Простые плохой редукции детских рисунков рода 0

А. М. ВАШЕВНИК
Московский государственный университет им. М. В. Ломоносова
e-mail: andrew@rosenergo.com

УДК 512.624.3

Ключевые слова: пары Белого, теория Гротендика, конечные поля, простая редукция, обобщённые многочлены Чебышёва.

Аннотация

Статья посвящена расширению частного случая теории Гротендика на произвольные поля. Приводится формальное определение функции Белого над произвольным полем. Обнаруживается, что свойства функций Белого над конечными полями существенно отличаются от классического случая поля характеристики 0. В работе также дано определение простых плохой редукции для детских рисунков и проведено вычисление простых плохой редукции для некоторых серий рисунков.

Abstract

A. M. Vashevnik, Prime numbers of bad reduction for dessins of genus 0, Fundamentalnaya i prikladnaya matematika, vol. 11 (2005), no. 2, pp. 25—43.

This article expands the special case of the Grothendieck theory to arbitrary fields. A formal definition of Belyi function over an arbitrary field is introduced. It turns out that the properties of Belyi functions over finite fields and the properties of classical Belyi functions are quite different. A definition of the primes of bad reduction is also given, and the primes of bad reduction are calculated for some dessin families.

Введение

Теория так называемых детских рисунков Гротендика, ведущая начало от работы [4], в настоящее время интенсивно развивается. Часть этой теории связывает комбинаторно-топологически объекты (графы на поверхностях, которые и называются детскими рисунками) с алгебраическими («функциями Белого»), определёнными над полем алгебраических чисел (см. [5]). Однако функции Белого имеют смысл и над произвольным полем и допускают независимое изучение.

Настоящая работа является продолжением работы [1], в которой был сделан шаг в направлении распространения частного случая теории (в котором функции Белого сводятся к обобщённым многочленам Чебышёва) на произвольные поля. В [1] были даны определения обобщённых многочленов Чебышёва над

Фундаментальная и прикладная математика, 2005, том 11, № 2, с. 25—43.

произвольными полями, установлены связи между ними и приведены примеры, показывающие их неравносильность. В данной статье будет продолжено рассмотрение свойств обобщённых многочленов Чебышёва над произвольными полями и их редукции.

В предыдущих работах (см., например, [7]) определение простых плохой редукции рисунка зависело от выбора функции Белого, соответствующей данному рисунку. В настоящей работе даётся точное определение простых плохой редукции для детского рисунка, которое не зависит от выбора функции Белого. Кроме того, приводятся способы нахождения некоторых простых плохой редукции исходя из комбинаторных свойств данного рисунка (например, оказывается, что делители валентностей вершин всегда являются простыми плохой редукции), а также примеры «скрытых» простых плохой редукции, которые не выражаются из комбинаторных параметров рисунка.

В первом разделе даются несколько определений функции Белого над произвольным полем и определение обобщённого многочлена Чебышёва над произвольным полем, а также приводятся примеры.

Во втором разделе показывается, как вычислять обобщённые многочлены Чебышёва для некоторых конкретных серий деревьев, приводятся примеры, когда набору кратностей не соответствует ни одного обобщённого многочлена Чебышёва или соответствует бесконечное их количество.

В третьем разделе устанавливаются соотношения между функциями Белого над полем характеристики 0 и над конечными полями.

В четвёртом разделе даётся определение простых плохой редукции и приводятся способы нахождения простых плохой редукции при помощи теорем из предыдущего раздела.

Автор благодарит Г. Б. Шабата за постановку задачи и за неоценимую помощь в написании этой статьи.

1. Определения функции Белого над произвольным полем

Рассмотрим рациональную функцию $\beta = \frac{P}{Q}$, где $P, Q \in \Bbbk[z]$ — многочлены над некоторым алгебраически замкнутым полем $\Bbbk$, не имеющие общих множителей, а также c^+, c^- — два различных элемента $\Bbbk$. Рассмотрим разложения

$$P(z) - c^{\pm}Q(z) = \lambda \prod_{i=1}^{m^{\pm}} (z - A_j^{\pm})^{v_j^{\pm}}, \quad Q(z) = \lambda \prod_{i=1}^{m^{\infty}} (z - A_j^{\infty})^{v_j^{\infty}}.$$

Обозначим $n = \deg(\beta)$, $p = \operatorname{char} \Bbbk$. Введём следующие условия.

Условие 1. Значения $\frac{P}{Q}$, взятые в корнях многочлена $P'Q - Q'P$, содержатся в множестве $\{c^+, c^-, \infty\}$.

Условие 2. Корни $\operatorname{Discr}(P - cQ) \in \Bbbk[c]$ содержатся в множестве $\{c^+, c^-\}$.

Условие 3. Уравнение $\frac{P}{Q} = c$ имеет n различных корней при $c \neq c^+$ и $c \neq c^-$.

Условие 4. В кольце $\Bbbk[z]$ имеет место делимость

$$Q(P - c^-Q)(P - c^+Q) \vdots P'Q - Q'P.$$

Условие 5. $\#\{\text{корни } P - c^+Q\} + \#\{\text{корни } P - c^-Q\} + \#\{\text{корни } Q\} = n + 2$.

Если $\deg(P - c^{\pm}Q) < n$ или $\deg Q < n$, будем предполагать, что ∞ является корнем соответствующего многочлена и увеличим m на единицу.

Обозначим $m^{\pm} = \#\{\text{корни } P - c^+Q\}$, $m^{\infty} = \#\{\text{корни } Q\}$.

Теорема 1. *Если $n \not\vdots p$, то* $1 \iff 2 \iff 3 \impliedby 4 \impliedby 5$.

Доказательство.

$1 \implies 3$. Пусть $\frac{P}{Q} = c$ имеет меньше чем n корней для некоторого $c \notin \{c^+, c^-, \infty\}$. Тогда у этого уравнения есть хотя бы один кратный корень z_0, т. е. $\frac{P(z_0)}{Q(z_0)} = c$, $P'(z_0)Q(z_0) - P(z_0)Q'(z_0) = 0$. Получаем, что условие 1 не выполнено.

$3 \implies 1$. Пусть $P'(z_0)Q(z_0) - P(z_0)Q'(z_0) = 0$ и $P(z_0)/Q(z_0) = c$, где $c \notin \{c^+, c^-, \infty\}$. Тогда уравнение $\frac{P}{Q} = c$ имеет кратный корень, и условие 3 не выполнено.

$2 \iff 3$. Если $\frac{P}{Q} = c$ имеет менее n корней для некоторого $c \notin \{c^+, c^-, \infty\}$, то многочлен $P - cQ$ имеет кратный корень. Тогда $\operatorname{Discr}(P - cQ) = 0$, и условие 2 не выполнено.

$3 \implies 2$. Если $\operatorname{Discr}(P - cQ) = 0$ для некоторого $c \notin \{c+, c^-, \infty\}$, то многочлен $P - cQ$ имеет кратный корень, поэтому уравнение $\frac{P}{Q} = c$ имеет менее n корней, и условие 3 не выполнено.

