МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
Балтийский федеральный университет имени Иммануила Канта
(БФУ им. И.Канта)

Институт физико-математических наук и информационных технологий

ВКР допущена к защите
Первый заместитель директора Института физико-математических наук и информационнах технологий, к.ф.-м.н., доцент
_____ Шпилевой А.А.
“____” _____2017 г.

Выпускная квалификационная работа

на тему: «Исследование свойств первых ступеней башни функциональных полей Гарсии – Штихтенота и свойств соответствующих алгеброгеометрических кодов»

ВКР защищена на оценку:
_____

Студент 6 курса
специальности «Компьютерная безопасность»
_____ Н.С. Колесников

Руководитель
К.т.н., доцент Института физико-математических наук и информационных технологий
_____ С.И. Алешников

Рецензент
Директор ООО «ТехникСервис»
_____ С.М. Колесников

Калининград
2018

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Как известно из фундаментальных работ К. Шеннона, одной из основных задач теории кодирования является построение эффективных кодов для передачи информации по зашумлённым каналам связи. Под словом «эффективные» мы будем подразумевать избыточные коды, исправляющие максимальное число ошибок, и при этом обладающие максимально возможной скоростью передачи информации.

На данный момент разработано много разных алгоритмов, позволяющих строить эффективные коды, исправляющие ошибки. Одним из первых, бинарный код Хэмминга, был предложен Ричардом Хэммингом в 1947 г. Сообщения из двоичного алфавита $\mathbb{F}_2$ разбиваются на блоки фиксированной длины и кодируются независимо друг от друга. При этом к каждому блоку добавляется несколько дополнительных проверочных символов, позволяющих выполнить коррекцию одной и обнаружение двух ошибок при декодировании. Позже было представлено семейство циклических кодов, частными случаями которых являются коды Рида – Соломона, коды БЧХ. Большой интерес представляет семейство линейных алгеброгеометрических кодов (АГ-кодов), предложенных В.Д. Гоппой [11] в 1970 г. Конструкция этих кодов использует методы алгебраической геометрии, и свойства зависят от первоначального выбора алгебраической кривой.

Оценки основных параметров эффективности АГ-кодов Гоппы связаны с числом точек функционального поля, соответствующего выбранной кривой. Это число удовлетворяет границе Хассе – Вейля

$$N \leq 1 + q + 2g\sqrt{q} \tag{1}$$

где $g = g(F)$ – род функционального поля, $\mathbb{F}_q$ – поле констант.

Однако в случае, если род поля $g(F)$ значительно превышает q, В.Г. Дринфельд и С.Г. Влэдуц в [1] показали, что граница Хассе – Вейля может быть улучшена, если рассмотреть предел отношения

$$A(q) \coloneqq \lim_{g\to\infty} Sup \frac{N_q(g)}{g} \tag{2}$$

где $N_q(g) \coloneqq max\{N(F)\colon F/\mathbb{F}_q - \text{функц. поле рода } g\}$.

В этом случае выполняется граница Дринфельда – Влэдуца:

$$A(q) \leq \sqrt{q} - 1 \tag{3}$$

Естественным образом возникает необходимость построения функциональных полей большого рода, достигающих границы Дринфельда – Влэдуца (3). С этой целью строят башни функциональных полей – последовательности алгебраических расширений изначально фиксированного функционального поля, и затем исследуют асимптотические свойства этой башни.

В 1995 г. А.Гарсиа и Х.Штихтенот предложили [9] рассмотреть башню функциональных полей $T = (T_1, T_2, \dots, T_n, \dots)$ над конечным полем $\mathbb{F}_{p^2}$ (p – простое число), задаваемую простым рекуррентным уравнением

$$x_{i+1}^p + x_{i+1} = \frac{x_i^{p+1}}{x_i^p + x_i} \tag{4}$$

где $T_1 \coloneqq \mathbb{F}_{p^2}(x_1)$ – рациональное функциональное поле, а для $i \geq 1$: $T_{i+1} \coloneqq T_i(x_{i+1})$.

Доказано, что построенная башня T является асимптотически оптимальной, и, таким образом, подходит для построения семейства АГ-кодов с хорошими асимптотическими характеристиками. Более того, согласно исследованиям А.И. Зайцева [18], из башни T можно построить другую башню $\tilde{T} = (\tilde{T}_1, \tilde{T}_2, \dots, \tilde{T}_n, \dots)$, в которой каждое расширение $\tilde{T}_n/\tilde{T}_1$ – оболочка Галуа расши-

рения T_n/T_1. Башня $\tilde{T}$ называется оболочкой Галуа башни T. Известно, что $\tilde{T}$ тоже является асимптотически оптимальной башней, однако род $g(\tilde{T}_n)$ растет быстрее, чем $g(T_n)$. Это дает возможность предположить, что уже на младших ступенях башни $\tilde{T}$ можно построить код с лучшими параметрами, чем на соответствующих ступенях башни T.

Целью настоящей работы является явное построение АГ-кодов на младших ступенях T_2 и T_3 башни T, исследование свойств построенных кодов, а также исследование свойств младших ступеней башни $\tilde{T}$ с целью переноса конструкции АГ-кода на башню $\tilde{T}$.

Для достижения указанной цели необходимо решить следующие **задачи**:

1. Определить род полей $g(T_2)$, $g(T_3)$, дифференты расширений T_2/T_1, T_3/T_2;
2. Определить картину ветвления точек в расширениях функциональных полей, перечислить все рациональные точки;
3. Построить базисы пространств Римана – Роха $L(lP_\infty) \subset T_2$ для произвольных достаточно больших $l \geq 2g(T_2) - 1$;
4. Реализовать в виде программы алгоритмы кодирования и декодирования;
5. Определить параметры кода, который можно построить на ступенях башни T_2 или T_3;
6. Определить минимальные многочлены порождающих элементов на каждой ступени $\tilde{T}_n$ башни $\tilde{T}$, определить картину ветвления точек.

ГЛАВА 1. ПРЕДВАРИТЕЛЬНЫЕ СВЕДЕНИЯ О ФУНКЦИОНАЛЬНЫХ ПОЛЯХ

1.1 Функциональные поля

Теория функциональных полей позволяет переносить структуру алгебраических кривых в чисто алгебраическую конструкцию и исследовать ее более элементарными математическими средствами. Так, всякой кривой соответствует некоторое функциональное поле, на которое естественным образом переносятся понятия точек и дивизоров. В этом разделе мы кратко приведем факты из теории функциональных полей, необходимые для построения АГ-кодов.

1.1.1 Определение. Пусть k – поле. *Алгебраическим функциональным полем* F/k от одной переменной над k называется любое поле $F \supseteq k$, являющееся алгебраическим расширением поля $k(x)$ конечной степени, где x – элемент поля F, трансцендентный над k. Множество элементов поля F, алгебраических над k, называется *полем констант* и обозначается $\tilde{k}$. При этом $k \subseteq \tilde{k} \subset F$. Если поле k алгебраически замкнуто в F, т.е. $k = \tilde{k}$, то k называют *полным полем констант*.

1.1.2 Определение. Кольцом нормирования функционального поля F/k называется такое собственное подкольцо $\mathcal{O} \subset F$, что $k \subset \mathcal{O}$ и $\forall f \in F$ хотя бы один из элементов f, f^{-1} лежит в $\mathcal{O}$.

1.1.3 Предложение (Свойства колец нормирования).

(а) Кольцо $\mathcal{O}$ локально, т.е. оно обладает единственным максимальным идеалом P, причем $P = \mathcal{O} \setminus \mathcal{O}^*$;

(б) Если $f \in F$ $(f \neq 0)$, то $f \in P \Leftrightarrow f^{-1} \notin \mathcal{O}$;

(в) $\tilde{k} \subseteq \mathcal{O}$ и $\tilde{k} \cap P = \{0\}$;

(г) P – главный идеал;

(д) Пусть $P = t\mathcal{O}$, тогда любой ненулевой элемент $f \in F$ единственным образом представляется в виде $f = t^n u$, где $n \in \mathbb{Z}$, $u \in \mathcal{O}^*$;

(е) $\mathcal{O}$ является кольцом главных идеалов, а именно, если $I \subset \mathcal{O}$ – нетривиальный собственный идеал, и $P = t\mathcal{O}$, то $I = t^n\mathcal{O}$ для некоторого $n \in \mathbb{N}$.

1.1.4 Определение. Идеал $P = t\mathcal{O}$ некоторого кольца нормирования $\mathcal{O} \subset F$ называется *точкой* поля F/k. При этом образующая идеала $t \in F$ называется *локальным (униформизующим) параметром* точки P. Кроме того, само кольцо $\mathcal{O}$ однозначно определяется своим максимальным идеалом P, и называется *кольцом нормирования точки* P, обозначается $\mathcal{O}_P := \mathcal{O}$. Множество всех точек функционального поля F будем обозначать $\mathbb{P}_F$.

1.1.5 Определение. *Дискретным нормированием* функционального поля F/k называется функция

$$v: F \to \mathbb{Z} \cup \{\infty\}, \tag{5}$$

обладающая следующими свойствами:

(а) $v(x \cdot y) = v(x) + v(y)$ для любых элементов $x, y \in F$;

(б) $v(x + y) \geq \min\{v(x), v(y)\}$ для любых $x, y \in F$, причем равенство достигается тогда и только тогда, когда $v(x) \neq v(y)$;

(в) $v(x) = \infty \Leftrightarrow x = 0$;

(г) $v(x) = 0 \quad \forall x \in k \setminus \{0\}$;

(д) $v(t) = 1$ для некоторого элемента $t \in F$.

1.1.6 Замечание. Пусть $P = t\mathcal{O}$ – точка функционального поля F/k. Определим функцию $v_P: F \to \mathbb{Z} \cup \{\infty\}$ следующим образом. Согласно п. 1.1.3 (г), любой ненулевой элемент $f \in F$ записывается в виде $f = t^n u$. Положим $v_P(f) = n$, $v_P(0) = \infty$. Можно доказать [16, с.5], что построенная таким образом функция v_P отвечает требованиям определения 1.1.5, и, следовательно, является дискретным нормированием. Она называется *дискретным нормированием, ассоциированным с точкой* $P \in \mathbb{P}_F$. Следует отметить, что дискретное нор-

мирование v_P не зависит от выбора локального параметра $t \in F$ точки P. Существует взаимно однозначное соответствие между дискретными нормированиями, точками и кольцами нормирования функционального поля F/k [16, с.6].

1.1.7 Определение. Пусть P – точка функционального поля F/k. Поле $F_P \coloneqq \mathcal{O}_P/P$ называется *полем классов вычетов точки* P. Оно является конечным расширением поля k, причем степень расширения $[F_P : k] = \deg(P)$ называется *степенью точки* P. Для элемента $f \in \mathcal{O}_P$ обозначим $f(P) \coloneqq f + P \in F_P$ – его класс вычетов по модулю P. Для $f \in F \backslash \mathcal{O}_P$ положим по определению $f(P) = \infty$. Таким образом, имеем отображение

$$\pi_P : \begin{cases} F \to F_P \cup \{\infty\} \\ f \mapsto f(P) \end{cases} \tag{6}$$

Образ элемента f при отображении π_P называется его *значением в точке* P, а элементы $f \in \mathcal{O}_P$ называются *регулярными в точке* P. Таким образом, элементы функционального поля иногда называют функциями [2, с.176].

1.1.7 Определение. Дивизором функционального поля F/k называется конечная формальная сумма точек

$$D = \sum_P n_P \cdot P, \tag{7}$$

Перечислим основные характеристики дивизоров:

— Носитель дивизора $Supp(D) \coloneqq \{P \mid n_P \neq 0\} \subset \mathbb{P}_F$.

— Степень дивизора $\deg(D) \coloneqq \sum_P n_P \cdot \deg(P)$.

1.1.8 Определение. Главным дивизором элемента $f \in F$ называется дивизор

$$(f) = \sum_P v_P(f) \cdot P, \tag{8}$$

где $v_P(f)$ – дискретное нормирование, ассоциированное с точкой P. Такой дивизор определен корректно, т.к. f может иметь лишь конечное число нулей ($v_P(f) > 0$) и полюсов ($v_P(f) < 0$) [16, с.15]. В остальных точках P нормирование $v_P(f) = 0$.

1.1.9 Определение. *Пространством Римана – Роха* дивизора $D \in Div_F$ называется конечномерное векторное пространство

$$L(D) \coloneqq \{f \in F\backslash\{0\} \mid (z) + D \geq 0\} \cup \{0\}. \tag{9}$$

Размерностью дивизора D называется размерность ассоциированного с ним пространства Римана-Роха: $\dim(D) = l(D) := \dim_k L(D)$.

1.1.10 Теорема (Римана). Существует целое число $g \geq 0$, зависящее только от самого функционального поля F/k, такое, что для любого дивизора $D \in Div_F$ выполняется

$$\dim(D) \geq \deg(D) + 1 - g, \tag{10}$$

причем, если степень дивизора достаточно велика, то в (10) выполняется равенство.

1.1.11 Теорема (Римана – Роха). Для любого дивизора $D \in Div_F$ выполняется

$$\dim(D) = \deg(D) + 1 - g + i(D), \tag{11}$$

где $i(D) \coloneqq \dim_k \Omega_{\mathbb{F}}(D)$ – индекс специальности дивизора (размерность ассоциированного пространства дифференциалов). Можно доказать [16, с. 31], что дивизоры степени $\deg(D) \geq 2g - 1$ являются неспециальными, т.е. $i(D) = 0$, и тогда выполняется равенство в (10).

1.1.12 Пример (Рациональное функциональное поле). Пусть k – поле, $F = k(x)$, где x – трансцендентный над k элемент. Функциональное поле F

называется *рациональным*. Перечислим основные свойства [16, с.8] рациональных функциональных полей:

(а) Каждая точка из $\mathbb{P}_{k(x)}$ соответствует неприводимому многочлену $p(x) \in k[x] \subset k(x)$ и обозначается $P_{p(x)}$. Степень точки равна степени соответствующего многочлена $p(x)$. Рациональные точки, соответствующие линейному двучлену $p(x) = x - \alpha$ будем обозначать P_α

(б) Кольцо нормирования точки и его максимальный идеал имеют вид

$$\mathcal{O}_{p(x)} = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in k[x], p(x) \nmid g(x) \right\}, \tag{12}$$

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in k[x], p(x) \nmid g(x), p(x) \mid f(x) \right\}. \tag{13}$$

(в) Значение элемента $z = \frac{f(x)}{g(x)}$ в точке P_α вычисляется как

$$z(P_\alpha) = \begin{cases} \dfrac{f(\alpha)}{g(\alpha)}, \text{если } g(\alpha) \neq 0, \\ \infty, \text{если } g(\alpha) = 0. \end{cases} \tag{14}$$

(г) Род рационального функционального поля $g(F) = 0$.

1.2 Расширения функциональных полей

1.2.1 Определение. Функциональное поле F'/k' называется расширением поля F/k, если $F \subset F'$ и $k \subset k'$.

1.2.2 Определение. Пусть $F \subset F'$ – конечное расширение функциональных полей, $P \in \mathbb{P}_F$ – точка, соответствующая локальному кольцу $\mathcal{O}_P$, и максимальному идеалу $P \subset \mathcal{O}_P$. Говорят, что точка $Q \in \mathbb{P}_{F'}$ лежит над точкой P, и пишут $Q|P$, если идеал P лежит в идеале Q.

1.2.3 Предложение. Следующие условия эквивалентны:

(а) Точка Q лежит над точкой P.

(б) $\mathcal{O}_P \subset \mathcal{O}_Q$.

(в) Существует целое число $e \geq 1$, такое, что $v_Q(f) = e \cdot v_P(f)$ для всех $f \in F$.

Если условия предложения 1.2.3 выполнены, то $P = Q \cap F$ и $\mathcal{O}_P = \mathcal{O}_Q \cap F$.

1.2.4 Определение. Будем считать, что поля констант функциональных полей F и F' совпадают. Тогда число e из п. 1.2.3 (в) называется *индексом ветвления* точки Q над точкой P. Если $e = 1$, то говорят, что точка Q неразветвлена над точкой P, а при $e > 1$ имеет место ветвление.

1.2.5 Теорема (Куммера). Приведем здесь сокращенную формулировку теоремы Куммера для исследования ветвления точек в расширениях рационального функционального поля. Полная формулировка теоремы с доказательством приводится в [16, с.86]. Пусть выполняются условия:

(а) $\varphi(T) = T^n + f_{n-1}(t)T^{n-1} + \cdots + f_0(t)$ – неприводимый многочлен над рациональным функциональным полем $F = k(t)$;

(б) $F' = k(t, y)$ – расширение функциональных полей, где $\varphi(y) = 0$;

(в) Все $f_j(t) \in \mathcal{O}_{P_\alpha}$, или, что эквивалентно, для всех констант $\alpha \in k$: $f_j(t)(P_\alpha) = f_j(\alpha) \neq \infty$. Это означает, что $\varphi(T) \in \mathcal{O}_{P_\alpha}[T]$, а элемент y – целый над $\mathcal{O}_{P_\alpha}$.

