Записки научных
семинаров ПОМИ
Том 498, 2020 г.

А. Л. Чистов

ЭФФЕКТИВНАЯ ОЦЕНКА КОРНЕЙ ИЗ ПОЛЯ ДРОБНО-СТЕПЕННЫХ РЯДОВ ЗАДАННОГО МНОГОЧЛЕНА В НЕНУЛЕВОЙ ХАРАКТЕРИСТИКЕ

Введение

В статье [1] мы обобщили алгоритм Ньютона–Пюизе на случай основного поля k ненулевой характеристики. Там мы получили канонический алгоритм для разложения многочленов над максимальным слабо разветвленным расширением Ω_0 поля степенных рядов $k((X))$ (в [1] мы определяем Ω_0 как объединение полей дробно-степенных рядов $k_s((X^{1/\nu}))$ по всем ν, взаимно простым с $p = \mathrm{char}(k)$, где k_s – сепарабельное замыкание поля k в его алгебраическом замыкании $\overline{k}$; чтобы иметь дело только с алгебраическими над $k((X))$ элементами, можно заменить в [1] (без всяких изменений в доказательствах) Ω_0 на поле Ω_0', являющееся объединением всех полей $k_1((X^{1/\nu}))$, где $k_1 \supset k$ – произвольное конечное расширение, такое, что $k_1 \subset k_s$ и $\mathrm{GCD}(\nu, p) = 1$)[1]. До сих пор считалось, что такой алгоритм либо невозможен в принципе, либо, если и существует, должен быть очень сложным. Поэтому результат из [1] является весьма важным.

Однако с точки зрения сложности вычислений здесь остается одна принципиальная проблема: оценить длины записи коэффициентов из конечных расширений поля k, появляющихся в этой естественной конструкции. Т.е. получить оценки, аналогичные оценкам из [3] (там поле k имеет нулевую характеристику). Но сейчас, в рассматриваемом случае $\mathrm{char}(k) = p > 1$, по-видимому, нет прямого аналога результатов из [3], достаточного для того чтобы получить требуемые оценки на длины записи коэффициентов. Здесь, по нашему мнению, следует вернуться к более классическому подходу и оценивать знаменатели этих

Ключевые слова: формальные степенные ряды, дробно-степенные ряды, ненулевая характеристика, алгоритм Ньютона–Пюизе, оценки неприводимых множителей.

[1] В [1] имеется одна несущественная неточность: если степень расширения $[k_s : k]$ равна $+\infty$, то $\Omega_0 \not\subset \overline{k((X))}$.

коэффициентов. Точнее, мы хотели бы сформулировать следующую гипотезу.

Пусть $k = \mathbb{F}_{p^m}(t_1, \dots, t_l)$, где $t_1, \dots, t_l$ алгебраически независимы над конечным полем $\mathbb{F}_{p^m}$ из p^m элементов, $m \geqslant 1$ – целое число. Пусть $f \in k[X, Y]$ – сепарабельный многочлен относительно Y (т.е. $\deg_Y f \geqslant 1$ и дискриминант многочлена f относительно Y не равен нулю) со старшим коэффициентом $\mathrm{lc}_Y f = 1$. Предположим, что $f \in \mathbb{F}_{p^m}[t_1, \dots, t_l, X, Y]$ и $\deg_{X,Y} f \leqslant d$, $\deg_{t_1,\dots,t_l} f \leqslant d_1$ для некоторых $d, d_1 \geqslant 2$.

Гипотеза. *Пусть $g \in k((X))[Y]$ – неприводимый (в этом кольце) множитель многочлена f, такой, что старший коэффициент $\mathrm{lc}_Y g$ равен 1. Тогда существуют ненулевой многочлен $\delta \in \mathbb{F}_{p^m}[t_1, \dots, t_l]$ степени $\deg_{t_1,\dots t_l} \delta = d_1 d^{O(1)}$ и многочлен $g_1 = g_1(t_1, \dots, t_l, X, Y) \in \mathbb{F}_{p^m}[t_1, \dots, t_l][[X]][Y]$, такие, что*

$$g = g_1(t_1, \dots, t_l, X/\delta, Y).$$

Заметим, что для доказательства этой гипотезы достаточно было бы получить хорошие оценки на аппроксимации в варианте леммы Гензеля, см. [4, теорема 1 в §3 гл. 4]. Но, к сожалению, такие оценки известны только в случае, когда многочлены $g|_{X=0}$ и $(f/g)|_{X=0}$ взаимно просты (возможно, еще и в некоторых других подобных случаях, но не в общем случае).