$1 \implies 4$. Это следствие очевидно.

$4 \impliedby 5$. Пусть A_0 — корень $\frac{P}{Q} = c$ кратности v_0, т. е. $\frac{P(z) - cQ(z)}{Q(z)} \vdots (z - A_0)^{v_0}$. Тогда $P'(z)Q(z) - P(z)Q'(z) \vdots (z - A_0)^{v_0 - 1}$. Поэтому

$$P'(z)Q(z) - P(z)Q'(z) \vdots \prod_{j=1}^{m^+} (z - A_j^+)^{v_j^+ - 1}.$$

Заметим, что $\prod\limits_{j=1}^{m^+} (z - A_j^+)^{v_j^+ - 1}$ — многочлен степени $n - m^+$.

Предположим, что $\deg(P - c^{\pm}Q) = \deg Q = n$. Тогда степень многочлена $P'Q - PQ'$ равна $2n - 2$, так как коэффициенты при степени $2n - 1$ сокращаются. Если сокращаются и коэффициенты при степени $2n - 2$, то ∞ — критическая точка рациональной функции β, тогда степень одного из многочленов $P - c^{\pm}Q$, Q была бы меньше n. Заметим, что $2n - 2 = (n - m^+) + (n - m^-) + (n - m^{\infty})$, откуда

$$P'(z)Q(z) - P(z)Q'(z) \sim \prod_{j=1}^{m^+} (z - A_j^+)^{v_j^+ - 1} \prod_{j=1}^{m^+} (z - A_j^-)^{v_j^- - 1} \prod_{j=1}^{m^{\infty}} (z - A_j^{\infty})^{v_j^{\infty} - 1}.$$

Пусть $\deg(P-c^+Q)<n$, или $\deg(P-c^-Q)<n$, или $\deg Q<n$. Рассмотрим случай $\deg Q<n$ (остальные случаи разбираются аналогично). Тогда

$$\deg(P'Q-PQ')=n+\deg Q-1=(n-m^+)+(n-m^-)+(\deg Q-(m^\infty-1)).$$

Но $m^\infty-1$ — число различных конечных корней многочлена Q, отсюда опять получаем, что

$$P'(z)Q(z)-P(z)Q'(z)\sim\prod_{j=1}^{m^+}(z-A_j^+)^{v_j^+-1}\prod_{j=1}^{m^+}(z-A_j^-)^{v_j^--1}\prod_{j=1}^{m^\infty}(z-A_j^\infty)^{v_j^\infty-1}.$$

Теорема доказана. □

Примеры, показывающие, что $3\not\Rightarrow 4$ и $4\not\Rightarrow 5$, будут приведены в разделе 1.3.

Следствие 1. *Для любой рациональной функции β выполнено*

$$m^+ + m^- + m^\infty \geqslant n+2,$$

где $m^\pm$, m^∞ определены в условии 5.

Доказательство. Для любой функции β получаем

$$P'(z)Q(z)-P(z)Q'(z)\,\vdots\prod_{j=1}^{m^+}(z-A_j^+)^{v_j^+-1}\prod_{j=1}^{m^+}(z-A_j^-)^{v_j^--1}\prod_{j=1}^{m^\infty}(z-A_j^\infty)^{v_j^\infty-1}.$$

Поэтому степень многочлена в левой части больше либо равна степени многочлена в правой части. Если $\deg(P-c^\pm Q)=\deg Q=n$, то $2n-2\geqslant(n-m^+)+$ $+(n-m^-)+(n-m^\infty)$, откуда $m^+ + m^- + m^\infty \geqslant n+2$. □

Определение 1. Рациональная функция $\beta=\frac{P}{Q}$ называется функцией Белого над $\Bbbk$, если она удовлетворяет условию 1.

Функция β называется регулярной функцией Белого над $\Bbbk$, если она удовлетворяет условию 5.

Будем считать, что если $n=\deg\beta$ делится на $p=\operatorname{char}\Bbbk$, то β по определению не может быть функцией Белого над $\Bbbk$.

Теорема 2. *Пусть $p=\operatorname{char}\Bbbk$, $\beta=\frac{P}{Q}$ — функция Белого над $\Bbbk$. Тогда эквивалентны следующие условия*:

1) *β — регулярная функция Белого*;
2) *ни одно из чисел $v_j^\pm$, v_j^∞ не делится на p.*

Доказательство. Пусть β — регулярная функция Белого. Тогда

$$P'(z)Q(z)-P(z)Q'(z)\sim\prod_{j=1}^{m^+}(z-A_j^+)^{v_j^+-1}\prod_{j=1}^{m^+}(z-A_j^-)^{v_j^--1}\prod_{j=1}^{m^\infty}(z-A_j^\infty)^{v_j^\infty-1}.$$

Если найдётся такое j, что $v_j^+ \vdots p$, то из соотношения $\frac{P(z)-cQ(z)}{Q(z)} \vdots (z-A_j^+)^{v_j^+}$ будет следовать $P'(z)Q(z)-P(z)Q'(z) \vdots (z-A_j^+)^{v_j^+}$. Приходим к противоречию. Аналогично рассматриваются случаи $v_j^- \vdots p$ и $v_j^\infty \vdots p$.

Пусть ни одно из чисел $v_j^\pm$, v_j^∞ не делится на p. Тогда имеет место делимость

$$\prod_{j=1}^{m^+}(z-A_j^+)^{v_j^+-1}\prod_{j=1}^{m^+}(z-A_j^-)^{v_j^--1}\prod_{j=1}^{m^\infty}(z-A_j^\infty)^{v_j^\infty-1} \vdots P'(z)Q(z)-P(z)Q'(z).$$

В самом деле, все корни $P'Q-PQ'$ являются корнями $Q(P-c^+Q)(P-c^-Q)$, так как β — функция Белого над $\Bbbk$, а кратность корней $A_j^\pm$ в многочлене $P'Q-PQ'$ равна в точности $v_j^\pm-1$, так как $v_j^\pm$ не делится на p. Поэтому $m^++m^-+m^\infty \leqslant$ $\leqslant n+2$, откуда по следствию 1 получаем $m^++m^-+m^\infty=n+2$. □

1.1. Определение обобщённого многочлена Чебышёва над произвольным полем

Если рациональная функция β является многочленом (т. е. $Q=\mathrm{const}$), то β называется обобщённым многочленом Чебышёва. Перепишем условия 1—5 для этого случая.

Условие 1′. Множество критических значений P содержится в множестве $\{c^-,c^+\}$.

Условие 2′. Множество корней многочлена $\mathrm{Discr}(P-c)$ содержится в множестве $\{c^-,c^+\}$.

Условие 3′. Уравнение $P=c$ имеет n различных корней при $c\neq c^+$ и $c\neq c^-$.

