

ФУНКЦИИ НАД КОНЕЧНЫМИ ПОЛЯМИ, ПОСТРОЕННЫЕ С ИСПОЛЬЗОВАНИЕМ МНОГОЧЛЕНОВ НАД КОЛЬЦАМИ ГАЛУА И ФУНКЦИИ СЛЕДА

Камловский О.В.

Минск, 04.06.2026 г.

Пусть $R = GR(q^n, p^n)$ — кольцо Галуа характеристики p^n , содержащее q^n элементов, где p — простое число и $q = p^t$. Некоторые свойства кольца R :



$$GR(q^n, p^n) \cong \mathbb{Z}_{p^n}[x]/f(x),$$

где $\bar{f}(x)$ (получен из $f(x)$ приведением всех его коэффициентов по модулю p) неприводим над $\mathbb{Z}_p$, $\deg f(x) = t$;

- если $t = 1$ кольцо $GR(q^n, p^n)$ совпадает с $\mathbb{Z}_{p^n}$, а если $n = 1$ $GR(q^n, p^n)$ совпадает с $GF(q)$;
- $\Gamma(R) = \{x \in R : x^q = x\}$ — разрядное множество, $|\Gamma(R)| = q$.

Справедливо разрядное представление элементов $x \in R$

$$x = x_0 + px_1 + \dots + p^{n-1}x_{n-1},$$

где $x_0, x_1, \dots, x_{n-1} \in \Gamma(R)$.

Аutomорфизм Фробениуса $\varphi : R \rightarrow R$ действует на элемент x по правилу

$$\varphi(x) = x_0^p + px_1^p + \dots + p^{n-1}x_{n-1}^p,$$

и функция «след» $\text{Tr}_{R_0}^R$ из R в подкольцо $R_0 = \{0, e, 2e, \dots, (p^n - 1)e\}$ задается равенством

$$\text{Tr}_{R_0}^R(x) = x + \varphi(x) + \dots + \varphi^{t-1}(x).$$

Для R факторкольцо $P = \bar{R} = R/pR$ — поле из q элементов. Образ $a \in R$ при естественном эпиморфизме колец $R \rightarrow \bar{R}$ обозначим через $\bar{a}$.

Естественный эпиморфизм колец $R \rightarrow \bar{R}$ индуцирует эпиморфизм колец многочленов $R[x] \rightarrow \bar{R}[x]$:

$$A(x) = \sum_{i \geq 0} a_i x^i \in R[x] \rightarrow \bar{A}(x) = \sum_{i \geq 0} \bar{a}_i x^i \in \bar{R}[x].$$

Пусть $F(x) \in P[x]$ примитивный над P , $m = \deg F(x)$,
 $T(F) = q^m - 1$.

Теорема

Найдется единственный унитарный многочлен $G(x) \in R[x]$ такой, что $\bar{G}(x) = F(x)$ и $T(G) = T(F)$.

(Нечаев А.А., 1977 г.)

Пусть α — корень многочлена $G(x)$ в расширении $S = GR(q^{nm}, p^n)$ степени m кольца R .

Зададим для $k \in \mathbb{N}$ подмножества $S[x]$

$$S_k[x] = \{h_0 + h_1x + \dots + h_kx^k : h_i = 0 \text{ для всех } i, \text{ кратных } p\} \setminus \{0\},$$

$$\tilde{S}_k[x] = \{h_0 + h_1x + \dots + h_kx^k : h_1 \in S^*, h_i = 0 \text{ для всех } i, \text{ кратных } p\},$$

где S^* — мультипликативная группа кольца S .

Для каждого $h(x) \in S_k[x]$ рассмотрим $v = v_{h(x)}$

$$v(i) = v_{h(x)}(i) = \text{Tr}_R^S(h(\alpha^i)), \quad i \geq 0,$$

где Tr_R^S — функция «след» из кольца S в кольцо R .

- Если $h(x)$ пробегает все множество $S_1[x]$, то $v_{h(x)}$ пробегает все ЛРП над R с характеристическим многочленом $G(x)$ (Нечаев А.А., Кузьмин А.С., Куракин В.Л. и др.).
- Построение семейств последовательностей с низкой кросс-корреляцией для CDMA (Hellesteth T., Kumar P.V., Shanbhag A.G.).
- Приложения в теории помехоустойчивого кодирования:
 - создание новых семейств кодов и описание свойств известных кодов (Нечаев А.А., Сидельников В.М., Hammons A.R., Kumar P.V., Calderbank A.R., Sloane N.J.A.);
 - построение двоичных кодов с низким значением PAPR (Sole P., Zinoviev D.).
- Построение кодов аутентификации (Hellesteth T., Johansson T.).

