Секция 2

ДИСКРЕТНЫЕ ФУНКЦИИ

УДК 511.32 DOI 10.17223/2226308X/11/10

ПОСТРОЕНИЕ ОДНОГО КЛАССА ФУНКЦИЙ НАД КОНЕЧНЫМИ ПОЛЯМИ С ИСПОЛЬЗОВАНИЕМ ЛИНЕЙНЫХ РЕКУРРЕНТ НАД КОЛЬЦАМИ ГАЛУА

А. Д. Бугров

Изучается класс функций над полем $\mathrm{GF}(q)$, построенных на основе линейных рекуррентных последовательностей (ЛРП) над кольцом $\mathrm{GR}(q^n, p^n)$ с отмеченным характеристическим многочленом. Порядок следования аргументов функций задаётся набором ЛРП над полем, а значения функций — усложнением ЛРП над кольцом. При выполнении некоторых условий, для близости исследуемых функций от m переменных к классу аффинных функций доказана оценка $C(f) \leqslant \leqslant q^{(m+n-1)/2}(p^{n-1}-1)(q-1)^{1/2}$. Рассматриваются вопросы, связанные с мощностью класса функций и его автоматной реализацией.

Ключевые слова: *линейные рекуррентные последовательности, усложнение последовательности, конечные поля, кольцо Галуа, кросс-корреляционная функция, оценка тригонометрической суммы.*

Введение

В [1, 2] изучались свойства булевых функций, построенных на основе старших разрядных последовательностей отмеченных линейных рекуррент над кольцом $R = \mathbb{Z}_{2^n}$. Получены оценки весов функций, вычислена их алгебраическая степень и доказана нижняя оценка нелинейности. В частности, показано, что этот класс функций достаточно удалён от класса аффинных булевых функций. Данная работа посвящена исследованию более широкого класса функций. Кроме того, класс функций рассматривается не только над полем из двух элементов, но и над произвольным конечным полем. Для этого приходится переходить от кольца вычетов по модулю 2^n к произвольному кольцу Галуа. Достоинством рассматриваемого класса является возможность его построения с использованием линейного регистра сдвига над кольцом Галуа.

1. Определение класса функций

Пусть p — простое число, $q = p^t$, $t \in \mathbb{N}$, $P = \mathrm{GF}(q)$ — конечное поле из q элементов, $R = \mathrm{GR}(q^n, p^n)$ — кольцо Галуа из q^n элементов характеристики p^n. Для кольца R фактор-кольцо $\bar{R} = R/pR$ является полем из q элементов. Далее для удобства изложения будем считать, что $\bar{R} = P$, а операцию сложения в R и $\bar{R}$ будем обозначать одним символом $+$. Образ элемента $a \in R$ при действии естественного эпиморфизма колец $R \to \bar{R}$ обозначим через $\bar{a}$. Естественный эпиморфизм колец $R \to \bar{R}$ индуцирует эпиморфизм колец многочленов $R[x] \to \bar{R}[x]$. Образ многочлена $A(x) = \sum a_i x^i \in R[x]$ при этом эпиморфизме будем обозначать через $\bar{A}(x)$, где $\bar{A}(x) = \sum \bar{a}_i x^i \in \bar{R}[x]$.

Многочлен $G(x) \in R[x]$ назовем унитарным, если его старший коэффициент равен единице, и реверсивным, если его свободный член обратим в R. Реверсивный мно-

гочлен $G(x) \in R[x]$ называется отмеченным, если периоды многочленов $G(x)$ и $\bar{G}(x)$ равны. Известно, что для каждого реверсивного многочлена $F(x) \in P[x]$, не имеющего кратных корней в своем поле разложения, найдётся единственный отмеченный многочлен $G \in R[x]$, такой, что $\bar{G}(x) = F(x)$ [3, § 4]. Способ построения отмеченного многочлена $G(x)$, соответствующего многочлену $F(x)$, основанный на применении алгоритма Гензеля, весьма сложен, но в случае $p = 2$ существует достаточно простой рекурсивный способ его построения по $F(x)$ [3]. Всюду далее $F(x) \in P[x]$, $G(x) \in R[x]$ — реверсивные многочлены, такие, что F неприводим над P, $m = \deg F = \deg G$, $\bar{G}(x) = F(x)$, $T = T(G) = T(F) = q^m - 1$.

Обозначим через $L_R(G)$ множество всех ЛРП над кольцом R с характеристическим многочленом $G(x)$ и через $L_R(G)^*$ — множество всех ЛРП $v \in L_R(G)$, для которых верно неравенство $\bar{v} \neq (0)$, где (0) — нулевая последовательность; $\bar{v}$ — последовательность, полученная из v действием естественного эпиморфизма $R \to \bar{R}$ на каждый её элемент. Последовательность $\bar{v}$ является ЛРП с характеристическим многочленом $F(x)$ [3]. Пусть $\psi : R \to P$ — произвольное отображение, $v \in L_R(G)^*$, последовательности $u_1, \ldots, u_m \in L_P(F)$ максимального периода и линейно независимы над P, то есть равенство $u_1 a_1 + \ldots + u_m a_m = (0)$ выполняется только для нулевого вектора $(a_1, \ldots, a_m)$. Определим последовательность u над P^m как $u(i) = (u_1(i), \ldots, u_m(i))$, $i \in \mathbb{N}_0$.

