Математические заметки

том 79 выпуск 1 январь 2006

УДК 517.51

АЛГОРИТМ БЕРЛЕКЕМПА–МЕССИ, ЦЕПНЫЕ ДРОБИ, АППРОКСИМАЦИИ ПАДЕ И ОРТОГОНАЛЬНЫЕ МНОГОЧЛЕНЫ

С. Б. Гашков, И. Б. Гашков

Алгоритм Берлекемпа–Месси (далее BMA) интерпретируется как алгоритм построения аппроксимаций Паде к ряду Лорана над произвольным полем с особенностью в бесконечности. Показано, что BMA является итеративной процедурой построения последовательности многочленов, каждый из которых ортогонален соответствующему пространству многочленов относительно скалярного произведения, определяемого по данному ряду. Дано применение BMA для разложения экспоненты в непрерывную дробь и вычисления ее аппроксимаций Паде.

Библиография: 14 названий.

1. Введение

Пусть дана последовательность $f_0, \dots, f_{n-1}, \dots$ элементов произвольного поля F. Известно (см. [1], [2]), что данная последовательность генерируется линейной сдвиговой схемой с обратными связями (LFSR), если она задается начальными условиями $f_0, \dots, f_{m-1}$ и линейными рекуррентными соотношениями

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

где $Q(x) = q_m x^m + q_{m-1} x^{m-1} + \cdots + q_0$, $q_m = 1$, есть многочлен обратной связи данной LFSR. Это определение отличается от стандартного тем, что многочлен обратных связей заменен возвратным к нему многочленом.

В случае поля $GF(2)$ LFSR с многочленом обратной связи $Q(x)$ есть линейный автомат, состоящий из $m+1$ регистра, в котором выход i-го регистра умножается на коэффициент q_i; все эти отводы суммируются по модулю 2 и результат подается на вход первого регистра (см. [2]).

Обозначим $L_n(f)$ наименьшую степень многочлена Λ_n, генерирующего последовательность $f_0, \dots, f_{n-1}$. Она называется (см. [1]) *линейной сложностью* последовательности $f_0, \dots, f_{n-1}$, а последовательность $\{L_n(f)\}$ называется *профилем линейной сложности* последовательности $\{f_n\}$. Месси [3] дал интерпретацию алгоритма Берлекемпа [4] как алгоритма для вычисления линейной сложности последовательности

Работа выполнена при поддержке Российского фонда фундаментальных исследований, грант № 05-01-00994, программы "Ведущие научные школы", грант № НШ-1807.2003.1, и программы "Университеты России", грант № УР.04.02.528.

$f_0, \dots, f_{n-1}$ и генерирующей ее LFSR с многочленом обратной связи минимальной степени (см. также [1], [2]).

ВМА имеет разнообразные приложения [1]–[4]. Известно [5], что ВМА в определенном смысле эквивалентен варианту алгоритма Евклида, предложенному в [6] для декодирования кодов БЧХ (см. [2]). Во многих работах исследовалась связь между ВМА и непрерывными дробями [7]–[10].

Мы предлагаем здесь интерпретацию ВМА с точки зрения теории аппроксимаций Паде и ортогональных многочленов.

2. Ряды Лорана, аппроксимации Паде и цепные дроби

Выражение вида $z^n(c_0 + c_1/z + c_2/z^2 + \cdots)$, $c_0 \neq 0$, при любом целом n, где коэффициенты $c_i \in F$, называется *формальным рядом Лорана*. На множестве $F((1/z))$ всех рядов Лорана стандартным образом определяются операции сложения и умножения, относительно которых оно образует поле (см. [11]). Далее будем рассматривать только ряды Лорана с нулевой целой частью, т.е. ряды вида $f(z) = f_0/z + f_1/z^2 + \cdots$. Такие ряды можно (см. [11]) разложить в цепную дробь

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

Дробь, образованная первыми n этажами цепной дроби для $f(z)$, называется *n-й подходящей дробью* и обозначается τ_n.

Легко проверить, что для произвольного такого ряда последовательность его коэффициентов удовлетворяет линейным рекуррентным соотношениям

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

тогда и только тогда, когда

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

Условие (2) равносильно условию

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

Поэтому LFSR с многочленом обратной связи $Q(z)$ генерирует последовательность $f_0, \dots, f_{L-1}$ тогда и только тогда, когда выполнено (2) (или (3)) при $n = L - \deg Q$.