Условие 4′. В кольце $\Bbbk[z]$ имеет место делимость $(P-c^-)(P-c^+) \vdots P'$.

Условие 5′. $m^++m^-=n+1$, где $m^\pm$ — число различных корней $P-c^\pm$.

Теорема 3. $1' \iff 2' \iff 3' \Longleftarrow 4' \Longleftarrow 5'$.

Определим обобщённый многочлен Чебышёва и регулярный обобщённый многочлен Чебышёва, как это было сделано в определении 1.

Рассмотрим разложение

$$P-c^\pm=\prod_{j=1}^{m^\pm}(x-A_j^\pm)^{v_j^\pm},$$

где $A_j^\pm \in \Bbbk$, $v_j^\pm \in \mathbb{N}$, все $A_j^\pm$ отличны друг от друга (такое представление существует и единственно, так как $\Bbbk$ алгебраически замкнуто). Тогда будем говорить, что обобщённому многочлену P соответствует набор кратностей $v_j^\pm$, и обозначать этот факт

$$\mathrm{val}(P)=[v_1^+,v_2^+,\ldots,v_{m^+}^+ \parallel v_1^-,v_2^-,\ldots,v_{m^-}^-].$$

1.2. Случай поля характеристики 0

В случае поля характеристики 0 определения функции Белого и обобщённого многочлена Чебышёва сводятся к стандартным (см. [6]).

Утверждение 1. *Если* $\operatorname{char}\Bbbk = 0$, *то условия* 1—5 (*а значит, и* $1'$—$5'$) *эквивалентны.*

Утверждение следует из теоремы 2.

Утверждение 2. *Если* $\Bbbk = \mathbb{C}$, *то условия* $1'$—$5'$ *равносильны классическому определению обобщённого многочлена Чебышёва. Комплексный многочлен* P *является обобщённым многочленом Чебышёва, если для некоторых* c^+ *и* c^- *прообраз отрезка* $[c^+, c^-]$ *является деревом* (*связным графом без циклов*).

Доказательство этого утверждения содержится в [6].

1.3. Примеры обобщённых многочленов Чебышёва

Пример 1. Пусть $\Bbbk = \bar{\mathbb{F}}_3$, $P(z) = z^4 + z$, $c^- = 0$, $c^+ = 1$. В данном случае

$$P = z(z+1)^3, \quad P - 1 = (z - A_1)(z - A_2)(z - A_3)(z - A_4),$$

где все A_1, A_2, A_3, A_4 из $\bar{\mathbb{F}}_3$ различны, т. е. многочлену P соответствует набор чисел $[1, 3 \parallel 1, 1, 1, 1]$, $\operatorname{Discr}(P - c) = c^3$. Поэтому P является нерегулярным обобщённым многочленом Чебышёва.

Пример 2. Пусть $\Bbbk$ — произвольное поле, $p = \operatorname{char}\Bbbk$. Пусть $k \in \mathbb{Z}$, $0 < k < p$, $m \in \mathbb{Z}$, $m > 0$, $\{B_i\}_{i=1}^m$ — произвольный набор элементов из $\Bbbk$, такой что не все B_i нули. Тогда

$$P = z^k \sum_{i=1}^{m} B_i z^{pi}$$

является обобщённым многочленом Чебышёва.

Для доказательства надо воспользоваться условием $2'$ и расписать дискриминант, учитывая, что $z\frac{dP}{dz} = kP$.

Пример 3. Пусть $\lambda \in \Bbbk$, $\lambda \neq 0$, $n, r \in \mathbb{Z}$, $r > 0$, $n > rp$, $\{C_i\}_{i=1}^r$ — произвольный набор элементов из $\Bbbk$. Тогда

$$P = \lambda z^n + \sum_{i=1}^{r} C_i z^{pi}$$

является обобщённым многочленом Чебышёва.

Доказательство аналогично указанному в примере 2, но нужно учесть, что $\frac{dP}{dz} = \lambda n z^{n-1}$. Заметим, что многочлен такого вида будет регулярным обобщённым многочленом Чебышёва, только если набор $\{C_i\}_{r=1}^m$ состоит из одних нулей.

2. Примеры обобщённых многочленов Чебышёва над произвольным полем

2.1. Обобщённые многочлены Чебышёва для деревьев диаметра 3

Определение 2. Валентностью вершины графа называется число выходящих из неё рёбер.

Вершины любого дерева можно раскрасить в два цвета так, чтобы соседние вершины имели разный цвет. Валентности всех вершин дерева будем записывать следующим образом: $[v_1^+, v_2^+, \ldots \parallel v_1^-, v_2^-, \ldots]$, где $v^\pm$ — валентности вершин каждого цвета.

Определение 3. Диаметром дерева называется длина максимальной цепи, которую содержит это дерево.

Вершины любого дерева можно раскрасить в два цвета так, что каждое ребро соединяет вершины разных цветов. Обозначим валентности вершин одного цвета через v_j^+, а другого — через v_j^-. В дальнейшем под нахождением обобщённого многочлена Чебышёва для некоторого дерева над алгебраически замкнутым полем $\Bbbk$ мы будем понимать решение системы уравнений

$$P - c^\pm = \prod_{j=1}^{m^\pm} (x - A_j^\pm)^{v_j^\pm},$$

где все $A_j^\pm$ попарно различны, а P — многочлен над $\Bbbk$, степень которого равна количеству рёбер дерева.

Теорема 4. *Если для дерева диаметра* 3 *существует обобщённый многочлен Чебышёва, то он равен выражению*

$$P_{ab}(z) = (1-z)^a \sum_{k=0}^{b-1} \binom{a+k-1}{k} z^k.$$

Доказательство. Рассмотрим дерево диаметра 3. У него есть только две вершины, валентности которых больше 1. Обозначим эти валентности a и b, а все дерево III_{ab}.

Поместим вершину валентности b в 0, вершину валентности a в 1, пусть $c^+ - c^- = 1$. Пусть $P_{ab}(z)$ — обобщённый многочлен Чебышёва, соответствующий данному дереву. Тогда имеют место представления

$$P_{ab}(z) = (1-z)^a Q_{ab}(z), \quad P_{ab}(z) = 1 + z^b R_{ab}(z),$$

где Q_{ab}, R_{ab} — некоторые многочлены. Найдём такой степенной ряд $S_a(z)$, что $(1-z)^a S(z) = 1$:

$$S_a(z) = ((1-z)^{-1})^a = (1 + z + z^2 + z^3 + \ldots)^a = \sum_{k=0}^{\infty} \binom{a+k-1}{k} z^k.$$

Покажем, что

$$Q_{ab}(z) = \sum_{k=0}^{b-1} \binom{a+k-1}{k} z^k.$$

Тогда Q_{ab} является урезанием степенного ряда S_a до многочлена степени $b-1$. Действительно,

$$(1-z)^a(S_a(z) - Q_{ab}(z)) = 1 - P_{ab}(z) = 1 - 1 - z^b R_{ab}(z) = -z^b R_{ab}(z).$$

откуда $S_a(z) - Q_{ab}(z) \vdots z^b$. Но $\deg(P_{ab}) = a+b-1$, поэтому $\deg(Q_{ab}) = b-1$. Отсюда получаем окончательный ответ:

$$P_{ab}(z) = (1-z)^a \sum_{k=0}^{b-1} \binom{a+k-1}{k} z^k.$$

Теорема доказана. □

Если $\operatorname{char} \Bbbk = 0$, то найденный многочлен всегда является обобщённым многочленом Чебышёва. Случай $\operatorname{char} \Bbbk > 0$ будет разобран в разделе 4.3.