(г) $\bar{\varphi}(T) = T^n + f_{n-1}(\alpha)T^{n-1} + \cdots + f_0(\alpha) \in F_{P_\alpha}[T]$ – класс $\varphi(T)$ в поле классов вычетов точки P. Имеем разложение $\bar{\varphi}(T)$ на неприводимые унитарные попарно различные многочлены $\psi_i \in k[T]$:

$$\bar{\varphi}(T) = \prod_{i=1}^{r} \psi_i(T). \tag{15}$$

Тогда:

— существует ровно r точек $P_1, \ldots, P_r$ поля F'/k, лежащих над точкой P_α;

— $t - \alpha \in P_i$;

— $\psi_i(y) \in P_i$;

— индекс ветвления $e(P_i|P_\alpha) = 1$, следовательно, $v_{P_i}(t-\alpha) = e(P_i|P_\alpha) \cdot v_{P_\alpha}(t-\alpha) = 1$, т.е. $t-\alpha$ – общий локальный параметр точек P_i;

— Относительные степени точек $f(P_i|P_\alpha) = \deg(\psi_i(T))$.

Если, вдобавок, $\bar{\varphi}(T)$ содержит линейный множитель, например, $deg\psi_1(T) = 1$, то $k' = k$ – полное поле констант в F'.

Если, более того, $\bar{\varphi}(T)$ полностью раскладывается на линейные множители, и $\beta_i(i = 1..n)$ – все его корни, то для всякого корня $\beta \in k$ существует единственная точка $P_{\alpha,\beta}$ поля F'/k, лежащая над P_α, и этими точками исчерпываются все точки F', лежащие над P_α. Причем все точки $P_{\alpha,\beta}$ – рациональные, т.е. $\deg(P_{\alpha,\beta}) = 1$, и значения элементов t и y в этих точках

$$t(P_{\alpha,\beta}) = \alpha, \tag{16}$$

$$y(P_{\alpha,\beta}) = \beta. \tag{17}$$

1.2.6 Определение. Пусть F/k и F'/k – функциональные поля, такие, что $F \subseteq F'$ – конечное сепарабельное расширение полей. Тогда все точки $Q \in \mathbb{P}_{F'}$, кроме, быть может, конечного числа, не разветвлены в расширении F'/F. Пусть $P \in \mathbb{P}_F$, $Q \in \mathbb{P}_{F'}$, причем $Q|P$. *Показателем дифференты* называется целое неотрицательное число $d(Q|P)$, обладающее свойством

$$d(Q|P) \geq e(Q|P) - 1. \tag{18}$$

Причем равенство в (18) достигается тогда и только тогда, когда $char(k) \nmid e(Q|P)$. *Дифферентой* расширения F'/F называется дивизор

$$Diff(F'/F) = \sum_Q e(Q|P) \cdot Q. \tag{19}$$

Носитель $Supp(Diff(F'/F))$ состоит из точек $Q \in \mathbb{P}_{F'}$, разветвленных в расширении F'/F.

1.2.7 Теорема (Формула Гурвица). При построении расширений функциональных полей важно не только определять ветвления точек, но и характеристики построенного поля. В частности, для нахождения рода расширения функционального поля можно воспользоваться формулой Гурвица. Пусть F'/k' – расширение поля F/k. При этом $g \coloneqq g(F)$, $g' \coloneqq g(F')$. Тогда справедливо равенство

$$2g' - 2 = \frac{[F':F]}{[k':k]} \cdot (2g-2) + \deg\left(Diff\left(\frac{F'}{F}\right)\right). \tag{20}$$

1.3 Башни функциональных полей

1.3.1 Определение. Башней функциональных полей $\mathcal{F}$ над конечным полем $\mathbb{F}_q$ (или $\mathbb{F}_q$-башней) называется бесконечная последовательность $\mathcal{F} = (F_0, F_1, F_2, \dots)$, в которой:

(а) F_i – функциональные поля над $\mathbb{F}_q$, в любом из которых $\mathbb{F}_q$ алгебраически замкнуто;

(б) Для любого индекса n имеем включения $F_n \subseteq F_{n+1}$, причем все расширения полей F_{n+1}/F_n сепарабельны;

(в) Род функционального поля $g(F_n) \to \infty$ при $n \to \infty$.

1.3.2 Определение. Будем обозначать $N(F_i)$ – число рациональных точек функционального поля $F_i/\mathbb{F}_q$. Введем в рассмотрение числовые параметры, характеризующие башню:

(а) Предел башни $\lambda(\mathcal{F}) \coloneqq \lim\limits_{i\to\infty} \frac{N(F_i)}{g(F_i)}$;

(б) Род над функциональным полем F_1: $\gamma(\mathcal{F}) \coloneqq \lim\limits_{i\to\infty} \frac{g(F_i)}{[F_i:F_1]}$;

(в) Скорость ветвления $\nu(\mathcal{F}) \coloneqq \lim\limits_{i\to\infty} \frac{N(F_i)}{[F_i:F_1]}$.

Из формулы Гурвица (20), позволяющей вычислить род функционального поля, следует, что предел $\lambda(\mathcal{F})$ всегда существует. При этом существуют вспомогательные пределы $\gamma(\mathcal{F})$ и $\nu(\mathcal{F})$, так как $\lambda(\mathcal{F}) = \frac{\nu(\mathcal{F})}{\gamma(\mathcal{F})}$. Башня называется *асимптотически хорошей* над $\mathbb{F}_q$, если $\lambda(\mathcal{F}) > 0$.

1.3.3 Теорема. Для предела башни справедлива следующая оценка: $0 \leq \lambda(\mathcal{F}) \leq \sqrt{q} - 1$.

Доказательство (а). $\lambda(\mathcal{F}) \geq 0$ следует из определения башни и ее предела, т.к. неотрицательно число точек $N(F_i) \geq 0$ и род $g(F_i) \geq 0\ \forall i$. Башня, у которой $\lambda(\mathcal{F}) = 0$, называется *асимптотически плохой*.

(б). Неравенство $\lambda(\mathcal{F}) \leq \sqrt{q} - 1$ называется границей Дринфельда – Влэдуца, и доказано в [1] (1983). Доказательство основано на принципах, близких к методу Ихары, который годом ранее в [13] доказал более слабое неравенство $\lambda(\mathcal{F}) \leq 2\sqrt{q}$.

Башня, предел которой достигает границы Дринфельда – Влэдуца, т.е. $\lambda(\mathcal{F}) = \sqrt{q} - 1$, называется *асимптотически оптимальной*.

1.3.4 Определение. Будем говорить, что башня $\mathcal{F}$ рекурсивно задана многочленом $f(X, Y) \in \mathbb{F}_q[X, Y]$, если $F_1 = \mathbb{F}_q(x_1)$ и для любого $n \in \mathbb{N}$: $F_{n+1} \coloneqq F_n(x_{n+1})$, где $f(x_n, x_{n+1}) = 0$.

1.3.5 Определение. Пусть $\mathcal{F} = (F_0, F_1, F_2, \dots)$ – башня функциональных полей над $\mathbb{F}_q$. Говорят, что точка P *расщепляется в башне* $\mathcal{F}$, если она $\mathbb{F}_q$–рациональна и полностью расщепляется во всех расширениях F_n/F_0. Если в некоторых расширениях F_n/F_0 точка P разветвляется, то говорят, что она *разветвляется в башне* $\mathcal{F}$. Множества расщепляющихся и разветвляющихся точек башни $\mathcal{F}$ над F_0 будем обозначать соответственно так:

$$Z(\mathcal{F}/F_0) \coloneqq \{P | P \text{ расщепляется в } \mathcal{F}\},$$

$$V(\mathcal{F}/F_0) \coloneqq \{P | P \text{ разветвляется в } \mathcal{F}\}.$$

1.3.6 Пример (Башня Гарсии – Штихтенота). Для определенности здесь и далее будем рассматривать $T = (T_1, T_2, \dots, T_n, \dots)$ – башню Гарсии-Штихтенота над полем $\mathbb{F}_{p^2} = \mathbb{F}_9$ (если другое поле не уточняется). Башня задана рекуррентным уравнением (4).

В [7, с.264] и [15, с.2229] приводится вывод следующих формул рода и числа рациональных точек функционального поля $T_n/\mathbb{F}_9$ для произвольного $n \geq 1$:

$$g_n \coloneqq g(T_n) = \begin{cases} \left(p^{\frac{n}{2}} - 1\right)^2, n \equiv 0 \; mod \; 2, \\ \left(p^{\frac{n+1}{2}} - 1\right)\left(p^{\frac{n-1}{2}} - 1\right), n \equiv 1 \; mod \; 2. \end{cases} \tag{21}$$

$$N_n \coloneqq N(T_n) = p^{n-1}(p^2 - p) + 2p, \; n \geq 2, \tag{22}$$

где $N_1 = N(T_1) = p^2 + 1$ – число точек рационального функционального поля (см. пример 1.1.12).

Теперь, разбивая башню на подбашни и вычисляя соответствующие пределы, как это предложено в [7, с.266], нетрудно вычислить предел башни $\lambda(T)$ и убедиться в том, что башня является асимптотически оптимальной:

$$\lambda(T) = \lim_{i \to \infty} \frac{N(T_i)}{g(T_i)} = \sqrt{p^2} - 1 = p - 1. \tag{23}$$

ГЛАВА 2. ОСНОВНЫЕ ТЕОРЕТИЧЕСКИЕ РЕЗУЛЬТАТЫ

2.1 Картина ветвления точек и рациональные точки в T_2

2.1.1 Расширение полей T_2/T_1. Напомним, $T = (T_1, T_2, \dots, T_n, \dots)$ – башня функциональных полей Гарсии – Штихтенота над полем $\mathbb{F}_{p^2} = \mathbb{F}_{3^2}$. При этом

- $T_1 = \mathbb{F}_9(x_1)$ – рациональное функциональное поле;
- $T_2 = \mathbb{F}_9(x_1, x_2) = T_1(x_2)$, где x_2 – корень неприводимого [9, с.214] над T_1 многочлена

$$f_2 \coloneqq X^3 + X - \frac{x_1^4}{x_1^3 + x_1} \in T_1[X].$$

2.1.2 Ветвление точек. Введем следующие обозначения.

- $Tr\colon \begin{cases} \mathbb{F}_{p^2} \to \mathbb{F}_p \\ x \mapsto x^p + x \end{cases}$ – функция следа;
- $K_- \coloneqq \{\omega \in \mathbb{F}_{p^2} \mid \omega^p = -\omega\} = Ker(Tr)$.

Согласно рассуждениям из [7, с.258], точки P_∞ и $P_\alpha, \alpha \in K_-\backslash\{0\}$ – все разветвленные точки в башне T, и все они вполне разветвлены. Обозначим $Q_\infty, Q_\alpha \in \mathbb{P}_{T_2}$ – точки поля T_2, лежащие над $P_\infty, P_\alpha \in \mathbb{P}_{T_1}$ соответственно. Разветвленность этих точек в расширении означает, что $e(Q_\infty|P_\infty) = e(Q_\alpha|P_\alpha) = p = 3$. Кроме того, показатели дифференты $d(Q_\infty|P_\infty) = d(Q_\alpha|P_\alpha) = 2 \cdot (p-1) = 4$. Таким образом, дифферента расширения имеет вид

$$Diff(T_2/T_1) = 4Q_\infty + 4 \sum_{\alpha \in K_-\backslash\{0\}} Q_\alpha. \tag{24}$$

Вычислим род поля $g(T_2)$ по формуле Гурвица (20):

$$g(T_2) = 1 - [T_2\colon \mathbb{F}_9(x_1)] + \frac{1}{2} deg Diff\big(T_2/\mathbb{F}_9(x_1)\big) = 1 - 3 + \frac{12}{2} = 4. \tag{25}$$

2.1.3 Расщепление точек. Исследуем теперь точки из $\mathbb{P}_{T_2}$, лежащие над точками $P_\beta \in \mathbb{P}_{T_1}$, $\beta \notin K_-$. Применим теорему Куммера 1.2.5.

- $\varphi(T) = T^p + T - \frac{x_1^p}{x_1^{p-1}+1}$ – неприводимый многочлен над T_1;
- $T_2 = \mathbb{F}_{p^2}(x_1, x_2)$, где $\varphi(x_2) = 0$;
- Единственными полюсами рациональной функции $\frac{x_1^p}{x_1^{p-1}+1}$ являются точки P_∞ и P_α, где $\alpha \in K_- \setminus \{0\}$. Следовательно, в рассматриваемых точках P_β коэффициенты многочлена $\varphi(T)$ конечны. Иначе говоря, $\varphi(T) \in \mathcal{O}_{P_\beta}[T]$.
- $\bar{\varphi}(T) = T^p + T - \frac{\beta^{p+1}}{\beta^p+\beta} = T^p + T - \frac{2\cdot Tr(\beta^{p+1})}{Tr(\beta)}$.

В самом деле, $Tr(\beta) = \beta^p + \beta$,

$Tr(\beta^{p+1}) = \beta^{p+1} + \beta^{p^2+p} = \beta^{p+1} + \beta^{p^2} \cdot \beta^p = 2\beta^{p+1}$.

- Найдем корни $\bar{\varphi}(T)$. $\bar{\varphi}(T) = 0 \Leftrightarrow T^p + T = \frac{2\cdot Tr(\beta^{p+1})}{Tr(\beta)} \in \mathbb{F}_p$. Таким образом, если γ – корень $\bar{\varphi}(T)$, то $Tr(\gamma) = \frac{2\cdot Tr(\beta^{p+1})}{Tr(\beta)}$. По свойствам функции следа, найдется ровно p элементов $\gamma_1, \dots, \gamma_p \in \mathbb{F}_{p^2}$, имеющих один и тот же образ $Tr(\gamma_1) = \cdots = Tr(\gamma_p) = \frac{2\cdot Tr(\beta^{p+1})}{Tr(\beta)} \in \mathbb{F}_p$.

Итак, $\bar{\varphi}(T)$ имеет p различных корней $\gamma_1,\dots,\gamma_p$. Следовательно, по теореме Куммера, все точки P_β расщепляются в расширении T_2/T_1, над каждой из них лежит ровно p точек $Q_{\beta,\gamma_1},\dots, Q_{\beta,\gamma_p} \in \mathbb{P}_{T_2}$. Соответственно, индексы ветвления равны $e(Q_{\beta,\gamma_1}|P_\beta) = \cdots = e\left(Q_{\beta,\gamma_p}\middle|P_\beta\right) = 1$.

Аналогичные рассуждения проведем для точки $P_0 \in \mathbb{P}_{T_1}$:

- $\varphi(T) = T^p + T$ – неприводимый многочлен над T_1;
- $\varphi(T) \in \mathcal{O}_{P_0}[T]$, т.к. все коэффициенты многочлена $\varphi(T)$ постоянны;
- $\bar{\varphi}(T) = T^p + T = 0$;

- Очевидно, что $\bar{\varphi}(\gamma) = 0 \Leftrightarrow \gamma \in K_{-}$.

Таким образом, по теореме Куммера, точка P_0 также расщепляется в расширении T_2/T_1, и над ней лежит p точек $Q_{0,\beta} \in \mathbb{P}_{T_2}$, где $\beta \in K_{-}$. Индексы ветвления равны $e\left(Q_{0,\beta}\middle|P_0\right) = 1$.

Подсчитаем число описанных точек. В п. 2.1.2 найдено $1 + (p-1) = p$ разветвленных точек, в п. 2.1.3 найдено $p \cdot (p^2 - 3) + p = p \cdot (p^2 - 2)$ неразветвленных точек. Всего описано $p + p \cdot (p^2 - 2) = 3 + 21 = 24$ рациональных точек. Всего в поле T_2 $N(T_2) = p \cdot (p^2 - p) + 2p = 18 + 6 = 24$ рациональных точек согласно формуле (22). Таким образом, описаны все рациональные точки. Обобщенная картина ветвления представлена на [рис 1].

2.2 Картина ветвления точек и рациональные точки в T_3

2.2.1 Расширение полей T_3/T_2. В п. 2.1.1 построены первые ступени T_1 и T_2 башни T. Расширение $T_3 = T_2(x_3)$ мы получаем, присоединяя корень x_3 неприводимого над T_2 многочлена

$$f_3 \coloneqq X^3 + X - \frac{x_2^4}{x_2^3 + x_2} \in T_2[X].$$

2.2.2 Ветвление точек. Картина ветвления точек полностью аналогична описанной в п. 2.1.2. Единственными разветвленными точками являются $Q_\infty, Q_\alpha \in \mathbb{P}_{T_2}$, $\alpha \in K_{-} \setminus \{0\}$ (над ними лежат соответственно точки $R_\infty, R_\alpha \in \mathbb{P}_{T_3}$), и все эти точки вполне разветвлены. Это означает, что индексы ветвления $e(R_\infty|Q_\infty) = e(R_\alpha|Q_\alpha) = p = 3$. Показатели дифференты равны $d(R_\infty|Q_\infty) = d(R_\alpha|Q_\alpha) = 2 \cdot (p-1) = 4$. Таким образом, дифферента расширения имеет вид

$$Diff(T_3/T_2) = 4R_\infty + 4 \sum_{\alpha \in K_{-} \setminus \{0\}} R_\alpha. \tag{26}$$

Вычислим род поля $g(T_3)$ по формуле Гурвица (20):

$$g(T_3) = \frac{1}{2} \cdot \left[2 + [T_3 : T_2] \cdot (2g(T_2) - 2) + degDiff\left(T_2/\mathbb{F}_9(x_1)\right)\right] = \\ = \frac{1}{2} \cdot [2 + 3 \cdot 6 + 12] = 16. \tag{27}$$

2.2.3 Расщепление точек $Q_{\beta,\gamma}$, где $\beta \notin K_-$. В п. 2.1 мы доказали, что точками такого вида исчерпываются все рациональные точки поля T_2, за исключением уже рассмотренных $Q_\infty, Q_\alpha \in \mathbb{P}_{T_2}$, и точек вида $Q_{0,\beta} \in \mathbb{P}_{T_2}$, которые будут рассмотрены отдельно.