Известно [11], что для любого n найдется удовлетворяющая этому условию правильная дробь P_n/G_n степени не выше n. Известно также [11], что все такие дроби определены однозначно с точностью до общего множителя у числителя и знаменателя, который можно сократить. Та из них, которая является несократимой, называется n-й

(диагональной) *аппроксимацией Паде* π_n ряда f. Ее числитель P_n и знаменатель G_n образуют *n-ю пару Паде*. Эти многочлены определены однозначно с точностью до постоянного множителя.

Дроби P/Q *произвольной* степени, удовлетворяющие условию (2) определены *неоднозначно*. Если $\pi_n = P_n/G_n$ и многочлен $Q = G_n$ есть многочлен наименьшей степени $m \leqslant n$, удовлетворяющий условию

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

то выполняются соотношения (1). Поэтому, если степень дроби π_n обозначить Π_n и выбрать многочлен той же степени G_n так, что $\pi_n = P_n/G_n$, то LFSR с многочленом обратных связей G_n и начальным состоянием регистров $f_0, \ldots, f_{\Pi_n - 1}$ будет генерировать последовательность $f_0, \ldots, f_{\Pi_n + n - 1}$, откуда имеем $L_{\Pi_n + n} \leqslant \Pi_n$. Легко проверить, что $L_{\Pi_n + n} = \Pi_n$.

Если степень знаменателя в n-й паре Паде равна n, т.е. пары Паде определены однозначно с точностью до постоянного множителя, то индекс n называется *нормальным*. Известно [11], что если $n_0 < n_1$ есть соседние нормальные индексы, то

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

т.е. точный порядок касания $\pi_{n_0}(z)$ ряда $f(z)$ равен $n_0 + n_1$, и все π_k при $n_1 > k > n_0$ равны π_{n_0}. Отсюда следует, что при $n_1 > k \geqslant n_0$

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

при некотором b_k, возможно нулевом. Поэтому справедлива

Лемма 1. *При $n_0 \leqslant k < n_1$ верны равенства*

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

Докажем следующее утверждение.

Теорема 1. *Профиль линейной сложности и последовательность нормальных индексов s_n, $n = 1, 2, \ldots$, связаны соотношениями*

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

Доказательство. Известно [11], что последовательность нормальных индексов совпадает с последовательностью степеней знаменателей подходящих дробей $s_0, s_1, s_2, \ldots$ и

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

т.е. аппроксимация Паде $\pi_{s_n} = \tau_n = P_n/Q_n$. Из леммы 1 следует, что при $s_n \leqslant k < s_{n+1}$ имеем $\pi_k = \tau_n$, $G_k = Q_n$; значит,

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

где $Q_n(z) = q_{n,s_n}z^{s_n} + \cdots + q_{n,0}$. Другими словами, LFSR с многочленом $Q_n(z)$ генерирует последовательность $\{f_0, \ldots, f_m\}$ при $m = s_n + s_{n+1} - 2$, но не генерирует ее при $m = s_n + s_{n+1} - 1$. Так как при $s_{n+1} > k \geqslant s_n$ имеем $s_n = L_{k+s_n}$, то для любой последовательности $\{f_0, \ldots, f_{s_n+k}\}$, $k = s_n - 1, \ldots, s_{n+1} - 2$, ее минимальная LFSR имеет многочлен обратной связи, равный Q_n. Из определения нормального индекса следует единственность с точностью до постоянного множителя многочлена $G_{s_n} = Q_n$ степени s_n такого, что для некоторой правильной дроби

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

Отсюда следует, что существует единственная LFSR сложности s_n, генерирующая последовательность $\{f_0, \ldots, f_{2s_n-1}\}$ и ее многочлен обратных связей равен с точностью до постоянного множителя многочлену Q_n. Она генерирует все последовательности $\{f_0, \ldots, f_{s_n+k}\}$, $k = s_n, \ldots, s_{n+1} - 2$. В частности, $L_{k+s_n} = s_n$, $k = s_n, \ldots, s_{n+1} - 1$. Верхние оценки теоремы следуют из доказанного выше равенства.

