ЛИТЕРАТУРА


1. *Сохацкий Ф. Н.* Об ассоциативности многоместных операций // Дискретная математика. 1992. Т. 4. № 1. С. 66–84.
2. *Сосинский Л. М.* О представлении функций бесповторными суперпозициями в трехзначной логике // Проблемы кибернетики. М.: Наука, 1964. Вып. 12. С. 57–68.
3. *Белоусов В. Д.* $n$-Арные квазигруппы. Кишинев: Штиинца, 1972. 277 с.
4. *Черемушкин А. В.* Некоторые асимптотические оценки для класса сильно зависимых функций // Вестник Томского госуниверситета. Приложение. 2006. № 17. С. 87–94.
5. *Черемушкин А. В.* Аналоги теорем Глускина — Хоссу и Малышева для сильно зависимых $n$-арных операций // Дискретная математика, 2018. Т. 30. Вып. 2. С. 15–24.
6. *Bruck R. H.* A survey of binary systems. Berlin; Heidelberg; New York: Springer, 1958. 185 p.
7. *Post E. L.* Polyadic groups // Trans. Amer. Math. Soc. 1940. V. 48. No. 2. P. 208–350.
8. *Черемушкин А. В.* Теорема Поста для сильно зависимых $n$-арных полугрупп // Дискретная математика. 2019. Т. 31. № 2. С. 153–158.
9. *Глускин Л. М.* Позиционные оперативы // Математич. сборник. 1965. Т. 68 (110). № 3. С. 444–472.
10. *Hosszu M.* On the explicit form of $n$-group operations // Publ. Math. 1963. V. 10. No. 1–4. P. 88–92.
11. *Гальмак А. М., Воробьев Г. Н.* О теореме Поста — Глускина — Хоссу // Проблемы физики, математики и техники. 2013. Вып. 1(14). С. 55–59.
12. *Черемушкин А. В.* Бесповторная декомпозиция сильно зависимых функций // Дискретная математика. 2004. Т. 16. Вып. 3. С. 3–42.
13. *Черемушкин А. В.* Декомпозиция и классификация дискретных функций. М.: Курс, 2018. 288 с.
14. *Khodabandeh H. and Shahryari M.* On the automorphisms and representations of polyadic groups // Commun. Algebra. 2012. V. 40. No. 6. P. 2199–2212.


УДК 519.728 DOI 10.17223/2226308X/12/11

# МИНИМАЛЬНОЕ ПРЕДСТАВИТЕЛЬНОЕ МНОЖЕСТВО ДЛЯ СИСТЕМЫ ЧАСТОТНЫХ КЛАССОВ НЕДООПРЕДЕЛЁННЫХ СЛОВ

Л. А. Шоломов

Частотный класс недоопределённых слов — это множество всех слов в некотором недоопределённом алфавите, имеющих заданную длину и заданные частоты вхождения символов. Рассматривается задача доопределения произвольной системы частотных классов. Предложен метод выделения из этой системы минимальной по мощности подсистемы, такой, что достаточно получить доопределения для классов этой подсистемы, а по ним доопределения других классов системы находятся просто.

**Ключевые слова:** *недоопределённые данные, доопределение, частотный класс, представительное множество.*

Пусть $M = \{0, 1, \ldots, m-1\}$ и выделена система $\mathcal{T} \subseteq 2^M$ некоторых непустых подмножеств $T \subseteq M$. С множеством $M$ связан алфавит $A_0 = \{a_i : i \in M\}$ *основных* символов, с множеством $\mathcal{T}$ — алфавит $A = \{a_T : T \in \mathcal{T}\}$ *недоопределённых* символов. *Доопределением символа* $a_T$ считается всякий основной символ $a_i$, $i \in T$, *доопределением слова* $v$ в алфавите $A$ — любое слово, полученное из $v$ заменой каждого символа каким-либо его доопределением, а *доопределением множества* $V$ слов в алфавите $A$ —

любое множество слов в алфавите $A_0$, содержащее для каждого слова $v \in V$ некоторое его доопределение. Символ $a_M$, доопределимый любым основным символом, называется *неопределённым* и обозначается $*$. Подробнее о недоопределённых данных в [1].

Будем говорить, что недоопределённый символ $a_T$ *чётче символа* $a_{T'}$, если $T \subseteq T'$, и что слово $v = a_{T_1} \dots a_{T_l}$ *чётче слова* $v' = a_{T'_1} \dots a_{T'_l}$, если каждый символ $a_{T_i}$ слова $v$ чётче соответствующего символа $a_{T'_i}$ слова $v'$. Ясно, что если $v$ чётче $v'$, то любое доопределение слова $v$ доопределяет $v'$.

