(x) + b_k\mu_m^{-1}x^{L_{k+1}-L_m}x^{m-k}\Lambda_m(x)\\ &= x^{d_{n+1}}\Lambda_k(x) + b_k\mu_m^{-1}Q_{n-1}(x), \qquad b_k \in F.\end{aligned}$$

As proved above, for $k = s_n+s_{n-1}, \dots, s_{n+1}+s_n-2$, we have

$$\begin{gathered}L_{k+1} = s_n = L_k, \qquad L_{k+1}-L_m = s_n - s_{n-1} = d_n,\\ L_{k+1}-L_m+m-k = d_n+s_n+s_{n-1}-1-k = 2s_n-1-k;\end{gathered}$$

then it follows that, for $k = s_n+s_{n-1}, \dots, 2s_n-1$, we can write

$$\begin{aligned}\Lambda_{k+1}(x) &= x^{L_{k+1}-L_k}\Lambda_k(x) + b_k\mu_m^{-1}x^{L_{k+1}-L_m}x^{m-k}\Lambda_m(x)\\ &= \Lambda_k(x) + b_k\mu_m^{-1}x^{2s_n-1-k}Q_{n-1}(x).\end{aligned}$$

The sequence Λ_k can be defined up to a constant factor; therefore, the first two equalities in the theorem are now proved. Earlier we proved that the LFSR with feedback polynomial cQ_n generates an arbitrary sequence $f_0, \dots, f_k$, where $k = 2s_n, \dots, s_n+s_{n+1}-1$. Hence, for any $k = 2s_n, \dots, s_n+s_{n+1}-2$, we obtain $\Lambda_{k+1} = \Lambda_k$. $\square$

4. INTERPRETATION OF THE BMA IN TERMS OF ORTHOGONAL POLYNOMIALS

In the preceding, we described a fragment of the theory of Padé approximations for Laurent series over an arbitrary field. The classical theory (see [11, 12]) is developed further for the field of complex numbers in close connection with the theory of orthogonal polynomials. In particular, in it, it is proved that, for so-called positive sequences f_n, the sequence of normal indices is $s_n = n$ and the following explicit formulas are valid:

$$Q_{n+1}(z) = (z+b_n)Q_n(z) + c_nQ_{n-1}(z).$$

On the basis of these considerations, an approach to BCH decoding was developed in [13].

In the general case, another method must be used, which naturally leads to an algorithm equivalent to the BMA. The remaining part of this paper does *not assume knowledge of the* BMA and can be used for its alternative description and justification.

Let Pol_n denote the n-dimensional space of polynomials of degree less than n over the field F under consideration. For a given sequence $\{f_0, \dots, f_{n-1}\}$ over the field F, we define the linear functional $l_f(P)$ on the space Pol_n by the relation

$$l_f(P) = \sum_{i=0}^{n-1} f_i p_i, \qquad P(z) = \sum_{i=0}^{n-1} p_i z^i.$$

On the space Pol_n, we define the inner product $(P, Q) = (P, Q)_f$ of the polynomials P, Q by the equality $(P, Q) = l_f(PQ)$. This inner product possesses the properties of bilinearity and symmetry. Moreover, the identity $(P, Q) = (PQ, 1)$ obviously holds.

4.1. Description of the sequence of denominators of Padé fractions in terms of orthogonality to the spaces Pol_n

Following [11], we rewrite the equalities

$$f_k q_0 + f_{k+1} q_1 + \dots + f_{k+m} q_m = 0, \qquad k = 0, \dots, s-1,$$

in the form

$$(Q(z), z^k) = 0, \qquad k = 0, \dots, s-1,$$

where $Q(z) = q_m z^m + q_{m-1} z^{m-1} + \dots + q_0$, $q_m = 1$, and, by (P, Q) we denote the inner product of the polynomials P, Q. The orthogonality of vectors (and of a vector to a subspace) is denoted the symbol $\perp$.