Нижние оценки докажем от противного. Допустим, что при некотором k, $s_n + s_{n-1} \leqslant k < 2s_n$, справедливо неравенство $L_k < s_n$. Тогда для некоторых многочленов P, Q справедливо условие (2) при $n = k - \deg Q$, $\deg Q < s_n$. Из равенства (4) при $m = n - 1$ следует, что

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

Умножая первое из равенств на Q_{n-1}, второе на Q и вычитая из первого второе, имеем

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

так как $d \neq 0$ и $s_n - \deg Q < k + 1 - s_{n-1} - \deg Q$. Слева стоит многочлен, а справа ненулевой ряд Лорана, поэтому получается противоречие. Теорема доказана.

Объединяя доказанные выше равенства, видим, что $L_k = s_n$ при $s_{n-1} + s_n \leqslant k < s_{n+1} + s_n$.

Стандартное доказательство корректности BMA использует следующую теорему [1], [2].

Теорема 2. *Для любого k верно следующее: или $L_{k+1}(f) = L_k(f)$, причем f_k есть очередной выход* LFSR *сложности $L_k(f)$, генерирующей последовательность $f_0, \ldots, f_{k-1}$, или $L_{k+1}(f) = \max\{L_k(f), k + 1 - L_k(f)\}$.*

Доказательство легко следует из равенств $L_k = s_n$, $s_{n-1} + s_n \leqslant k < s_{n+1} + s_n$. Действительно, достаточно проверить, что при $k = s_{n+1} + s_n - 1$ имеем

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

при $s_{n-1} + s_n \leqslant k < 2s_n$ имеем

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

и при $2s_n \leqslant k < s_n + s_{n+1}$ для любой последовательности $\{f_0, \ldots, f_{k-1}\}$ минимальная генерирующая ее LFSR имеет многочлен обратной связи, равный Q_n.

3. Алгоритм BMA

Мы покажем, что BMA вычисляет одновременно и элементы $a_n(z)$ цепной дроби в случае произвольного ряда $f(z)$ и последовательность $Q_n = a_n Q_{n-1} + Q_{n-2}, Q_1 = a_1$, $Q_0 = 1$, знаменателей ее подходящих дробей (они же дроби Паде). Также он вычисляет последовательность многочленов обратных связей Λ_n, генерирующих первые n членов последовательности $f_0, \dots, f_{n-1}, \dots$.

Приведем стандартное описание работы BMA (см. [2]). По предположению индукции для $i \leqslant k$ существует LFSR с многочленом Λ_i, порождающая последовательность $f_0, \dots, f_{i-1}$, и такая, что если $i < k$ и $f_i \neq f_{i+1}$, то $L_{i+1}(f) = \max\{L_i(f), i+1-L_i(f)\}$, а в противном случае $\Lambda_{i+1} = \Lambda_i$. База индукции обосновывается равенствами $i = 1$, $L_0(f) = 0, \Lambda_1(x) = 1 + x$.

Пусть m – наибольший индекс такой, что $L_m(f) < L_{m+1}(f)$; тогда положим $s = L_{m+1}(f), r = L_m(f)$. Из соотношений $s = L_k(f) = \cdots = L_{m+1}(f) > L_m(f) = r$ по предположению индукции следует, что $s = \max(r, m+1-r) = m+1-r$, так как, если бы $s = r$, то $L_{m+1}(f) = L_m(f)$, что невозможно. Пусть многочлен

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

тогда по определению

$$\sum_{i=1}^{s} c^{(k)}_i f_{j-i} = \begin{cases} f_j & \text{при } j = s, \dots, k-1, \\ a_k & \text{при } j = k \end{cases}$$

и, аналогично,

$$\sum_{i=1}^{r} c^{(m)}_i f_{j-i} = \begin{cases} f_j & \text{при } j = r, \dots, m-1, \\ t_m & \text{при } j = m \end{cases}$$

при некотором $t_m \neq a_m$, так как $f_{m+1} \neq f_m$ в силу выбора m. Положив $\mu_m = t_m - a_m \neq 0$, согласно BMA определим многочлен

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

степени

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

Он генерирует последовательность $f_0, \dots, f_k$.