Для заданного набора $\mathbf{r} = (r_T : T \in \mathcal{T})$ натуральных чисел положим $l = \sum\limits_{T \in \mathcal{T}} r_T$ и обозначим через $\mathcal{K}_l(\mathbf{r})$ класс всех слов длины $l$ в алфавите $A$, в которых каждый символ $a_T$ встречается $r_T$ раз (т. е. с частотой $r_T/l$). Такие классы называют *частотными*.

Скажем, что класс $\mathcal{K}_{l_1}(\mathbf{r}_1)$ *представительнее* класса $\mathcal{K}_{l_2}(\mathbf{r}_2)$, если $l_1 \geqslant l_2$ и, каково бы ни было доопределение $\mathcal{D}_{l_1}(\mathbf{r}_1)$ класса $\mathcal{K}_{l_1}(\mathbf{r}_1)$, множество $\mathcal{D}_{l_1}(\mathbf{r}_1)|_{l_2}$ начал длины $l_2$ слов, входящих в $\mathcal{D}_{l_1}(\mathbf{r}_1)$, образует некоторое доопределение класса $\mathcal{K}_{l_2}(\mathbf{r}_2)$. Отметим, что если в качестве возможных доопределений для $\mathcal{K}_{l_2}(\mathbf{r}_2)$ использовать вместо начал слов из $\mathcal{D}_{l_1}(\mathbf{r}_1)$ другие их фрагменты, расположенные в $l_2$ различных фиксированных разрядах, это не повлияет на введённое понятие, поскольку частотные классы замкнуты относительно перестановок символов в словах.

Пусть $\mathfrak{K}$ — некоторая конечная система частотных классов, заданная перечислением параметров $(l, \mathbf{r})$ входящих в неё классов $\mathcal{K}_l(\mathbf{r})$. Подсистему $\mathfrak{M} \subseteq \mathfrak{K}$ назовём *представительным множеством системы* $\mathfrak{K}$, если для любого $\mathcal{K}_l(\mathbf{r}) \in \mathfrak{K}$ в $\mathfrak{M}$ имеется класс, который представительнее $\mathcal{K}_l(\mathbf{r})$. Представительное множество $\mathfrak{M}$ называется *минимальным*, если не существует представительного множества для $\mathfrak{K}$, содержащего меньшее число частотных классов.

Цель данной работы — построение минимального представительного множества для заданной системы частотных классов. Такая задача возникает в некоторых методах сжатия недоопределённых данных и реализации недоопределённых функций (см., например, [2]). Они обобщают подход Э. И. Нечипорука [3]. Эти методы требуют нахождения доопределений для всех частотных классов подходящей системы. Решение задачи упрощается за счёт сведения к задаче доопределения минимального представительного множества этой системы.

Пусть заданы классы $\mathcal{K}_{l_1}(\mathbf{r}_1)$ и $\mathcal{K}_{l_2}(\mathbf{r}_2)$, $l_1 \geqslant l_2$, и требуется выяснить, является ли $\mathcal{K}_{l_1}(\mathbf{r}_1)$ более представительным. Образуем класс $\mathcal{K}_{l_1}(\mathbf{r}_2^+)$, слова которого получены из слов класса $\mathcal{K}_{l_2}(\mathbf{r}_2)$ добавлениями $l_1 - l_2$ символов $*$. Компоненты $r_{2,T}$ и $r'_{2,T}$ наборов $\mathbf{r}_2$ и $\mathbf{r}_2^+$ связаны соотношениями $r'_{2,*} = r_{2,*} + l_1 - l_2$ и $r'_{2,T} = r_{2,T}$, $a_T \neq *$.

**Лемма 1.** Класс $\mathcal{K}_{l_1}(\mathbf{r}_1)$ представительнее $\mathcal{K}_{l_2}(\mathbf{r}_2)$ тогда и только тогда, когда найдётся пара слов $(v, v')$, $v \in \mathcal{K}_{l_1}(\mathbf{r}_1)$, $v' \in \mathcal{K}_{l_1}(\mathbf{r}_2^+)$, в которой $v$ чётче $v'$.

***Доказательство.*** Пусть такая пара $(v, v')$ существует. Рассмотрим произвольное слово $w$ класса $\mathcal{K}_{l_2}(\mathbf{r}_2)$. Образуем слово $w' \in \mathcal{K}_{l_1}(\mathbf{r}_2^+)$ путём дописывания к $w$ в конце $l_1 - l_2$ символов $*$. Найдётся перестановка $\sigma$ символов слова $w'$, для которой $\sigma(w') = v'$. Построим слово $u = \sigma^{-1}(v)$. Оно чётче $w'$ и принадлежит классу $\mathcal{K}_{l_1}(\mathbf{r}_1)$. Любое доопределение слова $u$ доопределяет $w'$, а его начало длины $l_2$ доопределяет $w$.