Therefore, the system of equalities $(Q_n(z), z^k) = 0$, $k = 0, \dots, s_n - 1$, is equivalent to $Q_n(z) \perp \mathrm{Pol}_{s_n}$. Since $\deg G_n = s_n > s_{n-1} = \deg G_{n-1}$, this yields $Q_n \perp Q_{n-1}$.

Moreover, the polynomial $Q_n(z) = q_{n,s_n} z^{s_n} + \dots + q_{n,0}$ is uniquely defined (up to a constant factor) by the orthogonality condition indicated above, while the conditions

$$\sum_{i=0}^{s_n} f_{i+k} q_{n,i} = 0, \quad k = 0, \dots, s_{n+1} - 2, \qquad \sum_{i=0}^{s_n} f_{i+k} q_{n,i} \neq 0, \quad k = s_{n+1} - 1,$$

given in the previous section, are equivalent to the conditions

$$(Q_n(z), z^k) = 0, \quad k = 0, \dots, s_{n+1} - 2, \qquad (Q_n(z), z^k) \neq 0, \quad k = s_{n+1} - 1,$$

which, in turn, are equivalent to $Q_n \perp \mathrm{Pol}_{s_{n+1}-1}$ and to the nonorthogonality of Q_n to the space $\mathrm{Pol}_{s_{n+1}}$.

4.2. Algorithm for calculating the sequence of denominators of Padé fractions

Theorem 4. *The polynomial sequence Q_n defined above satisfies the recurrence relation*

$$Q_{n+1} = a_{n+1} Q_n + Q_{n-1}, \qquad \text{where} \quad \deg a_{n+1} = s_{n+1} - s_n.$$

The relation $\Lambda_{2s_n} = cQ_n$ holds; here c is a suitable constant. If we choose $Q_0 = 1$ and Q_1 equal to the denominator of the first convergent to the continued fraction

$$f(z) = \cfrac{1}{a_1(z) + \cfrac{1}{a_2(z) + \cfrac{1}{a_3(z) + \cdots}}},$$

then the sequence Q_n coincides with the sequence of denominators of the convergents to the continued fraction given above, while the sequence a_n coincides with the sequence of elements of this continued fraction.

We describe the algorithm and prove the theorem by induction. Assume that we have already calculated the polynomial Q_n from the given sequence $f_0, \dots, f_{2s_n-1}$. As noted above, it can thus be calculated uniquely up to a constant factor. Since this polynomial is of minimal degree among the polynomials generating the sequence $f_0, \dots, f_{2s_n-1}$ by means of the LFSR, it obviously follows that $\Lambda_{2s_n} = cQ_n$, where c is a suitable constant. Let us calculate

$$(Q_n(z), z^k) = \sum_{i=0}^{m} f_{i+k} q_{n,i}, \qquad m = s_n, \quad k = m, m+1, \dots,$$

until, for some k, we first obtain a nonzero element of the field F. After that, we find s_{n+1}, because we have $k = s_{n+1} - 1$ by the theory expounded above. Since the polynomial Q_n satisfies the conditions

$$\sum_{i=0}^{s_n} f_{i+k} q_{n,i} = 0, \qquad k = 0, \dots, s_{n+1} - 2,$$

it follows that the LFSR with feedback polynomial Q_n generates an arbitrary 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 obtain $d_{n+1} = s_{n+1} - s_n$.

The polynomial $Q_{n+1}(z)$ can be expressed as $a_{n+1}(z)Q_n(z) + Q_{n-1}(z)$, where $\deg a_{n+1} = d_{n+1}$. As pointed out above, it is defined up to a constant factor by the condition $Q_{n+1} \perp \mathrm{Pol}_{s_{n+1}}$. In fact, given $Q_n(z)$ and $Q_{n-1}(z)$, the polynomials a_{n+1}, Q_{n+1} are uniquely defined, because, otherwise, for different $a_{n+1} \neq b_{n+1}$, for nonzero constants $\lambda_1 \neq \lambda_2$, we have

$$\lambda_1\bigl(a_{n+1}(z)Q_n(z) + Q_{n-1}(z)\bigr) = \lambda_2\bigl(b_{n+1}(z)Q_n(z) + Q_{n-1}(z)\bigr);$$

hence

$$(\lambda_1 - \lambda_2)Q_{n-1}(z) = Q_n(z)(\lambda_2 b_{n+1} - \lambda_1 a_{n+1})$$

and, comparing the degrees, we arrive at a contradiction. Therefore, for fixed Q_0, Q_1, all the subsequent polynomials Q_n are uniquely defined.