Описание BMA закончено, но в нем предполагалось, что LFSR генерирует последовательность, определяемую линейными рекуррентными соотношениями

$$f_k q^*_0 + f_{k-1} q^*_1 + \cdots + f^*_{k-m} q_m = 0, \qquad k = m, m+1, \dots,$$

где $Q^*(x) = q^*_m x^m + q^*_{m-1} x^{m-1} + \cdots + q^*_0$, $q^*_m = 1$, – многочлен обратной связи данной LFSR. Мы использовали *другое определение* многочлена обратных связей

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

в котором последовательность, генерируемая LFSR, удовлетворяет линейным рекуррентными соотношениям $f_k q_0 + f_{k+1} q_1 + \cdots + f_{k+m} q_m = 0$, $k = 0, 1, 2, \ldots$. Связь между обоими способами определения многочлена обратных связей дается равенствами $q_i^* = q_{m-i}$, $i = 0, \ldots, m$, которые означают, что многочлены Q, Q^* взаимно возвратны, т.е. $Q(x) = x^m Q^*(1/x)$.

Пусть далее $\{s_n\}$ это последовательность нормальных индексов и мы не требуем, чтобы старший коэффициент у многочленов Λ_i был равен 1. Тогда справедлива

Теорема 3. *При* $k = s_{n+1} + s_n - 1$

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

при $k = s_n + s_{n-1}, \ldots, 2s_n - 1$

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

а при $k = 2s_n, \ldots, s_n + s_{n+1} - 2$ *имеем*

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

Доказательство. Равенство $\Lambda_{k+1}^*(x) = \Lambda_k^*(x) + b_k \mu_m^{-1} x^{k-m} \Lambda_m^*(x)$, определяющее шаг BMA, можно переписать, пользуясь возвратными многочленами:

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

Согласно доказанному выше при $s = L_k(f) = \cdots = L_{m+1}(f) > L_m(f) = r$ имеем $s = m+1-r$, $L_m(f)+k-m = r+k-m = (k+1)-(m+1-r) = k+1-s = k+1-L_k(f)$. Отсюда при $\Lambda_{k+1} \neq \Lambda_k$ следует, что $L_{k+1}(f) = k + 1 - L_k(f) = L_m(f) + k - m$, $L_{k+1}(f) - L_m(f) - k + m = 0$. При $k = s_{n+1} + s_n - 1$ очевидно, что $L_{k+1} = s_{n+1}$, $L_k = s_n$, $L_{k+1} - L_k = s_{n+1} - s_n = d_{n+1}$, $m = s_n + s_{n-1} - 1$, $L_m = s_{n-1}$, $\Lambda_m = Q_{n-1}$, поэтому

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

Так как согласно ранее доказанному при $k = s_n + s_{n-1}, \ldots, s_{n+1} + s_n - 2$ имеем

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

то при $k = s_n + s_{n-1}, \ldots, 2s_n - 1$ имеем

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

Последовательность Λ_k можно определять с точностью до постоянного множителя, поэтому первые два равенства теоремы доказаны. Ранее было доказано, что LFSR с многочленом обратной связи cQ_n генерирует любую последовательность $f_0, \ldots, f_k$, где $k = 2s_n, \ldots, s_n + s_{n+1} - 1$. Значит, при $k = 2s_n, \ldots, s_n + s_{n+1} - 2$ имеем $\Lambda_{k+1} = \Lambda_k$.

4. Интерпретация ВМА в терминах ортогональных многочленов

Выше был описан фрагмент теории аппроксимаций Паде для рядов Лорана над произвольным полем. Далее классическая теория (см. [11], [12]) развивается для поля комплексных чисел в тесной связи с теорией ортогональных многочленов. В частности, в ней доказывается, что для так называемых позитивных последовательностей f_n последовательность нормальных индексов $s_n = n$ и даются явные формулы вида

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

Использующий эти соображения подход к декодированию кодов BCH был развит в [13].

В общем случае надо рассуждать другим способом, который естественным путем приводит к алгоритму, эквивалентному ВМА. Оставшаяся часть статьи *не предполагает знакомства с* ВМА и может быть использована для его альтернативного описания и обоснования.

Обозначим Pol_n n-мерное пространство многочленов степени меньше n над рассматриваемым полем F. Для данной последовательности $\{f_0, \ldots, f_{n-1}\}$ над полем F определим на пространстве Pol_n линейный функционал $l_f(P)$ равенством

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

Определим на пространстве Pol_n скалярное произведение $(P, Q) = (P, Q)_f$ многочленов P, Q равенством $(P, Q) = l_f(PQ)$. Так определенное скалярное произведение обладает свойствами билинейности и симметричности. Кроме того, очевидно справедливо тождество $(P, Q) = (PQ, 1)$.

