*ЗАЩИТА ИНФОРМАЦИИ*

УДК 512.81, 519.95

*Е. С. Алексеенко*

# АЛГЕБРО-ГЕОМЕТРИЧЕСКИЙ КОД, АССОЦИИРОВАННЫЙ С КРИВОЙ РОДА 3 НАД КОНЕЧНЫМ ПОЛЕМ С ДИСКРИМИНАНТОМ –19

*Описаны построение AG-кода и процедура декодирования с точки зрения пространств, ассоциированных с дивизорами.*

*The construction of an AG-code and the process of decoding are described by the Rimann-Roch spaces.*

**Ключевые слова:** алгебро-геометрический код, алгебраическая кривая, пространство Римана-Роха.

**Key words:** algebraic-geometric code, algebraic curve, code automorphism, Riemann-Roch space.

Идея построения линейных кодов, ассоциированных с алгебраическими кривыми, определенными над конечным полем $\mathrm{F}_q$, была представлена Гоппой. Такие коды обычно называются *алгебро-геометрическими кодами (AG-кодами)*. Обычно AG-коды с хорошими параметрами ассоциированы с кривыми с больши́м числом $\mathrm{F}_q$ — рациональных точек в соответствии с родом кривых $g$.

Цель этой статьи — исследовать параметры AG-кода, ассоциированного с некоторым классом максимальных кривых. Число точек таких кривых удовлетворяет границе Хассе — Вейля — Серре.

Рассмотрим максимальную кривую $C:\begin{cases} z^2 = 5 + 45x + 30x^2 + 10y, \\ y^2 = x^3 + x + 38, \end{cases}$ определенную над полем $\mathrm{F}_{47}$, с числом рациональных точек, равным $n = C(\mathrm{F}_q) = 87$. Для упрощения дальнейших вычислений данную систему уравнений мы можем свести к следующему уравнению над $\mathrm{F}_{47}$:

$$z^4 + 37z^2 + 4z^2x + 34z^2x^2 + 32 + 21x + 22x^2 + 15x^3 + 7x^4 = 0. \qquad (1)$$

Перейдем непосредственно к вычислению параметров AG-кода. Пусть $C_L(D, G)$ — алгебро-геометрический код, определенный для рациональных дивизоров $D$ и $G$ на несингулярной проективной кривой $C$ над $\mathrm{F}_{47}$. В качестве дивизора $D = P_1 + \ldots + P_{87}$ рассмотрим дивизор, состоящий из суммы точек нашей кривой, где $P_1 = (2, 46, 8), \ldots, P_{87} = (46, 6, 35)$. Если же свести нашу систему к уравнению (1), то достаточно рассмотреть точки $P_1 = (2, 8), \ldots, P_{87} = (46, 35)$. Отметим, что степени точек равны $\deg P_i = 1$ для $i$ = 1, …, 87. В качестве дивизора $G$, такого, что $\mathrm{s\,upp}\, G \bigcap \mathrm{supp}\, D = \varnothing$, рассмотрим $G = 5\mathrm{O}$, где $G = f^{-1}(\infty') = \sum_{\mathrm{O}|\infty'} e(\mathrm{O}\,|\,\infty')\cdot \mathrm{O}$, и $f : C \to E, \infty' \in E, \infty \in \mathrm{P}^1$. Поскольку $\deg \mathrm{O} = 2$, то $\deg G = 10$, и $\dim G = \deg G + 1 - g = 8$ (по теореме Римана — Роха).

Пусть $L(G)$ — пространство, ассоциированное с дивизором $G$. В качестве базиса $L(G)$ рассмотрим $\left\{1, x, x^2, x^3, z, z^2, xz^2, x^2z^2\right\}$. Тогда код

$$C_L(D, G) = \left\{(1(P_1), \ldots, 1(P_{87}), \ldots, x^2z^2(P_1), \ldots, x^2z^2(P_{87}) \,|\, 1, \ldots, x^2z^2 \in L(G)\right\} \subseteq \mathrm{F}_{47}^{87}.$$

Параметры кода найдем с помощью следующей теоремы.

**Теорема.** *Если степень дивизора G меньше n, то* $C_L(D, G)$ *— [n, k, d]-код, где* $d > n - \deg G - 1$ *и* $k = \dim G > \deg G + 1 - g - 1$.