Покажем, что все точки $Q_{\beta,\gamma}$, где $\beta \notin K_-$ расщепляются в расширении T_3/T_2. Для этого применим теорему Куммера 1.2.5.

- $\varphi(T) = T^p + T - \frac{x_2^p}{x_2^{p-1}+1}$ – неприводимый многочлен над T_2;
- $T_3 = T_2(x_3)$, где $\varphi(x_3) = 0$;
- Единственными полюсами рациональной функции $\frac{x_2^p}{x_2^{p-1}+1}$ являются точки Q_∞ и Q_α, где $\alpha \in K_- \setminus \{0\}$. Следовательно, в рассматриваемых точках $Q_{\beta,\gamma}$ коэффициенты многочлена $\varphi(T)$ конечны. Иначе говоря, $\varphi(T) \in \mathcal{O}_{Q_{\beta,\gamma}}[T]$.
- $\bar{\varphi}(T) = T^p + T - \frac{x_2^{p+1}}{x_2^p + x_2}(Q_{\beta,\gamma}) = T^p + T - \frac{\gamma^{p+1}}{\gamma^p+\gamma} = T^p + T - \frac{2 \cdot Tr(\gamma^{p+1})}{Tr(\gamma)}$.

Следует отметить, что в случае расширения рационального функционального поля T_3/T_1 значения порождающих элементов в точках вычисляются как $x_2\left(R_{\alpha,\beta,\gamma}\right) = \beta$, $x_3\left(R_{\alpha,\beta,\gamma}\right) = \gamma$.

- Аналогично п. 2.1.3, т.к. $\frac{2 \cdot Tr(\gamma^{p+1})}{Tr(\gamma)} \in \mathbb{F}_p$, уравнение $T^p + T = \frac{2 \cdot Tr(\gamma^{p+1})}{Tr(\gamma)}$ имеет p различных корней. Обозначим их $\delta_1, \dots, \delta_p \in \mathbb{F}_{p^2}$. Следовательно, по теореме Куммера, все точки $Q_{\beta,\gamma}$ расщепляются в расширении T_3/T_2, над каждой

из них лежит ровно p точек $R_{\beta,\gamma,\delta_1},\ldots,R_{\beta,\gamma,\delta_p} \in \mathbb{P}_{T_3}$. Соответственно, индексы ветвления равны $e\left(R_{\beta,\gamma,\delta_1}\middle|Q_{\beta,\gamma}\right) = \cdots = e\left(R_{\beta,\gamma,\delta_p}\middle|Q_{\beta,\gamma}\right) = 1$.

2.2.4 Расщепление точек $Q_{0,\beta}$, где $\beta \in K_-$. Аналогично применим теорему Куммера к точкам вида $Q_{0,\beta} \in \mathbb{P}_{T_2}$.

- $\varphi(T) = T^p + T - \frac{x_2^p}{x_2^{p-1}+1}$;
- Полюсами рациональной функции $\frac{x_2^p}{x_2^{p-1}+1}$ являются точки Q_∞, а также точки Q, такие, что $\left(x_2^{p-1}+1\right)(Q) = 0$. Это точки $Q_{\alpha,\beta}$, где $\beta^{p-1}+1 = 0 \Leftrightarrow$ $\Leftrightarrow \beta \in K_- \setminus \{0\}$. Над этими точками нет рациональных точек в $\mathbb{P}_{T_3}$. Тем не менее, $\varphi(T) \in \mathcal{O}_{Q_{0,0}}[T]$.
- $\bar{\varphi}(T) = T^p + T = 0$;
- Очевидно, что $\bar{\varphi}(\delta) = 0 \Leftrightarrow \delta \in K_-$

Таким образом, по теореме Куммера, точка $Q_{0,0}$ расщепляется в расширении T_3/T_2, и над ней лежит p точек $R_{0,0,\delta} \in \mathbb{P}_{T_3}$, где $\delta \in K_-$. Индексы ветвления равны $e\left(R_{0,0,\delta}\middle|Q_{0,0}\right) = 1$. Над остальными точками $Q_{0,\alpha} \in \mathbb{P}_{T_2}$, $\alpha \in K_- \setminus \{0\}$ точек в расширении T_3/T_2 нет.

Подсчитаем число описанных точек. В п. 2.2.2 найдено $1 + (p-1) = p =$ $= 3$ разветвленных точек, в п. 2.2.3-2.2.4 найдено $p \cdot p \cdot (p^2 - p) + p =$ $= p^2 \cdot (p^2 - p) + p = 54 + 3 = 57$ неразветвленных точек. Всего описано $N(T_2) = p^2 \cdot (p^2 - p) + 2p = 54 + 6 = 60$ рациональных точек согласно формуле (22). Таким образом, описаны все рациональные точки. Обобщенная картина ветвления представлена на [рис 1].

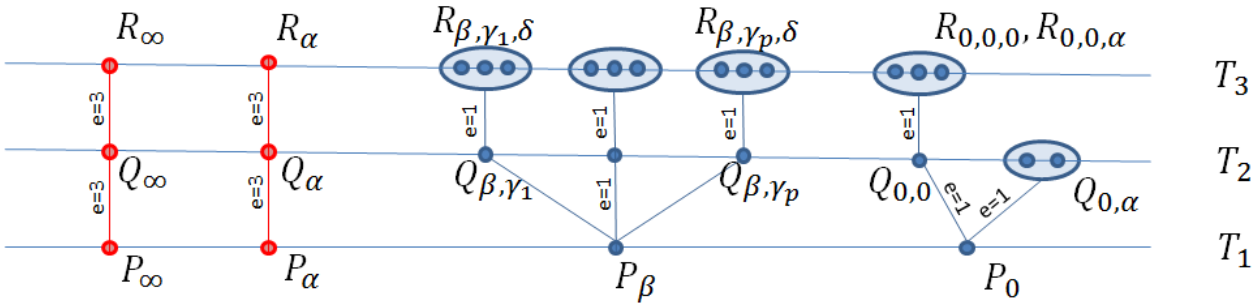

Рис 1. Картина ветвления точек в T_3/T_2 и T_2/T_1

2.3 Построение оболочки Галуа башни Гарсии – Штихтенота и анализ ее свойств

2.3.1 Определение. Пусть F/k – конечное сепарабельное расширение полей, поле K алгебраически замкнуто и $F \subset K$. Тогда поле $\tilde{F}$ называется оболочкой Галуа расширения F/k, если:

(а) $F \subset \tilde{F} \subset K$, причем $\tilde{F}/k$ – расширение Галуа (нормально и сепарабельно);

(б) Если $F \subseteq N \subseteq K$ и N/k – расширение Галуа, то $\tilde{F} \subseteq N$.

2.3.2 Определение. Пусть $T = (T_1, T_2, \dots, T_n, \dots)$ – башня Гарсии – Штихтенота (4) над полем $\mathbb{F}_{p^2}$. В этом разделе мы рассмотрим ее оболочку Галуа, т.е. башню $\tilde{T} = (\tilde{T}_1, \tilde{T}_2, \dots, \tilde{T}_n, \dots)$. В этой башне всякое поле $\tilde{T}_i$ является оболочкой Галуа расширения T_i/T_1, т.е. расширение $\tilde{T}_i/\tilde{T}_1$ – расширение Галуа.

2.3.3 Определение. Пусть K/F, L/F – расширения поля F, содержащиеся в некотором большем расширении M/F. Композитом полей L и K называется наименьшее подполе $K \cdot L \subset M$, содержащее одновременно K и L.

В случае, если K/F и L/F – конечные расширения, легко видеть, что композит полей существует и определяется однозначно: для заданных расширений существует конечная система образующих. Пусть, например, $K = F(\theta)$, $L = F(\psi)$; $\theta \in K$, $\psi \in L$ – образующие. В качестве их общего поля M можем взять поле разложения минимального многочлена $\mu_{\theta,F}(x) \cdot \mu_{\psi,F}(x)$. Тогда композитом полей является $KL = F(\theta, \psi)$.

Можно доказать, что композит произвольных расширений полей также существует и однозначно определен [14, с.70].

2.3.4 Предложение. Пусть K/F – конечное сепарабельное расширение полей степени $[K:F]=n$; $\{\sigma_i\}_{i=1}^{n}$ – все вложения K/F в алгебраическое замыкание $\overline{K}$ поля K. Тогда оболочка Галуа $L \subset \overline{K}$ расширения K/F равна композиту полей:

$$L = \sigma_1(K) \cdot \sigma_2(K) \cdot \ldots \cdot \sigma_n(K).$$

2.3.5 Порождающие элементы $\tilde{T}_n/\tilde{T}_{n-1}$. Введем следующие обозначения:

- $g(x) = \frac{x^{p+1}}{x^p+x}$ – рациональная функция;
- $f_\alpha := X^p + X - g(x_2+\alpha) \in \tilde{T}_2[X]$, где $\alpha \in K_-$ – неприводимый над T_2 многочлен, u_α – его корень в расширении $\tilde{T}_3/\tilde{T}_2$. Заметим, что u_0 порождает третью ступень башни Гарсии-Штихтенота $T_3 = T_2(u_0)$.
- $f_{(c_1,\ldots,c_n)} := X^p + X - g\left(u_{(c_1,\ldots,c_{n-1})} + c_n\right) \in \tilde{T}_{n+1}[X]$ – неприводимый над $\tilde{T}_{n+1}$ многочлен, $u_{(c_1,\ldots,c_n)}$ – его корень в расширении $\tilde{T}_{n+2}/\tilde{T}_{n+1}$. Заметим, что $f_{0^n} = X^p + X - g(u_{0^{n-1}}) = X^p + X - g(x^{n+1})$ – минимальный многочлен элемента u_{0^n}, порождающего $(n+2)$-ю ступень башни T: $T_{n+2} = T_{n+1}(u_{0^n})$.
- $\Gamma_n := Gal(\tilde{T}_n/T_1)$ – группа Галуа расширения $\tilde{T}_n/T_1$.

Тогда:

(а) Расширение T_2/T_1 рационального функционального поля нормально и сепарабельно [8]. Следовательно, расширение полей T_2/T_1 – расширение Галуа, как, впрочем, и любое расширение T_n/T_{n-1}, и выполняется

$$\tilde{T}_1 = T_1, \tag{28}$$

$$\tilde{T}_2 = T_2 = \mathbb{F}_{p^2}(x_1, x_2). \tag{29}$$

(б) Для $n \geq 3$ расширение $\tilde{T}_n/\tilde{T}_{n-1}$ порождается присоединением всех элементов $u_{(c)}$, где $c \in K_-^{n-2}$.

Доказательство. Докажем последнее утверждение по индукции по номеру $n \geq 3$. При $n = 3$, поле T_3 есть композит полей

$$\tilde{T}_3 = \prod_{\sigma \in \Gamma_3} \tilde{T}_2\big(\sigma(x_3)\big). \tag{30}$$

Применяя автоморфизм σ к (4) при $i = 1$, получаем $\sigma(x_2)^p + \sigma(x_2) = \frac{x_1^{p+1}}{x_1^p + x_1}$. Следовательно, $\sigma(x_2)$ – корень многочлена $X^p + X - g(x_1)$. Иными словами, $Tr\big(\sigma(x_2)\big) = g(x_1) \Rightarrow \sigma(x_2) = x_2 + \alpha_1$, где $\alpha_1 \in K_-$.

Аналогичным образом применяем σ к (4) при $i = 2$, получаем $\sigma(x_3)^p + \sigma(x_3) = \frac{\sigma(x_2)^{p+1}}{\sigma(x_2)^p + \sigma(x_2)} = \frac{(x_2+\alpha_1)^{p+1}}{x_2^p + \alpha_1^p + x_2 + \alpha_1} = \frac{(x_2+\alpha_1)^{p+1}}{Tr(x_2)}$. Следовательно, $\sigma(x_3)$ – корень многочлена $X^p + X - g(x_2 + \alpha_1)$. Иными словами, $Tr\big(\sigma(x_3)\big) = g(x_2 + \alpha_1) \Rightarrow \sigma(x_3) = u_{\alpha_2} + \alpha_1$, где $\alpha_1, \alpha_2 \in K_-$. Таким образом, $\tilde{T}_3 = \tilde{T}_2(u_c | c \in K_-)$ в силу (30).

Продолжим доказательство по индукции.

$$\tilde{T}_{n+1} = \prod_{\sigma \in \Gamma_{n+1}} \sigma(T_{n+1}) = \prod_{\sigma \in \Gamma_{n+1}} \tilde{T}_n(\sigma(x_{n+1})). \tag{31}$$

Снова применяя автоморфизм σ к (4) при $i = n$, получим

$$Tr\big(\sigma(x_{n+1})\big) = g\big(u_{(\alpha_1,\dots,\alpha_{n-1})} + \alpha_n\big) \Rightarrow \sigma(x_n) = u_{(\alpha_1,\dots,\alpha_{n-1})} + \alpha_n.$$

Таким образом, согласно (31), $\tilde{T}_{n+1} = \tilde{T}_n(u_c | c \in K_-^{n-2})$.

2.3.6 Степень расширения $\tilde{T}_n/\tilde{T}_{n-1}$. В [5, с.576] приводятся формулы для вычисления степеней расширения ступеней башни $\tilde{T}/\mathbb{F}_{p^2}$:

$$[\tilde{T}_n : T_1] = \begin{cases} p^{2n-3}, & n \in \{2,3\}, \\ p^{3n-6}, & n \geq 4. \end{cases} \tag{32}$$

Из этой формулы, согласно транзитивности степени расширения, получаем:

$$[\tilde{T}_2 : T_1] = p,$$

$$[\tilde{T}_3 : \tilde{T}_2] = \frac{[\tilde{T}_3 : T_1]}{[\tilde{T}_2 : T_1]} = \frac{p^3}{p} = p^2, \tag{33}$$

$$[\tilde{T}_n : \tilde{T}_{n-1}] = \frac{[\tilde{T}_n : T_1]}{[\tilde{T}_{n-1} : T_1]} = \frac{p^{3n-6}}{p^{3n-9}} = p^3, \ \ n \geq 4.$$

Легко видеть, что построенная в п. 2.3.5 система образующих расширения T_{n-1}/T_n не является базисом, т.к. для достаточно большого n (например, $n \geq 6$) $\#\{u_{(c)} : c \in K_-^{n-2}\} = p \cdot (n-2)$, и т.к. каждый $u_{(c)}$ – корень многочлена степени p, то если бы среди $u_{(c)}$ не было бы сопряженных корней, мы бы получили расширение степени $p^2 \cdot (n-2) > p^3$

2.3.7 Лемма. Пусть $Q \in \mathbb{P}_{\tilde{T}_n}$ – точка, лежащая над рациональной точкой $P_\beta \in \mathbb{P}_{T_1}$ ($\beta \notin K_-$). Тогда при $n \geq 3$, для любого $c \in K_-^{n-2}$, $\alpha \in K_-$, значение $u_{(c)}(Q) \in \mathbb{F}_{p^2} \setminus K_-$, и многочлен $f \coloneqq X^p + X - g\big(u_{(c)} + \alpha\big)$ раскладывается над $\mathbb{F}_{p^2}$ в точке Q на линейные множители.

Доказательство. Докажем утверждение по индукции по n, начиная с $n = 3$. Для $n = 3$ рассматриваемый многочлен имеет вид $f \coloneqq X^p + X - g(x_2 + \alpha)$. В этом случае $g(x_2 + \alpha) = \frac{(x_2+\alpha)^{p+1}}{Tr(x_2)} =$ $= \frac{2Tr((x_2+\alpha)^{p+1})}{Tr(x_2)} \in \mathbb{F}_p^*$. Следовательно, для любого $\alpha \in K_-$: $u_\alpha(Q) \in \mathbb{F}_{p^2} \setminus K_-$. Рассуждая аналогично п. 2.1.3, приходим к выводу, что f раскладывается на линейные множители над $\mathbb{F}_{p^2}$.

Далее обозначим $Q_{n-1} \coloneqq Q_n \cap \tilde{T}_{n-1}$. Пусть теперь для произвольного $c \in K_-^{n-3}$: $u_{(c)}(Q_{n-1}) \in \mathbb{F}_{p^2} \setminus K_-$. Тогда для любого $\alpha \in K_-$ можно записать $g\big(u_{(c)} + \alpha\big) = \frac{(u_{(c)}+\alpha)^{p+1}}{Tr(u_{(c)})} \in \mathbb{F}_p^*$, причем $g\big(u_{(c)} + \alpha\big)(Q_{n-1}) \neq 0$. Это означает, что рассматриваемый многочлен f в точке Q_{n-1} раскладывается на линейные множители над $\mathbb{F}_{p^2}$ и не имеет корней в K_-. Следовательно, $u_{(c,\alpha)}(Q) \in \mathbb{F}_{p^2} \setminus K_-$.

2.3.8 Оценка числа рациональных точек в T_n. Из леммы 2.3.7 следует, что минимальные многочлены $f_{(c_1,..,c_n)}$ порождающих элементов башни $u_{(c_1,..,c_n)}$ в точках поля $Q \in \mathbb{P}_{\tilde{T}_n}$, лежащих над точками $P_\beta \in \mathbb{P}_{T_1}$ ($\beta \notin K_-$), раскладываются на линейные множители. Это означает, что все такие точки полностью расщепляются в башне $\tilde{T}$ (что следует из теоремы Куммера 1.2.5). Всего таких точек на $\tilde{T}_n$ ступени башни $N(\tilde{T}_n) \geq (p^2 - p) \cdot [\tilde{T}_n : \tilde{T}_1]$. Это число дает нижнюю оценку числа рациональных точек в функциональном поле $\tilde{T}$.