Лемма 1. Последовательности $u_1, \ldots, u_m$ линейно независимы над P тогда и только тогда, когда на цикле последовательности u появляются по одному разу все ненулевые векторы P^m.

Рассмотрим функцию $f = f_{u,v,\psi}$ от m переменных, определённую по правилу: $f(0, 0, \ldots, 0) = \psi(0)$ и для всех $i = 0, 1, \ldots, T - 1$

$$f(u(i)) = \psi(v(i)). \tag{1}$$

Из леммы 1 следует, что правило (1) корректно задаёт функцию f. Таблицу функции можно построить с использованием регистров сдвига над кольцом R и m регистров сдвига над полем P. В наиболее интересном с практической точки зрения случае можно выбрать $u_1 = \bar{v}$, $u_2 = x\bar{v}$, $\ldots$, $u_m = x^{m-1}\bar{v}$, и тогда функция строится с использованием одного линейного регистра сдвига над кольцом R. Введём следующие обозначения для классов функций:

$$D(F, u, \psi) = \bigcup_v f_{u,v,\psi}, \quad D(F, \psi) = \bigcup_u D(F, u, \psi),$$

где объединения берутся по всем возможным v и u, которые указаны в определении функции $f_{u,v,\psi}$.

2. Близость между дискретными функциями

Пусть $f, g : P^m \to P$ — некоторые отображения. Для любого $a \in P$ через χ_a будем обозначать аддитивный характер поля P:

$$\chi_a(x) = e^{2\pi i \frac{\mathrm{tr}_{P_0}^P(ax)}{p}}, \quad x \in P.$$

Определим коэффициент кросс-корреляции между функциями f и g равенством

$$C_a(f, g) = \sum_{\mathbf{x} \in P^n} \chi_a(f(\mathbf{x}) - g(\mathbf{x})), \quad a \in P \backslash \{0\}.$$

Обозначим

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

Пусть $\langle \mathbf{a}, \mathbf{x} \rangle$ — скалярное произведение векторов, g пробегает множество аффинных функций от n переменных над полем P, то есть

$$g(\mathbf{x}) = g(x_1, \ldots, x_m) = \langle \mathbf{a}, \mathbf{x} \rangle + b = a_1 x_1 + a_2 x_2 + \ldots + a_m x_m + b,$$

где $a_1, \ldots, a_m, b$ — элементы из P. Далее будем использовать величину

$$C(f) = \max_g C(f,g) = \max_g \max_{a \in P \setminus \{0\}} |C_a(f,g)|,$$

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

3. Свойства класса функций

3.1. Близость между функциями

Приведём некоторые обозначения и результаты из теории колец Галуа [4, § 2, 3]. Введём p-адическое множество $\Gamma(R) = \{\alpha \in R : \alpha^q = \alpha\}$. Каждый элемент x кольца R может быть единственным образом представлен в виде p-адического разложения

$$x = \gamma_0(x) + p\gamma_1(x) + \ldots + p^{n-1}\gamma_{n-1}(x),$$

где $\gamma_j : R \to \Gamma(R)$, $j \in \{0, \ldots, n-1\}$ — разрядные функции кольца R. Назовём отображение $\psi : R \to P$ сбалансированным [5], если при каждом $a \in P$ уравнение $\psi(x) = a$ имеет ровно $|R|/|P| = q^{n-1}$ решений относительно неизвестного $x \in R$.

Теорема 1. Пусть $\psi_1, \psi_2 : R \to P$ — сбалансированные функции, последовательность v линейно не выражается через $x^k v$ в кольце R. Тогда

$$C(f_{u,v,\psi_1}, f_{u,x^k v,\psi_2}) \leqslant q^{m/2+n}(p^{n-1} - 1).$$

Будем говорить, что отображение ψ биективно по старшему разряду, если его ограничение на любом подмножестве элементов кольца R с одинаковыми значениями $n-1$ младших разрядов является биекцией. Частным случаем отображения, биективного по старшему разряду, является отображение, линейное по старшему разряду, то есть такое, что для каждого $a \in R$ с p-адическим представлением

$$a = a_0 + pa_1 + p^2 a_2 + \ldots + p^{n-1} a_{n-1}, \quad a_0, a_1, \ldots, a_{n-1} \in \Gamma(R),$$

выполнено равенство

$$\psi(a) = \alpha \bar{a}_{n-1} + \eta(a_0, a_1, \ldots, a_{n-2}), \tag{2}$$

где $\alpha \in P \setminus \{0\}$; $\eta : \Gamma(R)^{n-1} \to P$ — произвольное отображение. Отметим, что биективные по старшему разряду отображения являются сбалансированными.