Можно даже уточнить эту гипотезу. Именно, пусть $y_1, \dots, y_n \in \overline{k((X))}$ – все попарно различные корни многочлена f (здесь $n = \deg_Y f$ и $\overline{k((X))}$ является алгебраическим замыканием поля $k((X))$). Рассмотрим многочлен $F = \prod\limits_{1 \leqslant i \neq j \leqslant n} (Z - y_i + y_j)$, где Z – новая переменная; таким образом, $F \in \mathbb{F}_{p^m}[t_1, \dots, t_l, X, Z]$. Пусть $F = \sum\limits_{i,j} F_{i,j} X^i Z^j$, где $F_{i,j} \in \mathbb{F}_{p^m}[t_1, \dots, t_l]$. Пусть V является множеством всех вершин ломаной Ньютона многочлена F, рассматриваемого как элемент из $k[[X]][Z]$. Положим $\delta_1 = \prod\limits_{(i,j) \in V} F_{i,j}$. Тогда в формулировке гипотезы можно дополнительно выбрать δ, делящим δ_1^N для некоторого целого числа $N = d^{O(1)}$ (но в этой статье мы не доказываем частный случай этого дополнительного утверждения в теореме 1 ниже).

Эта гипотеза (если она верна) является ключом к получению хороших оценок на длины записи коэффициентов из k_s в конструкции

из [1]. Для доказательства этой гипотезы надо тщательно проанализировать алгоритм из [1] (сейчас мы не видим никакого другого подхода). У нас есть предварительный план такого анализа. Общий случай является сложным. Но кое-что здесь удается сделать уже сейчас. В настоящее время мы можем получить хорошие оценки в важном частном случае, когда $\deg_Y g = 1$. Мы доказываем следующую теорему.

Теорема 1. *Пусть многочлен f – такой же, как и выше, и поле k есть $\mathbb{F}_{p^m}(t_1, \dots, t_l)$. Сформулированная гипотеза верна, если $\deg g = 1$. Более того, справедливы следующие утверждения.*

(a) *Пусть $Y = u \in \overline{k((X))}$ – корень многочлена f, такой, что расширение полей $k((X))[u] \supset k((X))$ является слабо разветвленным. Тогда существует элемент η, алгебраический сепарабельный над полем k с минимальным многочленом $\Phi \in \mathbb{F}_{p^m}[t_1, \dots, t_l, Z]$, неприводимым в этом кольце, со старшим коэффициентом $\mathrm{lc}_Z \Phi = 1$ и степенями $\deg_Y \Phi \leqslant n$, $\deg_{t_1,\dots,t_l} \Phi = d_1 d^{O(1)}$. Следовательно, $\Phi(t_1, \dots, t_l, \eta) = 0$. Существуют ненулевой многочлен $\delta \in \mathbb{F}_{p^m}[t_1, \dots, t_l]$, такой, что $\deg_{t_1,\dots,t_l} \delta = d_1 d^{O(1)}$, и целое число ν, взаимно простое с p, из интервала $1 \leqslant \nu \leqslant n$. Далее, можно представить u в виде*

$$u = \sum_{i \geqslant 0} \sum_{0 \leqslant j < \deg_Z \Phi} u_{i,j} \eta^j X^{i/\nu} / \delta^i,$$

где $u_{i,j} \in \mathbb{F}_{p^m}[t_1, \dots, t_l]$ и степени $\deg_{t_1,\dots,t_l} u_{i,j}$ ограничены сверху величиной $(i+1) d_1 d^{O(1)}$ для всех i, j. Здесь везде константы в $O(1)$ абсолютные.