Since, by the induction hypothesis, $Q_n \perp \mathrm{Pol}_{s_{n+1}-1}$, but Q_n is not orthogonal to $\mathrm{Pol}_{s_{n+1}}$, it follows that $(Q_n(z), z^{s_{n+1}-1}) = \Delta_{s_n+s_{n+1}-1} \neq 0$. For any polynomial a_{n+1} of degree d_{n+1} and $k \le s_n - 2$, we have

$$(a_{n+1}(z)Q_n(z) + Q_{n-1}(z), z^k) = (Q_n(z), a_{n+1}(z)z^k) + (Q_{n-1}(z), z^k) = 0,$$

because $a_{n+1}(z)z^k \in \mathrm{Pol}_{s_{n+1}-1}$, $z^k \in \mathrm{Pol}_{s_n-1}$, i.e., $a_{n+1}(z)Q_n(z) + Q_{n-1}(z) \perp \mathrm{Pol}_{s_n-1}$.

To choose a_{n+1} so that the polynomial $a_{n+1}(z)Q_n(z) + Q_{n-1}(z)$ is orthogonal to the space generated by the polynomials $z^{s_n-1}, \dots, z^{s_{n+1}-1}$, we must choose it so that the projections of the polynomials $a_{n+1}(z)Q_n(z)$ and $Q_{n-1}(z)$ on this space are opposite in sign, i.e., the following equalities are valid:

$$(a_{n+1}(z)Q_n(z), z^k) = -(Q_{n-1}(z), z^k), \qquad k = s_n - 1, \dots, s_{n+1} - 1.$$

These equalities for the coefficients of the polynomial a_{n+1} define a linear system of equations with triangular matrix which can be solved by the following iterative algorithm.

4.3. Algorithm for calculating the next polynomial Q_{n+1}

4.3.1. First step. At the first step, we construct the polynomial

$$Q_{n+1}^{(1)} = cz^{d_{n+1}}Q_n + Q_{n-1}\,, \qquad \deg Q_{n+1}^{(1)} = \deg Q_{n+1}\,, \quad Q_{n+1}^{(1)} \perp z^{s_n-1}.$$

To do this, we choose c so that the projections of $cz^{d_{n+1}}Q_n$ and Q_{n-1} on the vector z^{s_n-1} are opposite in sign, i.e.,

$$c(z^{d_{n+1}}Q_n\,, z^{s_n-1}) = -(z^{s_n-1}, Q_{n-1}).$$

Since

$$(z^{d_{n+1}}Q_n\,, z^{s_n-1}) = (Q_n\,, z^{d_{n+1}+s_n-1}) = (Q_n\,, z^{s_{n+1}-1}) \neq 0,$$

it follows that, for $k = s_{n+1} - 1$, given the sequence $f_0, \dots, f_{s_n+s_{n+1}-1}$, calculating the *residual*

$$\Delta_{s_n+s_{n+1}-1} = (Q_n(z)\,, z^k) = \sum_{i=0}^{s_n} f_{i+k}q_{n,i}$$

and the inner product

$$(Q_{n-1}(z)\,, z^{s_n-1}) = \sum_{i=0}^{s_{n-1}} f_{i+s_n-1}q_{n-1,i}$$

we can set $c = -(z^{s_n-1}, Q_{n-1})/\Delta_{s_n+s_{n+1}-1}$. Since $Q_{n+1}^{(1)} \perp \mathrm{Pol}_{s_n}$, the LFSR with this feedback polynomial generates the sequence $f_0, \dots, f_{s_n+s_{n+1}-1}$; hence $\Lambda_{s_n+s_{n+1}} = Q_{n+1}^{(1)}$.