Более того, из теоремы Куммера 1.2.5 следует еще один важный результат: поле $\mathbb{F}_{p^2}$ является полным полем констант в башне $\tilde{T}$, т.к. на любой ступени башни существует расщепляющаяся точка.

2.3.9 Оптимальность башни. В статье [18] рассмотрены точки ветвления башни $\tilde{T}$, вычисляется степень дифференты $Diff(\tilde{T}_n/\tilde{T}_1)$ и род поля $\tilde{T}_n$ ($n > 4$):

$$g(\tilde{T}_n) = [\tilde{T}_n : T_1] \cdot (p - p^{3-n} - p^{2-n}) + 1. \tag{34}$$

Таким образом, нетрудно вычислить предел башни:

$$\lambda(\tilde{T}) = \lim_{n\to\infty} \frac{N(\tilde{T}_n)}{g(\tilde{T}_n)} \geq \lim_{n\to\infty} \frac{(p^2 - p) \cdot [\tilde{T}_n : \tilde{T}_1]}{[\tilde{T}_n : T_1] \cdot (p - p^{3-n} - p^{2-n}) + 1} = p - 1. \tag{35}$$

Так, башня $\tilde{T}$ является оптимальной согласно теореме 1.3.3.

2.4 Конструкция и свойства алгеброгеометрических кодов

В этом разделе будет рассмотрена реализация алгоритмов сверточного кодирования и списочного декодирования, предложенные В. Гурусвами в [12] для младших ступеней башни Гарсии – Штихтенота.

2.4.1 Построение алгоритма кодирования. Введем следующие обозначения:

- $T_e \coloneqq \mathbb{F}_{r^2}(x_1, \dots, x_e)$ – ступень башни Гарсии – Штихтенота с номером $e \geq 2$;
- $q \coloneqq r^2$;
- $\mathbb{F}_{r^2} = \mathbb{F}_r(\zeta)$, т.е. ζ – примитивный корень поля $\mathbb{F}_{r^2}$;
- $G = lP_\infty$ – дивизор, определяющий кодирующее преобразование;
- $\sigma \in Aut(T_e/\mathbb{F}_q)$: $\sigma(x_i) \coloneqq \zeta^{(r+1)r^{i-1}} x_i$, $1 \leq i \leq e$ – автоморфизм поля T_e. В п. 2.2.4 мы доказали, что все точки $Q \in \mathbb{P}_{T_e}$, лежащие над точками $P_\alpha \in \mathbb{P}_{T_1}$, где $Tr(\alpha) \neq 0$, полностью расщепляются в башне T. Следовательно, число точек $\#\{Q \in \mathbb{P}_{T_e}, \text{где } Q|P_\alpha,\ Tr(\alpha \neq 0)\} = (r-1)r^e$. Автоморфизм σ делит это множество на r^e орбит, каждая из которых имеет $r-1$ точку. Выбрав целое число m, $0 \leq m \leq r-1$, мы можем выбрать $m \cdot N$ различных расщепляющихся точек $Q_1, Q_1^\sigma, \dots, Q_1^{\sigma^{m-1}}, \dots, Q_N, Q_N^\sigma, \dots, Q_N^{\sigma^{m-1}}$, где $N \leq r^e \cdot \left\lfloor \frac{r-1}{m} \right\rfloor$.
- $\frac{l}{m} < N \leq r^e \cdot \left\lfloor \frac{r-1}{m} \right\rfloor$ – число точек кода, определяет длину кода. Соответственно, точки $\{Q_1, \dots, Q_N\} \subset \{Q \in \mathbb{P}_{T_e}, \text{где } Q|P_\alpha,\ Tr(\alpha \neq 0)\}$ следует выбрать произвольно из множества расщепляющихся точек $\mathbb{P}_{T_e}$.

Тогда кодирующее отображение имеет вид:

$$FGS: L(lP_\infty) \to \mathbb{F}_q^N,$$

$$f \mapsto \left(\begin{bmatrix} f(P_1) \\ f(P_1^\sigma) \\ \dots \\ f(P_1^{\sigma^{m-1}}) \end{bmatrix}, \begin{bmatrix} f(P_2) \\ f(P_2^\sigma) \\ \dots \\ f(P_2^{\sigma^{m-1}}) \end{bmatrix}, \dots, \begin{bmatrix} f(P_N) \\ f(P_N^\sigma) \\ \dots \\ f(P_N^{\sigma^{m-1}}) \end{bmatrix} \right). \quad (36)$$

Можно доказать [12, с.25], что отображение FGS определяет $\mathbb{F}_q$-линейный код $FGS(N, l, q, e, m)$ над алфавитом мощности q, причем:

- Длина кода равна $n \coloneqq Nm$;
- Размерность кода $k \coloneqq \dim(lP_\infty) = l + 1 - g_e$;
- Скорость кода $R \geq \frac{k}{n} = \frac{l - g_e + 1}{Nm}$;

- Минимальное расстояние кода $d \geq N - \frac{l}{m}$

Согласно [12, с.28 ф.(23)], число t верно принятых элементов кодового слова $FGS(f)$ можно оценить сверху

$$t \leq N - \frac{Ns}{s+1} \cdot \left(1 - \frac{k}{N(m-s+1)}\right) + \frac{3g_e}{m-s+1}. \quad (37)$$

С другой стороны, число гарантированно исправляемых ошибок любого линейного кода связано с минимальным расстоянием кода и может быть вычислено по формуле $t^* := \left\lfloor \frac{d-1}{2} \right\rfloor$. Тогда число t верно принятых элементов кодового слова

$$t \geq mN - t^* = mN - \left\lfloor \frac{d-1}{2} \right\rfloor. \quad (38)$$

Таким образом, число исправляемых ошибок t^* построенного кода будет находиться в диапазоне

$$\left\lfloor \frac{d-1}{2} \right\rfloor \leq t^* \leq N(m-1) + \frac{Ns}{s+1} \cdot \left(1 - \frac{k}{N(m-s+1)}\right) - \frac{3g_e}{m-s+1}. \quad (39)$$

Рассмотрим ограничения на первоначальный выбор числа l при задании дивизора $G = lQ_\infty$. С одной стороны, размерность кода должна быть положительной, т.е. $k = l - 2g_e + 1 \geq 1$, следовательно, $l \geq 2g_e$. С другой стороны, $\frac{l}{m} \leq r^e \cdot \left\lfloor \frac{r-1}{m} \right\rfloor$, т.к. в противном случае не удастся подобрать подходящее значение числа точек кода $\frac{l}{m} < N \leq r^e \cdot \left\lfloor \frac{r-1}{m} \right\rfloor$. Таким образом, l ограничивается

$$2g_e \leq l \leq mr^e \cdot \left\lfloor \frac{r-1}{m} \right\rfloor. \quad (40)$$

В приложении Б приведены таблицы с числовыми значениями рассмотренных выше параметров кода на младших ступенях башни T.

2.4.2 Построение алгоритма списочного декодирования. Введем следующие обозначения:

- $s \geq 1$ – константа декодера;
- $k \coloneqq \dim(lP_\infty) = l + 1 - g_e$ – размерность кода;
- $D \coloneqq \left\lfloor \frac{N(m-s+1)-k+(s-1)\cdot g_e+1}{s+1} \right\rfloor$ – степенной параметр.

Тогда алгоритм списочного декодирования состоит из двух шагов. Пусть принято сообщение $y = (y_{ij})_{i=1..m, j=1..N}$, в котором не более t^* элементов ошибочны.

Шаг 1. Строим вспомогательный многочлен $Q \in T_e[Y_1, \dots, Y_s]$:

$Q = A_0 + A_1 Y_1 + \cdots + A_s Y_s$, где $A_i \in L(DP_\infty)$ для $i \geq 1$, $A_0 \in L((D+l)P_\infty)$. Этот многочлен должен обладать следующим свойством:

$$Q(y_{ij}, y_{i,j+1}, \dots, y_{j+s-1}) =$$

$$= A_0(P_i^{\sigma_j}) + A_1(P_i^{\sigma_j}) y_{i,j+1} + \cdots + A_s(P_i^{\sigma_j}) y_{i,j+s} = 0 \qquad (41)$$

где $i = 1..N, j = 0..m-s$.

Покажем, что такой многочлен $Q(Y_1, \dots, Y_s)$ всегда существует. Для этого запишем разложение элемента A_0 по базису пространства $L((D+l)P_\infty)$ с неопределенными коэффициентами, а элементы A_i $(i \geq 1)$ – разложим по базису пространства $L(DP_\infty)$. Тогда ограничения (41) дадут нам систему $N(m-s+1)$ однородных линейных уравнений над $\mathbb{F}_q$. Т.к. число неизвестных в этой системе превышает $N(m-s+1)$, система совместна, можно выбрать любое ее нетривиальное решение.

Шаг 2. Согласно конструкции многочлена $Q(Y_1, \dots, Y_s)$, для любого сообщения f, кодируемого в кодовое слово y, выполняется

$$Q\left(f, f^{\sigma^{-1}}, \dots, f^{\sigma^{-(s-1)}}\right) = 0 \qquad (42)$$

Подпространство таких сообщений f может быть найдено с помощью решения системы N линейных уравнений с $dim(G) = k$ неизвестными. Более того, если число ошибок не превышает верхнюю границу (39), то подпростран-

ство сообщений имеет размерность 1, и, следовательно, декодирование выполняется корректно.

2.5 Реализация алгеброгеометрического кода над T_2

Приведем пример реализации сверточного алгеброгеометрического кода на ступенях башни T_2 и T_3. Основные задачи, которые необходимо решить для построения такого кода, – нахождение всех рациональных точек функционального поля и нахождение базисов пространств Римана – Роха $L(lP_\infty) \subset L(DP_\infty) \subset L((D+l)P_\infty)$. Первая задача решена для произвольной ступени башни T_e, все ее рациональные точки описаны в 2.2.

2.5.1 Базис пространства Римана – Роха $L(lQ_\infty) \subset T_e$. Сначала опишем общую идею нахождения базиса пространства Римана – Роха в функциональном поле T_e для дивизора вида lQ_∞. Введем следующие обозначения:

$$L(\infty Q_\infty) \coloneqq \bigcup_{m \geq 0} L(mQ_\infty),$$
$$R_e \coloneqq \bigcap_{P \nmid P_\infty} \mathcal{O}_P. \tag{43}$$

Кольцо R_e, согласно (43), состоит из элементов $f \in T_e$, регулярных во всех точках $Q \in \mathbb{P}_{T_e}$, кроме, быть может, $Q_\infty | P_\infty$. Именно такие элементы входят в $L(lQ_\infty)$, по определению (9). Следовательно, $L(G) \subseteq R_e$.

В статье [15] приводится конструкция целого базиса расширения T_e/T_1:

$$Z_e \coloneqq \{z_\alpha\} = \left\{ \prod_{j=1}^{e-1} \pi_{j-1} u_{j,\alpha_j} \mid 0 \leq \alpha_j \leq r-1 \ \forall i \right\}, \tag{44}$$

где для $0 \leq k \leq e$ определены вспомогательные элементы

$$u_{k,\alpha} \coloneqq \begin{cases} x_{k+1}^{\alpha}, & 0 \leq \alpha < r-1, \\ x_{k+1}^{r-1} + 1, & \alpha = r-1, \end{cases}$$

$$g_k \coloneqq x_{k+1}^{r-1} + 1,$$

$$\pi_k \coloneqq g_0 g_1 \cdot \ldots \cdot g_k.$$

Более того, доказано, что элементы вида $\pi_{j-1} u_{j,\alpha_j}$, образующие целый базис расширения T_e/T_1, имеют полюс только в точке $Q_\infty \in \mathbb{P}_{T_e}$, лежащей над точкой P_∞ рационального функционального поля [15, с.2230]. Следовательно, $R_e \subseteq Span_{R_{e-1}}(Z_e) \coloneqq \{z_\alpha \cdot \beta \mid z_\alpha \in Z_e,\ \beta \in R_{e-1}\}$ $(e \geq 3)$.

Таким образом, справедлива цепочка включений

$$L(G) \subseteq R_e \subseteq Span_{R_{e-1}}(Z_e). \tag{45}$$

Иначе говоря, $Span_{R_{e-1}}(Z_e)$ содержит систему образующих пространства Римана – Роха $L(G)$. Базис последнего может быть выбран из его системы образующих.

2.5.2 Построение базиса $L(lQ_\infty) \subset T_2$. Опишем алгоритм нахождения базиса пространства Римана – Роха $L(lQ_\infty)$ в функциональном поле T_2. Согласно [15, с.2234], систему образующих кольца $R_2 \subset T_2$, можно построить в явном виде

$$B \coloneqq \left\{x_1^{e_1} \mid e_1 \geq 0\right\} \cup \left\{g_0 x_1^{e_1} x_2^{e_2} \mid e_1 \geq 0,\ \ 0 \leq e_2 \leq r-1\right\}. \tag{46}$$

Вычислим константу g_0:

Таблица 1 – Элементы π_k для $0 \leq k \leq 2$

$u_{0,0} = x_1^0 = 1$	$u_{0,1} = x_1^1 = x_1$	$u_{0,2} = x_1^2 + 1$
$u_{1,0} = x_2^0 = 1$	$u_{1,1} = x_2^1 = x_2$	$u_{1,2} = x_2^2 + 1$
$u_{2,0} = x_3^0 = 1$	$u_{2,1} = x_3^1 = x_3$	$u_{2,2} = x_3^2 + 1$
$g_0 = x_1^2 + 1$	$g_1 = x_2^2 + 1$	$g_2 = x_3^2 + 1$
$\pi_0 = g_0 = x_1^2 + 1$	$\pi_1 = g_0 g_1 =$ $= (x_1^2 + 1)(x_2^2 + 1)$	$\pi_2 = g_0 g_1 g_2 = \cdots$

Замечание. Для нахождения системы образующих кольца R_e, $e \geq 3$ следует действовать по п. 2.5.1: сначала определить целый базис Z_e расширения T_e/T_1, затем найти линейную оболочку найденных элементов $Span_{R_{e-1}}(Z_e)$ над кольцом R_{e-1}. При $e = 3$ необходимо использовать систему образующих $B \subset R_2$, построенную в п. 2.5.2.

Так как $L(lQ_\infty) \subseteq R_2 =< B >$, то базис $L(lQ_\infty)$ можно выбрать из системы элементов B. Известно, что элементы этой системы не имеют других полюсов, кроме, быть может, Q_∞, следовательно, нормирования во всех точках поля $Q \in \mathbb{P}_{T_2} \setminus \{Q_\infty\}$ неотрицательны. Таким образом, $f \in L(lQ_\infty) \Leftrightarrow v_{Q_\infty}(f) \geq -l$, где $f \in B$, по определению (9). Вычислим нормирования элементов $f \in B$ в точке $Q_\infty \in \mathbb{P}_{T_2}$:

- $v_{Q_\infty}\left(x_1^{e_1}\right) = e_1 \cdot v_{Q_\infty}(x_1) = e_1 \cdot e(Q_\infty|P_\infty) \cdot v_{P_\infty}(x_1) = -3e_1.$

Вычислим $v_{Q_\infty}(x_2)$. Для начала вычислим дискретные нормирования в точке Q_∞ элементов правой и левой частей уравнения функционального поля T_2 (4) при $i = 2$.

$$v_{Q_\infty}(x_2^3 + x_2) = v_{Q_\infty}\left(\frac{x_1^4}{x_1^3 + x_1}\right) = e(Q_\infty|P_\infty) \cdot v_{P_\infty}\left(\frac{x_1^4}{x_1^3 + x_1}\right) = -3.$$

Применим в левой части неравенство треугольника:

$$v_{Q_\infty}(x_2^3 + x_2) \geq min\{3v_{Q_\infty}(x_2), v_{Q_\infty}(x_2)\}.$$

Если предположить, что строгое неравенство треугольника не выполняется, т.е. $v_{Q_\infty}(x_2^3 + x_2) > min\{3v_{Q_\infty}(x_2), v_{Q_\infty}(x_2)\}$, то $3v_{Q_\infty}(x_2) \neq v_{Q_\infty}(x_2)$. Это возможно тогда и только тогда, когда $v_{Q_\infty}(x_2) = 0$. Но тогда имеем $v_{Q_\infty}(x_2^3 + x_2) > min\{3v_{Q_\infty}(x_2), v_{Q_\infty}(x_2)\} = 0$, что противоречит $v_{Q_\infty}(x_2^3 + x_2) = -3$. Таким образом,

$$v_{Q_\infty}(x_2^3 + x_2) = min\{3v_{Q_\infty}(x_2), v_{Q_\infty}(x_2)\} = -3.$$

Следовательно, $v_{Q_\infty}(x_2) = -1$.

- $v_{Q_\infty}(g_0) = v_{Q_\infty}(x_1^2 + 1) = 2v_{Q_\infty}(x_1) = -6$.
- $v_{Q_\infty}\left(g_0 x_1^{e_1} x_2^{e_2}\right) = -6 + e_1 v_{Q_\infty}(x_1) + e_2 v_{Q_\infty}(x_2) = -6 - 3e_1 - e_2$.