2.2. Обобщённые многочлены Чебышёва для деревьев диаметра 4

Рассмотрим дерево диаметра 4. У него есть единственная вершина, расстояние от которой до любой другой не больше 2. Обозначим её валентность s, валентности соседних с ней вершин — $a_1, a_2, \ldots, a_s$. Таким образом, набор валентностей этого дерева $[a_1, a_2, \ldots, a_s \parallel s, 1, 1, \ldots, 1]$. Обозначим всё дерево $\mathrm{IV}_{a_1,a_2,\ldots,a_s}$. Этот набор может иметь несколько реализаций. Напишем условия на обобщённые многочлены Чебышёва. Поместим центральную вершину в 0. Пусть вершины валентностей a_i находятся в точках A_i. Тогда

$$P(z) = \prod_{i=1}^{s} (z - A_i)^{a_i}.$$

Используя то, что 0 — вершина валентности s, получаем

$$P' = n\left(\prod_{i=1}^{s} (z-A_i)^{a_i-1}\right) z^{s-1}, \quad \sum_{i=1}^{s} a_i \prod_{j\neq i} (z - A_j) = nz^{s-1}.$$

Из существования и единственности обобщённого многочлена Чебышёва следует, что это уравнение имеет $(s-1)!$ различных решений $(A_1, A_2, \ldots, A_s) \in \in \mathbb{P}^s(\mathbb{C})$, причём все A_i попарно различны и отличны от 0. Сделав замену $x_i = \frac{1}{A_i}$, получим систему

$$\forall 1 \leqslant k \leqslant s-1 \ \sum_{i=1}^{s} a_i x_i^k = 0. \qquad (*)$$

Эта система называется антивандермондовой (подробнее см. [3]). Система $(*)$ сводится к полиномиальному уравнению $R(x) = 0$ степени не выше $(s-1)!$. Если $\Bbbk = \mathbb{C}$, то у него есть $(s-1)!$ различных корней.

Определение 4. Назовём решение x_i системы $(*)$ паразитическим, если найдётся i, для которого $x_i = 0$, или найдутся i, j, $i \neq j$, для которых $x_i = x_j$.

2.3. Примеры обобщённых многочленов Чебышёва для деревьев диаметра 4

Сделаем следующие предположения: a_i не делятся на p при каждом i, сумма всех a_i тоже не делится на p. Как и в предыдущих разделах, s — валентность центральной вершины.

1. $s = 2$. Обобщённый многочлен Чебышёва единствен:

$$P = z^{a_1}(z-1)^{a_2}.$$

2. $s = 3$. Найдётся два обобщённых многочлена Чебышёва, если $a_1 + a_2$, $a_1 + a_3, a_2 + a_3 \not\vdots p$. Если хотя бы два из этих чисел делятся на p, то таких обобщённых многочленов Чебышёва нет.

Пусть $a_1 + a_2 \vdots p$, $a_1 + a_3 \not\vdots p$, $a_2 + a_3 \not\vdots p$. Тогда существует единственное непаразитическое решение $(*)$ $(x_1, x_2, x_3) = \left(\frac{a_1+a_3}{2a_1}, \frac{a_2+a_3}{2a_2}, 1\right)$, откуда

$$P(z) = \left(z - \frac{2a_1}{a_1+a_3}\right)^{a_1} \left(z - \frac{2a_2}{a_2+a_3}\right)^{a_2} (z-1)^{a_3}.$$

Заметим, что данному набору валентностей соответствуют два (зеркально-симметричных) плоских дерева. Однако про найденный обобщённый многочлен нельзя сказать, что он соответствует какому-то конкретному дереву из этих двух.

3. $s = 4$. Решение

$$P(z) = (z^2 - a)^a (z^2 + b)^b$$

существует всегда (даже при $p = 3$). Оно соответствует IV_{abab} (т. е. относительно центральной вершины разных валентностей чередуются). При условиях $a + 2b \not\vdots p$, $b + 2a \not\vdots p$ есть ещё обобщённый многочлен Чебышёва

$$P(z) = \left(z^2 - z + \frac{a+2b}{6b}\right)^a \left(z^2 + \frac{a}{b}z + \frac{b+2a}{6a}\frac{a^2}{b^2}\right)^b.$$

Это решение соответствует IV_{aabb}.

2.4. Соотношения для деревьев диаметра 4 над $\overline{\mathbb{F}}_p$

Определим следующие числа:

$N_1(T)$ — количество обобщённых многочленов Чебышёва (с учётом симметрий) для дерева T диаметра 4;

$N_2(T)$ — количество решений системы

$$\forall 1 \leqslant k \leqslant s-1 \ \sum_{i=0}^{s} a_i x_i^k = 0, \qquad (*)$$

таких что x_i попарно различны и отличны от 0;

$N_3(T)$ — количество корней $R(x)$ без учёта кратностей.

Будем считать, что $R \neq 0$. Тогда $N_1(T) \leqslant N_2(T) \leqslant N_3(T) \leqslant (s-1)!$. В случае поля характеристики 0 везде вместо неравенства имеет место равенство. Чтобы выяснить, когда $N_1(T) = (s-1)!$, попытаемся понять, когда вместо неравенств будут иметь место равенства.

Теорема 5. *Паразитическое решение системы* $(*)$ *существует тогда и только тогда, когда найдутся числа* $l_1 < l_2 < \ldots < l_k$, *такие что* $\sum\limits_{i=1}^{k} a_{l_i} \vdots p$.

Доказательство.

$\Longleftarrow$. В этой ситуации набор чисел $\{x_i\}$, где $x_i = 1$, если найдётся такое j, что $j : i = l_j$, иначе $x_i = 0$, будет паразитическим решением.