4.3.2. Step with an arbitrary number. In the general case, at the ith step, we correct $Q_{n+1}^{(i-1)}$ if

$$\Delta_{s_n+s_{n+1}+i-2} = (Q_{n+1}^{(i-1)}, z^{s_n+i-2}) \neq 0,$$

and search for $Q_{n+1}^{(i)}$ as $Q_{n+1}^{(i-1)} + cQ_n z^{d_{n+1}-i+1}$ such that $Q_{n+1}^{(i)} \perp z^{s_n+i-2}$. To do this, we choose c so that the projections of $Q_{n+1}^{(i-1)}$ and $cQ_n z^{d_{n+1}-i+1}$ on the vector z^{s_n+i-2} are opposite in sign, i.e.,

$$\begin{aligned} -\Delta_{s_n+s_{n+1}+i-2} &= -(Q_{n+1}^{(i-1)}, z^{s_n+i-2}) = c(Q_n z^{d_{n+1}-i+1}, z^{s_n+i-2}) \\ &= c(Q_n\,, z^{s_n+d_{n+1}-1}) = c(Q_n\,, z^{s_{n+1}-1}) = c\Delta_{s_n+s_{n+1}-1}\,; \end{aligned}$$

hence $c = -\Delta_{s_n+s_{n+1}+i-2}/\Delta_{s_n+s_{n+1}-1}$. Note that, by the induction assumption, we must have $Q_{n+1}^{(i-1)} \perp z^{s_n+k}$ for $-1 \le k \le i-3$, because $Q_{n+1}^{(i-1)} \perp \mathrm{Pol}_{s_n+i-2}$; therefore,

$$(Q_{n+1}^{(i)}, z^{s_n+k}) = (Q_{n+1}^{(i-1)}, z^{s_n+k}) + (cQ_n z^{d_{n+1}-i+1}, z^{s_n+k}) = c(Q_n\,, z^{s_{n+1}+k+1-i}) = 0,$$

because $Q_n \perp \mathrm{Pol}_{s_{n+1}-2}$. Since $Q_{n+1}^{(i)} \perp \mathrm{Pol}_{s_n+i-1}$, it follows that the LFSR with this feedback polynomial generates the sequence $f_0, \dots, f_{s_n+s_{n+1}+i-2}$; hence $\Lambda_{s_n+s_{n+1}+i-2} = Q_{n+1}^{(i)}$. Next, given the sequence $f_0, \dots, f_{s_n+s_{n+1}+i-1}$, we obtain the residual

$$\Delta_{s_n+s_{n+1}+i-1} = (Q_{n+1}^{(i)}, z^{s_n+1}) = \sum_{i=0}^{s_{n+1}} f_{i+s_n+i-1}q_{n+1,i}$$

and take the $(i+1)$th step.

4.3.3. Termination of the operation of the algorithm. At the end of the operation of the algorithm at the $(d_{n+1}+1)$th step, we obtain the polynomial

$$Q_{n+1}^{(d_{n+1}+1)} = Q_n a_{n+1} + Q_{n-1}, \qquad \deg Q_{n+1}^{(d_{n+1}+1)} = s_{n+1},$$
$$Q_{n+1}^{(d_{n+1}+1)} \perp \mathrm{Pol}_{s_n+d_{n+1}} = \mathrm{Pol}_{s_{n+1}}.$$

By the foregoing, it coincides with the polynomial Q_{n+1}. Since the LFSR with this feedback polynomial generates the sequence $f_0, \dots, f_{2s_{n+1}-1}$, it follows that $\Lambda_{2s_{n+1}}$ coincides with cQ_{n+1}.

