Таким образом, предыдущая известная итеративная нижняя оценка изменяется на слагаемое, соответствующее самодуальным бент-функциям от $n-4$ переменных.

Работа выполнена в рамках государственного задания ИМ СО РАН (проект № FWNF-2022-0018).

Список литературы

1. Rothaus O. On bent functions // J. Combin. Theory. Ser. A. — 1976. — V. 11, no. 5. — P. 300–305.

2. Кузьмин А. С., Марков В. Т., Нечаев А. А., Шишкин В. А., Шишков А. Б. Бент-функции и гипербент-функции над полем из 2^l элементов // Пробл. передачи информации. — 2008. — Т. 44, вып. 1. — С. 15–37.

3. Tokareva N. Bent Functions: Results and Applications to Cryptography. — London: Acad. Press, 2015.

4. Carlet C., Danielsen L. E., Parker M. G., Solé P. Self dual bent functions // Int. J. Inform. Coding Theory. — 2010. — V. 1 — P. 384–399.

5. Hou X.-D. Classification of self dual quadratic bent functions // Des. Codes Cryptogr. — 2012. — V. 62, no. 2. — P. 183–198.

6. Feulner T., Sok L., Solé P., Wassermann A. Towards the classification of self-dual bent functions in eight variables // Des. Codes Cryptogr. — 2013. — V. 68, no. 1. — P. 395–406.

7. Luo G., Cao X., Mesnager S. Several new classes of self-dual bent functions derived from involutions // Cryptogr. Commun. — 2019. — V. 11, no. 6. — P. 1261–1273.

8. Li Y., Kan H., Mesnager S., Peng J., How Tan C., Zheng L. Generic Constructions of (Boolean and Vectorial) Bent Functions and Their Consequences // IEEE Trans. Inform. Theory. — 2022. — V. 68, no. 4. — P. 2735–2751.

DOI: 10.20948/dms-2022-85

ПОСТРОЕНИЕ ДУАЛЬНОГО АГ-КОДА МАЛОЙ РАЗМЕРНОСТИ В ЭЛЛИПТИЧЕСКОМ СЛУЧАЕ

Е. С. Малыгина (Калининград)

Пусть $F/\mathbb{F}_p$ — функциональное поле, определенное над конечным полем $\mathbb{F}_p$, где p — простое число. Будем считать, что поле F задается

уравнением $y^2 = f(x)$, где $f(x) \in \mathbb{F}_p[x]$ — свободный от квадратов многочлен степени $\deg f = 2g + 1$, g — род поля F.

Зафиксируем обозначения:
$P_1, P_2, \ldots, P_n$ — попарно различные точки $F/\mathbb{F}_p$ степени один;
$D = P_1 + \ldots + P_n$ — дивизор, состоящий из точек P_i, $i = 1, \ldots, n$;
G — дивизор, в чьей записи не участвуют точки дивизора D.

АГ-код $\mathcal{C}_{\mathcal{L}}(D, G)$ определим следующим образом:

$$\mathcal{C}_{\mathcal{L}}(D, G) = \{(h(P_1), \ldots, h(P_n)) : h \in \mathcal{L}(G)\} \subseteq \mathbb{F}_p^n,$$

где $\mathcal{L}(G)$ — пространство Римана-Роха [1].

Автоморфизмы $F/\mathbb{F}_p$ образуют группу

$$Aut(F/\mathbb{F}_p) = \{\sigma : \sigma(a) = a,\ a \in \mathbb{F}_p\},$$

которая действует на точки поля как $\sigma(P) = \{\sigma(x) : x \in P\}$. Действие $Aut(F/\mathbb{F}_p)$ на точки можно продолжить до действия на дивизоры, полагая $\sigma\left(\sum n_P P\right) = \sum n_P \sigma(P)$. Определим

$$Aut_{D,G}(F/\mathbb{F}_p) = \{\sigma \in Aut(F/\mathbb{F}_q) : \sigma(D) = D, \sigma(G) = G\}.$$

Обозначим за P_∞ общий полюс функций x и y. Определим точки функционального поля F степени 1, отличные от P_∞, как $\mathbb{P}_F^{(1)}$ для вычисления $f(x)$ следующим образом. Пусть $\alpha \in \mathbb{F}_p$, тогда:
1. Если $f(\alpha) = 0$, то главный дивизор $(x - \alpha)$ имеет вид:

$$(x - \alpha) = 2P_{\alpha,0} - 2P_\infty, \quad \text{где} \quad \deg P_{\alpha,0} = 1.$$

2. Если $f(\alpha) = \beta^2$ и $\beta \in \mathbb{F}_p$, то главный дивизор $(x - \alpha)$ имеет вид:

$$(x - \alpha) = P_{\alpha,\beta} + P_{\alpha,-\beta} - 2P_\infty, \quad \text{где} \quad \deg P_{\alpha,\beta} = \deg P_{\alpha,-\beta} = 1.$$

3. Если $f(\alpha) = \beta^2$ и $\beta \notin \mathbb{F}_p$, то главный дивизор $(x - \alpha)$ имеет вид:

$$(x - \alpha) = P_\alpha - 2P_\infty, \quad \text{где} \quad \deg P_\alpha = 2.$$

Согласно [1] группа автоморфизмов $Aut_{D,G}(F/\mathbb{F}_p)$ функционального поля является подгруппой группы автоморфизмов $Aut(\mathcal{C}_{\mathcal{L}}(D, G))$ АГ-кода $\mathcal{C}_{\mathcal{L}}(D, G)$ при $\deg D > 2g + 2$. Выбирая соответствующим образом дивизор G, мы можем найти все элементы $Aut_{D,G}(F/\mathbb{F}_p)$. Для начала необходимо вычислить $Aut(F/\mathbb{F}_p)$, а затем выбрать те автоморфизмы, которые оставляют неподвижными дивизоры D и G.