$\Longrightarrow$. Возьмём паразитическое решение x_i. Проделаем с ним следующие операции: выбросим нулевые элементы x_i, одинаковые элементы объединим в один, взяв в качестве нового a'_i сумму соответствующих коэффициентов a_i. Тогда новый набор x'_i не содержит нулей, все элементы попарно различны и он удовлетворяет следующей системе:

$$\forall 1 \leqslant k \leqslant s' \ \sum_{i=0}^{s'} a'_i {x'_i}^k = 0.$$

Рассмотрим её как систему на a'_i. Матрица

$$C = \begin{pmatrix} x'_1 & x'_2 & \ldots & x'_{s'} \\ {x'_1}^2 & {x'_2}^2 & \ldots & {x'_{s'}}^2 \\ \vdots & \vdots & \ddots & \vdots \\ {x'_1}^{s'} & {x'_2}^{s'} & \ldots & {x'_{s'}}^{s'} \end{pmatrix}$$

невырожденная:

$$\det(C) = \prod_{i=1}^{s'} {x_i}' \prod_{i \neq j} ({x_i}' - {x_j}') \neq 0.$$

Следовательно, $a'_i = 0$ для каждого i, откуда следует требуемое соотношение. □

Теорема 6. *Если* $p > s$, *то* $N_1 = N_2$, *т. е. каждое непаразитическое решение* $(*)$ *будет соответствовать обобщённому многочлену Чебышёва.*

Доказательство. 0 — корень кратности $s-1$ многочлена P', следовательно, 0 — корень кратности s многочлена $P - c^{\pm}$. □

2.5. Примеры, когда не существует ни одного обобщённого многочлена Чебышёва с данным набором кратностей

Пусть P — обобщённый многочлен Чебышёва над $\bar{\mathbb{F}}_p$. По определению $P - c^{\pm} = \prod_{j=1}^{m^{\pm}} (x - A_j^{\pm})^{v_j^{\pm}}$. В этом разделе будут сформулированы необходимые и достаточные условия реализуемости данного набора кратностей над $\Bbbk$, т. е. существования в $\Bbbk[z]$ обобщённого многочлена Чебышёва с данным набором кратностей $v_j^{\pm}$. Обозначим $n = \sum_{j=1}^{m^+} v_j^+ = \sum_{j=1}^{m^-} v_j^-$. Пусть $k_j^{\pm}$ — кратность корня $A_j^{\pm}$ многочлена P'. В [1] было доказано, что

1) если $v_j^{\pm} \not\vdots\, p$, то $k_j^{\pm} = v_j^{\pm} - 1$;
2) если $v_j^{\pm} \vdots\, p$, то $k_j^{\pm} \geqslant v_j^{\pm}$.

Пусть

$$l^{\pm} = \sum_{j=1,\ v_j^{\pm} \vdots p}^{m^{\pm}} 1 -$$

число корней кратности, делящейся на p;

$$s^{\pm} = \sum_{j=1}^{m^{\pm}} (k_j^{\pm} - v_j^{\pm} + 1).$$

Из предыдущих соотношений следует, что $l^{\pm} \leqslant s^{\pm}$.

Теорема 7. *Для любого многочлена $P \in \Bbbk[z]$ имеет место следующая цепочка неравенств*:

$$0 \leqslant l^+ + l^- \leqslant s^+ + s^- \leqslant m^+ + m^- - (n+1),$$

причём P является обобщённым многочленом Чебышёва тогда и только тогда, когда $s^+ + s^- = m^+ + m^- - (n+1)$.

Доказательство. Имеем

$$\begin{aligned} s^+ + s^- &= \sum_{j=1}^{m^+} (k_j^+ - v_j^+ + 1) + \sum_{j=1}^{m^-} (k_j^- - v_j^- + 1) = \\ &= \left(\sum_{j=1}^{m^+} k_j^+ + \sum_{j=1}^{m^-} k_j^- \right) + m^+ + m^- - 2n \leqslant \\ &\leqslant \deg(P') + m^+ + m^- - 2n = m^+ + m^- - (n+1), \end{aligned}$$

причём равенство достигается тогда и только тогда, когда все корни P' являются корнями $P - c^{\pm}$, т. е. P является обобщённым многочленом Чебышёва. □

Следствие 2. *Если для некоторого набора кратностей*

$$l^+ + l^- > m^+ + m^- - (n+1),$$

то этот набор кратностей нереализуем для всех $\Bbbk$*, таких что* $\operatorname{char}\Bbbk = p$.

Есть примеры, когда для набора $v_j^\pm$ неравенство

$$l^+ + l^- \leqslant m^+ + m^- - (n+1)$$

выполнено, но набору $v_j^\pm$ не соответствует никакой обобщённый многочлен Чебышёва. Эти примеры могут быть построены при помощи следующей теоремы.

Теорема 8. *Пусть* $l^+ = 1$, $l^- = 0$, $m^+ + m^- - (n+1) \vdots p$ *(т. е. среди набора чисел* $v_j^\pm$ *ровно одно делится на* p *и общее количество вершин имеет тот же остаток от деления на* p*, что и* $n+1$*). Тогда набор* $v_j^\pm$ *нереализуем.*

Доказательство. Пусть $v_0^+ \vdots p$. Тогда $k_j^\pm = v_j^\pm - 1$ для каждого $j \geqslant 1$. Имеем

$$n-1 = \sum_{j=1}^{m^+}(k_j^\pm) + \sum_{j=1}^{m^-}(k_j^\pm) = k_0^+ - v_0^+ + 1 + \sum_{j=1}^{m^+}(v_j^+ - 1) + \sum_{j=1}^{m^-}(v_j^- - 1) = \\ = k_0^+ - v_0^+ + 1 + n - m^+ + n - m^-,$$

откуда

$$k_0^+ = v_0 - 1 + (m^+ + m^- - (n+1)) \equiv -1 \pmod p.$$

Но у $\frac{dP}{dx}$ все коэффициенты при x^{kp-1} (k целое) равны 0, откуда у P' не может быть корней кратности k, если $k \equiv -1 \pmod p$. □

Пример 4. Если $p = 3$, $v_j^\pm = [3, 1^3 \parallel 1^6]$, то условия теоремы 8 выполнены, а значит, этот набор кратностей нереализуем.

2.6. Примеры, когда не существует бесконечно много обобщённых многочленов Чебышёва с данным набором кратностей

Пример 5. Рассмотрим набор кратностей $[3, 1, 1 \parallel 2, 1, 1, 1]$ (для удобства будем записывать его так: $[3, 1^2 \parallel 2, 1^3]$).

Заметим, что если некоторый многочлен P степени 5 с коэффициентами из $\bar{\mathbb{F}}_3$ представляется в виде $P - c^+ = (x-A)^3 Q_1(x)$, $P - c^- = (x-B)^2 Q_2(x)$, где $c^+ \neq c^-$ и A не является корнем Q_1, то P является обобщённым многочленом Чебышёва и многочлены Q_1, Q_2 не имеют кратных корней. Действительно, $l^+ + l^- \geqslant 1$, $m^+ \leqslant 3$, $m^- \leqslant 4$ и $m^+ + m^- - (n+1) \leqslant 1$, следовательно, $l^+ + l^- = s^+ + s^- = m^+ + m^- - (n+1) = 1$ и P является обобщённым многочленом Чебышёва, $m^+ = 3$, $m^- = 4$, т. е. Q_1, Q_2 не имеют кратных корней. Оказывается, что этому набору соответствует целое семейство обобщённых многочленов Чебышёва $P_u(x) = x^3((x-1)^2 + u)$, $P_u(x) - u = (x-1)^2(x^3 + u(x-1))$,

где $u \neq 0$, $u \neq -1$. При любых $u_1 \neq u_2$ соответствующие многочлены не эквивалентны друг другу.