The complexity of the algorithm can be estimated by

$$\Big(3-\frac{1}{n}\Big)s_n^2 + 3\big((n-1)s_{n-1} + d_n - d_1\big) + 5(n-1) - 2d_1^2 < \Big(3-\frac{1}{n}\Big)s_n^2 + 3ns_n.$$

4.3.4. Comparison with Euclid's algorithm. If the finite Laurent series $f_0/z + \dots + f_{k-1}/z^k$ is written as the fraction $f(z)/z^k$, where $f(z) = f_0 z^{k-1} + \dots + f_{k-1}$, then it can be expanded in a continued fraction, using the ordinary Euclid algorithm, which, obviously, can also be applied to an arbitrary fraction $f(z)/g(z)$. But, in that case, the convergents to this continued fraction will not be calculated. To calculate them, one can apply the *extended Euclid algorithm* in which the numerators and the denominators of the convergents appear as *Bezout coefficients* in the linear representations $q_i = u_i f + v_i g$ of the intermediate polynomials q_i calculated in the ordinary Euclid algorithm

$$(f, g) = (g, q_1) = (q_1, q_2) = \cdots.$$

Although the extended Euclid algorithm and the interpretation (given above) of the BMA are equivalent in the sense that they both calculate the sequences of denominators Q_n of the convergents and the elements a_n of the continued fraction, the order of calculations in them is different. For example, to calculate the polynomials $a_0, a_1, \dots$ with small indices in the BMA, only the initial segment of the given sequence $f_0, f_1, \dots$ is required, while, in Euclid's algorithm, one must know the *whole sequence* $f_0, \dots, f_{k-1}$.

5. APPLICATION OF THE BMA TO THE EXPANSION OF THE EXPONENTIAL IN A CONTINUED FRACTION

Let us apply the BMA to the sequence $f_n = 1/(n+1)!$, $n = 0, 1, \dots$, over the field of rational numbers. Then the function $f(z) = f_0 + f_1/z + f_2/z^2 + \cdots$ coincides with $e^{1/z} - 1$ and the first element of its continued fraction is equal to $a_1(z) = [f^{-1}] = z - 1/2$. If we set $Q_0 = 1$, $Q_1 = z - 1/2$, then the algorithm calculates all the elements a_n of the continued fraction and all the denominators Q_n of the convergent by the recurrence formula $Q_{n+1} = a_{n+1}Q_n + Q_{n-1}$. However, it is convenient to choose $Q_1 = 2z - 1$; then also $(Q_1, 1) = 0$. By the induction assumption, assume that $s_m = m$,

$$Q_m = \sum_{k=0}^{m} (-1)^{m-k} \frac{(m+k)!}{k!(m-k)!} z^k = \sum_{k=0}^{m} q_{m,k} z^k, \qquad m \le n, \quad Q_m \perp \mathrm{Pol}_{s_{m+1}-1} = \mathrm{Pol}_m.$$

At the first step, we construct the polynomial

$$Q_{n+1}^{(1)} = cz^{d_{n+1}} Q_n + Q_{n-1}, \qquad Q_{n+1}^{(1)} \perp z^{s_n - 1} = z^{n-1}.$$

To this end, we choose $c = -(z^{s_n-1}, Q_{n-1})/\Delta_{s_n+s_{n+1}-1}$, where

$$\Delta_{s_n+s_{n+1}-1} = (Q_n(z), z^k) = \sum_{i=0}^{s_n} f_{i+k} q_{n,i} \neq 0, \qquad k = s_{n+1} - 1,$$
$$\Delta_{s_n+s_{n+1}-2} = (Q_n(z), z^k) = \sum_{i=0}^{s_n} f_{i+k} q_{n,i} = 0, \qquad k = s_{n+1} - 2.$$