4.1. Описание последовательности знаменателей дробей Паде в терминах ортогональности пространствам Pol_n. Следуя [11], перепишем равенства

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

в виде

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

где $Q(z) = q_m z^m + q_{m-1} z^{m-1} + \cdots + q_0$, $q_m = 1$, и через (P, Q) обозначается скалярное произведение многочленов P, Q. Ортогональность векторов (и вектора подпространству) обозначаем символом $\perp$.

Поэтому система равенств $(Q_n(z), z^k) = 0$, $k = 0, \ldots, s_n - 1$, равносильна $Q_n(z) \perp \mathrm{Pol}_{s_n}$. Так как $\deg G_n = s_n > s_{n-1} = \deg G_{n-1}$, отсюда следует, что $Q_n \perp Q_{n-1}$.

Более того, многочлен $Q_n(z) = q_{n,s_n} z^{s_n} + \cdots + q_{n,0}$ определяется однозначно с точностью до постоянного множителя указанным выше условием ортогональности, а указанные в предыдущей секции условия

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

равносильны условиям $(Q_n(z), z^k) = 0$, $k = 0, \ldots, s_{n+1} - 2$, $(Q_n(z), z^k) \neq 0$, $k = s_{n+1} - 1$, которые равносильны $Q_n \perp \mathrm{Pol}_{s_{n+1}-1}$ и неортогональности Q_n пространству $\mathrm{Pol}_{s_{n+1}}$.

4.2. Алгоритм вычисления последовательности знаменателей дробей Паде.

Теорема 4. *Полиномиальная последовательность Q_n удовлетворяет рекуррентному соотношению $Q_{n+1} = a_{n+1}Q_n + Q_{n-1}$, где $\deg a_{n+1} = s_{n+1} - s_n$. Справедливо равенство $\Lambda_{2s_n} = cQ_n$, где c – подходящая константа. Если выбрать $Q_0 = 1$ и Q_1 равным знаменателю первой подходящей дроби для цепной дроби*

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

то последовательность Q_n совпадает с последовательностью знаменателей подходящих дробей для указанной цепной дроби, а последовательность a_n совпадает с последовательностью элементов этой цепной дроби.

Описание алгоритма и доказательство теоремы выполним индуктивно. Допустим, что мы уже вычислили многочлен Q_n по данной последовательности $f_0, \ldots, f_{2s_n-1}$. Как отмечалось выше, по ней он вычисляется однозначно с точностью до постоянного множителя. Так как этот многочлен имеет минимальную степень среди многочленов, генерирующих с помощью LFSR последовательность $f_0, \ldots, f_{2s_n-1}$, очевидно, $\Lambda_{2s_n} = cQ_n$, где c – подходящая константа. Вычисляем

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

до тех пор, пока при некотором k не получим впервые отличный от нуля элемент поля F. Потом находим s_{n+1}, так как согласно описанной выше теории это $k = s_{n+1} - 1$. Так как многочлен Q_n удовлетворяет условиям

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

то LFSR с многочленом обратной связи Q_n генерирует любую последовательность f_0, $\ldots, f_k$, где $k = 2s_n, \ldots, s_n + s_{n+1} - 2$. Поэтому имеем $\Lambda_k = Q_n$, $k = 2s_n, \ldots,$ $s_n + s_{n+1} - 1$. Далее находим $d_{n+1} = s_{n+1} - s_n$.

Многочлен $Q_{n+1}(z)$ представляется в виде $a_{n+1}(z)Q_n(z) + Q_{n-1}(z)$, где $\deg a_{n+1} = d_{n+1}$. Согласно сказанному выше он определяется с точностью до постоянного множителя условием $Q_{n+1} \perp \mathrm{Pol}_{s_{n+1}}$. На самом деле при данных $Q_n(z), Q_{n-1}(z)$ многочлены a_{n+1}, Q_{n+1} определяются однозначно, так как в противном случае при различных $a_{n+1} \neq b_{n+1}$ имеем для некоторых ненулевых констант $\lambda_1 \neq \lambda_2$

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

откуда

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

и сравнение степеней приводит к противоречию. Поэтому при фиксированных Q_0, Q_1 все последующие многочлены Q_n указанным алгоритмом определяются однозначно.