Приведём другие примеры неединственности обобщённого многочлена Чебышёва.

Пример 6. Для $v_j^{\pm} = [3^2, 1 \parallel 1^7]$ имеем $P_u(x) = (x-1)^3(x+1)^3(x-u)$, $u \neq \pm 1$, $P_u \sim P_w$ при $u = -w$.

Пример 7. Для $v_j^{\pm} = [3, 2, 1^2 \parallel 2^2, 1^3]$ имеем $P_u(x) = (x-1)^3x^2(x^2+2u^2x+u)$.

Пример 8. Для $v_j^{\pm} = [3, 1^3 \parallel 3, 1^3]$ имеем $P_{u,v}(x) - c^{\pm} = (z \mp 1)^3((z \pm 1)^4 + + (u \mp 1)x^3 + (v \pm u))$, $c^- = v + 1$, $c^+ = v - 1$.

3. Теоремы о редукции

Пусть $\Bbbk$ — алгебраически замкнутое поле, $\mathcal{O} \subset \Bbbk$ — коммутативное кольцо без делителей нуля, F — алгебраическое замыкание поля частных кольца $\mathcal{O}$.

Определение 5. Рациональная функция β называется функцией Белого над $\mathcal{O}$, если β — функция Белого над F, а коэффициенты β и критические значения лежат в $\mathcal{O}$.

Очевидно, что любой обобщённый многочлен Чебышёва является также обобщённым многочленом Чебышёва над кольцом целых своего поля определения.

Теорема 9. *Пусть $\beta = \frac{P}{Q}$ — функция Белого над $\mathcal{O}$, $\operatorname{char}\Bbbk = 0$, $\wp \lhd \mathcal{O}$ — простой идеал, $P(z) = \sum\limits_{k=0}^{n} a_k z^k$, $Q(z) = \sum\limits_{k=0}^{s} b_k z^k$. Пусть выполнены следующие условия*:

1) $n = \deg(\beta) \notin \wp$;
2) $\deg\left(\frac{P \bmod \wp}{Q \bmod \wp}\right) = \deg\beta$;
3) $c^+ - c^- \notin \wp$.

Тогда рациональная функция $\beta \bmod \wp = \frac{P \bmod \wp}{Q \bmod \wp}$ является регулярной функцией Белого над алгебраическим замыканием поля частных кольца $\mathcal{O}/\wp$, а также совпадают наборы кратностей функций β и $\beta \bmod \wp$.

Доказательство. Из того, что $\operatorname{char}\Bbbk = 0$, по теореме 2 следует, что β — регулярная функция Белого, т. е. $m^+ + m^- + m^\infty = n+2$ (условие 5). При редукции корни могут только сливаться, поэтому $m_p^+ \leqslant m^+$, $4m_p^- \leqslant m^-$, $m_p^\infty \leqslant m^\infty$, где числа $m_p^\pm$, m_p^∞ определяются аналогично числам $m^\pm$, m^∞ для рациональной функции $\frac{P \bmod \wp}{Q \bmod \wp}$ (заметим, что степень β при редукции не падает и критические значения не сливаются). Поэтому $m_p^+ + m_p^- + m_p^\infty \leqslant n+2$. Но согласно следствию 1 $m_p^+ + m_p^- + m_p^\infty \geqslant n+2$. Итак, $m_p^+ + m_p^- + m_p^\infty = n+2$. Поэтому $\beta \bmod \wp$ — регулярная функция Белого и набор кратностей у неё такой же, как у функции β. □

3.1. Теорема о редукции для многочленов

Теорема 10. *Пусть* $Q(z) = \sum\limits_{k=0}^{n} a_k z^k$ *является обобщённым многочленом Чебышёва над* $\mathcal{O}$, $\operatorname{char}\Bbbk = 0$, $\wp \lhd \mathcal{O}$ *— простой идеал. Пусть выполнены следующие условия*:

1) $n = \deg(Q) \notin \wp$;
2) $a_n \notin \wp$;
3) $c^+ - c^- \notin \wp$.

Тогда многочлен $Q \bmod \wp$ *является обобщённым многочленом Чебышёва над алгебраическим замыканием поля частных кольца* $\mathcal{O}/\wp$, *причём многочлену* $Q \bmod \wp$ *соответствует тот же набор кратностей, что и многочлену* Q.

Теорема 11. *Рассмотрим два многочлена* Q_1 *и* Q_2, *которые являются многочленами над* $\mathcal{O}$, *соответствуют одному и тому же набору кратностей и удовлетворяют условию теоремы* 10, *а также являются эквивалентными, т. е.*

$$Q_1(z) = AQ_2(az + b) + B,$$

где $A, b, a, B \in \Bbbk$, $a \neq 0$, $A \neq 0$. *Тогда* $Q_1 \bmod \wp$ *и* $Q_2 \bmod \wp$ *эквивалентны, т. е.*

$$(Q_1 \bmod \wp)(z) = A_p(Q_2 \bmod \wp)(a_p z + b_p) + B_p$$

для некоторых $A_p, B_p, a_p, b_p \in \mathcal{O}/\wp$, *причём* $A_p \neq 0$, $a_p \neq 0$.

Доказательство. Существуют такие $A, B, a, b \in F$, что

$$Q_1(z) = AQ_2(az + b) + B.$$

Докажем, что это равенство можно редуцировать (знаменатели A, B, a, b не лежат в $\wp$). Очевидно, что для критических значений выполнено $c_1^{\pm} = Ac_2^{\pm} + B$. Следовательно, $c_1^+ - c_1^- = A(c_2^+ - c_2^-)$. Но $c_i^+ - c_i^-$ целое и не лежит в $\wp$, поэтому $v_\wp(A) = 0$, т. е. A можно редуцировать и получить ненулевое число.

Теперь рассмотрим a. Старшие коэффициенты у многочленов такие: $(a_1)_n = A((a_2)_n)a^n$. Отсюда $v_\wp(a) = 0$.

Критические значение целые, поэтому $v_\wp(B) \geqslant 0$.

Докажем, что $v_\wp(b) \geqslant 0$. Пусть $b = dp^{-k}$, где $v_\wp(d) = 0$, а $p \in \wp$. Тогда свободный член многочлена Q_1 будет равен $\sum\limits_{j=0}^{n} b^j (a_2)_j + B$. Это выражение должно лежать в $\mathcal{O}$, поэтому если его умножить на p^{kn}, то оно должно лежать в $\wp$. Все коэффициенты $(a_2)_j$ целые, поэтому при всех $j < n$ выражение $b^j (a_2)_j p^{kn}$ лежит в $\wp$. Из того, что $B \in \mathcal{O}$, заключаем, что $b^n p^{kn} (a_2)_n$ лежит в $\wp$. Но $(a_2)_n$ не лежит в $\wp$ по условию теоремы 10, а $b^n p^{kn}$ по предположению. Противоречие. Тогда $v_\wp(b) \geqslant 0$.