Допустим теперь, что пара $(v, v')$ с указанным свойством отсутствует, т. е. для любых $v \in \mathcal{K}_{l_1}(\mathbf{r}_1)$ и $v' \in \mathcal{K}_{l_1}(\mathbf{r}_2^+)$ слово $v$ не чётче $v'$. Возьмём некоторое слово $w \in \mathcal{K}_{l_2}(\mathbf{r}_2)$ и образуем из него слово $v' \in \mathcal{K}_{l_1}(\mathbf{r}_2^+)$ приписыванием $l_1 - l_2$ символов $*$. Всякое слово $v \in \mathcal{K}_{l_1}(\mathbf{r}_1)$ не чётче $v'$, а потому в нём присутствует символ $a_{T_i}$, хотя бы одно из доопределений которого не доопределяет соответствующий символ $a_{T'_i}$ слова $v'$. По-

скольку последними $l_1 - l_2$ символами слова $v'$ являются $*$, символ $a_{T_i}$ принадлежит началу слова $v$. Это означает возможность доопределить слово $v$ так, чтобы начало этого доопределения не являлось доопределением слова $w$. В силу произвольности слова $v \in \mathcal{K}_{l_1}(\mathbf{r}_1)$ отсюда следует существование для класса $\mathcal{K}_{l_1}(\mathbf{r}_1)$ такого доопределения, среди начал слов которого нет доопределений слова $w \in \mathcal{K}_{l_2}(\mathbf{r}_2)$, а потому $\mathcal{K}_{l_1}(\mathbf{r}_1)$ не представительнее класса $\mathcal{K}_{l_2}(\mathbf{r}_2)$. ■

Пусть, как и раньше, $\mathbf{r}_1 = (r_{1,T} : T \in \mathcal{T}_1)$, $\mathbf{r}_2^+ = (r'_{2,T'} : T' \in \mathcal{T}_2)$, где

$$\sum_{T \in \mathcal{T}_1} r_{1,T} = \sum_{T' \in \mathcal{T}_2} r'_{2,T'} = l_1.$$

Построим ориентированную потоковую сеть [4] с полюсами $s$ (источник) и $t$ (сток), с внутренними вершинами $\alpha_T$, $T \in \mathcal{T}_1$, и $\beta_{T'}$, $T' \in \mathcal{T}_2$, с дугами $(s, \alpha_T)$, имеющими пропускные способности $r_{1,T}$, с дугами $(\beta_{T'}, t)$, имеющими пропускные способности $r'_{2,T'}$, а также с дугами $(\alpha_T, \beta_{T'})$, $T \subseteq T'$, обладающими достаточно большими пропускными способностями (например, равными $l_1$).

**Лемма 2.** Пара слов $(v, v')$, такая, что $v \in \mathcal{K}_{l_1}(\mathbf{r}_1)$, $v' \in \mathcal{K}_{l_1}(\mathbf{r}_2^+)$ и $v$ чётче $v'$, существует тогда и только тогда, когда максимальный поток в построенной сети равен $l_1$.

***Доказательство.*** Пусть максимальный поток равен $l_1$. Поскольку совокупность дуг $(s, \alpha_T)$, $T \in \mathcal{T}_1$, образует разрез, из равенства $\sum\limits_T r_{1,T} = l_1$ следует, что в каждой из них поток совпадает с пропускной способностью $r_{1,T}$. Аналогичные рассуждения показывают, что и в дугах $(\beta_{T'}, t)$, $T' \in \mathcal{T}_2$, достигается пропускная способность $r'_{2,T'}$.

Обозначим через $z_{TT'}$ поток в дуге $(\alpha_T, \beta_{T'})$. В соответствии с теоремой Форда — Фалкерсона величины $z_{TT'}$ можно считать целыми. По набору чисел $z_{TT'}$, где $T \in \mathcal{T}_1$, $T' \in \mathcal{T}_2$, $T \subseteq T'$, образуем слова $v$ и $v'$ так, чтобы в них имелось ровно $z_{TT'}$ позиций, в которых в слове $v$ находится символ $a_T$, а в слове $v'$ — символ $a_{T'}$. Из конструкции сети и сказанного выше о достижимости в дугах $(s, \alpha_T)$ и $(\beta_{T'}, t)$ пропускных способностей следует, что $\sum\limits_{T'} z_{TT'} = r_{1,T}$, $\sum\limits_T z_{TT'} = r'_{2,T'}$, а потому $v \in \mathcal{K}_{l_1}(\mathbf{r}_1)$, $v' \in \mathcal{K}_{l_1}(\mathbf{r}_2^+)$. Кроме того, $v$ очевидно чётче $v'$ и, следовательно, пара слов $(v, v')$ обладает требуемыми свойствами.