Так как по предположению индукции $Q_n \perp \mathrm{Pol}_{s_{n+1}-1}$, но Q_n не ортогонален $\mathrm{Pol}_{s_{n+1}}$, то $(Q_n(z), z^{s_{n+1}-1}) = \Delta_{s_n+s_{n+1}-1} \neq 0$. Для любого многочлена a_{n+1} степени d_{n+1} и $k \leqslant s_n - 2$ имеем

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

так как $a_{n+1}(z)z^k \in \mathrm{Pol}_{s_{n+1}-1}$, $z^k \in \mathrm{Pol}_{s_n-1}$, т.е. $a_{n+1}(z)Q_n(z) + Q_{n-1}(z) \perp \mathrm{Pol}_{s_n-1}$.

Для того, чтобы выбрать a_{n+1} так, чтобы многочлен $a_{n+1}(z)Q_n(z) + Q_{n-1}(z)$ был ортогонален пространству, порожденному многочленами $z^{s_n-1}, \ldots, z^{s_{n+1}-1}$, нужно его выбрать так, чтобы проекции многочленов $a_{n+1}(z)Q_n(z)$ и $Q_{n-1}(z)$ на это пространство были противоположны по знаку, т.е. выполнялись бы равенства

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

Эти равенства относительно коэффициентов многочлена a_{n+1} определяют линейную систему уравнений с треугольной матрицей, которая решается следующим итеративным алгоритмом.

4.3. Алгоритм вычисления очередного многочлена Q_{n+1}. 4.3.1. *Первый шаг.* На первом шаге построим многочлен $Q^{(1)}_{n+1} = cz^{d_{n+1}}Q_n + Q_{n-1}$, $\deg Q^{(1)}_{n+1} = \deg Q_{n+1}$, $Q^{(1)}_{n+1} \perp z^{s_n-1}$. Для этого выберем c так, чтобы проекции $cz^{d_{n+1}}Q_n$ и Q_{n-1} на вектор z^{s_n-1} были противоположны по знаку, т.е. чтобы

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

Так как

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

то, вычисляя при $k = s_{n+1} - 1$ по данной последовательности $f_0, \ldots, f_{s_n+s_{n+1}-1}$ *невязку*

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

и скалярное произведение

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

можно положить $c = -(z^{s_n-1}, Q_{n-1})/\Delta_{s_n+s_{n+1}-1}$. Так как $Q^{(1)}_{n+1} \perp \mathrm{Pol}_{s_n}$, то LFSR с этим многочленом обратных связей генерирует последовательность $f_0, \ldots, f_{s_n+s_{n+1}-1}$; значит, $\Lambda_{s_n+s_{n+1}} = Q^{(1)}_{n+1}$.

4.3.2. *Шаг с произвольным номером.* В общем случае на i-м шаге корректируем $Q_{n+1}^{(i-1)}$, если

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

и ищем $Q_{n+1}^{(i)}$ в виде $Q_{n+1}^{(i-1)} + cQ_n z^{d_{n+1}-i+1}$ так, чтобы $Q_{n+1}^{(i)} \perp z^{s_n+i-2}$. Для этого выбираем c так, чтобы проекции $Q_{n+1}^{(i-1)}$, $cQ_n z^{d_{n+1}-i+1}$ на вектор z^{s_n+i-2} были противоположны по знаку, т.е.

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

откуда $c = -\Delta_{s_n+s_{n+1}+i-2}/\Delta_{s_n+s_{n+1}-1}$. Заметим, что при $-1 \leqslant k \leqslant i-3$ согласно предположению индукции $Q_{n+1}^{(i-1)} \perp z^{s_n+k}$, так как $Q_{n+1}^{(i-1)} \perp \mathrm{Pol}_{s_n+i-2}$, поэтому

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

потому что многочлен $Q_n \perp \mathrm{Pol}_{s_{n+1}-2}$. Так как $Q_{n+1}^{(i)} \perp \mathrm{Pol}_{s_n+i-1}$, то LFSR с этим многочленом обратных связей генерирует последовательность $f_0, \ldots, f_{s_n+s_{n+1}+i-2}$; значит, $\Lambda_{s_n+s_{n+1}+i-2} = Q_{n+1}^{(i)}$. После этого по данной последовательности $f_0, \ldots, f_{s_n+s_{n+1}+i-1}$ находим невязку

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

и делаем $(i+1)$-й шаг.