Since $Q_n \perp \mathrm{Pol}_n$, it follows that $(Q_n(z), z^{n-1}) = 0$. Therefore, to prove the equality $s_{n+1} = n+1$, it suffices to verify that

$$\Delta_{2n} = (Q_n(z), z^n) = \sum_{i=0}^{n} f_{i+n} q_{n,i} \neq 0.$$

Since

$$\begin{aligned}\sum_{i=0}^{n} f_{i+n} q_{n,i} &= \sum_{i=0}^{n} (-1)^{n-i} \frac{(n+i)!}{(n+i+1)!\, i!(n-i)!} = \sum_{i=0}^{n} (-1)^{n-i} \frac{1}{(n+i+1)\, i!(n-i)!} \\ &= \frac{1}{n!} \sum_{i=0}^{n} (-1)^{n-i} \frac{\binom{n}{i}}{n+i+1} = \frac{1}{n!} \Delta^n \Big(\frac{1}{x}\Big)\Big|_{x=n+1},\end{aligned}$$

where

$$\Delta^n(f(x)) = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} f(x+i), \qquad \Delta^n(f(x)) = \Delta\big(\Delta^{n-1}(f(x))\big)$$

is the nth difference operator, it follows from the well-known identity [14, Sec. 5.3] (which can easily be verified by induction)

$$\frac{1}{n!} \Delta^n \Big(\frac{1}{x}\Big) = \frac{(-1)^n}{x(x+1)\cdots(x+n)}$$

that

$$\Delta_{2n} = \sum_{i=0}^{n} f_{i+n} q_{n,i} = \frac{(-1)^n}{(n+1)\cdots(2n)(2n+1)}.$$

Therefore,

$$c = -\frac{(z^{s_n - 1}, Q_{n-1})}{\Delta_{s_n + s_{n+1} - 1}} = -\frac{(z^{n-1}, Q_{n-1})}{\Delta_{2n}} = -\frac{\Delta_{2n-2}}{\Delta_{2n}} = \frac{2n(2n+1)}{n} = 2(2n+1).$$

Further, let us calculate $d_{n+1} = s_{n+1} - s_n = 1$,

$$\begin{aligned}\Delta_{2n+1} = \Delta_{s_n + s_{n+1}} &= (Q_{n+1}^{(1)}, z^{s_n}) = (Q_{n+1}^{(1)}, z^n) = (czQ_n + Q_{n-1}, z^n) \\ &= c(Q_n, z^{n+1}) + (Q_{n-1}, z^n) = 2(2n+1)(Q_n, z^{n+1}) + (Q_{n-1}, z^n)\end{aligned}$$

using the fact that

$$\begin{aligned}(Q_{n-1}, z^n) &= \sum_{i=0}^{n-1} f_{i+n} q_{n-1,i} = \sum_{i=0}^{n-1} (-1)^{n-1-i} \frac{(n+i-1)!}{(n+i+1)!\, i!(n-1-i)!} \\ &= \frac{1}{(n-1)!} \sum_{i=0}^{n-1} (-1)^{n-1-i} \frac{\binom{n-1}{i}}{(n+i+1)(n+i)} \\ &= \frac{1}{(n-1)!} \Delta^{n-1} \Big(\frac{1}{x(x+1)}\Big)\Big|_{x=n} = \frac{1}{(n-1)!} \Delta^{n-1} \Big(-\Delta\Big(\frac{1}{x}\Big)\Big)\Big|_{x=n} \\ &= -\frac{1}{(n-1)!} \Delta^n \Big(\frac{1}{x}\Big)\Big|_{x=n} = -\frac{n(-1)^n}{x(x+1)\cdots(x+n)}\Big|_{x=n} = \frac{(-1)^{n-1}}{(n+1)\cdots 2n};\end{aligned}$$

this yields

$$(Q_n, z^{n+1}) = \frac{(-1)^n}{(n+2)\cdots(2n+2)},$$

and hence

$$\begin{aligned}\Delta_{s_n+s_{n+1}} &= \Delta_{2n+1} = 2(2n+1)(Q_n, z^{n+1}) + (Q_{n-1}, z^n)\\ &= \frac{(-1)^n 2(2n+1)}{(n+2)\cdots(2n+2)} + \frac{(-1)^{n-1}}{(n+1)\cdots 2n} = 0.\end{aligned}$$