Эти рассуждения допускают обращение. По паре $(v, v')$ с указанными свойствами может быть построен поток, равный $l_1$, который максимален. ■

**Лемма 3.** Существует полиномиальный алгоритм выяснения по наборам параметров $(l_1, \mathbf{r}_1)$ и $(l_2, \mathbf{r}_2)$, является ли класс $\mathcal{K}_{l_1}(\mathbf{r}_1)$ более представительным, чем $\mathcal{K}_{l_2}(\mathbf{r}_2)$.

***Доказательство.*** Если $l_1 < l_2$, то ответ отрицателен. Дальше считаем $l_1 \geqslant l_2$.

Образуем из $\mathbf{r}_2$ набор $\mathbf{r}_2^+$ заменой компоненты $r_{2,*}$ на $r_{2,*} + l_1 - l_2$ и построим по $(l_1, \mathbf{r}_1)$ и $(l_2, \mathbf{r}_2^+)$ потоковую сеть описанным выше способом. Применением полиномиального алгоритма найдём в ней максимальный поток [4]. Из лемм 1 и 2 следует, что класс $\mathcal{K}_{l_1}(\mathbf{r}_1)$ представительнее $\mathcal{K}_{l_2}(\mathbf{r}_2)$ тогда и только тогда, когда этот поток равен $l_1$. ■

**Теорема 1.** Для любой системы $\mathfrak{K}$ частотных классов имеется единственное минимальное представительное множество $\mathfrak{M}$. Оно может быть найдено со сложностью, ограниченной полиномом от максимальной длины $l$ слов из $\mathfrak{K}$.

***Доказательство.*** Отношение представительности частотных классов — частичный порядок. В конечной системе $\mathfrak{K}$ частотных классов имеется единственная подсистема классов, максимальных по этому отношению, которая и образует минимальное

представительное множество. Оно может быть найдено путём попарного сравнения частотных классов системы $\mathfrak{K}$ по отношению представительности с использованием леммы 3. Мощность системы $\mathfrak{K}$ ограничена числом частотных классов с длиной слов не выше $l$, которое не превосходит $l^{|A|}$, где $|A|$ — мощность алфавита $A$, а число пар классов из $\mathfrak{K}$ не больше $l^{2|A|}$. Поскольку $|A|$ — константа, а трудоёмкость сравнения одной пары по представительности полиномиальна, процедура выделения минимального представительного множества полиномиальна по $l$. ■

ЛИТЕРАТУРА

1. *Шоломов Л. А.* Элементы теории недоопределённой информации // Прикладная дискретная математика. Приложение. 2009. № 2. С. 18–42.
2. *Шоломов Л. А.* О функционалах, характеризующих сложность систем недоопределенных булевых функций // Проблемы кибернетики. Вып. 19. М.: Физматлит, 1967. С. 123–139.
3. *Нечипорук Э. И.* О сложности вентильных схем, реализующих булевские матрицы с неопределенными элементами // ДАН СССР. 1965. Т. 163. № 1. С. 40–42.
4. *Адельсон-Вельский Г. М., Диниц Е. А., Карзанов А. В.* Потоковые алгоритмы. М.: Наука, 1975.

UDC 512.772.7 DOI 10.17223/2226308X/12/12

## CHARACTERISTIC POLYNOMIALS OF THE CURVE $y^2 = x^7 + ax^4 + bx$ OVER FINITE FIELDS

S. A. Novoselov[1], Y. F. Boltnev

In this work, we list all possible characteristic polynomials of the Frobenius endomorphism for genus 3 hyperelliptic curves of type $y^2 = x^7 + ax^4 + bx$ over finite field $\mathbb{F}_q$ of characteristic $p > 3$.

**Keywords:** *hyperelliptic curves, characteristic polynomials, point-counting, genus* 3.

### Introduction

Let $\mathbb{F}_q$ be a finite field of size $q = p^n$, $p > 2$. In this note, we study the hyperelliptic curves of genus $g = 3$ of the form

$$C : y^2 = x^{2g+1} + ax^{g+1} + bx.$$

The Jacobian $J_C$ of the curves is split [1] over certain finite field extension:

$$J_C \sim J_{D_1} \times J_{D_2},$$

where $D_1$ and $D_2$ are explicitly given curves. This fact allows us to reduce the problem of point-counting on the curve $C$ to counting points on the curves $D_1$ and $D_2$.

For genus 2 case it was done in the works [2, 3]. The work [1] contains algorithms for $g > 2$ case. In this work, we give explicit formulae for the number of points on the Jacobian in the case of $g = 3$.

The point-counting on the curve is equivalent to finding of zeta-function of the curve

$$Z(C/\mathbb{F}_q; T) = \exp\left(\sum_{k=1}^{\infty} \#C(\mathbb{F}_{q^k})\frac{T^k}{k}\right) = \frac{L_{C,q}(T)}{(1-T)(1-qT)},$$

[1]The author is supported by RFBR according to the research project No. 18-31-00244.