(b) *Для всякого целого числа $N \geqslant 0$ можно построить семейство шестерок*

$$\bigl(u^{(r)}, \eta^{(r)}, \Phi^{(r)}, \delta^{(r)}, \nu^{(r)}, \{u^{(r)}_{i,j}\}_{0 \leqslant i \leqslant N,\, 0 \leqslant j < \deg_Z \Phi^{(r)}}\bigr), \quad 1 \leqslant r \leqslant \mu \qquad (1)$$

(здесь все $u^{(r)}, \eta^{(r)}, \Phi^{(r)}, \delta^{(r)}, \nu^{(r)}, u^{(r)}_{i,j}$ не зависят от N; элементы $\eta^{(r)}$ лежат в $\overline{k}$), удовлетворяющее следующим свойствам. Для всякого корня u из утверждения (a) *существуют единственное целое число r, $1 \leqslant r \leqslant \mu$, и вложение полей $\sigma : k[\eta^{(r)}] \to \overline{k}$ над k, такие, что*

$$\bigl(u, \eta, \Phi, \delta, \nu, \{u_{i,j}\}_{0 \leqslant i \leqslant N,\, 0 \leqslant j < \deg_Z \Phi}\bigr) = \bigl(u^{(r)}, \sigma(\eta^{(r)}), \Phi^{(r)}, \delta^{(r)}, \nu^{(r)}, \{u^{(r)}_{i,j}\}_{0 \leqslant i \leqslant N,\, 0 \leqslant j < \deg_Z \Phi^{(r)}}\bigr).$$

Обратно, пусть r *– произвольное целое число из интервала* $1 \leqslant r \leqslant \mu$. *Положим* $(u, \eta, \Phi, \delta, \nu) = (u^{(r)}, \eta^{(r)}, \Phi^{(r)}, \delta^{(r)}, \nu^{(r)})$ *и* $u_{i,j} = u_{i,j}^{(r)}$ *для всех* i, j. *Тогда утверждение* (a) *выполняется для этих* $u, \eta, \Phi, \delta, \nu$ *и* $u_{i,j}$.

Для всякого $N \geqslant 0$ *время работы алгоритма для построения семейства всех шестерок* (1) *полиномиально от* $((N+1)d_1d)^{l+1}$, m *и* p. *Следовательно, время работы алгоритма для построения семейства всех пятерок* $(u^{(r)}, \eta^{(r)}, \Phi^{(r)}, \delta^{(r)}, \nu^{(r)})$, $1 \leqslant r \leqslant \mu$, *полиномиально от* $(d_1d)^{l+1}$, m *и* p.

Сформулированная теорема обобщает результат из [3] на случай ненулевой характеристики. Но здесь еще важно, что доказать ее стало возможным благодаря предложенному новому методу, который можно применить также и в нулевой характеристике и получить другим способом результат из [3]. Грубо говоря, суть этого метода состоит в использовании теоремы о производных неявной функции в общей точке (или, что эквивалентно, версии леммы Гензеля в общей точке) с последующей специализацией значений этой общей точки.

§1. Доказательство теоремы 1

Сейчас основным является случай ненулевой характеристики, но всё даже значительно проще в случае нулевой характеристики. Мы оставляем подробности в нулевой характеристике заинтересованному читателю.

Рассмотрим сепарабельную алгебру $A = K[Y]/(f)$, где $K = k((X))$. Положим $y = Y \bmod f \in A$. Пусть Z, W – новые переменные. Для всякого $\varphi \in k[[X]]$ элемент $\varphi(X+Z) \in k[[X, Z]] \subset K[[Z]]$ определяется естественным образом. Так что $f(X+Z, W) \in K[[Z]][W]$. Положим $B = K[[Z]][W]/(f(X+Z, W))$ и $w = W \bmod f(X+Z, W) \in B$. Неформально говоря, $w = y(X+Z) = y|_{X:=X+Z}$.

Мы имеем $(\partial f(X+Z, W)/\partial W)|_{W=w} \neq 0$. Следовательно, согласно версии леммы Гензеля, существует вложение $K[[Z]]$-алгебр

$$K[[Z]][w] \to K[y][[Z]], \qquad w \mapsto \sum_{i \geqslant 0} w_i Z^i, \tag{2}$$

где $w_i \in K[y] = A$ и $w_0 = y$. Положим $D_i(y) = w_i$ для всякого $i \geqslant 0$.

Замечание 1. Положим K_s' равным подполю всех алгебраических над K элементов поля $k_s((X))$, т.е. объединению всех полей $k_1((X))$,

где $k_1 \supset k$ – произвольное конечное расширение и $k_1 \subset k_s$. Если заменить поле K на K'_s, то определения алгебр A, B и вложения (2) справедливы также в случае, когда $f \in k_s[[X]][Y] \cap K'_s[Y]$ является сепарабельным многочленом относительно Y и $\mathrm{lc}_Y f = 1$. В частности, в этом случае $D_i(y) \in K'_s[Y]/(f)$ для всех i.