*Вестник Российского государственного университета им. И. Канта. 2010. Вып. 10. С. 104 – 107.*

Окончательно, учитывая нижнюю границу для минимального расстояния, получаем код с параметрами [87, 8, *d*], где $76 < d < 81$. Значение *d* уточним с помощью следующей теоремы.

**Теорема.** *Пусть* $C_L(D, G)$ — [*n*, *k*, *d*]-*линейный код над полем* $\mathrm{F}_q$ *с проверочной матрицей B*, $s \in \mathrm{N}$. *Тогда d = s тогда и только тогда, когда любые* $s-1$ *столбцов матрицы B являются линейно независимыми и существуют s линейно зависимых столбцов.*

Учитывая, что порождающая матрица $A = \begin{pmatrix} f_1(P_1) & \dots & f_1(P_n) \\ \vdots & & \vdots \\ f_k(P_1) & \dots & f_k(P_n) \end{pmatrix}$,

где $f_i$ — элементы базиса пространства $L(G)$ для $i = 1, \dots, k$, а также решая систему уравнений $B \cdot A^T = 0$ и учитывая предыдущую теорему, окончательно получаем, что параметр *d* = 77.

Таким образом, код $C_L(D, G)$ является [87, 8, 77]-кодом.

Опишем процедуру декодирования для $C_L(D, G)$. Пусть *a* — вектор, который мы желаем декодировать. Отметим, что расстояние от *a* до кодового слова $C_L(D, G)$ минимально. Также мы найдем функцию локатора ошибок вектора *a*, которую можно определить, решив систему линейных уравнений. Пусть *t* — целое, удовлетворяющее условию

$$0 < t < (d^* - 1)/2, \qquad (2)$$

где $d^*$ — определяющее расстояние кода $C_L(D, G)$. Следующая теорема даст нам условия, относительно которых мы найдем пространство функций локатора ошибок.

**Теорема.** *Если есть дивизор* $G_1$ *на кривой C, удовлетворяющий условиям*

$$\operatorname{supp} G_1 \cap \operatorname{supp} D = \varnothing,\ \deg G_1 < \deg G - (2g-2) - t,\ \dim G_1 > t, \qquad (3)$$

*то* $L(G_1)$ *содержит функцию локатора ошибок для вектора a. В частности,* $f \in L(G_1)$ *является функцией локатора ошибок тогда и только тогда, когда* $f = \sum_{\mu=1}^{l} \alpha_\mu \xi_\mu$, *где* $(x_1, \dots, x_l) = (\alpha_1, \dots, \alpha_l)$ — *нетривиальное решение линейной системы*

$$\sum_{\mu=1}^{l} [a, \xi_\mu \eta_\rho] \cdot x_\mu = 0, \text{ для } \rho = 1, \dots, k, \qquad (4)$$

*где* $\{\xi_1, \dots, \xi_l\}$ и $\{\eta_1, \dots, \eta_k\}$ — *базисы пространств* $L(G_1)$ *и* $L(G - G_1)$ *соответственно.*

В нашем случае в качестве дивизора $G_1$, удовлетворяющего условию (3) предыдущей теоремы, следует рассмотреть $G_1 = 2O$. При этом очевидно, что *t* = 2 удовлетворяет условию (2).

Теперь определим базисы пространств: $L(G_1), L(G - G_1), L(G)$. Для этого первоначально найдем размерности дивизоров, ассоциированных с этими пространствами.

$$\dim G_1 = \dim 2O = 3 = l,\ \dim(G - G_1) = \dim 3O = 4 = k.$$

Имеем: $\{\xi_1, \dots, \xi_l\} = \{1, x, z\}$ — базис $L(G_1)$; $\{\eta_1, \dots, \eta_k\} = \{1, x, z, x^2\}$ — базис $L(G - G_1)$; $\{\xi_1, \dots, \xi_m\} = \left\{1, x, x^2, x^3, z, z^2, xz^2, x^2z^2\right\}$ — базис $L(G)$.