4.3.3. *Завершение работы алгоритма.* В конце работы алгоритма на $(d_{n+1}+1)$-м шаге получим многочлен

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

Согласно сказанному выше он совпадает с многочленом Q_{n+1}. Так как LFSR с этим многочленом обратных связей генерирует последовательность $f_0, \ldots, f_{2s_{n+1}-1}$, значит, $\Lambda_{2s_{n+1}}$ совпадает с cQ_{n+1}.

Сложность алгоритма может быть оценена как

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

4.3.4. *Сравнение с алгоритмом Евклида.* Если конечный ряд Лорана $f_0/z + \cdots + f_{k-1}/z^k$ записать в виде дроби $f(z)/z^k$, где $f(z) = f_0 z^{k-1} + \cdots + f_{k-1}$, то ее можно разложить в непрерывную дробь, используя обычный алгоритм Евклида, который применим конечно и для произвольной дроби $f(z)/g(z)$. Но при этом не будут вычислены подходящие дроби для этой непрерывной дроби. Для их вычисления применяется *расширенный алгоритм Евклида*, в котором числители и знаменатели подходящих дробей появляются как *коэффициенты Безу* в линейных представлениях $q_i = u_i f + v_i g$ промежуточных многочленов q_i, вычисляемых в обычном алгоритме Евклида

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

Хотя расширенный алгоритм Евклида и указанная выше интерпретация ВМА эквивалентны в том смысле, что оба они вычисляют последовательности знаменателей подходящих дробей Q_n и сами элементы a_n цепной дроби, но порядок вычислений в них разный. Например, для вычисления многочленов $a_0, a_1, \ldots$ с малыми индексами в ВМА требуется знать только начальный отрезок данной последовательности $f_0, f_1, \ldots$, а в алгоритме Евклида надо знать *всю последовательность* $f_0, \ldots, f_{k-1}$.

5. Применение ВМА для разложения экспоненты в цепную дробь

Применим ВМА к последовательности $f_n = 1/(n+1)!$, $n = 0, 1, \ldots$, над полем рациональных чисел. Тогда функция $f(z) = f_0 + f_1/z + f_2/z^2 + \cdots$ совпадает с $e^{1/z} - 1$, и первый элемент ее цепной дроби равен $a_1(z) = [f^{-1}] = z - 1/2$. Если положить $Q_0 = 1$, $Q_1 = z - 1/2$, то алгоритм вычислит все элементы a_n цепной дроби и все знаменатели Q_n подходящих дробей по рекуррентной формуле $Q_{n+1} = a_{n+1} Q_n + Q_{n-1}$. Однако удобнее выбрать $Q_1 = 2z - 1$; тогда тоже $(Q_1, 1) = 0$. Допустим по предположению индукции, что $s_m = m$,

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

На первом шаге построим многочлен

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

Для этого выберем $c = -(z^{s_n - 1}, Q_{n-1})/\Delta_{s_n + s_{n+1} - 1}$, где

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

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

Так как $Q_n \perp \mathrm{Pol}_n$, то $(Q_n(z), z^{n-1}) = 0$. Поэтому для доказательства равенства $s_{n+1} = n + 1$ достаточно проверить, что

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

Так как

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

где

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

оператор n-й разности, то согласно известному (и непосредственно проверяемому по индукции) тождеству [14, п. 5.3]

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

имеем

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

Поэтому

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

Далее вычисляем $d_{n+1} = s_{n+1} - s_n = 1$,

$$\Delta_{2n+1} = \Delta_{s_n+s_{n+1}} = (Q^{(1)}_{n+1}, z^{s_n}) = (Q^{(1)}_{n+1}, z^n) = (czQ_n + Q_{n-1}, z^n) = c(Q_n, z^{n+1}) + (Q_{n-1}, z^n) = 2(2n+1)(Q_n, z^{n+1}) + (Q_{n-1}, z^n),$$