Сейчас $f \in k[X,Y]$. Рассмотрим в B подкольца

$$k(X)[y] \subset k(X)[y][Z][w] \subset B.$$

Мы имеем естественные изоморфизмы $k(X)[y] \simeq k(X)[Y]/(f)$ и $k(X)[y][Z][w] \simeq k(X)[y][Z,W]/(f(X+Z,W))$. Заметим, что фактически, согласно лемме Гензеля, над сепарабельной алгеброй $k(X)[y]$ (рассматриваемой как основное кольцо) мы имеем вложение

$$k(X)[y][Z][w] \to k(X)[y][[Z]], \quad w \mapsto \sum_{i \geqslant 0} w_i Z^i.$$

Оно индуцирует вложение (2). Следовательно, $w_i \in k(X)[y] \subset A$ для всех i.

Положим $\Delta = \mathrm{Res}_Y(f, f'_Y) \in k[X]$ равным дискриминанту многочлена f. Тогда $\Delta \neq 0$.

Лемма 1. *Для всякого $i \geqslant 1$ можно представить w_i в виде*

$$w_i = \frac{P_i(X,y)}{f'_Y(X,y)^{2i-1}} = \frac{Q_i(X,y)}{\Delta^{2i-1}},$$

где $P_i, Q_i \in \mathbb{F}_{p^m}[t_1, \ldots, t_l, X, Y]$ – многочлены, такие, что $\deg_Y P_i \leqslant n-1$, $\deg_Y Q_i \leqslant n-1$, степени $\deg_X P_i$, $\deg_X Q_i$ ограничены сверху величиной $i\, d^{O(1)}$, а степени $\deg_{t_1,\ldots,t_l} P_i$, $\deg_{t_1,\ldots,t_l} Q_i$ ограничены сверху величиной $i\, d_1 d^{O(1)}$. Степень $\deg_{t_1,\ldots,t_l} \Delta$ ограничена сверху величиной $d_1 d^{O(1)}$. Здесь все константы в $O(1)$ являются абсолютными. Можно построить многочлены P_i, Q_i за время, полиномиальное от $(id_1 d)^{l+1}$ и $m \log p$.

Доказательство. Это немедленно следует из явной конструкции подъёма по лемме Гензеля. Мы оставляем подробности читателю. □

В нулевой характеристике, очевидно, имеем $D_i(y) = (1/i!) d^i y / dX^i$. В ненулевой характеристике для $D_i(y)$ также можно получить некоторую формулу. Именно, для целого числа $s \geqslant 0$ на кольце $k((X^{p^s}))[y^{p^s}]$

можно определить оператор дифференцирования $\delta_s = d/dX^{p^s}$. Далее, если $z \in k((X))[y]$, то представим z в виде $z = \sum\limits_{0 \leqslant i < p^s} z_i X^i$, где $z_i \in k((X^{p^s}))[y^{p^s}]$. По определению положим

$$\delta_s(z) = \sum_{0 \leqslant i < p^s} \delta_s(z_i) X^i \in A.$$

Здесь мы хотели бы подчеркнуть, что из этого определения следует, что для всех $z_1, z_2 \in A$ мы имеем $\delta_s(z_1 z_2^{p^{s+1}}) = \delta_s(z_1) z_2^{p^{s+1}}$.

Теперь представим i в виде $i = i_0 + i_1 p + \ldots + i_r p^r$, где все i_j, $0 \leqslant j \leqslant r$, являются целыми числами, такими, что $0 \leqslant i_j < p$ и $i_r \neq 0$ (при $i \neq 0$). Тогда мы имеем

$$D_i(y) = \frac{1}{i_0! i_1! \ldots i_r!} \delta_0^{i_0} \delta_1^{i_1} \ldots \delta_r^{i_r}(y). \tag{3}$$

Мы оставляем доказательство формулы (3) читателю (это несложное упражнение). Таким образом, получается интересный аналог формулы Тейлора для алгебраических функций в ненулевой характеристике.