Осталось выбрать $\dim(lQ_\infty) = l + 1 - g_2 = l - 3$ линейно независимых элементов $f \in B$ таким образом, чтобы $v_{Q_\infty}(f) \geq -l$.

Замечание. Для того, чтобы оценки параметров кода были верны, необходимо выбирать достаточно большое l так, чтобы дивизор $G = lQ_\infty$ оказался неспециальным, и его размерность можно было вычислить по формуле (11) с $i(G) = 0$. В частности, для $G \in Div_{T_2}$ следует выбирать $l \geq 2g_2 - 1 = 7$. Для построения базиса $L(G)$ такого дивизора можно, к примеру, выбрать $\{1, x_1\} \subset$ $\subset \left\{x_1^{e_1} \mid e_1 \geq 0\right\}$, а остальные $l - 3 - 2 = l - 5$ элементов выбрать из множества $\left\{g_0 x_1^{e_1} x_2^{e_2} \mid e_1 \geq 0,\ 0 \leq e_2 \leq r - 1\right\}$. Затем необходимо убедиться в их линейной независимости над $\mathbb{F}_{p^2}$.

ГЛАВА 3. АЛГОРИТМЫ

3.1 Алгоритм кодирования

Вход: $N, l, r, e = 2, m, f$.

Ограничения: r – простое число, характеристика поля констант башни; $l \geq 7$ – целое число; $\frac{l}{m} < N \leq r^2 \cdot \left\lfloor \frac{r-1}{m} \right\rfloor$ – целое число, $m \in \{1,2\}$, $f \in L(lQ_\infty)$ – кодируемое сообщение.

Алгоритм (шаги):

1. Положить $q \coloneqq r^e = r^2$. Построить конечное поле $\mathbb{F}_{r^2} = \mathbb{F}_r(\zeta)$.
2. Вычислить элементы $Km[j] \coloneqq \{\alpha \in \mathbb{F}_{r^2} : Tr(\alpha) = j\}$ для $0 \leq j \leq r-1$.
3. Задать $Q_{1..N}$ – пустой массив, в который будут записаны точки кода.
4. Для всех $\beta \notin Km[0]$, и пока $len(Q) < N$ выполнять:
    4.1. Вычислить $c \coloneqq \frac{2Tr(\beta^{r+1})}{Tr(\beta)} \in \mathbb{F}_r$.
    4.2. Для всех $\gamma \in Km[c]$, и пока $len(Q) < N$ выполнять:
        4.2.1. Добавить в список Q точку $Q_{len(Q)} \coloneqq [\beta, \gamma]$.
5. Задать $y[1..m, 1..N]$ – пустой массив;
6. Для $i = 1..m$ выполнять:
    6.1. Для $j = 1..N$ выполнять:
        6.1.1. $y[i,j] \coloneqq f\left(x_1 = Q_i[1] \cdot 2^{i-1}, x_2 = Q_i[2] \cdot 2^{i-1}\right)$.

Выход: Кодовое слово $y \in \mathbb{F}_{r^2}^{mN}$.

3.2 Алгоритм декодирования

Вход: $N, l, e = 2, r, m, Q_{1..N}, y$.

Ограничения: r – простое число, характеристика поля констант башни; $l \geq 7$ – целое число; $\frac{l}{m} < N \leq r^2 \cdot \left\lfloor \frac{r-1}{m} \right\rfloor$ – целое число, $m \in \{1,2\}$, $Q_{1..N}$ – точки кода, сгенерированные при кодировании, $y \in \mathbb{F}_{r^2}^{mN}$ – кодовое слово.

Алгоритм (шаги):

1. Положить $q \coloneqq r^e = r^2$. Построить конечное поле $\mathbb{F}_{r^2} = \mathbb{F}_r(\zeta)$.

2. Вычислить элементы $Km \coloneqq \{\alpha \in \mathbb{F}_{r^2} : Tr(\alpha) = 0\}$.

3. Положить $s = 1$.

4. $k \coloneqq l - 3$.

5. $D \coloneqq \left\lfloor \frac{N(m-s+1)-k+(s-1)\cdot g_e+1}{s+1} \right\rfloor$.

6. Построить множества $L_1[1..l-3]$, $L_2[1..D-3]$, $L_3[1..D+l-3]$ – базисы пространств Римана – Роха $L(lQ_\infty)$, $L(DQ_\infty)$, $L((D+l)Q_\infty)$ соответственно.

7. Задать

$$A_0 = \sum_{i=1}^{D+l-3} a_0[i] \cdot L_3[i], \qquad A_1 = \sum_{i=1}^{D-3} a_1[i] \cdot L_2[i].$$

8. Составить систему однородных линейных уравнений и найти любое ее нетривиальное решение $\{a_0[i], a_1[i]\}$.

$$\begin{cases} A_0\big(x_1 = Q_j[1], x_2 = Q_j[2]\big) + A_1\big(x_1 = Q_j[1], x_2 = Q_j[2]\big) \cdot y[1,j] \\ A_0\big(x_1 = 2Q_j[1], x_2 = 2Q_j[2]\big) + A_1\big(x_1 = 2Q_j[1], x_2 = 2Q_j[2]\big) \cdot y[2,j] \end{cases}$$

$$(1 \leq j \leq N)$$

9. $Q \coloneqq A_0 + A_1 Y$.

10. Задать

$$f = \sum_{i=1}^{l-3} f[i] \cdot L_1[i].$$

11. Составить и решить систему однородных линейных уравнений относительно $\{f[i]\}$

$$f\big(x_1 = Q_j[1], x_2 = Q_j[2]\big) = 0$$

$(1 \le j \le N)$

12. Если последняя система несовместна или имеет бесконечно много решений, корректное декодирование невозможно. Иначе вывести $f \in L(lQ_\infty)$.

Выход: искомое сообщение $f \in L(lQ_\infty)$ или “Неудача”.

3.3 Алгоритм построения базиса $\boldsymbol{L(lQ_\infty) \subset T_2}$

Вход: $l, e = 2, r = 3$.

Ограничения: $l \ge 7$.

Алгоритм (шаги):

1. Задать $L[1..l-3]$ – пустой массив, в который будут записаны базисные элементы.

2. Положить $L[1] \coloneqq 1$, $L[2] \coloneqq x_1$.

3. $i \coloneqq 0$.

4. Пока $len(L) < l - 3$, выполнять:

    4.1. Для $j = 0..r-1$ выполнять:

        4.1.1. $dv \coloneqq -6 - 3i - j$.

        4.1.2. Если $dv \ge -l$, добавить элемент $(x_1^2 + 1)x_1^i x_2^j$ в массив L.

    4.2. $i \coloneqq i + 1$.

Выход: Массив $L[1..l-3]$.

3.4 Оценка эффективности алгоритмов

3.4.1 Эффективность алгоритма построения базиса $\boldsymbol{L(lQ_\infty) \subset T_2}$. Посчитаем число бинарных операций, требуемых для построения базиса пространства $L(lQ_\infty)$.

Оценим число итераций цикла на шаге '4' алгоритма. В результате выполнения двух вложенных циклов строится последовательность целых чисел $\{dv\} = \{(-6,-7,-8),(-9,-10,-11),(-12,-13,-14),\dots\}$, где в круглые скоб-

ки взяты элементы последовательности, полученные на i–м шаге цикла '4'. Видим, что условие '4.1.2' внутри цикла перестает выполняться при

$$-6-3i-j<-l \quad \Leftrightarrow \quad 3i+j>l-6 \quad \Rightarrow \quad i\geq\left\lceil\frac{l-6}{3}\right\rceil$$

При этом будет найдено, по меньшей мере, $l-5$ подходящих элементов с дискретным нормированием $dv<-l$. Следовательно, цикл '4' завершится через конечное число шагов, не превышающее $\left\lceil\frac{l-6}{3}\right\rceil$.

Таким образом, максимально будет выполнено не более $\left\lceil\frac{l-6}{3}\right\rceil$ итераций цикла '4', на каждой из которых выполняется $3r$ бинарных операций для вычисления и присвоения dv, одна проверка условия и одна запись в список L. Таким образом, всего требуется не более

$$\left\lceil\frac{l-6}{3}\right\rceil\cdot(3r+2)=11\cdot\left\lceil\frac{l-6}{3}\right\rceil=O(l) \tag{47}$$

бинарных операций.

Замечание. Здесь и далее не будем учитывать при подсчете операции, не зависящие от входных параметров, а также операции выделения памяти.

3.4.2 Эффективность алгоритма кодирования. Рассмотрим алгоритм, описанный в 3.1.

Предварительные вычисления: требуется $2r^2$ операций для построения таблицы индексов поля $\mathbb{F}_{r^2}$, r^2 операций для построения множества $km[j]$.

Для нахождения N рациональных точек кода, выполняется цикл '4', число итераций в котором не превосходит $\left\lceil\frac{N}{r}\right\rceil$, т.к. на каждом шаге цикла алгоритм находит и добавляет r точек в массив Q. Вычисление c на шаге '4.1' требует $2(r+2)+2=2(r+3)$ бинарных операций. Таким образом, для нахождения N точек кода требуется $2(r+3)\left\lceil\frac{N}{r}\right\rceil$ операций.

Для непосредственно кодирования необходимо вычислить значения элемента $f \in L(G)$ в mN точках кода. Каждое такое вычисление на шаге '6.1.1' требует $2i$ умножений и вычисление по модулю r. Всего не более $2m^2N$ двоичных операций.

Таким образом, всего требуется не более

$$3r^2 + 2(r+3)\left\lceil \frac{N}{r} \right\rceil + 2m^2N \tag{48}$$

бинарных операций.

3.4.3 Эффективность алгоритма декодирования. Рассмотрим алгоритм, описанный в п. 3.2.

Рассуждая аналогично п. 3.4.2, для предварительных вычислений (шаги '1' – '2' алгоритма) потребуется $2r^2 + r$ бинарных операций.

Для построения системы $2N$ линейных уравнений (41) с $2D + l - 6$ неизвестными потребуется $4N + (D-3)N = (D+1)N$ операций умножения и $4N(D-3) + 2N(D+l-3) = (6D + 2l - 18)N$ вычислений по модулю r. Для решения такой системы методом Гаусса потребуется

$$\frac{2N(2N-1)(4N-1)}{3} + \frac{2N(2N-1)}{2} = \frac{4N(2N-1)(4N-1) + 6N(2N-1)}{6} =$$

$$= \frac{(2N-1)(8N^2-N)}{3} = \frac{16}{3}N^3 + O(N^2)$$

бинарных операций согласно [4].

Для решения системы линейных однородных уравнений (42) методом Гаусса согласно [4] потребуется

$$\frac{N(N-1)(2N-1)}{3} + \frac{N(N-1)}{2} = \frac{(N-1)(4N^2-2N) + 3N(N-1)}{6} =$$

$$= \frac{(N-1)(4N^2+N)}{6} = \frac{4}{6}N^3 + O(N^2)$$

бинарных операций.

Таким образом, общее количество элементарных операций, требуемых для выполнения алгоритма декодирования, составляет

$$2r^2 + r + (7D + 2l - 17)N + \frac{(2N-1)(8N^2-N)}{3} + \frac{(N-1)(4N^2+N)}{6}. \quad (49)$$

3.5 Пример работы алгоритмов

Приведем пример кодирования и декодирования конкретного сообщения по алгоритмам 3.1-3.3, зафиксировав следующие параметры кода:

- $r = 3$, т.е. поле констант башни $\mathbb{F}_{r^2} = \mathbb{F}_{3^2}$;
- $e = 2$, ступень башни T_2;
- $l = 8, N = 9$.

Числа l и N выбраны из таблицы Б.1 приложения Б. Согласно этой таблице, при декодировании степенной параметр равен $D = 9$, код гарантированно исправляет не менее двух ошибок.

Предварительные построения:

1. $\mathbb{F}_{3^2} = \mathbb{F}_3(\zeta)$, где ζ – корень неприводимого над $\mathbb{F}_3$ многочлена

$$fpoly \coloneqq x^2 + x + 2,$$

$$\mathbb{F}_{3^2}^* = \{\zeta, 2\zeta + 1, 2\zeta + 2, 2, 2\zeta, \zeta + 2, \zeta + 1, 1\},$$

$$Km = \{\alpha \in \mathbb{F}_{3^2} : Tr(\alpha) = 0\} = \{0, 2\zeta + 1, \zeta + 2\},$$

$$Kms \coloneqq Km \setminus \{0\} = \{2\zeta + 1, \zeta + 2\}.$$

2. Выберем $N = 9$ точек Q_i по алгоритму 3.1, вычислим соответствующие им Q_i^σ:

- $\beta = \zeta \Rightarrow c = \frac{2Tr(\beta^{r+1})}{Tr(\beta)} = 1$.

Находим $\{\alpha \in \mathbb{F}_{3^2} : Tr(\alpha) = 1\} = \{2, 2\zeta, \zeta + 1\}$.

$Q_1 = Q_{[\zeta,2]}$	$Q_1^\sigma = Q_{[2\zeta,1]}$
$Q_2 = Q_{[\zeta,2\zeta]}$	$Q_2^\sigma = Q_{[2\zeta,\zeta]}$

$Q_3 = Q_{[\zeta,\zeta+1]}$	$Q_3^\sigma = Q_{[2\zeta,2\zeta+2]}$

- $\beta = 2\zeta + 2 \Rightarrow c = \frac{2Tr(\beta^{r+1})}{Tr(\beta)} = 1.$

$Q_4 = Q_{[2\zeta+2,2]}$	$Q_4^\sigma = Q_{[\zeta+1,1]}$
$Q_5 = Q_{[2\zeta+2,2\zeta]}$	$Q_5^\sigma = Q_{[\zeta+1,\zeta]}$
$Q_6 = Q_{[2\zeta+2,\zeta+1]}$	$Q_6^\sigma = Q_{[\zeta+1,2\zeta+2]}$

- $\beta = 2 \Rightarrow c = \frac{2Tr(\beta^{r+1})}{Tr(\beta)} = 1.$

$Q_7 = Q_{[2,2]}$	$Q_7^\sigma = Q_{[1,1]}$
$Q_8 = Q_{[2,2\zeta]}$	$Q_8^\sigma = Q_{[1,\zeta]}$
$Q_9 = Q_{[2,\zeta+1]}$	$Q_9^\sigma = Q_{[1,2\zeta+2]}$

3. Вычислим базисы пространств Римана – Роха:

- $L(lQ_\infty)$: $L_1 = \{1, x_1, x_1^2 + 1, x_2(x_1^2 + 1), x_2^2(x_1^2 + 1)\}$.
- $L(DQ_\infty)$: $L_2 = \{1, x_1, x_1^2 + 1, x_2(x_1^2 + 1), x_2^2(x_1^2 + 1),\ x_1(x_1^2 + 1)\}$.
- $L\big((l + D)Q_\infty\big)$: $L_2 = \{1, x_1, x_1^2 + 1, x_2(x_1^2 + 1), x_2^2(x_1^2 + 1),$
  $x_1(x_1^2 + 1), x_1x_2(x_1^2 + 1), x_1x_2^2(x_1^2 + 1), x_1^2(x_1^2 + 1), x_1^2x_2(x_1^2 + 1),$
  $x_1^2x_2^2(x_1^2 + 1), x_1^3(x_1^2 + 1), x_1^3x_2(x_1^2 + 1), x_1^3x_2^2(x_1^2 + 1)\}$.
- $l_1 \coloneqq 5, l_2 \coloneqq 6, l_3 \coloneqq 14$ – размерности соответствующих пространств.

Выберем сообщение $f \coloneqq (1, 2, \zeta, 2, \zeta + 1) \in \mathbb{F}_9^{l_1}$,

$f \longmapsto 1 + 2x_1 + \zeta(x_1^2 + 1) + 2x_2(x_1^2 + 1) + (\zeta + 1)x_2^2(x_1^2 + 1) \in L(lQ_\infty)$.