Therefore, it is not necessary to correct $Q_{n+1}^{(1)}$ and we immediately have

$$Q_{n+1}(z) = Q_{n+1}^{(1)}(z) = a_{n+1}(z)Q_n(z) + Q_{n-1}(z), \qquad a_{n+1}(z) = 2(2n+1)z.$$

It remains to to verify that

$$\begin{aligned}Q_{n+1}(z) &= a_{n+1}(z)Q_n(z) + Q_{n-1}(z) = 2(2n+1)zQ_n(z) + Q_{n-1}(z)\\ &= \sum_{k=0}^{n+1}(-1)^{n+1-k}\frac{(n+1+k)!}{k!(n+1-k)!}z^k.\end{aligned}$$

To do this, it suffices to verify that

$$\begin{aligned}&(-1)^{n-(k-1)}2(2n+1)\frac{(n+k-1)!}{(k-1)!(n-(k-1))!} + (-1)^{n-1-k}\frac{(n-1+k)!}{k!(n-1-k)!}\\ &\quad= (-1)^{n-1-k}\frac{(n+k-1)!((n-k)(n-k+1)+2(2n+1)k)}{k!(n+1-k)!}\\ &\quad= (-1)^{n+1-k}\frac{(n+k+1)!}{k!(n+1-k)!},\end{aligned}$$

because

$$(n-k)(n-k+1) + 2(2n+1)k = (n+k+1)(n+k).$$

If the algorithm is initiated by the values of $Q_0 = 1$, $Q_1 = z - 1/2$, then, repeating the calculations already carried out, we can easily see that, for an even n, Q_n does not change and a_n is divisible by 2, while, for an odd n, Q_n is divisible by 2 and a_n is multiplied by 2. Since $Q_0 = 1$ and the Q_1 coincide with the denominators of the convergents to the continued fraction for $f(z)$, it follows that, as noted above, the resulting polynomial Q_n coincides for any n with the denominator of the nth convergent and the sequence $a_n(z) = 2^{(-1)^{n+1}}2(2n+1)z$ for $n > 1$ coincides with the sequence of elements of the continued fraction for $f(z) = e^{1/z} - 1$. Hence we have the following regular continued fraction for $e^{1/z}$:

$$e^{1/z} = 1 + \cfrac{1}{z - 1/2 + \cfrac{1}{12z + \cfrac{1}{5z + \cfrac{1}{28z + \cdots}}}},$$

which, on making the change of variable $x = 1/z$, becomes the Euler continued fraction for e^x. Returning to the continued fraction for $f(z) = e^{1/z} - 1$, we note, following [11], that to find explicit expressions for the numerators of its convergents P_n/Q_n or, equivalently, for the diagonal Padé approximations, we can use the relation for the Padé approximations

$$f(z)Q_n(z) = P_n(z) + \frac{c}{z^{n+1}} + \cdots, \qquad c \in F, \quad \deg P_n < \deg Q_n = n,$$

and note that $P_n(z) = (-1)^n Q_n(-z) - Q_n(z)$. Indeed, multiplying both sides of the equality

$$e^{1/z} Q_n(z) = (P_n + Q_n)(z) + \frac{c}{z^{n+1}} + \cdots$$

by $e^{-1/z}$, we find that

$$Q_n(z) = (P_n + Q_n)(z) e^{-1/z} + \frac{c}{z^{n+1}} + \cdots ;$$

hence, after the substitution $x = -z$, we obtain the relation

$$-P_n(-x) = (P_n + Q_n)(-x)(e^{1/x} - 1) + \frac{c(-1)^{n+1}}{x^{n+1}} + \cdots , \qquad \deg Q_n + P_n = n > \deg P_n ,$$

from which, by the definition of Padé approximations, we have

$$(P_n + Q_n)(-x) = (-1)^n Q_n(x).$$

Further, note that, after the polynomials $Q_n(z)$ have been guessed, to prove that they are the denominators of the Padé approximations, it suffices to verify that $s_n = n$, $Q_n \perp \mathrm{Pol}_n$, i.e., $(Q_n(z), z^k) = 0$, $k < n$. But this readily follows from the relations