Теперь пусть $f = \prod\limits_{j \in J} f_j$, где все $f_j \in K_s'[Y]$ являются неприводимыми в этом кольце многочленами и $\operatorname{lc}_Y f_j = 1$. Тогда фактически все f_j лежат в $k_s[[X]][Y] \cap K_s'[Y]$, поскольку коэффициенты многочленов f_j из K_s являются целыми над $k[X]$, $k[X] \subset k_s[[X]]$, кольцо $k_s[[X]]$ целозамкнуто и K_s' является подполем поля частных кольца $k_s[[X]]$. Для того чтобы избежать двусмысленности, мы будем предполагать, что все индексы $j \in J$ не являются целыми числами. Положим $y_j = Y \bmod f_j \in K_s'[Y]/(f_j) = A_j$ для всех $j \in J$. По китайской теореме об остатках мы рассматриваем отождествление

$$A \otimes_K K_s' = \prod_{j \in J} A_j. \tag{4}$$

Очевидно, при этом отождествлении $y = \{y_j\}_{j \in J}$.

Далее, согласно замечанию 1 для всех $j \in J$ и всех целых чисел $i \geqslant 0$ определены элементы $D_i(y_j)$. По китайской теореме об остатках и свойству единственности в лемме Гензеля мы имеем $D_i(y) = \{D_i(y_j)\}_{j \in J}$ при отождествлении (4) для всякого $i \geqslant 0$ (здесь мы оставляем подробности читателю).

Если $\deg_Y f_j = 1$, то, очевидно, $y_j \in k_s[[X]]$. Поэтому $w = y_j(X + Z) \in k_s[[X, Z]]$ и $D_i(y_j) \in k_s[[X]]$ для всех $i \geqslant 0$. В этом случае мы имеем $w|_{X=0} = y(Z) \in k_s[[Z]]$.

Рассмотрим отображение нормы $\mathcal{N} : k(X)[y] \to k(X)$, $q \mapsto \det(Q)$, где $q \in k(X)[y]$ – произвольный элемент и Q – матрица $k(X)$-линейного отображения $z \mapsto qz$ алгебры $k(X)[y]$ в некотором $k(X)$-базисе этой алгебры. Естественным образом $\mathcal{N}$ индуцирует отображение нормы на кольце многочленов $k(X)[y][Z] \to k(X)[Z]$. Мы будем обозначать его снова через $\mathcal{N}$.

Если $q \in k(X)[y]$, то многочлен $\varphi = \mathcal{N}(Z - q) \in k(X)[Z]$ является ненулевым и $\varphi(q) = 0$. Напомним, что $n = \deg_Y f$. Пусть $a_q \in \mathbb{F}_{p^m}[t_1, \dots, t_l, X]$ – многочлен наименьшей степени, такой, что $a_q q = \sum\limits_{0 \leqslant i \leqslant n-1} a_{q,i} y^i$, где $a_{q,i} \in \mathbb{F}_{p^m}[t_1, \dots, t_l, X]$. Тогда, a_q однозначно определён с точностью до ненулевого множителя из $\mathbb{F}_{p^m}$. Имеем $a_q^n \mathcal{N}(Z - q) \in \mathbb{F}_{p^m}[t_1, \dots, t_l, X, Z]$. Положим

$$\deg_{t_1,\dots,t_l} a_q = \max_{0 \leqslant i \leqslant n-1} \deg_{t_1,\dots,t_l} a_{q,i}.$$

Для произвольного элемента $q \in k(X)[y]$ по определению положим $\varphi_q = a_q^n \mathcal{N}(Z - q)/X^b$, где $b \geqslant 0$ является наибольшим целым числом, таким, что X^b делит $a_q^n \mathcal{N}(Z - q)$ в кольце $k[X, Z]$. Многочлен φ_q однозначно определён с точностью до ненулевого множителя из $\mathbb{F}_{p^m}$. Мы имеем $\varphi_q \in \mathbb{F}_{p^m}[t_1, \dots, t_l, X, Z]$, $\varphi_q(q) = 0$, $\operatorname{lc}_Z \varphi_q = a_q^n / X^b$, $\deg_Z \varphi_q \leqslant n$, и степень $\deg_{t_1,\dots,t_l} \varphi_q$ ограничена сверху величиной

$$(d_1 + \deg_{t_1,\dots,t_l} a_q + \deg_{t_1,\dots,t_l}(a_q q)) d^{O(1)}$$

(здесь мы оставляем детали читателю). Если элемент q задан, то можно построить многочлен φ_q за время, полиномиальное от d_1,$\deg_{t_1,\dots,t_l} a_q$, $\deg_{t_1,\dots,t_l}(a_q q)$, d и $m \log p$.

Для рассматриваемого q пусть $q = \{q_j\}_{j \in J}$ при отождествлении (4). Тогда, очевидно, $\varphi_q(q_j) = 0$ для всякого $j \in J$. Если $q_j \in k_s[[X]]$ для некоторого $j \in J$, то $\varphi_q(0, q_j(0)) = 0$.