Выполним кодирование:

$$\text{y} \coloneqq \begin{pmatrix} f(Q_1) & \dots & f(Q_9) \\ f(Q_1^\sigma) & \dots & f(Q_9^\sigma) \end{pmatrix},$$

$$\mathrm{y} \coloneqq \begin{pmatrix} 0 & 2\zeta+1 & 0 & \zeta+1 & \zeta+2 & \zeta+1 & \zeta & 2 & \zeta \\ \zeta+2 & \zeta & 2 & 2 & \zeta+1 & 2\zeta+1 & \zeta & 2\zeta & 2\zeta+2 \end{pmatrix}.$$

Внесем в кодовое слово две ошибки, например, в позиции $y[2,3] \coloneqq \zeta + 2$ и $y[1,1] \coloneqq 1$. Выполним декодирование полученного кодового слова y'.

$$\mathrm{y}' \coloneqq \begin{pmatrix} 1 & 2\zeta+1 & 0 & \zeta+1 & \zeta+2 & \zeta+1 & \zeta & 2 & \zeta \\ \zeta+2 & \zeta+2 & 2 & 2 & \zeta+1 & 2\zeta+1 & \zeta & 2\zeta & 2\zeta+2 \end{pmatrix}.$$

Сначала найдем вспомогательный многочлен $Q(Y) \coloneqq A_0 + A_1 Y$. Для этого запишем разложения A_0 и A_1 по соответствующим базисам пространств Римана – Роха, как указано на шаге '7' алгоритма:

$$A_0 = \sum_{i=1}^{l_3} a_i \cdot L_3[i], \qquad A_1 = \sum_{i=1}^{l_2} b_i \cdot L_2[i].$$

Затем составим систему однородных линейных уравнений (41) для нахождения этих коэффициентов. Система в данных условиях задается следующей матрицей

$$\begin{bmatrix}
1 & \zeta & 2\zeta+2 & \zeta+1 & 2\zeta+2 & 2 & 1 & 2 & 2\zeta & \zeta & 2\zeta & \zeta+2 & 2\zeta+1 & \zeta+2 & 1 & \zeta & 2\zeta+2 & \zeta+1 & 2\zeta+2 & 2 \\
1 & 2\zeta & 2\zeta+2 & 2\zeta+2 & 2\zeta+2 & 1 & 1 & 1 & 2\zeta & 2\zeta & 2\zeta & 2\zeta+1 & 2\zeta+1 & 2\zeta+1 & \zeta+2 & 2\zeta+2 & \zeta & \zeta & \zeta & \zeta+2 \\
1 & \zeta & 2\zeta+2 & 1 & 2\zeta & 2 & \zeta & \zeta+2 & 2\zeta & 2\zeta+1 & \zeta+1 & \zeta+2 & 2\zeta+2 & 1 & 2\zeta+1 & 2\zeta+2 & 2\zeta & 2\zeta+1 & \zeta+1 & \zeta+2 \\
1 & 2\zeta & 2\zeta+2 & 2 & 2\zeta & 1 & \zeta & 2\zeta+1 & 2\zeta & \zeta+2 & \zeta+1 & 2\zeta+1 & 2\zeta+2 & 2 & \zeta & \zeta+2 & 2 & 2\zeta & \zeta+2 & \zeta \\
1 & \zeta & 2\zeta+2 & 2\zeta+1 & \zeta & 2 & 2\zeta+2 & 2\zeta+1 & 2\zeta & 2 & 2\zeta+2 & \zeta+2 & 2\zeta & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 2\zeta & 2\zeta+2 & \zeta+2 & \zeta & 1 & 2\zeta+2 & \zeta+2 & 2\zeta & 1 & 2\zeta+2 & 2\zeta+1 & 2\zeta & 1 & \zeta+2 & 2\zeta+2 & \zeta & 2 & \zeta+1 & \zeta+2 \\
1 & 2\zeta+2 & \zeta & 2\zeta & \zeta & 2 & 1 & 2 & \zeta+1 & 2\zeta+2 & \zeta+1 & 2\zeta+1 & \zeta+2 & 2\zeta+1 & \zeta+1 & 2\zeta+1 & 1 & 2 & 1 & 2\zeta+2 \\
1 & \zeta+1 & \zeta & \zeta & \zeta & 1 & 1 & 1 & \zeta+1 & \zeta+1 & \zeta+1 & \zeta+2 & \zeta+2 & \zeta+2 & 2 & 2\zeta+2 & 2\zeta & 2\zeta & 2\zeta & 2 \\
1 & 2\zeta+2 & \zeta & \zeta+2 & 2\zeta+2 & 2 & \zeta & \zeta+2 & \zeta+1 & 2 & \zeta & 2\zeta+1 & \zeta+1 & 2 & \zeta+2 & \zeta & \zeta+1 & 2 & \zeta & 2\zeta+1 \\
1 & \zeta+1 & \zeta & 2\zeta+1 & 2\zeta+2 & 1 & \zeta & 2\zeta+1 & \zeta+1 & 1 & \zeta & \zeta+2 & \zeta+1 & 1 & \zeta+1 & \zeta+2 & 1 & \zeta & 2\zeta+1 & \zeta+1 \\
1 & 2\zeta+2 & \zeta & 1 & \zeta+1 & 2 & 2\zeta+2 & 2\zeta+1 & \zeta+1 & \zeta+2 & 2\zeta & 2\zeta+1 & \zeta & 1 & \zeta+1 & 2\zeta+1 & 1 & \zeta+1 & \zeta+2 & 2\zeta+2 \\
1 & \zeta+1 & \zeta & 2 & \zeta+1 & 1 & 2\zeta+2 & \zeta+2 & \zeta+1 & 2\zeta+1 & 2\zeta & \zeta+2 & \zeta & 2 & 2\zeta+1 & \zeta & 2\zeta+2 & \zeta+2 & \zeta & 2\zeta+1 \\
1 & 2 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & \zeta & 2\zeta & 2\zeta & \zeta & 2\zeta & \zeta \\
1 & 1 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & \zeta & \zeta & 2\zeta & 2\zeta & 2\zeta & 2\zeta \\
1 & 2 & 2 & \zeta & \zeta+2 & 1 & 2\zeta & 2\zeta+1 & 2 & \zeta & \zeta+2 & 1 & 2\zeta & 2\zeta+1 & 2 & 1 & 1 & 2\zeta & 2\zeta+1 & 2 \\
1 & 1 & 2 & 2\zeta & \zeta+2 & 2 & 2\zeta & \zeta+2 & 2 & 2\zeta & \zeta+2 & 2 & 2\zeta & \zeta+2 & 2\zeta & 2\zeta & \zeta & 2\zeta+1 & 2\zeta+2 & \zeta \\
1 & 2 & 2 & 2\zeta+2 & 2\zeta+1 & 1 & \zeta+1 & \zeta+2 & 2 & 2\zeta+2 & 2\zeta+1 & 1 & \zeta+1 & \zeta+2 & \zeta & 2\zeta & 2\zeta & 2 & 2\zeta+2 & \zeta \\
1 & 1 & 2 & \zeta+1 & 2\zeta+1 & 2 & \zeta+1 & 2\zeta+1 & 2 & \zeta+1 & 2\zeta+1 & 2 & \zeta+1 & 2\zeta+1 & 2\zeta+2 & 2\zeta+2 & \zeta+1 & 2\zeta+1 & 2\zeta & \zeta+1
\end{bmatrix}$$

Одно из частных решений этой системы имеет вид

$$(a_1, a_2, \ldots, a_{14}, b_1, b_2, \ldots, b_6) =$$

$$= (\zeta, \zeta, \zeta + 2, 0, 2\zeta, \zeta + 1, 2\zeta + 2, 2\zeta + 1, 2\zeta + 1, 1, 2\zeta + 1, \zeta, 2\zeta,$$
$$2\zeta + 2, 0, 2\zeta, 1, 1, 1, 1).$$

Таким образом,

$$A_0 = \zeta + \zeta x_1 + (\zeta + 2)(x_1^2 + 1) + 2\zeta x_2^2(x_1^2 + 1) + (\zeta + 1)x_1(x_1^2 + 1) +$$
$$+(2\zeta + 2)x_1x_2(x_1^2 + 1) + (2\zeta + 1)x_1x_2^2(x_1^2 + 1) +$$
$$+(2\zeta + 1)x_1^2(x_1^2 + 1) + x_1^2x_2(x_1^2 + 1) + (2\zeta + 1)x_1^2x_2^2(x_1^2 + 1) +$$
$$+\zeta x_1^3(x_1^2 + 1) + 2\zeta x_1^3x_2(x_1^2 + 1) + (2\zeta + 2)x_1^3x_2^2(x_1^2 + 1),$$

$$A_1 = 2\zeta x_1 + x_1^2 + 1 + x_2(x_1^2 + 1) + x_2^2(x_1^2 + 1) + x_1(x_1^2 + 1),$$

$$Q(Y) \coloneqq A_0 + A_1Y.$$

Далее задаем элемент $f \in L(lQ_\infty)$ его разложением по базису L_1 с неопределенными коэффициентами и находим эти коэффициенты:

$$f = \sum_{i=1}^{l_1} f_i \cdot L_1[i].$$

В данных условиях система уравнений будет иметь следующий матричный вид (матрица коэффициентов системы и столбец свободных членов):

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 2\zeta+1 & 2\zeta+2 & 2\zeta & 2\zeta+1 & \zeta+1 \\ 1 & \zeta & 2\zeta+2 & 2\zeta+1 & \zeta \\ \zeta & 2 & 2\zeta+1 & \zeta+2 & 2\zeta+1 \\ \zeta+1 & 2\zeta+1 & 1 & 2\zeta & 2\zeta+1 \\ 2\zeta+2 & \zeta+2 & 2 & 2\zeta+2 & 2\zeta+1 \\ \zeta & 2\zeta & 2\zeta & \zeta & 2\zeta \\ 2 & 1 & 1 & 2\zeta & 2\zeta+1 \\ 2\zeta & \zeta & \zeta & 1 & \zeta+1 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 0 \\ 1 \\ 2\zeta \\ 2\zeta+1 \\ \zeta^2 \\ 1 \\ \zeta+2 \end{bmatrix},$$

Эта система имеет единственное решение

$$(f_1, \dots, f_5) = (1, 2, \zeta, 2, \zeta + 1).$$

Таким образом, успешно декодировано сообщение

$$f = (1, 2, \zeta, 2, \zeta + 1) \in \mathbb{F}_9^{l_1},$$

$$f \longmapsto 1 + 2x_1 + \zeta(x_1^2 + 1) + 2x_2(x_1^2 + 1) + (\zeta + 1)x_2^2(x_1^2 + 1) \in L(lQ_\infty).$$

Замечание. Аналогичный код можно построить и на старших ступенях башни Гарсии – Штихтенота T_e, где $e \geq 3$. При этом точки кода следует выбирать из расщепляющихся точек $P \in \mathbb{P}_{T_e}$, а базисы пространств Римана – Роха дивизоров $G = lQ_\infty \in Div_{T_e}$ – выбирать из множества $Span_{R_{e-1}}(Z_e)$ в соотношении (45). Для сравнения свойств кодов, которые можно построить на ступенях башни $2 \leq e \leq 4$, были построены таблицы всевозможных параметров N, l, D кода на e–й ступени башни. Указанные таблицы приведены в приложении Б, и из них следует, что построенные коды обладают относительно низкой скоростью ($R \leq 60\%$), либо исправляют малое число ошибок по отношению к длине кода. При этом на каждой следующей ступени башни резко возрастает число точек, требуемых для работы алгоритма кодирования, следовательно, заметно увеличивается время кодирования и декодирования. Таким образом, остается актуальной задача переноса построенных кодов на оболочку Галуа $\tilde{T}$ башни Гарсии – Штихтенота.

ЗАКЛЮЧЕНИЕ

В дипломной работе проведено исследование свойств первых ступеней T_2 и T_3 башни Гарсии – Штихтенота над конечным полем $\mathbb{F}_{p^2}$, необходимых для построения АГ – кодов Гоппы. Решены вспомогательные задачи, возникшие в процессе исследования, в том числе:

1. Полностью описана картина ветвления рациональных точек всех расширений T_n/T_{n-1}, что позволило выбирать точки при построении АГ–кода;
2. Построены дифференты расширений T_2/T_1, T_3/T_2, что позволило вычислить род функциональных полей $g(T_2)$ и $g(T_3)$.

При исследовании указанных свойств башни T в основном применялись методы теории функциональных полей, описанные в главе 1 “Предварительные сведения”.

В качестве алгоритма кодирования был выбран сверточный код, для построения которого на T_2 и T_3 была решена задача нахождения базиса пространств Римана – Роха дивизоров особого вида $G = lQ_\infty$. Алгоритмы кодирования и декодирования на $T_2/\mathbb{F}_9$ были формализованы, проиллюстрированы программой в системе научных расчетов Maple 18.0, оценена сложность алгоритмов. **Таким образом, цель работы была достигнута.**

Дополнительно в дипломной работе исследован метод построения оболочки Галуа башни Гарсии – Штихтенота $\tilde{T}$, которая также может быть использована для построения кодов, превосходящих границу Варшамова – Гильберта. Определена система образующих $\tilde{T}_n/\tilde{T}_{n-1}$, картина ветвления точек. Однако пока не удалось определить базисы пространств $L(G)$ на ступенях башни $\tilde{T}$, поэтому построение соответствующих АГ–кодов осталось за рамками дипломной работы и открывает перспективы для дальнейших исследований.

СПИСОК ЛИТЕРАТУРЫ

1. Влэдуц С.Г., Дринфельд В.Г. О числе точек алгебраической кривой // Функциональный анализ и его приложения. – 1983. Т.17, вып. 1. – 68-69 с.
2. Влэдуц С.Г. Алгеброгеометрические коды. Основные понятия / Влэдуц С.Г., Ногин Д.Ю., Цфасман М.А. – М.: НМУ, 2003.
3. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки / перевод с англ. И.И.Грушко, В.А.Зиновьева под ред. Л.А.Бассалыго. – М.: Связь, 1979.
4. Kendall E. Atkinson Solving linear systems // Lectures section 8.1, 2015 http://homepage.divms.uiowa.edu/~atkinson/m171.dir/sec_8-1.pdf
5. Bassa A., Beelen P. The Galois closure of Drinfeld modular towers // Journal of number theory. – 2011. p. 561-577.
6. Beelen P., Garcia A. & Stichtenoth H. On towers of function fields over finite fields // Seminaires & Congres 11, 2005. p.1-20.
7. Garcia A., Stichtenoth H. On the asymptotic behavior of some towers of function fields over finite fields // Journal of number theory – 61, 1996. p. 248-273.
8. Garcia A., Stichtenoth H. On the Galois closure of towers // Recent Trends in Coding Theory and Its Applications. 2007.
9. Garcia A., Stichtenoth H. The tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound // Inventiones mathematicae vol. 121. - 1995. – p. 211-222.
10. Garcia A., Stichtenoth H. Topics in geometry, coding theory and cryptography // Algebra and applications. – Springer 2007. vol. 6.
11. Goppa V.D. Geometry and codes // Kluwer academic publishers. – Boston 1998.
12. Guruswami V, Xing C. Optimal rate list decoding over bounded alphabets using algebraic-geometry codes // Arxiv:1708.01070 arxiv.org – 2017.
13. Ihara Y. Some remarks on the number of rational points of algebraic curves over finite fields // J. Fac. Sci. Univ. Tokyo sect. IA Math 28. 1981. p.721-724.

14. Newman Stephen C. A classical introduction to Galois theory // John Wiley&Sons Inc. publication. Hoboken. – New Jersey, 2012.
15. Shum Kenneth W., Aleshnikov I., Kumar Vijay P., Stichtenoth H., Deolalikar V. A low-complexity algorithm for the construction of algebraic-geometric codes better than the Gilbert-Varshamov bound // IEEE Transactions on information theory, vol.46, no.6, September 2001.
16. Stichtenoth H. Algebraic function fields and codes // Graduate texts in mathematics 254. – Springer-Verlag 2009. second edition.
17. Stichtenoth H. Transitive and self-dual codes attaining the Tsfasman-Vladut-Zink bound // Arxiv:math/0506264v1 [math.ag], 14 June 2005.
18. Zaytsev A. The Galois closure of the Garcia-Stichtenoth tower // Finite fields and their applications. – 2007. issue 13, p. 751-761.

ПРИЛОЖЕНИЕ А. ПРОГРАММНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМОВ

Приведем реализацию алгоритмов сверточного кодирования и декодирования на ступени башни Гарсии – Штихтенота $T_2/\mathbb{F}_9$. Соответствующие алгоритмы описаны в п. 3.1-3.3.

В качестве средства программирования выбрана система компьютерной алгебры Maple 18.00, так как она позволяет наглядно продемонстрировать полученные теоретические результаты. В случае реализации алгоритмов кодирования на языке программирования высокого уровня общего назначения, следовало бы сначала реализовать выполнение операций в конечных полях, векторных пространствах, алгоритмы решения систем линейных уравнений, и т.д. Это представляет собой отдельную трудоемкую задачу, которая не входит в рамки настоящей научно-исследовательской работы.

Параметры N, l, D в алгоритмах кодирования и декодирования следует выбирать из таблицы Б.1 приложения Б.