пользуясь тем, что

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

откуда

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

следовательно,

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

Поэтому корректировать $Q^{(1)}_{n+1}$ не надо и сразу имеем, что

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

Остается непосредственно проверить, что

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

Для этого достаточно убедиться в том, что

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

так как $(n-k)(n-k+1)+2(2n+1)k = (n+k+1)(n+k)$. Если инициализировать алгоритм значениями $Q_0 = 1$, $Q_1 = z - 1/2$, то, повторяя проведенные вычисления, легко видеть, что при четном n Q_n не меняется, а a_n делится на 2, а при нечетном n Q_n делится на 2, а a_n умножается на 2. Так как $Q_0 = 1$, Q_1 совпадают со знаменателями подходящих дробей к цепной дроби для $f(z)$, то, как было отмечено выше, при любом n полученный многочлен Q_n совпадает со знаменателем n-й подходящей дроби, а последовательность $a_n(z) = 2^{(-1)^{n+1}}2(2n+1)z$ совпадает при $n > 1$ с последовательностью элементов цепной дроби для $f(z) = e^{1/z} - 1$. Отсюда имеем правильную цепную дробь для $e^{1/z}$

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

которая после замены переменной $x = 1/z$ превращается в эйлерову цепную дробь для e^x. Возвращаясь к цепной дроби для $f(z) = e^{1/z} - 1$, заметим, следуя [11], что

для нахождения в явном виде числителей ее подходящих дробей P_n/Q_n, или, что то же самое, диагональных аппроксимаций Паде можно воспользоваться соотношением для аппроксимаций Паде

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

и заметить, что $P_n(z) = (-1)^n Q_n(-z) - Q_n(z)$. Действительно, умножая обе части равенства

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

на $e^{-1/z}$, имеем

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

откуда после замены $x = -z$ получаем соотношение

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

из которого согласно определению аппроксимаций Паде следует, что

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

Заметим еще, что после того как угаданы многочлены $Q_n(z)$, для доказательства того, что они являются знаменателями аппроксимаций Паде, достаточно проверить, что $s_n = n$, $Q_n \perp \mathrm{Pol}_n$, т.е. $(Q_n(z), z^k) = 0$, $k < n$. Но это немедленно следует из соотношений

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

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

так как многочлен $(x+n)\cdots(x+k+2)$ имеет степень $n-k-1 < n$ и после n-кратного применения разностного оператора Δ превращается в нуль.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

[1] Jungnickel D. Finite fields. Structure and arithmetic. Mannheim–Leipzig–Wien–Zurich: Wissenschaftsverlag, 1993.
[2] Блейхут Р. Э. Теория и практика кодов, контролирующих ошибки. М.: Мир, 1986.
[3] Massey J. L. Feedback Shift Register Synthesis and BCH decoding // IEEE Trans. Inform. Theory. 1969. V. IT-15. P. 122–128.
[4] Берлекемп Э. Р. Алгебраическая теория кодирования. М.: Мир, 1972.
[5] Dornstetter J. L. On the equivalence between Berlekamp's and Euclid's algorithms // IEEE Trans. Inform. Theory. 1987. V. IT-33. №3. P. 428–431.
[6] Sugiyama Y., Kasahara M., Hirasawa S., Namekawa T. A method for solving key equation for decoding Goppa codes // Inform. Control. 1975. V. 27. №1. P. 87–99.
[7] Welch L. R., Scholtz R. A. Continued fractions and Berlekamp's algorithm // IEEE Trans. Inform. Theory. 1979. V. IT-25. №1. P. 18–27.
[8] Cheng U. On the continued fractions and Berlekamp's algorithm // IEEE Trans. Inform. Theory. 1984. V. IT-30. №3. P. 541–544.
[9] Mills W. H. Continued fractions and linear recurrence // Math. Comp. 1975. V. 29. P. 173–180.
[10] Zongduo Dai, Kencheng Zeng. Continued fractions and Berlekamp–Massey algorithm // Advances in Cryptology—Auscript-90. Berlin: Springer-Verlag, 1990. P. 24–31.
[11] Никишин Е. М., Сорокин В. Н. Рациональные аппроксимации и ортогональность. М.: Наука, 1988.
[12] Сегё Г. Ортогональные многочлены. М.: Физматгиз, 1962.
[13] Сидельников В. М. Декодирование кодов Рида–Соломона с числом ошибок большим чем $(d-1)/2$ и нули полиномов нескольких переменных // Проблемы передачи информации. 1994. Т. 30. №1. С. 51–69.
[14] Грэхем Р., Кнут Д., Паташник О. Конкретная математика. М.: Мир, 1998.

(С. Б. Гашков) Московский государственный университет им. М. В. Ломоносова
(И. Б. Гашков) Karlstads Universitet, Швеция
E-mail: gashkov@lsili.ru, Igor.Gachkov@kau.se

Поступило
16.02.2005