Обозначим через $J_1 \subset J$ подмножество всех индексов $j \in J$, таких, что $\deg f_j = 1$. Обозначим через $\operatorname{Gal}(k_s/k)$ группу Галуа расширения полей $k_s \supset k$. Эта группа действует естественным образом (покоэффициентно) на кольце $k_s[[X]]$. Можно представить J_1 в виде $J_1 = \bigcup\limits_{\alpha \in A} J_{1,\alpha}$, где для всякого $\alpha \in A$ множество

$$\{y_j : j \in J_{1,\alpha}\} = \{\sigma(y_{j_0}) : \sigma \in \operatorname{Gal}(k_s/k)\}$$

является классом сопряжёных элементов произвольного элемента y_{j_0}, $j_0 \in J_{1,\alpha}$. Далее, можно представить f в виде $f = \prod\limits_{\alpha\in A} f_\alpha$, где все $f_\alpha \in k((X))[Y]$ являются неприводимыми над $k((X))$ многочленами, $f_\alpha = \prod\limits_{j\in J_{1,\alpha}} (Y - y_j)$ и фактически $f_\alpha \in k[[X]][Y]$.

Пусть $\beta \geqslant 0$ – максимальное целое число, такое, что X^β делит Δ. Тогда $\beta = d^{O(1)}$. Для всякого $j \in J_{1,\alpha}$ обозначим через k_j алгебраическое расширение поля k, порождённое элементами $D_i(y_j)(0)$ (здесь $D_i(y_j)(0) = D_i(y_j)|_{X=0}$), $0 \leqslant i \leqslant \beta+1$. Тогда из [4, теорема 1 в § 3 гл. 4] следует, что $D_i(y_j)(0) \in k_j$ для всех $i \geqslant 0$. Кроме того, $[k_j : k] = \#J_{1,\alpha}$ для всякого $j \in J_{1,\alpha}$.

Теперь мы собираемся описать алгоритм для построения всех пятёрок $(u^{(r)}, \eta^{(r)}, \Phi^{(r)}, \delta^{(r)}, \nu^{(r)})$, таких, что $\nu^{(r)} = 1$, см. формулировку теоремы 1.

Выберем подмножество $\mathcal{I} \in \mathbb{F}_{p^m}[t_1, \ldots, t_l]$, такое, что

$$\#\mathcal{I} = n(n-1)(\beta+1)/2 + 1$$

и

$$\max\{\deg_{t_1,\ldots,t_l} c \,:\, c \in \mathcal{I}\} \leqslant \log(n(n-1)(\beta+1)/2+1)$$

$/(m \log p)$,..$\deg_{t_1,\ldots,t_l} c$ являются малыми для всех $c \in \mathcal{I}$ (это возможно). Заметим, что существует элемент $c \in \mathcal{I}$, такой, что все элементы

$$q_{c,j} = \sum_{0\leqslant i\leqslant\beta+1} c^i D_i(y_j), \quad j \in J_1,$$

попарно различны. Отсюда следует, что для всякого $\alpha \in A$ для всякого $j \in J_{1,\alpha}$ мы имеем $k[q_{c,j}] = k_j$, т.е., $q_{c,j}$ является примитивным элементом расширения полей $k_j \supset k$.

Мы перебираем элементы $c \in \mathcal{I}$. Пусть t – новый трансцендентный элемент. Мы можем расширить основное поле k до $k(t)$ (заменяя l на $l+1$). Для рассматриваемого c положим

$$q_{c,t} = \sum_{0\leqslant i\leqslant\beta+1} (c^i + t^{i+1}) D_i(y) \in k(X)[t][y].$$

Мы вычисляем все $D_i(y)$, $0 \leqslant i \leqslant \beta+1$, и после этого многочлен $\varphi_{q_{c,t}} \in \mathbb{F}_{p^m}[t_1, \ldots, t_l, t, X, Z]$ (заметим, что $a_{q_{c,t}} \in \mathbb{F}_{p^m}[t_1, \ldots, t_l, t, X]$).