1. Предварительные вычисления.

```
restart;
with(numtheory);
interface(prettyprint=0, rtablesize=10);
p := 3;
n := 2;
q := p^n;
N := 10;
l := 8;
Dp := 7;
```

[GIgcd, bigomega, cfrac, cfracpol, cyclotomic, divisors, factorEQ, factorset, fermat, imagunit, index, integral_basis, invcfrac, invphi, iscyclotomic, issqrfree, ithrational, jacobi, kronecker, λ, legendre, mcombine, mersenne, migcdex, minkowski, mipolys, mlog, mobius, mroot, msqrt, nearestp, nthconver, nthdenom, nthnumer, nthpow, order, pdexpand, ϕ, π, pprimroot, primroot, quadres, rootsunity, safeprime, σ, sq2factor, sum2sqr, τ, thue]

3, 10

3

2

9

10

8

7

```
# Построим таблицу индексов поле F_q=F_p(zeta)
# Выведем таблицу индексов поля F_q
fpoly := x^2 + x + 2;
alias(zeta = RootOf(fpoly, x) mod p);
for i from 1 to q - 1 do
 evala(zeta^i) mod p;
end do;
```

$x^2 + x + 2$

ζ

ζ

$2\zeta + 1$

$2\zeta + 2$

2

2ζ

$\zeta + 2$

$\zeta + 1$

1

```
# Найдем элементы F_q, след которых равен 0
Km := [0]:
 for i from 1 to q − 1 do
  if evala(zeta^(i·p) + zeta^i) mod p = 0 then
   Km := [op(Km), evala(zeta^i) mod p];
 end if;
 end do;
'Km'= Km;
 Kms := convert({op(Km)} minus {0}, list):
'Kms'= Kms;
```

$$Km = [0, 2\zeta + 1, \zeta + 2]$$

$$Kms = [\zeta + 2, 2\zeta + 1]$$

2. Вспомогательные процедуры

```
# Carl Love 12216 from mapleprimes.com
# https://www.mapleprimes.com/questions/204469-How-Can-I-Find-The-
    Coefficients-Of-Linear
# CoeffsOfLinCombo находит коэффициенты в разложении элемента
    векторного пространства по заданной системе образующих
# PolyLinearCombo находит нетривиальную линейную комбинацию
    элементов системы образующих векторного пространства, равную 0
 # Пример использования:
 # F := [1, alpha·x, (2·alpha + 1)·x^2]; - система образующих;
 # f := x; — элемент векторного пространства;
 # C := PolyLinearCombo(F, f, {x, y}); - f по системе F;
 # CoeffsOfLinComb(F, {x, y});
     - найти нетривиальную линейную комбинацию элементов из F,
     равную 0

CoeffsOfLinComb := proc(
   L :: list(polynom),
   V :: set(name) := indets(L, And(name, Not(constant)))
 )
local
   c, k, C := {c[k] $ k = 1 ..nops(L)},
   S := solve({coeffs(expand(`+`((C*~L)[])), V)}, C),
   F := indets(rhs~(S), name) intersect C =~ 1
;
   eval([C[]], eval(S, F)) union F)
end proc:


PolyLinearCombo := proc(
   F :: list(polynom),
   f :: And(polynom, Not(identical(0))),
   V :: set(name) := indets([F, f], And(name, Not(constant)))
 )
local C := CoeffsOfLinComb([f, F[]], V);
   if C[1] = 0 then (false, []) else (true, -C[2 ..] /~ C[1]) end if
 end proc:
```

3. Процедура поиска базиса пространства $L(Q_\infty)$

```
# поиск базиса пространства Римана-Роха L(lQ_∞), l ≥ 7
RRBasis := proc(l)
 local B, dval, i, i1, i2;
 global p, n, q;
 dval := 1; # Нормирование текущего элемент в точке Q_∞
 B := [1, x1];
 for i1 from 0 to n + 1/3 do
 for i2 from 0 to p - 1 do
 dval := -6 - i1·p - i2;
    #` `Вычиляем нормирование текущего элемента в` `Q_∞
 if (dval ≥ -l) then
 B := [op(B), x1^i1·x2^i2·(x1^2 + 1)];
 end if;
 end do;
 end do;
 if convert(CoeffsOfLinComb(B, {x1, x2}), set) ≠ {0} or l + 1 - 4
     ≠ nops(B) then
  print("RRBasis() FAILED!!!");
 end if;
 return B;
 end proc;
```

4. Процедура выбора *N* точек кода

```
# Выбрать N точек кода
Find_points :=proc(N)
 local i, j, Q, beta, gamm, sp, trac;
 global p, n, q, Km, Kms;
 beta := [ ] :
 for i from 1 to p − 1 do
 gamm[i] := [ ]; # Элементы поля, след которых равен i
 end do:

for i from 1 to q − 1 do
 if not (evala(zeta^i) mod p in Km) then
    # Составляем список допустимых beta
 beta := [op(beta), evala(zeta^i) mod p];
 end if;
 trac := evala(Trace(zeta^i)) mod p;
 gamm[trac] := [op(gamm[trac]), evala(zeta^i) mod p];
 end do:
 if (nops(beta) < ceil(N/p)) then
print("Недопустимое N");
 return 0;
 end if;

 for i from 1 to ceil(N/p) do # Находим вторые координаты точек
sp := evala((beta[i]^p)/(beta[i]^(p−1) + 1)) mod p;
 for j from 1 to nops(gamm[sp]) do
Q[p·(i − 1) + j] := [beta[i], gamm[sp][j]];
 end do:
 end do:
 return Q;
 end proc;
```

5. Процедура кодирования сообщения

```
FGS_encode := proc(f)
 local i, j, L1, Q, sigm, y, f_rr;
 global p, n, q, Km, Kms, N, l;
 L1 := RRBasis(l); # Предварительные вычисления
 Q := Find_points(N);
 print('Базис lQ_inf'= L1);
 print('Точки кода Q');
 for i from 1 to N do
  print(Q[i]);
  end do:
 f_rr := 0; # Сообщение как элемент L(lQ_inf)
 for i from 1 to nops(L1) do
 f_rr := f_rr + L1[i]·f[i];
 end do;
 print('Сообщение' f);
 print('Сообщение как элемент L(lQ_inf)' f_rr);
 sigm := x→2·x mod p; # Автоморфизм F_q
y := Matrix(1..2, 1..N) : # Кодирование сообщения
 for i from 1 to N do
y[1, i] := evala(eval(f_rr, {x1 = Q[i][1], x2 = Q[i][2]})) mod p;
y[2, i] := evala(eval(f_rr, {x1 = sigm(Q[i][1]), x2 = sigm(Q[i][2])}))
     mod p;
 end do:
print('Кодовое слово');
 return y;
 end proc;
```

6. Процедура декодирования

```
FGS_decode := proc(y)
 local i, j, L1, L2, L3, l2, l3, Q, sigm, f, f_rr, A0, A1, ar, as, jsu, ln1, ln2,
      coeff_matrix, b, x, Q_poly, fk, fka;
 global p, n, q, Km, Kms, N, l, Dp;
 L1 := RRBasis(l); # Предварительные вычисления
 L2 := RRBasis(Dp);
 l2 := Dp - 3;
 L3 := RRBasis(Dp + l);
 l3 := Dp + l - 3;
 Q := Find_points(N);
 print('Базис lQ_inf'= L1);
 print('Базис DQ_inf'= L2);
 print('Базис (D + l)Q_inf'= L3);
 print('Точки кода Q');
 for i from 1 to N do
  print(Q[i]);
 end do:
 sigm := x→2·x mod p; # Автоморфизм F_q
 # Задаем A0 и A1 с неопределенными коэффициентами
A0 := sum(ar[jsu]·L3[jsu], jsu = 1 ..nops(L3));
A1 := sum(as[jsu]·L2[jsu], jsu = 1 ..nops(L2)); coeff_matrix := Matrix(1
      ..2·N, 1 ..l2 + l3) :
for i from 1 to N do
ln1 := evala(eval(A0 + A1·y[1, i], {x1 = Q[i][1], x2 = Q[i][2]}))
     mod p :
for j from 1 to l3 do
 coeff_matrix[2· i - 1, j] := coeff(ln1, ar[j]);
end do;
 for j from l3 + 1 to l3 + l2 do
 coeff_matrix[2· i - 1, j] := coeff(ln1, as[j - l3]);
end do;

ln2 := evala(eval(A0 + A1·y[2, i], {x1 = sigm(Q[i][1]), x2
      = sigm(Q[i][2])})) mod p :
 for j from 1 to l3 do
  coeff_matrix[2· i, j] := coeff(ln2, ar[j]);
 end do;
 for j from l3 + 1 to l3 + l2 do
  coeff_matrix[2· i, j] := coeff(ln2, as[j - l3]);
 end do;
 end do:
b := Vector(2·N) :
 for i from 1 to 2·N do
 b[i] := 0;
 end do:
```

```
x := Linsolve(coeff_matrix, b) mod p;
    # Находим решения для неопределенных коэффициентов A0 и A1
for i from 1 to 3·N + 2 do # Находим нетривиальное частное решение
x := eval(x, _t[i] = 1);
 end do:
 x := evala(x) mod p;

 print('Система уравнений для нахождения многочлена Q');
 print(coeff_matrix, b);
print('Частное решение системы');
 print(x);

 A0 := 0 : # Составляем A0 и A1
for i from 1 to nops(L3) do
  A0 := A0 + x[i]·L3[i];
 end do:
 print('A0'= A0);
A1 := 0 :
for i from 1 to nops(L2) do
  A1 := A1 + x[nops(L3) + i]·L2[i];
 end do:
 print('A1'= A1);
 Q_poly := A0 + A1·Y :


    # Записываем декодируемое сообщение с неопределенными
    коэффициентами
 fk := sum(fka[jsu]·L1[jsu], jsu = 1 ..nops(L1));
 # Составляем новую систему линейных уравнений
coeff_matrix := Matrix(1 .. N, 1 ..nops(L1)) :
b := Vector(N) :
 for i from 1 to N do
  ln1 := evala(eval(eval(Q_poly, Y = fk), {x1 = Q[i][1], x2 = Q[i][2]}))
     mod p :
  for j from 1 to nops(L1) do
   coeff_matrix[i, j] := evala(coeff(ln1, fka[j])) mod p;
   ln1 := ln1 − coeff_matrix[i, j]·fka[j];
  end do:
 b[i] := −evala(ln1) mod p;
 end do:
x := Linsolve(coeff_matrix, b) mod p;
```

```
print('Система уравнений для декодирования f');
print(coeff_matrix, b);
print('Решение системы');
 print(x);

 f := convert(x, list);
f_rr := 0; # Сообщение как элемент L(lQ_inf)
 for i from 1 to nops(L1) do
 f_rr := f_rr + L1[i]·f[i];
 end do;
 print('Декодированное сообщение' f);
 print('Декодированное сообщение как элемент L(lQ_inf) ' f_rr);

 end proc;
```

7. Пример

$msg := [2, zeta, 0, 2, 1];$
$y := FGS\_encode(10, 8, msg);$
$y[2, 3] := y[2, 3] + zeta;$

$$[2, \zeta, 0, 2, 1]$$

$$Базис\ lQ\_inf = [1, x1, x1^2 + 1, x2\,(x1^2 + 1), x2^2\,(x1^2 + 1)]$$

Точки кода Q

$$[\zeta, 2]$$
$$[\zeta, 2\,\zeta]$$
$$[\zeta, \zeta + 1]$$
$$[2\,\zeta + 2, 2]$$
$$[2\,\zeta + 2, 2\,\zeta]$$
$$[2\,\zeta + 2, \zeta + 1]$$
$$[2, 2]$$
$$[2, 2\,\zeta]$$
$$[2, \zeta + 1]$$
$$[2\,\zeta, \zeta]$$

$$Сообщение\ [2, \zeta, 0, 2, 1]$$

$$Сообщение\ как\ элемент\ L(lQ\_inf)\ (2 + x1\,\zeta + 2\,x2\,(x1^2 + 1) + x2^2\,(x1^2 + 1))$$

Кодовое слово

$$\begin{bmatrix} 1 & \zeta+2 & \zeta+2 & 2\zeta+1 & \zeta+1 & \zeta+1 & 2\zeta & 2\zeta+1 & 2\zeta+1 & 2 \\ \zeta+1 & 2 & \zeta+2 & 0 & 1 & \zeta+2 & \zeta+2 & 1 & 2\zeta+2 & \zeta+2 \end{bmatrix}$$

$$2\,\zeta + 2$$

$FGS\_decode(10, 8, 7, y);$

$$Базис\ lQ\_inf = [1, x1, x1^2 + 1, x2\,(x1^2 + 1), x2^2\,(x1^2 + 1)]$$

$$Базис\ DQ\_inf = [1, x1, x1^2 + 1, x2\,(x1^2 + 1)]$$

$$Базис\ (D + 8)\ Q\_inf = [1, x1, x1^2 + 1, x2\,(x1^2 + 1), x2^2\,(x1^2 + 1), x1\,(x1^2 + 1), x1\,x2\,(x1^2 + 1), x1\,x2^2\,(x1^2 + 1), x1^2\,(x1^2 + 1), x1^2\,x2\,(x1^2 + 1), x1^2\,x2^2\,(x1^2 + 1), x1^3\,(x1^2 + 1)]$$

Точки кода Q

$$[\zeta, 2]$$
$$[\zeta, 2\,\zeta]$$
$$[\zeta, \zeta + 1]$$
$$[2\,\zeta + 2, 2]$$
$$[2\,\zeta + 2, 2\,\zeta]$$
$$[2\,\zeta + 2, \zeta + 1]$$
$$[2, 2]$$
$$[2, 2\,\zeta]$$
$$[2, \zeta + 1]$$
$$[2\,\zeta, \zeta]$$

Система уравнений для нахождения многочлена Q

$$\begin{bmatrix} 20\ x\ 16\ Matrix \\ Data\ Type:\ anything \\ Storage:\ rectangular \\ Order:\ Fortran\_order \end{bmatrix}, \begin{bmatrix} 1\ ..\ 20\ Vector_{column} \\ Data\ Type:\ anything \\ Storage:\ rectangular \\ Order:\ Fortran\_order \end{bmatrix}$$

Частное решение системы

$$\begin{bmatrix} 1\ ..\ 16\ Vector_{column} \\ Data\ Type:\ anything \\ Storage:\ rectangular \\ Order:\ Fortran\_order \end{bmatrix}$$

$$A0 = 2\,\zeta + 2 + 2\,x1\,\zeta + (2\,\zeta + 1)\,(x1^2 + 1) + (\zeta + 2)\,x2\,(x1^2 + 1) + (2\,\zeta + 1)\,x2^2\,(x1^2 + 1) + 2\,\zeta\,x1\,(x1^2 + 1) + (2\,\zeta + 1)\,x1\,x2\,(x1^2 + 1) + 2\,x1\,x2^2\,(x1^2 + 1) + 2\,x1^2\,x2\,(x1^2 + 1) + 2\,x1^3\,(x1^2 + 1)$$

$$A1 = \zeta + 3 + x1 + x1^2 + x2\,(x1^2 + 1)$$

Система уравнений для декодирования f

$$\begin{bmatrix} 2\zeta+2 & 2 & \zeta+2 & 2\zeta+1 & \zeta+2 \\ \zeta+2 & \zeta+1 & \zeta & \zeta+2 & 2\zeta+2 \\ 2 & 2\zeta & \zeta+1 & \zeta+2 & 2\zeta \\ 1 & 2\zeta+2 & \zeta & 2\zeta & \zeta \\ 2\zeta & 1 & \zeta+2 & 2\zeta+2 & 1 \\ \zeta+2 & \zeta & \zeta+1 & \zeta+2 & 2\zeta \\ \zeta+1 & 2\zeta+2 & 2\zeta+2 & \zeta+1 & 2\zeta+2 \\ 2\zeta & \zeta & \zeta & \zeta+2 & 2\zeta+2 \\ 2 & 1 & 1 & \zeta+1 & \zeta+2 \\ 2\zeta & 2\zeta+1 & 1 & \zeta & 2\zeta+1 \end{bmatrix}, \begin{bmatrix} 2\zeta+2 \\ 2 \\ 2\zeta+1 \\ 2\zeta+1 \\ 2 \\ 2\zeta \\ 2(\zeta+1)\zeta \\ \zeta(\zeta+2) \\ \zeta+2 \\ \zeta \end{bmatrix}$$

Решение системы

$$\begin{bmatrix} 2 \\ \zeta \\ 0 \\ 2 \\ 1 \end{bmatrix}$$

Декодированное сообщение $[2, \zeta, 0, 2, 1]$

Декодированное сообщение как элемент $L(lQ\_inf)$ $\left(2 + x1\,\zeta + 2\,x2\left(x1^2 + 1\right) + x2^2\left(x1^2 + 1\right)\right)$

ПРИЛОЖЕНИЕ Б. ТАБЛИЦЫ ПАРАМЕТРОВ КОДА НА МЛАДШИХ СТУПЕНЯХ БАШНИ T

В приведенных ниже таблицах мы перечислим основные свойства сверточных АГ – кодов, построенных на ступенях T_2, T_3, T_4 по схеме, описанной в п. 2.4. Во-первых, вычислим род указанных функциональных полей по формуле (21):

$g_2 = g(T_2) = 4$	$g_3 = g(T_3) = 16$	$g_4 = g(T_4) = 64$

Во-вторых, свойства и все остальные параметры кода главным образом зависят от первоначального выбора l: $G = lQ_\infty$. Рассмотрим все возможные выборы l исходя из ограничений (40). Затем для каждого l рассмотрим все возможные выборы числа точек $\frac{l}{m} < N \leq r^e \cdot \left\lfloor \frac{r-1}{m} \right\rfloor$ и вычислим основные параметры кода:

- D – степенной параметр, используется в конструкции алгоритма декодирования;
- Nm – длина кода;
- $k = \deg(G) + 1 - g_e$ – размерность кода;
- $R = \frac{k}{Nm}$ – скорость кода;
- $t_{min} \leq t^* \leq t_{max}$ – число исправляемых ошибок согласно (39).

Поле констант башни $\mathbb{F}_{r^2} = \mathbb{F}_{3^2}$ и параметры $m = 2$, $s = 1$ зафиксируем.