Обозначим за $H(\mathbb{F}_p)$ все точки степени 1, образующие абелеву группу относительно операции $\oplus$ вместе с нейтральным элементом P_∞. Пусть $Aut_\infty(F/\mathbb{F}_p)$ — группа автоморфизмов функционального поля F, которая фиксирует точку P_∞, и распространяет свое действие на группу $H(\mathbb{F}_p)$.

Лемма. *Пусть $F/\mathbb{F}_p$ — эллиптическое функциональное поле. Тогда существует биекция $H(\mathbb{F}_p) \times Aut_\infty(F/\mathbb{F}_p) \to Aut(F/\mathbb{F}_p)$, $(P, \sigma) \mapsto \tau_P \circ \sigma$, где $\tau_P(Q) = Q \oplus P$.*

В эллиптическом случае группу $Aut(F/\mathbb{F}_p)$ достаточно легко вычислить, если $\dim \mathcal{C} < 6$. Однако задача вычисления группы автоморфизмов АГ-кодов высокой размерности порой неосуществима с вычислительной точки зрения. Поскольку $Aut(\mathcal{C}) = Aut(\mathcal{C}^\perp)$, то нахождение порождающей матрицы дуального кода существенно быстрее, нежели исходного. Если $\mathcal{C} = [n, k]$, то $\mathcal{C}^\perp = [n, n-k]$. При этом, если (I_k, M) — порождающая матрица кода $\mathcal{C}_\mathcal{L}(D, G)$, то $(-M^t, I_{n-k})$ — порождающая матрица дуального кода ${\mathcal{C}^\perp}_\mathcal{L}(D, G)$. Стоит отметить, что такой подход хорош только в том случае, если размерность дуального кода достаточно мала.

Рассмотрим эллиптическое функциональное поле $F/\mathbb{F}_p$ с уравнением $y^2 = x(x-\alpha)(x-\beta)$. Построим дуальный код к АГ-коду, ассоциированному с эти полем. Отметим, что точки стемепни 1 единственным образом определяют значения функций x и y. Для точки $P \in \mathbb{P}_F^{(1)}$ будем обозначать $P = (x(P), y(P))$. Также отметим, что отображение $\tau_P(Q) = P \oplus Q$ для фиксированной точки $Q \in \mathbb{P}_F^{(1)}$ является автоморфизмом поля F.

Поскольку $f(x) = x(x-\alpha)(x-\beta)$, то функциональное поле F имеет 4 разветвляющиеся точки над $\mathbb{F}_p(x)$. Обозначим эти точки как $P_1 = (0, 0)$, $P_2 = (\alpha, 0)$, $P_3 = (\beta, 0)$ и P_∞ — общий полюс функций x и y. Пусть $|\mathbb{P}_F^{(1)}| = n$. Обозначим оставшиеся разветвляющиеся точки поля F степени 1 как $P_4, P_5, \ldots, P_n$.

Существует 4 автоморфизма поля F, фиксирующих точку P_∞, которые образуют циклическую группу, обозначаемую $\langle\sigma\rangle$:

$$\sigma(x) = -x, \quad \sigma(y) = \xi y,$$

где $\xi^4 \equiv 1 \pmod p$ и $p \equiv 1 \pmod 4$.

В качестве дивизоров, участвующих в построении АГ-кода, ассо-

циированного с эллиптической кривой, рассмотрим

$$D = \sum_{i=4}^{n} P_i \quad \text{и} \quad G = k_1 P_1 + k_2 P_2 + k_3 P_3 + k_0 P_\infty, \quad k_i \geq 0.$$

Теорема. *Пусть* $D = \sum_{i=4}^{n} P_i$. *Если*

$$G = k_1 P_1 + k_2 P_2 + k_3 P_3 + k_0 P_\infty, \quad k_i \geq 0, \quad i = 0, \ldots, 3$$

и $1 \leq \deg G \leq 11$, *то*

$$\mathcal{C}_{\mathcal{L}}(D, G)^{\perp} = v \cdot \mathcal{C}_{\mathcal{L}}(D, G'),$$

где $G' = 3(P_1 + P_2 + P_3 + P_\infty) - G$, $v = (h(P_4), \ldots, h(P_n))$ *и*

$$h = \frac{(x - \gamma_1)(x - \gamma_2)}{\prod_{i=1}^{\frac{n-8}{4}} g_i(x)},$$

$\gamma_1 \in \{0, \alpha, \beta\}$, $\gamma_2 \in \{0, \alpha, \beta\} \setminus \{\gamma_1\}$, $g_i(x)$ — *неприводимые многочлены, участвующие в разложении* $\frac{d((x-P_4)\cdot\ldots\cdot(x-P_n))}{dx}$.

Очевидно, что $Aut_{D,G}(F/\mathbb{F}_p)$ совпадает с $Aut_{D,G'}(F/\mathbb{F}_p)$, что существенно упрощает вычисление группы автоморфизмов исходного кода. Также отметим, что умножая каждую координату кода на ненулевой элемент базового поля, мы получаем эквивалентный код, который имеет ту же размерность и минимальное расстояние.

Работа выполнена при финансовой поддержке Программы мобильности 5-100, а также при финансовой поддержке Минобрнауки России (соглашение № 075-02-2022-872).

Список литературы

1. Stichtenoth H. Algebraic Function Fields and Codes. — Springer Verlag, 1991.

DOI: 10.20948/dms-2022-86