Положим $\psi_{c,t} = \varphi_{c,t}|_{X=0} \in \mathbb{F}_{p^m}[t_1, \dots, t_l, t, Z]$. Используя алгоритм из [3], построим разложение на неприводимые в $\mathbb{F}_{p^m}[t_1, \dots, t_l, t, Z]$ множители

$$\psi_{c,t} = a_{c,0} \prod_{\alpha \in A''_c} \psi_\alpha,$$

где все $\psi_\alpha \in \mathbb{F}_{p^m}[t_1, \dots, t_l, t, Z]$, $\alpha \in A''_c$, являются неприводимыми многочленами в $k(t)[Z]$ и $a_{c,0} \in \mathbb{F}_{p^m}[t_1, \dots, t_l, t]$.

Обозначим через A'_c подмножество всех индексов $\alpha \in A''_c$, таких, что $\operatorname{lc}_Z \psi_\alpha \in \mathbb{F}_{p^m}[t_1, \dots, t_l]$ и $\psi_\alpha|_{t=0} = \psi_\alpha(t_1, \dots, t_l, 0, Z) \in k[Z]$ является неприводимым многочленом. Мы строим A'_c, снова используя алгоритм из [3]. Следовательно, $\deg_Z \psi_\alpha = \deg_Z(\psi_\alpha|_{t=0})$ для всякого $\alpha \in A'_c$.

Пусть $\alpha \in A'_c$. Положим $d_\alpha = \deg_Z(\psi_\alpha|_{t=0})$ и $\eta_\alpha = Z \bmod \psi_\alpha \in k[Z]/(\psi_\alpha)$ для всякого $\alpha \in A'_c$. Мы имеем $\psi_\alpha|_{t=0} = (Z - \eta_\alpha)g(Z)$, где $g(Z) \in k[\eta_\alpha][Z]$. Теперь можно применить лемму Гензеля и получить разложение

$$\psi_\alpha = \Big(Z - \eta_\alpha - \sum_{i \geqslant 1} \eta_{\alpha,i} t^i\Big)\widetilde{g}(Z),$$

где $\eta_{\alpha,i} \in k[\eta_\alpha]$ и $\widetilde{g}(Z) \in k[\eta_\alpha][[t]][Z]$. Заметим (ср. лемма 1), что можно представить $\eta_{\alpha,i}$ в виде $\eta_{\alpha,i} = \sum\limits_{0 \leqslant j < d_\alpha} Q_{\alpha,i,j} \eta_\alpha^j / Q_\alpha^i$, где $Q_{\alpha,i,j}, Q_\alpha \in \mathbb{F}_{p^m}[t_1, \dots, t_l]$, все степени $\deg_{t_1,\dots,t_l} Q_{\alpha,i,j}$ ограничены сверху величиной $(i+1)\, d_1 d^{O(1)}$ и $\deg_{t_1,\dots,t_l} Q_\alpha$ ограничена сверху величиной $d_1 d^{O(1)}$. Мы строим, применяя подъём по лемме Гензеля, все $Q_{\alpha,i,j}$ и Q_α для $1 \leqslant i \leqslant \beta + 2$, $0 \leqslant j < d_\alpha$, $\alpha \in A'_\alpha$.

Обозначим через A_c подмножество всех индексов $\alpha \in A'_c$, удовлетворяющих следующим условиям:

(i) $\eta_{\alpha,i} = 0$ для всех $i > \beta + 2$, т.е. элемент $Z - \eta_\alpha - \sum\limits_{0 \leqslant i \leqslant \beta+1} \eta_{\alpha,i} t^{i+1}$ делит ψ_α.

(ii) существует такой корень $y_\alpha = \sum\limits_{i \geqslant 0} y_{\alpha,i} Z^i \in k_s[[Z]]$ многочлена $f(Z, Y) \in k((Z))[Y]$, что $y_{\alpha,i} \in k[\eta_\alpha]$, $\eta_\alpha = \sum\limits_{0 \leqslant i \leqslant \beta+1} c^i y_{\alpha,i}$ и $y_{\alpha,i} = \eta_{\alpha,i}$ при $0 \leqslant i \leqslant \beta + 1$.