Таблица Б.1 Параметры кода над T_2

l	N	D	t_{min}	t_{max}	k	R
8	5	5	0	1	5	0.5
	6	6	0	2	5	0.417
	7	7	1	4	5	0.357
	8	8	1	5	5	0.313
	9	9	2	7	5	0.278
9	5	4	---	1	6	0.6
	6	5	0	2	6	0.5
	7	6	0	4	6	0.429
	8	7	1	5	6	0.375
	9	8	1	7	6	0.333
10	6	5	0	2	7	0.583
	7	6	0	3	7	0.5
	8	7	1	5	7	0.438
	9	8	1	6	7	0.389

l	N	D	t_{min}	t_{max}	k	R
11	6	4	---	2	8	0.667
	7	5	0	3	8	0.571
	8	6	0	5	8	0.5
	9	7	1	6	8	0.444
12	7	5	0	3	9	0.643
	8	6	0	4	9	0.563
	9	7	1	6	9	0.5
13	7	4	---	3	10	0.714
	8	5	0	4	10	0.625
	9	6	0	6	10	0.556
14	8	5	0	4	11	0.688
	9	6	0	5	11	0.611
15	8	4	---	4	12	0.75
	9	5	0	5	12	0.667
16	9	5	0	5	13	0.722
17	9	4	---	5	14	0.778

Таблица Б.2 Параметры кода над T_3

l	N	D	t_{min}	t_{max}	k	R
32	17	17	0	1	17	0.5
	18	18	0	2	17	0.472
	19	19	1	4	17	0.447
	20	20	1	5	17	0.425
	21	21	2	7	17	0.405
	22	22	2	8	17	0.386
	23	23	3	10	17	0.37
	24	24	3	11	17	0.354
	25	25	4	13	17	0.34
	26	26	4	14	17	0.327
	27	27	5	16	17	0.315
33	17	16	---	1	18	0.529
	18	17	0	2	18	0.5
	19	18	0	4	18	0.474
	20	19	1	5	18	0.45
	21	20	1	7	18	0.429
	22	21	2	8	18	0.409
	23	22	2	10	18	0.391
	24	23	3	11	18	0.375
	25	24	3	13	18	0.36
	26	25	4	14	18	0.346
	27	26	4	16	18	0.333
34	18	17	0	2	19	0.528
	19	18	0	3	19	0.5
	20	19	1	5	19	0.475
	21	20	1	6	19	0.452
	22	21	2	8	19	0.432
	23	22	2	9	19	0.413
	24	23	3	11	19	0.396
	25	24	3	12	19	0.38
	26	25	4	14	19	0.365
	27	26	4	15	19	0.352

l	N	D	t_{min}	t_{max}	k	R
35	18	16	---	2	20	0.556
	19	17	0	3	20	0.526
	20	18	0	5	20	0.5
	21	19	1	6	20	0.476
	22	20	1	8	20	0.455
	23	21	2	9	20	0.435
	24	22	2	11	20	0.417
	25	23	3	12	20	0.4
	26	24	3	14	20	0.385
	27	25	4	15	20	0.37
36	19	17	0	3	21	0.553
	20	18	0	4	21	0.525
	21	19	1	6	21	0.5
	22	20	1	7	21	0.477
	23	21	2	9	21	0.457
	24	22	2	10	21	0.438
	25	23	3	12	21	0.42
	26	24	3	13	21	0.404
	27	25	4	15	21	0.389
37	19	16	---	3	22	0.579
	20	17	0	4	22	0.55
	21	18	0	6	22	0.524
	22	19	1	7	22	0.5
	23	20	1	9	22	0.478
	24	21	2	10	22	0.458
	25	22	2	12	22	0.44
	26	23	3	13	22	0.423
	27	24	3	15	22	0.407

Таблица Б.2 Параметры кода над T_3 (продолжение)

l	N	D	t_{min}	t_{max}	k	R
38	20	17	0	4	23	0.575
	21	18	0	5	23	0.548
	22	19	1	7	23	0.523
	23	20	1	8	23	0.5
	24	21	2	10	23	0.479
	25	22	2	11	23	0.46
	26	23	3	13	23	0.442
	27	24	3	14	23	0.426
39	20	16	---	4	24	0.6
	21	17	0	5	24	0.571
	22	18	0	7	24	0.545
	23	19	1	8	24	0.522
	24	20	1	10	24	0.5
	25	21	2	11	24	0.48
	26	22	2	13	24	0.462
	27	23	3	14	24	0.444
40	21	17	0	5	25	0.595
	22	18	0	6	25	0.568
	23	19	1	8	25	0.543
	24	20	1	9	25	0.521
	25	21	2	11	25	0.5
	26	22	2	12	25	0.481
	27	23	3	14	25	0.463
41	21	16	---	5	26	0.619
	22	17	0	6	26	0.591
	23	18	0	8	26	0.565
	24	19	1	9	26	0.542
	25	20	1	11	26	0.52
	26	21	2	12	26	0.5
	27	22	2	14	26	0.481
42	22	17	0	6	27	0.614
	23	18	0	7	27	0.587
	24	19	1	9	27	0.563
	25	20	1	10	27	0.54
	26	21	2	12	27	0.519
	27	22	2	13	27	0.5
43	22	16	---	6	28	0.636
	23	17	0	7	28	0.609
	24	18	0	9	28	0.583
	25	19	1	10	28	0.56
	26	20	1	12	28	0.538
	27	21	2	13	28	0.519
44	23	17	0	7	29	0.63
	24	18	0	8	29	0.604
	25	19	1	10	29	0.58
	26	20	1	11	29	0.558
	27	21	2	13	29	0.537
45	23	16	---	7	30	0.652
	24	17	0	8	30	0.625
	25	18	0	10	30	0.6
	26	19	1	11	30	0.577
	27	20	1	13	30	0.556
46	24	17	0	8	31	0.646
	25	18	0	9	31	0.62
	26	19	1	11	31	0.596
	27	20	1	12	31	0.574
47	24	16	---	8	32	0.667
	25	17	0	9	32	0.64
	26	18	0	11	32	0.615
	27	19	1	12	32	0.593

Таблица Б.2 Параметры кода над T_3 (продолжение)

l	N	D	t_{min}	t_{max}	k	R
48	25	17	0	9	33	0.66
	26	18	0	10	33	0.635
	27	19	1	12	33	0.611
49	25	16	---	9	34	0.68
	26	17	0	10	34	0.654
	27	18	0	12	34	0.63
50	26	17	0	10	35	0.673
	27	18	0	11	35	0.648
51	26	16	---	10	36	0.692
	27	17	0	11	36	0.667
52	27	17	0	11	37	0.685
53	27	16	---	11	38	0.704

Таблица Б.3 Параметры кода над T_4

l	N	D	t_{min}	t_{max}	k	R
128	65	65	0	1	65	0.5
	66	66	0	2	65	0.492
	67	67	1	4	65	0.485
	68	68	1	5	65	0.478
	69	69	2	7	65	0.471
	70	70	2	8	65	0.464
	71	71	3	10	65	0.458
	72	72	3	11	65	0.451
	73	73	4	13	65	0.445
	74	74	4	14	65	0.439
	75	75	5	16	65	0.433
	76	76	5	17	65	0.428
	77	77	6	19	65	0.422
	78	78	6	20	65	0.417
	79	79	7	22	65	0.411
	80	80	7	23	65	0.406
	81	81	8	25	65	0.401
129	65	64	---	1	66	0.508
	66	65	0	2	66	0.5
	67	66	0	4	66	0.493
	68	67	1	5	66	0.485
	69	68	1	7	66	0.478
	70	69	2	8	66	0.471
	71	70	2	10	66	0.465
	72	71	3	11	66	0.458
	73	72	3	13	66	0.452
	74	73	4	14	66	0.446
	75	74	4	16	66	0.44
	76	75	5	17	66	0.434
	77	76	5	19	66	0.429
	78	77	6	20	66	0.423
	79	78	6	22	66	0.418
	80	79	7	23	66	0.413
	81	80	7	25	66	0.407
130	66	65	0	2	67	0.508
	67	66	0	3	67	0.5
	68	67	1	5	67	0.493
	69	68	1	6	67	0.486
	70	69	2	8	67	0.479
	71	70	2	9	67	0.472
	72	71	3	11	67	0.465
	73	72	3	12	67	0.459
	74	73	4	14	67	0.453
	75	74	4	15	67	0.447
	76	75	5	17	67	0.441
	77	76	5	18	67	0.435
	78	77	6	20	67	0.429
	79	78	6	21	67	0.424
	80	79	7	23	67	0.419
	81	80	7	24	67	0.414
131	66	64	---	2	68	0.515
	67	65	0	3	68	0.507
	68	66	0	5	68	0.5
	69	67	1	6	68	0.493
	70	68	1	8	68	0.486
	71	69	2	9	68	0.479
	72	70	2	11	68	0.472
	73	71	3	12	68	0.466
	74	72	3	14	68	0.459
	75	73	4	15	68	0.453
	76	74	4	17	68	0.447
	77	75	5	18	68	0.442

Таблица Б.3 Параметры кода над T_4 (продолжение)

l	N	D	t_{min}	t_{max}	k	R
131	78	76	5	20	68	0.436
	79	77	6	21	68	0.43
	80	78	6	23	68	0.425
	81	79	7	24	68	0.42
132	67	65	0	3	69	0.515
	68	66	0	4	69	0.507
	69	67	1	6	69	0.5
	70	68	1	7	69	0.493
	71	69	2	9	69	0.486
	72	70	2	10	69	0.479
	73	71	3	12	69	0.473
	74	72	3	13	69	0.466
	75	73	4	15	69	0.46
	76	74	4	16	69	0.454
	77	75	5	18	69	0.448
	78	76	5	19	69	0.442
	79	77	6	21	69	0.437
	80	78	6	22	69	0.431
	81	79	7	24	69	0.426
133	67	64	---	3	70	0.522
	68	65	0	4	70	0.515
	69	66	0	6	70	0.507
	70	67	1	7	70	0.5
	71	68	1	9	70	0.493
	72	69	2	10	70	0.486
	73	70	2	12	70	0.479
	74	71	3	13	70	0.473
	75	72	3	15	70	0.467
	76	73	4	16	70	0.461
	77	74	4	18	70	0.455
	78	75	5	19	70	0.449

l	N	D	t_{min}	t_{max}	k	R
133	79	76	5	21	70	0.443
	80	77	6	22	70	0.438
	81	78	6	24	70	0.432
134	68	65	0	4	71	0.522
	69	66	0	5	71	0.514
	70	67	1	7	71	0.507
	71	68	1	8	71	0.5
	72	69	2	10	71	0.493
	73	70	2	11	71	0.486
	74	71	3	13	71	0.48
	75	72	3	14	71	0.473
	76	73	4	16	71	0.467
	77	74	4	17	71	0.461
	78	75	5	19	71	0.455
	79	76	5	20	71	0.449
	80	77	6	22	71	0.444
	81	78	6	23	71	0.438
135	68	64	---	4	72	0.529
	69	65	0	5	72	0.522
	70	66	0	7	72	0.514
	71	67	1	8	72	0.507
	72	68	1	10	72	0.5
	73	69	2	11	72	0.493
	74	70	2	13	72	0.486
	75	71	3	14	72	0.48
	76	72	3	16	72	0.474
	77	73	4	17	72	0.468
	78	74	4	19	72	0.462
	79	75	5	20	72	0.456
	80	76	5	22	72	0.45
	81	77	6	23	72	0.444

Таблица Б.3 Параметры кода над T_4 (продолжение)

l	N	D	t_{min}	t_{max}	k	R
136	69	65	0	5	73	0.529
	70	66	0	6	73	0.521
	71	67	1	8	73	0.514
	72	68	1	9	73	0.507
	73	69	2	11	73	0.5
	74	70	2	12	73	0.493
	75	71	3	14	73	0.487
	76	72	3	15	73	0.48
	77	73	4	17	73	0.474
	78	74	4	18	73	0.468
	79	75	5	20	73	0.462
	80	76	5	21	73	0.456
	81	77	6	23	73	0.451
137	69	64	---	5	74	0.536
	70	65	0	6	74	0.529
	71	66	0	8	74	0.521
	72	67	1	9	74	0.514
	73	68	1	11	74	0.507
	74	69	2	12	74	0.5
	75	70	2	14	74	0.493
	76	71	3	15	74	0.487
	77	72	3	17	74	0.481
	78	73	4	18	74	0.474
	79	74	4	20	74	0.468
	80	75	5	21	74	0.463
	81	76	5	23	74	0.457
138	70	65	0	6	75	0.536
	71	66	0	7	75	0.528
	72	67	1	9	75	0.521
	73	68	1	10	75	0.514
	74	69	2	12	75	0.507
	75	70	2	13	75	0.5

l	N	D	t_{min}	t_{max}	k	R
138	76	71	3	15	75	0.493
	77	72	3	16	75	0.487
	78	73	4	18	75	0.481
	79	74	4	19	75	0.475
	80	75	5	21	75	0.469
	81	76	5	22	75	0.463
139	70	64	---	6	76	0.543
	71	65	0	7	76	0.535
	72	66	0	9	76	0.528
	73	67	1	10	76	0.521
	74	68	1	12	76	0.514
	75	69	2	13	76	0.507
	76	70	2	15	76	0.5
	77	71	3	16	76	0.494
	78	72	3	18	76	0.487
	79	73	4	19	76	0.481
	80	74	4	21	76	0.475
	81	75	5	22	76	0.469
140	71	65	0	7	77	0.542
	72	66	0	8	77	0.535
	73	67	1	10	77	0.527
	74	68	1	11	77	0.52
	75	69	2	13	77	0.513
	76	70	2	14	77	0.507
	77	71	3	16	77	0.5
	78	72	3	17	77	0.494
	79	73	4	19	77	0.487
	80	74	4	20	77	0.481
	81	75	5	22	77	0.475
141	71	64	---	7	78	0.549
	72	65	0	8	78	0.542
	73	66	0	10	78	0.534

Таблица Б.3 Параметры кода над T_4 (продолжение)

l	N	D	t_{min}	t_{max}	k	R
141	74	67	1	11	78	0.527
	75	68	1	13	78	0.52
	76	69	2	14	78	0.513
	77	70	2	16	78	0.506
	78	71	3	17	78	0.5
	79	72	3	19	78	0.494
	80	73	4	20	78	0.488
	81	74	4	22	78	0.481
142	72	65	0	8	79	0.549
	73	66	0	9	79	0.541
	74	67	1	11	79	0.534
	75	68	1	12	79	0.527
	76	69	2	14	79	0.52
	77	70	2	15	79	0.513
	78	71	3	17	79	0.506
	79	72	3	18	79	0.5
	80	73	4	20	79	0.494
	81	74	4	21	79	0.488
143	72	64	---	8	80	0.556
	73	65	0	9	80	0.548
	74	66	0	11	80	0.541
	75	67	1	12	80	0.533
	76	68	1	14	80	0.526
	77	69	2	15	80	0.519
	78	70	2	17	80	0.513
	79	71	3	18	80	0.506
	80	72	3	20	80	0.5
	81	73	4	21	80	0.494
144	73	65	0	9	81	0.555
	74	66	0	10	81	0.547
	75	67	1	12	81	0.54
	76	68	1	13	81	0.533
144	77	69	2	15	81	0.526
	78	70	2	16	81	0.519
	79	71	3	18	81	0.513
	80	72	3	19	81	0.506
	81	73	4	21	81	0.5
145	73	64	---	9	82	0.562
	74	65	0	10	82	0.554
	75	66	0	12	82	0.547
	76	67	1	13	82	0.539
	77	68	1	15	82	0.532
	78	69	2	16	82	0.526
	79	70	2	18	82	0.519
	80	71	3	19	82	0.513
	81	72	3	21	82	0.506
146	74	65	0	10	83	0.561
	75	66	0	11	83	0.553
	76	67	1	13	83	0.546
	77	68	1	14	83	0.539
	78	69	2	16	83	0.532
	79	70	2	17	83	0.525
	80	71	3	19	83	0.519
	81	72	3	20	83	0.512
147	74	64	---	10	84	0.568
	75	65	0	11	84	0.56
	76	66	0	13	84	0.553
	77	67	1	14	84	0.545
	78	68	1	16	84	0.538
	79	69	2	17	84	0.532
	80	70	2	19	84	0.525
	81	71	3	20	84	0.519
148	75	65	0	11	85	0.567
	76	66	0	12	85	0.559

Таблица Б.3 Параметры кода над T_4 (продолжение)

l	N	D	t_{min}	t_{max}	k	R
148	77	67	1	14	85	0.552
	78	68	1	15	85	0.545
	79	69	2	17	85	0.538
	80	70	2	18	85	0.531
	81	71	3	20	85	0.525
149	75	64	---	11	86	0.573
	76	65	0	12	86	0.566
	77	66	0	14	86	0.558
	78	67	1	15	86	0.551
	79	68	1	17	86	0.544
	80	69	2	18	86	0.538
	81	70	2	20	86	0.531
150	76	65	0	12	87	0.572
	77	66	0	13	87	0.565
	78	67	1	15	87	0.558
	79	68	1	16	87	0.551
	80	69	2	18	87	0.544
	81	70	2	19	87	0.537
151	76	64	---	12	88	0.579
	77	65	0	13	88	0.571
	78	66	0	15	88	0.564
	79	67	1	16	88	0.557
	80	68	1	18	88	0.55
	81	69	2	19	88	0.543
152	77	65	0	13	89	0.578
	78	66	0	14	89	0.571
	79	67	1	16	89	0.563
	80	68	1	17	89	0.556
	81	69	2	19	89	0.549
153	77	64	---	13	90	0.584
	78	65	0	14	90	0.577
	79	66	0	16	90	0.57
	80	67	1	17	90	0.563
	81	68	1	19	90	0.556
154	78	65	0	14	91	0.583
	79	66	0	15	91	0.576
	80	67	1	17	91	0.569
	81	68	1	18	91	0.562
155	78	64	---	14	92	0.59
	79	65	0	15	92	0.582
	80	66	0	17	92	0.575
	81	67	1	18	92	0.568
156	79	65	0	15	93	0.589
	80	66	0	16	93	0.581
	81	67	1	18	93	0.574
157	79	64	---	15	94	0.595
	80	65	0	16	94	0.588
	81	66	0	18	94	0.58
158	80	65	0	16	95	0.594
	81	66	0	17	95	0.586
159	80	64	---	16	96	0.6
	81	65	0	17	96	0.593
160	81	65	0	17	97	0.599
161	81	64	---	17	98	0.605