Итак, все числа A, B, a, b можно редуцировать по модулю $\wp$. Кроме того, A и a при редукции дадут ненулевые числа. Теорема 11 доказана. □

Теорема 12. *Пусть обобщённые многочлены Чебышёва $Q_1, Q_2 \in \mathcal{O}[z]$ эквивалентны, Q_2 удовлетворяет условиям теоремы* 10*, Q_1 удовлетворяет всем условиям, кроме условия* 3*). Тогда $Q_1 \bmod \wp = \mathrm{const}$.*

Доказательство. Имеем

$$Q_1(z) = AQ_2(az + b) + B.$$

Как и в доказательстве теоремы 11, получим, что $v_\wp(A) = 0$, но в этом случае $v_\wp(a) > 0$, поэтому при редукции Q_1 по $\wp$ получается константа. □

Теорема 13. *Пусть многочлен $Q = \sum\limits_{k=0}^{n} a_k z^k$ удовлетворяет всем условиям теоремы* 10*, кроме условия* 2*), причём найдётся $j > 0$, для которого $v_\wp(a_j) < j$. Тогда нет ни одного многочлена, эквивалентного Q, который удовлетворял бы всем условиям теоремы* 10*.*

Доказательство. Пусть существует многочлен Q_2, удовлетворяющий условиям теоремы 10, такой что

$$Q(z) = AQ_2(az + b) + B.$$

Как и в доказательствах предыдущих теорем, можно получить, что $v_\wp(A) = 0$, $v_\wp(B) \geqslant 0$, $v_\wp(a) \geqslant 0$, $v_\wp(b) \geqslant 0$. Поскольку a_n делится на p, то $v_\wp(a) \geqslant 1$. Следовательно, при всех j элемент a_j лежит в $\wp^j$. □

Используя теоремы о редукции, можно получить список простых плохой редукции для валентностей вершин, которым соответствуют обобщённые многочлены Чебышёва с целыми коэффициентами, как будет показано в следующем разделе.

3.2. Редукция, когда степень многочлена делится на характеристику поля

Теорема 14. *Пусть $Q(z) = \sum\limits_{k=0}^{n} a_k z^k$ является обобщённым многочленом Чебышёва над $\mathcal{O}$, $\wp \lhd \mathcal{O}$ — простой идеал. Пусть выполнены следующие условия*:

1) $n = \deg(Q) \in \wp$;
2) $a_n \notin \wp$;
3) $c^+ - c^- \notin \wp$.

Тогда $d(Q \bmod \wp)/dz \equiv 0$.

Доказательство. То, что Q — обобщённый многочлен Чебышёва над $\mathcal{O}$, эквивалентно тому, что найдутся $k \in \mathcal{O}$, $k^+, k^- \in \mathbb{N}$, такие что

$$\mathrm{Discr}(Q - c) = k(c - c^+)^{k^+}(c - c^-)^{k^-}$$

(равенство многочленов от c).

Возьмём редукцию этого равенства по $\wp$ (так как слева и справа находятся многочлены с коэффициентами из $\mathcal{O}$, то это возможно). Получим

$$\mathrm{Discr}(Q \bmod \wp - c) = (k \bmod \wp)(c - (c^+ \bmod \wp))^{k^+}(c - (c^- \bmod \wp))^{k^-}.$$

Но дискриминант равен определителю $((2n-1) \times (2n-1))$-матрицы, составленной из коэффициентов многочлена $Q \bmod \wp$ и его производной. Старший коэффициент у многочлена $(Q \bmod \wp - c)$ (т. е. коэффициент при c^{n-1}) равен $\pm(na_n)^n$. Поэтому он равен 0 и $k \bmod \wp = 0$. Тогда $\mathrm{Discr}(Q \bmod \wp - c) = 0$ и $d(Q \bmod \wp)/dz = 0$. Теорема доказана. □

Следствие 3. *Пусть P — обобщённый многочлен Чебышёва над $\mathcal{O}$, $\deg P = p$ — простое число и $p\mathbb{Z} \lhd \mathcal{O}$ — простой идеал. Тогда при редукции P по $p\mathbb{Z}$ получается многочлен вида*

$$P(z) = A(az + b)^p + B,$$

где $A, a, b, B \in \bar{\mathbb{F}}_p$, $a \neq 0$, $A \neq 0$.

4. Простые плохой редукции

4.1. Определение простых плохой редукции

Дадим центральное определение данной статьи — определение простых плохой редукции. Особенность данного определения состоит в том, что простые плохой редукции определяются не для обобщённого многочлена Чебышёва, а для набора валентностей. Такое определение даёт возможность говорить о простых плохой редукции, не вычисляя непосредственно обобщённого многочлена Чебышёва.

Определение 6. Простое число p называется простым плохой редукции для набора валентностей $v_j^{\pm}$, если в $\bar{\mathbb{F}}_p$ нет ни одного обобщённого многочлена Чебышёва P с критическими значениями $c^{\pm}$, такого что

$$P(x) - c^{\pm} = \prod_i (x - A_i^{\pm})^{v_j^{\pm}},$$

где $A_i^{\pm}$ — набор попарно различных чисел из $\bar{F}_p$.

4.2. Простые плохой редукции для цепочек

Найдём простые плохой редукции для набора кратностей, которые являются валентностями цепочки из n звеньев. Цепочка — дерево с набором валентностей $[2, 2, \ldots, 2, 1 \parallel 2, 2, \ldots, 2, 1]$ или $[2, 2, \ldots, 2, 1, 1 \parallel 2, 2, \ldots, 2, 2]$. Его обобщённым многочленом Чебышёва является многочлен Чебышёва $T_n(z) = \cos(n \arccos z)$.

Теорема 15. *Пусть $n > 1$, тогда множество простых плохой редукции для цепочки из n звеньев состоит из двойки и всех делителей n.*

Доказательство. Из теоремы 2 следует, что все эти простые являются простыми плохой редукции (как делители степени многочлена и делители валентностей вершин). Докажем, что других нет. T_n — многочлен с целыми коэффициентами и с целыми критическими значениями, поэтому он является обобщённым многочленом Чебышёва над $\mathbb{Z}$. Возьмём простое p, не равное 2 и не являющееся делителем n. Убедимся, что выполнены условия теоремы 10:

1) $n = \deg T_n \not\vdots p$ из условий;
2) $a_n \not\vdots p$, так как $a_n = 2^{n-1}$;
3) $c^+ - c^- \not\vdots p$, так как $c^+ = 1$, $c^- = -1$.