Для всякого $\alpha \in A'_c$ можно выяснить, верно ли, что α удовлетворяет условию (ii), применяя [4, теорема 1 в §3 гл. 4]. Следовательно, можно построить подмножество A_c. Теперь из цитированной теоремы

следует также, что если $\alpha \in A_c$, то для всякого $i \geqslant 0$ существует представление $y_{\alpha,i} = \sum\limits_{0 \leqslant j < d_\alpha} R_{\alpha,i,j} \eta_\alpha^j / R_\alpha^i$, где $R_{\alpha,i,j}, R_\alpha \in \mathbb{F}_{p^m}[t_1, \ldots, t_l]$, все степени $\deg_{t_1,\ldots,t_l} R_{\alpha,i,j}$ ограничены сверху величиной $(i+1)d_1 d^{O(1)}$ и степень $\deg_{t_1,\ldots,t_l} R_\alpha$ ограничена сверху величиной $d_1 d^{O(1)}$. Более точно, используя эту теорему, для всякого $N \geqslant 0$ можно также построить R_α и семейство $\{R_{\alpha,i,j}\}_{0 \leqslant i \leqslant N,\, 0 \leqslant j < d_\alpha}$ за время, полиномиальное от $((N+1)\ d_1 d)^{l+1}$, m, p.

Выберем элемент $c_0 \in \mathcal{I}$, такой, что $\#A_{c_0} = \max\{\#A_c \,:\, c \in \mathcal{I}\}$. Мы предполагаем дополнительно, что $\nu^{(j)} \leqslant \nu^{(j+1)}$ при $1 \leqslant j \leqslant r-1$, см. (1). Для всякого целого числа ν, $1 \leqslant \nu \leqslant n$, положим

$$r^{(\nu)} = \max\{j \,:\, \nu^{(j)} \leqslant \nu\}.$$

Теперь мы имеем $r^{(1)} = \#A_{c_0}$ и по определению положим

$$\begin{aligned}\{(u^{(r)}, \Phi^{(r)}, \eta^{(r)}, \delta^{(r)}, 1, \{u_{i,j}\}_{0 \leqslant i \leqslant N, 0 \leqslant j < \deg_Z \Phi^{(r)}}) \,:\, 1 \leqslant r \leqslant r^{(1)}\} \\ = \{(y_\alpha, \psi_\alpha|_{t=0}, \eta_\alpha, R_\alpha, 1, \{R_{\alpha,i,j}\}_{0 \leqslant i \leqslant N,\, 0 \leqslant j < d_\alpha}) \,:\, \alpha \in A_{c_0}\}.\end{aligned}$$

Это определение корректно. Здесь мы оставляем детали читателю.

Наконец, для всякого $\nu = 2, 3, \ldots, n$, такого, что $\mathrm{GCD}(\nu, p) = 1$, в описанной конструкции можно заменить многочлен f на $f(X^\nu, Y)$. Таким образом можно последовательно построить каждое подмножество

$$\{(u^{(r)}, \Phi^{(r)}, \eta^{(r)}, \delta^{(r)}, \nu^{(r)}, \{u_{i,j}\}_{0 \leqslant i \leqslant N, 0 \leqslant j < \deg_Z \Phi^{(r)}}) \,:\, 1 \leqslant r \leqslant r^{(\nu)}\}.$$

Здесь мы оставляем подробности читателю. Теорема доказана.

Список литературы

1. А. Л. Чистов, *Расширение алгоритма Ньютона–Пюизе на случай ненулевой характеристики основного поля.* I. — Алгебра и анализ **28**, вып. 6 (2016), 147–188.
2. A. L. Chistov, *Polynomial complexity of the Newton–Puiseux algorithm*, in: J. Gruska, B. Rovan, J. Wiedermann (eds.), International Symposium on Mathematical Foundations of Computer Science 1986, Lect. Notes Comput. Sci. **233**, Springer, Berlin, 1986, pp. 247–255.
3. А. Л. Чистов, *Алгоритм полиномиальной сложности для разложения многочленов на неприводимые множители и нахождение компонент многообразия в субэкспоненциальное время.* — Зап. научн. семин. ЛОМИ **137** (1984), 124–188.
4. З. И. Боревич, И. Р. Шафаревич, *Теория чисел*, Наука, М., 1964.

Chistov A. L. Efficient estimation of roots from the field of fractional power series of a given polynomial in nonzero characteristic.

We discuss some results and problems related to the Newton–Puiseux algorithm and its generalization for nonzero characteristic obtained by the author earlier. A new method is suggested for obtaining efficient estimates of the roots of a polynomial in the field of fractional power series in the case of arbitrary characteristic.

С.-Петербургское отделение
Математического института
им. В.А. Стеклова РАН,
наб. Фонтанки, д. 27,
191023 С.-Петербург, Россия
E-mail: alch@pdmi.ras.ru

Поступило 31 августа 2020 г.