УДК 519.17 DOI 10.17223/2226308X/11/36

# ИССЛЕДОВАНИЕ ГРУППЫ АВТОМОРФИЗМОВ КОДА, АССОЦИИРОВАННОГО С ОПТИМАЛЬНОЙ КРИВОЙ РОДА ТРИ

Е. С. Малыгина

Установлены условия, при которых группа автоморфизмов оптимальной кривой рода три над конечным полем с дискриминантом из множества $\{-19, -43, -67, -163\}$ изоморфна группе автоморфизмов АГ-кода, асоциированного с такой кривой.

**Ключевые слова:** *оптимальная кривая, дискриминант конечного поля, АГ-код, группа автоморфизмов кода, группа афтоморфизмов кривой.*

В последнее время в современной криптографии актуальным направлением развития считается исследование и использование криптосистем на основе кодов. Их преимущество заключается в высокой скорости криптографического преобразования информации, однако существуют трудности в их практическом применении из-за большого объёма ключа. Поскольку известные схемы, построенные на кодах Рида — Соломона, могут быть взломаны с полиномиальной сложностью, перспективным представляется использование алгебро-геометрических кодов (АГ-кодов).

АГ-коды предложены В. Д. Гоппой в 1977 г. В современной теории кодирования они называются геометрическими кодами Гоппы, с их помощью можно доказать существование длинных линейных кодов, являющихся лучшими, нежели коды, достигающие границы Варшамова — Гилберта. Благодаря геометрическим кодам Гоппы получено много новых интересных кодов на специальных кривых с большим числом рациональных точек. В теории кодирования весьма часто представляют интерес коды, имеющие большую группу автоморфизмов. В свое время Х. Штихтенот, внеся коррективы в работы Гоппы, заключил, что автоморфизмы кривой рода 0 индуцируют автоморфизмы ассоциированного с этой кривой кода [1]. Те же рассуждения удалось применить К. Ксингу к некоторым эллиптическим и эрмитовым кривым [2, 3]. Возникает вопрос, чем же так примечательна группа автоморфизмов АГ-кода? Оказывается, знание группы автоморфизмов кода или даже части этой группы даёт информацию о структуре кода и зачастую может быть использовано в алгоритме декодирования.

Пусть $C$ — гладкая неприводимая проективная кривая рода $g$, определённая над конечным полем $\mathbb{F}_q$.

**Определение 1.** Если число рациональных точек кривой $C/\mathbb{F}_q$ удовлетворяет границе Хассе — Вейля — Серра

$$\#C(\mathbb{F}_q) = q + 1 \pm g[2\sqrt{q}],$$

то кривая называется *оптимальной*.

Введём понятие дискриминанта конечного поля, поскольку далее будем рассматривать оптимальные кривые над конечными полями с заданными дискриминантами.

**Определение 2.** Число $d(\mathbb{F}_q) = d = \lfloor 2\sqrt{(q)}\rfloor^2 - 4q$ называется *дискриминантом* конечного поля $\mathbb{F}_q$.

Учитывая эквивалентность по Ж.-П. Серру [4] между категорией обычных абелевых многообразий и категорией $\mathcal{O}_K$-модулей, где $K = \mathbb{Q}(\sqrt{d})$, применяя далее

теорему Торелли [5] и рассматривая конечные поля с дискриминантами $d(\mathbb{F}_q) \in \{-19, -43, -67, -163\}$, можем использовать таблицу классификации эрмитовых модулей с заданными дискриминантами, откуда следует, что порядок группы автоморфизмов оптимальной кривой рода три над конечным полем с указанными дискриминантами равен 6. Следующая теорема описывает структуру группы $\mathrm{Aut}_{\mathbb{F}_q}(C)$.

**Теорема 1** [6]. Пусть $C$ – оптимальная кривая рода три над конечным полем $\mathbb{F}_q$ с дискриминантом $d(\mathbb{F}_q) \in \{-19, -43, -67, -167\}$. Тогда

$$\mathrm{Aut}_{\mathbb{F}_q}(C) \cong D_3,$$

где $D_3$ — диэдральная группа порядка 6.

Существование оптимальных кривых рода три над рассматриваемыми конечными полями доказано в [7]. Следующая теорема даёт явное описание оптимальных кривых.

**Теорема 2** [7]. Оптимальная кривая $C$ рода три над конечным полем $\mathbb{F}_q$ с дискриминантом $d \in \{-19, -43, -67, -163\}$ задаётся следующими уравнениями:

$$\begin{cases} z^2 = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \beta_0 y, \\ y^2 = x^3 + ax + b, \end{cases}$$

или

$$\begin{cases} z^2 = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + (\beta_0 + \beta_1 x) y, \\ y^2 = x^3 + ax + b, \end{cases}$$

или

$$\begin{cases} z^2 = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3 + (\beta_0 + \beta_1 x) y, \\ y^2 = x^3 + ax + b, \end{cases}$$

где $\alpha_0, \alpha_1, \alpha_2, \beta_0, \beta_1, a, b \in \mathbb{F}_q$.

Отметим, что в условиях предыдущей теоремы кривая $C$ является двойным накрытием оптимальной эллиптической кривой, заданной уравнением $y^2 = x^3 + ax + b$.