Таким образом, теорема 10 применима, и p не является простым плохой редукции. □

4.3. Простые плохой редукции для деревьев диаметра 3

Из формулы

$$P(z) = (1-z)^a \sum_{k=0}^{b-1} \binom{a+k-1}{k} z^k,$$

доказанной в разделе 2.1, следует, что простые плохой редукции — это такие p, что $n = a+b-1 \vdots p$ или $\binom{a+b-2}{a-1} \vdots p$.

Определение 7. Назовём набор валентностей $v_j^{\pm}$, где $v_j^{\pm} > 0$, $\sum\limits_{j=1}^{m^+} v_j^+ = \sum\limits_{j=1}^{m^-} v_j^- = n$, регулярным, если $m^+ + m^- = n+1$.

Определение 8. Обобщённый многочлен Чебышёва называется регулярным, если ему соответствует регулярный набор валентностей.

Определение 9. Многочлен с одним критическим значением будем называть ежом.

Утверждение 3. *Существуют нерегулярные ежи.*

Утверждение 4. *Все регулярные ежи имеют вид* $P_n(z) = A(az+b)^n + B$, *где* $A, a, b, B \in \bar{\mathbb{F}}_p$, $a \neq 0$, $A \neq 0$.

См. примеры 2 и 3.

Определение 10. Многочлен с одной критической точкой будем называть псевдорегулярным ежом, или, что эквивалентно, псевдорегулярный ёж — ёж с не более чем одной вершиной валентности, большей единицы.

Утверждение 5. *Все псевдорегулярные ежи имеют вид* $P(z) = A(az+b)^n + B(z)$, *где* $A, a, b \in \bar{\mathbb{F}}_p$, $A \neq 0$, $a \neq 0$, $B \in \bar{\mathbb{F}}_p[z]$, $\deg B < n$, $\frac{dB}{dz} = 0$.

Рассмотрим деревья Ш_{ab} ($a > 1$, $b > 1$) и простое p, где p не делит $n = a+b-1$. Для набора валентностей, соответствующих дереву диаметру 3, построим обобщённый многочлен Чебышёва Q_{ab} над $\mathbb{Z}$ со старшим коэффициентом, равным 1.

Определение 11. Назовём p простым очень плохой редукции, если $Q_{ab} \bmod p$ является регулярным ежом.

Такое определение было впервые приведено в [2].

Теорема 16. *Число p является простым плохой редукции тогда и только тогда, когда $Q_{ab} \bmod p$ является ежом (не обязательно регулярным).*

Доказательство. Пусть p не является простым плохой редукции, тогда $Q_{ab} \bmod p$ — обобщённый многочлен Чебышёва по теореме 10, причём с тем же самым набором кратностей, поэтому он не является ежом. Пусть p — простое плохой редукции. Из построения Q_{ab} следует, что в теореме 10 выполнены все условия, кроме $c^+ - c^- \not\vdots p$. Рассмотрим разложение

$$\operatorname{Discr}(Q - c) = K(c - c^-)^{k^-}(c - c^+)^{k^+}.$$

После редукции по модулю p получим

$$\operatorname{Discr}((Q \bmod p) - c) = K(c - c^+)^{n-1},$$

т. е. $Q \bmod p$ является ежом. □

Следствие 4. *Простые очень плохой редукции являются простыми плохой редукции.*

Теорема 17. *Число p является простым плохой редукции тогда и только тогда, когда $Q_{ab} \bmod p$ является псевдорегулярным ежом.*

Доказательство. Пусть p — простое плохой редукции. Поместим вершину валентности a в 0, пусть вершина валентности b попала в q. Из построения Q следует, что q целое. Докажем, что $q \bmod p = 0$. Действительно, иначе у $Q_{ab} \bmod p - c^+$ есть один корень кратности как минимум a, другой корень кратности как минимум b, но этого не бывает, так как его степень $a + b - 1$ ($c^+ - c^- \vdots p$ из-за того, что p — простое плохой редукции). Следовательно, две критические точки при редукции по модулю p совпадут, поэтому у $Q_{ab} \bmod p$ есть только одна критическая точка. Следовательно, $Q_{ab} \bmod p$ — псевдорегулярный ёж. □

4.4. Простые плохой редукции для деревьев диаметра 4

Теорема 18. *Рассмотрим деревья диаметра 4 центральной валентности s, у которых центральная вершина находится в точке 0, боковые валентности $a_1, a_2, \ldots a_s$, координаты боковых вершин $A_1, A_2, \ldots, A_s$. Пусть p — простое число и $p^m < s \leqslant p^{m+1}$. Тогда если для всех $1 \leqslant i \leqslant s$ справедливо $a_i = b_i \pmod{p^{m+1}}$, то координаты вершин для деревьев $\mathrm{IV}_{s;a_1,a_2,\ldots,a_s}$ и $\mathrm{IV}_{s;b_1,b_2,\ldots,b_s}$, посчитанные в $\bar{\mathbb{F}}_p$, совпадают.*

Доказательство. Рассмотрим систему уравнений на A_i, полученную из того, что у многочлена $\prod_{i=1}^{s}(z - A_i)^{a_i}$ коэффициенты при $z, z^2, \ldots, z^{s-1}$ равны нулю.

В эти уравнения a_i входят только как $\binom{a_i}{r}$, где $0 \leqslant r \leqslant s-1$. Но из того, что $r < p^{m+1}$, следует, что $\binom{a_i}{r} = \binom{b_i}{r} \pmod p$. Поэтому системы уравнений на вершины совпадают по модулю p, откуда координаты вершин равны. □

Следствие 5. *В условиях теоремы* 18 *p — простое плохой редукции для $\mathrm{IV}_{s;a_1,a_2,\ldots,a_s}$ тогда и только тогда, когда p — простое плохой редукции для дерева $\mathrm{IV}_{s;b_1,b_2,\ldots,b_s}$.*

Литература

[1] Вашевник А. М. К определению обобщённых многочленов Чебышёва над конечными полями // Функцион. анализ и его прил. — 2001. — № 3.

[2] Золотарская В. Неопубликованная работа.

[3] Кочетков Ю. Ю. Антивандермондовы системы и плоские деревья // Функцион. анализ и его прил. — 2002. — Т. 36.

[4] Grothendieck A. Esquisse d'un programme // Geometric Galois Actions. — Cambridge Univ. Press, 1977. — London Math. Society, Lecture Notes Series, vol. 243. — P. 3—43.

[5] Shabat G., Voevodsky V. Drawing curves over number fields // The Grothendieck Festschrift. Vol. 3. — Birkhäuser, 1990. — P. 199—227.

[6] Shabat G., Zvonkin A. Plane trees and algebraic numbers // Contemp. Math. — 1994. — Vol. 178. — P. 233—275.

[7] Wewers S. Three point covers with bad reduction // J. Amer. Math. Soc. — 2003. — Vol. 16. — P. 991—1032.