Исследуемый класс функций

Выберем линейно независимую систему ЛРП $u_1, u_2, \dots, u_m$ над полем P с характеристическим многочленом $F(x)$.

Для произвольного отображения $\psi : R \rightarrow P$ рассмотрим дискретную функцию $f = f_{v,\psi} : P^m \rightarrow P$ от m переменных, построенную по правилам:

$$f(\bar{0}, \dots, \bar{0}) = \psi(0);$$

а для всех $i = 0, 1, \dots, q^m - 2$

$$f(u_1(i), \dots, u_m(i)) = \psi(v(i)).$$

Будем изучать свойства функций из классов

$$D_m(G, \psi, k) = \{f_{v,\psi} : v = v_{h(x)}, h(x) \in S_k[x]\},$$

$$\tilde{D}_m(G, \psi, k) = \{f_{v,\psi} : v = v_{h(x)}, h(x) \in \tilde{S}_k[x]\}.$$

- $P = GF(q)$, $F(x) \in P[x]$ — примитивный, $\deg F(x) = m$;
- $R = GR(q^n, p^n)$, $G(x) \in R[x]$ — отмеченный, $\bar{G}(x) = F(x)$;
- $S = GR(q^{nm}, p^n)$, $\alpha \in S$, $G(\alpha) = 0$;
- $h(x) \in S_k[x]$;
- $v \in R^\infty$, $v(i) = \text{Tr}_R^S(h(\alpha^i))$;
- $u_1, u_2, \dots, u_m$ — линейно независимая система ЛРП над P с характеристическим многочленом $F(x)$;
- $\psi : R \rightarrow P$;
- $f(\bar{0}, \dots, \bar{0}) = \psi(0)$, $f(u_1(i), \dots, u_m(i)) = \psi(v(i))$ для всех $i = 0, 1, \dots, q^m - 2$.

- Функции из класса $D_m(G, \psi, 1)$
 - частный случай (Sole P., Zinoviev D., 2006 г.; Былков Д.Н., Камловский О.В., 2012 г.);
 - общий способ построения, выбор упорядочивания аргументов (Нечаев А.А., 2013 г.);
 - случай $P = GF(2)$ (Былков Д.Н., 2014 г.);
 - случай $P = GF(q)$ (Бугров А.Д., Камловский О.В., 2018 г.).
- Функции, построенные из нескольких ЛРП
 - случай $P = GF(2)$ (Груба А.А., 2023 г.);
 - случай $P = GF(q)$ (Груба А.А., Камловский О.В., 2024 г.).

Коэффициент кросс-корреляции между функциями

Пусть χ — канонический аддитивный характер поля P

$$\chi(x) = e^{2\pi i \frac{\text{Tr}_{P_0}^P(x)}{p}}, \quad x \in P.$$

Группа всех аддитивных характеров поля P имеет вид $\{\chi_b : b \in P\}$, где $\chi_b(x) = \chi(bx)$.

Коэффициентом кросс-корреляции между функциями $f, g : P^m \rightarrow P$, соответствующим характеру χ_b , назовем

$$C_b(f, g) = \sum_{\vec{x} \in P^m} \chi_b(f(\vec{x}) - g(\vec{x})).$$

Введем обозначение

$$C(f, g) = \max_{b \in P \setminus \{0\}} |C_b(f, g)|.$$

Теорема

Пусть ψ — сбалансированное отображение, $f_1, f_2 \in D_m(G, \psi, k)$, $f_1 = f_{v_1}$, $f_2 = f_{v_2}$, $v_1 = v_{h_1(x)}$, $v_2 = v_{h_2(x)}$ и система многочленов $h_1(x), h_2(x) \in S_k[x]$ линейно независима над кольцом R . Тогда

$$C(f_1, f_2) \leq (kp^{n-1} - 1)q^{\frac{m}{2}+n}.$$

Следствие

Пусть в условиях теоремы дополнительно выполнено неравенство $m \geq 2n + 2 \log_q(kp^{n-1})$. Тогда функции f_1 и f_2 будут разными.