Система (4) принимает вид

$$[a, \eta_\rho] \cdot x_1 + [a, x(P_i) \cdot \eta_\rho] \cdot x_2 + [a, z(P_i) \cdot \eta_\rho] \cdot x_3 = 0, \rho = 1, \dots, 4; i = 1, \dots, 87,$$

или более подробно:

$$\begin{cases} [a, 1] \cdot x_1 + [a, x(P_i)] \cdot x_2 + [a, z(P_i)] \cdot x_3 = 0, \\ [a, x(P_i)] \cdot x_1 + [a, x^2(P_i)] \cdot x_2 + [a, xz(P_i)] \cdot x_3 = 0, \\ [a, z(P_i)] \cdot x_1 + [a, xz(P_i)] \cdot x_2 + [a, z^2(P_i)] \cdot x_3 = 0, \\ [a, x^2(P_i)] \cdot x_1 + [a, x^3(P_i)] \cdot x_2 + [a, x^2z(P_i)] \cdot x_3 = 0. \end{cases}$$

Окончательно система сводится к следующему виду:

$$\begin{cases} 39 \cdot x_3 = 0, \\ 13 \cdot x_3 = 0, \\ 39 \cdot x_1 + 13 \cdot x_2 + 21 \cdot x_3 = 0, \\ 38 \cdot x_3 = 0. \end{cases}$$

Итак, уравнение имеет нетривиальное решение: $(x_1, 44x_1, 0)$ в поле $F_{47}$. Положив $x_1 = 1$, имеем решение системы (1, 44, 0).

Итак, получаем функцию локатора ошибок $f = \sum_{\mu=1}^{l} \alpha_\mu \xi_\mu$, то есть $f(P_i) = 1 + 44 \cdot x(P_i)$ для $i = 1, \ldots,$ 87. Наконец, решим систему

$$\sum_{\nu \in N(f)} \zeta_\mu(P_\nu) \cdot x_\nu = [a, \zeta_\mu],$$

где $N(f) = \{\nu \mid f(P_\nu) = 0, \nu = 1, ..., 87\}$. Решением является вектор $x$ = = (0,…, 0, 46, 46, 1, 1, 0,…, 0), где на $i$-х местах стоят нули при $i \neq 31, 32, 33, 34$.

Полагая $e = x$, получаем, что

$c = a - e$ = (34, 7, 41, 0, 9, 1, 1, 31, 1, 1, 34, 0, 1,…, 2, 2, 0, 0, 1,…, 2, 0) —

кодовое слово, ассоциированное с вектором $a$ (на местах многоточия стоит соответствующее число единиц). Следует также отметить, что $c \in C_\Omega(D, G)$ и $w(e) < t + 1$, где $C_\Omega(D, G)$ — код, дуальный к $C_L(D, G)$, $w(e)$ — вес вектора ошибок $e$.

Если же положить $G = 41O$, то процедуры построения кода и декодирования осуществляются аналогичным образом, за исключением громоздких вычислений и выкладок. Поэтому ограничимся лишь представлением конечного результата, а именно: $C_L(D, G)$ является [87, 80, 5]-кодом Гоппы.

Мы показали процедуру декодирования с точностью до $t = 2$ ошибок для геометрического кода Гоппы $C_L(D, G)$. Следует также отметить, что все вычисления проверены и в системе компьютерной алгебры MAGMA. Таким образом, можно сделать вывод, что AG-коды, основанные на максимальных кривых, определенных в [1] над конечным полем с дискриминантом –19, являются пригодными для кодирования информации.

**Список литературы**

1. *Alekseenko E., Aleshnikov S., Markin N., Zaytsev A.* Optimal curves of genus 3 over finite fields with discriminant –19 // arXiv: 0902.1091v1 [math. AG], Feb. 2009.

2. *Алексеенко Е. С., Алешников С. И., Зайцев А. И.* Общие уравнения оптимальных кривых над конечным полем с дискриминантом –19 // Вестник Российского государственного университета им. И. Канта. 2008. Вып. 10. С. 73—79.

3. *Stichtenoth H.* Algebraic function fields and codes. N.-Y.: Springe-Verlag, 1991.

4. *Goppa V. D.* Codes on algebraic curves // Dokl. Akad. Nauk. SSSR. 1981. **259**. P. 1289—1290.

5. *Blahut R.E.* Decoding of cyclic codes and codes on curves // Handbook of coding theory. V. S. PLess, W. C. Huffman and R. A. Brualdi, eds. Amsterdam: Elsevier, 1998.

6. *Feng G.-L., Rao T. R. N.* Improved geometric Goppa codes. Part I: Basic Theory // IEEE Trans. Inform. Theory. 1995. Vol. 41. P. 1678—1693.

**Об авторе**

Екатерина Сергеевна Алексеенко — ассист., РГУ им. И. Канта, e-mail: ekkat@inbox.ru

**Author**

Ekaterina Alekseenko — assistant, IKSUR, e-mail: ekkat@inbox.ru