$$\Delta_{2n} = (Q_n(z), z^n) = \sum_{i=0}^{n} f_{i+n} q_{n,i} \neq 0,$$

$$\begin{aligned} (Q_n(z), z^k) &= \sum_{i=0}^{n} f_{i+k} q_{n,i} = \sum_{i=0}^{n} (-1)^{n-i} \frac{(n+i)!}{(k+i+1)!\, i!(n-i)!} \\ &= \frac{1}{n!} \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} (n+i) \cdots (k+i+1) = \frac{1}{n!} \Delta^n \big((x+n) \cdots (x+k+2)\big)\Big|_{x=0} = 0, \end{aligned}$$

because the polynomial $(x+n) \cdots (x+k+2)$ is of degree $n - k - 1 < n$ and, after applying the difference operator Δ n times, it becomes zero.

ACKNOWLEDGMENTS

This research was supported by the Russian Foundation for Basic Research under grant no. 05-01-00994, by the program "Leading Scientific Schools" under grant no. NSh-1807.2003.1, and by the program "Universities of Russia" under grant no. UR.04.02.528.

REFERENCES

1. D. Jungnickel, *Finite Fields: Structure and Arithmetic*, Wissenschaftsverlag, Mannheim–Leipzig–Wien, 1993.
2. R. Blahut, *Theory and Practice of Error Control Codes*, Addison–Wesley, Reading, MA, 1983; Russian translation: Mir, Moscow, 1986.
3. J. L. Massey, "Feedback Shift Register Synthesis and BCH decoding," *IEEE Trans. Inform. Theory*, **IT-15** (1969), 122–128.
4. E. R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, New York, 1968; Russian translation: Mir, Moscow, 1972.
5. J. L. Dornstetter, "On the equivalence between Berlekamp's and Euclid's algorithms," *IEEE Trans. Inform. Theory*, **IT-33** (1987), no. 3, 428–431.

6. Y. Sugiyama, M. Kasahara, S. Hirasawa, and T. Namekawa, "A method for solving key equation for decoding Goppa codes," *Inform. Control*, **27** (1975), no. 1, 87–99.
7. L. R. Welch and R. A. Scholtz, "Continued fractions and Berlekamp's algorithm," *IEEE Trans. Inform. Theory*, **IT-25** (1979), no. 1, 18–27.
8. U. Cheng, "On the continued fractions and Berlekamp's algorithm," *IEEE Trans. Inform. Theory*, **IT-30** (1984), no. 3, 541–544.
9. W. H. Mills, "Continued fractions and linear recurrence," *Math. Comp.*, **29** (1975), 173–180.
10. Zongduo Dai and Kencheng Zeng, "Continued fractions and Berlekamp–Massey algorithm," in: *Advances in Cryptology—Auscript-90*, Springer-Verlag, Berlin, 1990, pp. 24–31.
11. E. M. Nikishin and V. N. Sorokin, *Rational Approximations and Orthogonality* [in Russian] Nauka, Moscow, 1988.
12. G. Szegö, *Orthogonal Polynomials*, Colloquium Publ., vol. XXIII, Amer. Math. Soc., Providence, RI, 1959; Russian translation, Fizmatgiz, Moscow, 1962.
13. V. M. Sidel′nikov, "Decoding of the Reed–Solomon codes with the number of errors greater than $(d-1)/2$ and zeros of polynomials of several variables," *Problemy Peredachi Informatsii* [*Problems Inform. Transmission*], **30** (1994), no. 1, 51–69.
14. R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics*, Addison-Wesley, Reading, MA, 1994; Russian translation: Mir, Moscow, 1998.

(S. B. Gashkov) M. V. Lomonosov Moscow State University
E-mail: gashkov@lsili.ru
(I. B. Gashkov)) Karlstads Universitet, Sweden
E-mail: Igor.Gachkov@kau.se