Переходя к исследованию группы автоморфизмов кода, ассоциированного с оптимальной кривой, полученной выше, введём ряд обозначений:

- $J \subseteq \mathbb{P}^{(1)}_C \setminus P_\infty$, где $P_\infty | \infty' \in E$, а $\infty' | \infty \in \mathbb{P}^1$ при отображениях $f : C \to E$ и $E \to \mathbb{P}^1$; отметим, что $f$ — двойное накрытие оптимальной эллиптической кривой $E$;
- $n = |J|$;
- $D = \sum\limits_{P \in J} P = P_1 + P_2 + \ldots + P_n$;
- $C_{\mathcal{L}}(D, rP_\infty)$ — АГ-код, ассоциированный с дивизорами $D$ и $rP_\infty$ (очевидно, что $\mathrm{supp}(D) \cap \mathrm{supp}(rP_\infty) = \varnothing$);
- $\mathrm{Aut}(C_{\mathcal{L}}(D, rP_\infty))$ — группа автоморфизмов кода $C_{\mathcal{L}}(D, rP_\infty)$.

Переобозначим группу автоморфизмов кривой в терминах группы автоморфизмов функционального поля этой кривой, ассоциированной с дивизорами $D$ и $rP_\infty$, как $\mathrm{Aut}_{D,rP_\infty}(C/\mathbb{F}_q)$.

Согласно [8], любой элемент группы $\mathrm{Aut}_{D,rP_\infty}(C/\mathbb{F}_q)$ индуцирует автоморфизм соответствующего кода $C_{\mathcal{L}}(D, rP_\infty)$. Таким образом, $\mathrm{Aut}_{D,rP_\infty}(C/\mathbb{F}_q) \subseteq \mathrm{Aut}(C_{\mathcal{L}}(D, rP_\infty))$. Однако благодаря следующей теореме получаем изоморфизм между соответствующими группами автоморфизмов.

**Теорема 3.** Пусть $C/\mathbb{F}_q$ — оптимальная кривая рода три, определённая над конечным полем с дискриминантом из $\{-19, -43, -67, -163\}$; элементы $x, y, z \in C(\mathbb{F}_q)$

такие, что $(x)_\infty = kP_\infty$, $(y)_\infty = mP_\infty$ и $(z)_\infty = lP_\infty$, где $m > l > k$. Пусть $D = \sum\limits_{P \in J} P$, где $J \subseteq \mathbb{P}_C^{(1)} \setminus P_\infty$. Если $n > \max\{3r, 2\,(l + (k-1)/\mu)\,, 2\,(m + (k-1)/\eta)\}$, причём $\mu = \min\{k-1, \zeta : z^\zeta \in \mathcal{L}(rP_\infty)\}$, $\eta = \min\{k-1, \xi : y^\xi \in \mathcal{L}(rP_\infty)\}$, то

$$\mathrm{Aut}(C_\mathcal{L}(D, rP_\infty)) \cong \mathrm{Aut}_{D,rP_\infty}(C/\mathbb{F}_q).$$

## ЛИТЕРАТУРА


1. *Stichtenoth H.* On automorphisms of geometric Goppa codes // J. Algebra. 1990. V. 130. Iss. 1. P. 113–121.
2. *Xing C.* Automorphism group of elliptic codes // Communication in Algebra. 1995. No. 23(11). P. 4061–4072.
3. *Xing C.* On automorphism groups of the Hermitian codes // IEEE Trans. Inform. Theory. 1995. No. 41(6). P. 1629–1635.
4. *Lauter K.* Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields. With an appendix by J.-P. Serre // Algebraic Geometry. 2001. No. 10(1). P. 19–36.
5. *Milne J. S.* Abelian Varieties. 2008. `www.jmilne.org/math/`
6. *Alekseenko E. and Zaytsew A.* Explicit equations of optimal curves of genus 3 over certain fields with three parametrs // Contemporary Math. 2015. No. 637. P. 245–256.
7. *Alekseenko E., Aleshnikov S., Markin N., and Zaytsew A.* Optimal curves over finite fields with discriminant $-19$ // Finite Fields and Their Applications. 2011. No. 17(4). P. 350–358.
8. *Stichtenoth H.* Algebraic Function Fields and Codes. Springer, 2009.


УДК 519.7 DOI 10.17223/2226308X/11/37

# ПРИМЕНЕНИЕ КОНЕЧНЫХ АВТОМАТОВ ДЛЯ НЕЧЁТКОГО БИНАРНОГО ПОИСКА

И. В. Панкратов

Рассматривается задача нечёткого поиска булевых векторов в потоке данных. Под нечётким вхождением искомого вектора понимается вхождение вектора, близкого к искомому в смысле расстояния Хемминга. Предлагается метод построения конечного автомата для решения данной задачи по заданному набору искомых шаблонов в виде булевых векторов (возможно, частично определённых) и допустимого отклонения для каждого шаблона. Возможно построение автомата, принимающего на вход отдельные биты данных, и автомата, принимающего сразу группы битов. Приводятся оценки размеров таблиц переходов и выходов автомата. Представлены экспериментальные данные производительности поисковых автоматов, принимающих на вход отдельные биты данных, четвёрки битов и восьмёрки битов, а также производительность классического подхода к задаче нечёткого поиска, основанного на регистре сдвига.

**Ключевые слова:** *поисковые автоматы, нечёткий поиск, бинарный поиск, синхропосылка, поиск подстроки, КМП-поиск, алгоритм Ахо — Корасик.*

## 1. Задача бинарного поиска в потоке данных и классический подход к ней

Рассматриваемую задачу можно сформулировать так. Имеется двоичная последовательность (*поток данных*) и набор из $n$ булевых векторов (слов) различной длины, далее называемых *шаблонами*. Необходимо найти в последовательности вхождения