Пусть g пробегает все множество $A_m(P)$ аффинных функций от m переменных над полем P , то есть

$$g(\vec{x}) = g(x_1, \dots, x_m) = a_1x_1 + a_2x_2 + \dots + a_mx_m + c,$$

где $a_1, \dots, a_m, c \in P$.

Рассмотрим линейную характеристику функции f , которая определяется по правилу

$$C(f) = \max_{g \in A_m(P)} C(f, g).$$

Она характеризует «близость» f к классу всех аффинных функций от m переменных над полем P .

Назовем отображение $\psi : R \rightarrow P$ биективным по старшему разряду, если для каждого $a = a_0 + pa_1 + \dots + p^{n-1}a_{n-1} \in R$ при любых фиксированных $a_0, \dots, a_{n-2} \in \Gamma(R)$ отображение $\psi_{a_0, \dots, a_{n-2}} : \Gamma(R) \rightarrow P$, действующее по правилу

$$\psi_{a_0, \dots, a_{n-2}}(a_{n-1}) = \psi(a), \quad a_{n-1} \in \Gamma(R)$$

является биективным.

Теорема

Пусть $f \in \tilde{D}_m(G, \psi, k)$, $n > 1$, отображение ψ биективно по старшему разряду и $\psi(0) = \bar{0}$. Тогда

$$C(f) \leq (kp^{n-1} - 1)q^{\frac{m+n}{2}}.$$

Оценка из теоремы имеет вид $C(f) \leq C(n, q, p, k)q^{\frac{m}{2}}$.

Следствие

При фиксированных n, q, p, k и $m \rightarrow \infty$ в условиях теоремы

$$C(f) = O(q^{\frac{m}{2}}).$$

Аналогичное асимптотическое равенство имеет место для бент-функций от m переменных над полем P .

Следствие

Если в условиях теоремы выполнено неравенство

$$m \geq n + 2 \log_q(p^{n-1}k),$$

то в классе $\tilde{D}_m(G, \psi, k)$ нет аффинных функций.

Для каждого $a \in P$ и функции $f : P^m \rightarrow P$ рассмотрим

$$f^{-1}(a) = \{(b_1, \dots, b_m) \in P^m : f(b_1, \dots, b_m) = a\}.$$

Теорема

Пусть ψ — сбалансированное отображение и $\psi(0) = \bar{0}$. Тогда для каждой функции $f \in \tilde{D}_m(G, \psi, k)$ и любого $a \in P$

$$||f^{-1}(a)| - q^{m-1}| \leq (kp^{n-1} - 1)(q - 1)q^{\frac{m+n}{2}-1}.$$

Выбирались: $P = GF(2)$, $G(x) \in \mathbb{Z}_{2^n}[x]$, $\psi(a) = a_{n-1}$,
 $f \in \tilde{D}_8(G, \psi, 1)$.

n	$G(x)$	$(nl, \deg) - N$
2	$x^8 + 3x^7 + 2x^6 + x^5 + 3x^3 + 1$	$(120, 2) - 65280$
3	$x^8 + 2x^7 + 3x^6 + 5x^5 + 2x^4 + 5x^3 + 2x^2 + 4x + 1$ Случайная выборка	$(110, 4) - 32$, $(106, 4) - 6493$ $(102, 4) - 4968$, $(98, 4) - 1424$ $(94, 4) - 112$
4	$x^8 + 2x^7 + 11x^6 + 5x^5 + 11x^4 + 6x^3 + 10x^2 + 4x + 1$ Случайная выборка	$(111, 8) - 58$, $(109, 8) - 2593$ $(107, 8) - 20290$, $(105, 8) - 32043$ $(103, 8) - 26128$, $(101, 8) - 14802$ $(99, 8) - 7355$, $(97, 8) - 2470$ $(95, 8) - 666$, $(93, 8) - 378$ $(91, 8) - 85$

- Определить подклассы $D_m(G, \psi, k)$, отличные от $D_m(G, \psi, 1)$, которые «удобны» для реализации.
- Найти условия, при которых класс $D_m(G, \psi, k)$ содержит сбалансированные функции.
- Обобщить результаты на случай отмеченных многочленов периода $T(G) = (q^m - 1)/d$ и d последовательностей.

Спасибо за внимание!