Следствие 1. Если функции ψ_1, ψ_2 биективны по старшему разряду, то в условиях теоремы 1 верна оценка

$$C(f_{u,v,\psi_1}, f_{u,x^k v,\psi_2}) \leqslant q^{m/2+n}(p^{n-1} - 1)(q-1).$$

Теорема 2. Пусть $\deg F = m$, $f \in D(F, \psi)$. Если $n = 1$ и $\psi : R \to P$ — произвольная функция, то верно равенство $C(f) = q^m$ и f — аффинная функция над полем P. Если $n > 1$ и функция ψ биективна по старшему разряду, то для близости функции f к классу аффинных функций от m переменных верно неравенство

$$C(f) \leqslant q^{(m+n-1)/2}(p^{n-1} - 1)(q - 1)^{1/2}.$$

Следствие 2. Пусть $\deg F = m$, $n > 1$ и функция ψ биективна по старшему разряду. Тогда при $m \geqslant (2n - 2)/t + n$ в классе $D(F, \psi)$ нет аффинных функций, в частности не существует начального заполнения рекурренты v, такого, что $(\bar{v}(0), \ldots, \bar{v}(m - 1)) \neq (0, \ldots, 0)$ и $\psi(v) = (0)$.

3.2. Мощность класса и вес функций

Утверждение 1. Пусть ψ — сбалансированное отображение, $\deg F = m$, тогда верна следующая оценка, достижимая сверху и снизу:

$$q^{mn} - q^{(n-1)m} \geqslant |D(F, u, \psi)| \geqslant q^m - 1.$$

Рассмотрим случай, когда $n = 1$, то есть $R = \mathrm{GR}(q, p) = \mathrm{GF}(q) = P$.

Следствие 3. Если $\deg F = m$, $n = 1$ и функция ψ сбалансированная, то $D(F, u, \psi) = \{\langle \mathbf{a}, \mathbf{x} \rangle + \psi(0) : \mathbf{a} \in P^m \backslash (0, \ldots, 0)\}$.

Теорема 3. Пусть отображение ψ биективно по старшему разряду, тогда при $m \geqslant$ $\geqslant 2(n - 1)/t + 2n$ разным начальным заполнениям рекурренты v соответствуют разные функции класса $D(F, u, \psi)$ и имеют место равенства

$$|D(F, u, \psi)| = |L_R(G)^*| = q^{nm} - q^{(n-1)m}.$$

Прообраз элемента z при отображении f будем обозначать как $f^{-1}(z)$.

Утверждение 2. Пусть ψ — сбалансированное отображение, $\deg F = m$, $f \in$ $\in D(F, \psi)$, тогда для любого $z \in P$ верно

$$\left| |f^{-1}(z)| - q^{m-1} \right| \leqslant q^{m/2+n-1}(p^{n-1} - 1)(q - 1).$$

3.3. Случай произвольного разрядного множества

Разрядным множеством кольца R называется любое его подмножество

$$K = \{k_0, k_1, \ldots, k_{q-1}\},$$

такое, что все его элементы попарно несравнимы по идеалу pR [6, 7]. Например, множество $\Gamma(R)$ является разрядным множеством кольца R [4, лемма 3]. Если K — разрядное множество кольца R, то каждый элемент $a \in R$ однозначно представим в виде

$$a = a_0 + pa_1 + \ldots + p^{n-1}a_{n-1}, \tag{3}$$

где $a_i \in K$, $i \in \{0, \ldots, n - 1\}$. Равенство (3) называется разрядным представлением элемента a в множестве K; элемент a_i — i-м разрядом элемента a в множестве K, a_{n-1} — старшим разрядом. Для каждого $i \in \{0, \ldots, n - 1\}$ зададим разрядное отображение $\varkappa_i^K(a) = a_i$. Всюду далее K — произвольное разрядное множество кольца R.

Обобщим понятие биективной по старшему разряду функции. Будем говорить, что отображение ψ биективно по старшему разряду относительно разрядного множества K, если ограничение отображения ψ на любом подмножестве элементов кольца R с одинаковыми значениями $n-1$ младших разрядов в множестве K является биекцией.

Утверждение 3. Если функция ψ биективна по старшему разряду относительно некоторого разрядного множества K, то она биективна по старшему разряду относительно любого разрядного множества кольца R, в том числе относительно $\Gamma(R)$.

Следствие 4. Если функция ψ биективна по старшему разряду относительно произвольного разрядного множества K, то верны следствие 1, теорема 2, следствие 2, теорема 3.

Рассмотрим разрядные множества кольца $R = \mathbb{Z}_{p^n}$. Будем говорить, что K образует арифметическую прогрессию, если $K = \{a, a+d, a+2d, \ldots, a+(p-1)d\}$ для некоторых элементов $a, d \in R$, $a \equiv 0 \pmod p$, $(d, p) = 1$. В этом случае будем использовать обозначение $K = K_{a,d}$. Важным примером разрядного множества, образующего арифметическую прогрессию, является p-ичное разрядное множество $K_{0,1} = \{0, 1, \ldots, p-1\}$.

Рассмотрим случай, когда $R = \mathbb{Z}_{p^n}$ и в равенстве (2) функция η тождественно равна 0.

Следствие 5. Пусть $\deg F = m$, $R = \mathbb{Z}_{p^n}$, $P = \mathbb{Z}_p$, $n \geqslant 2$, разрядное множество $K_{a,d}$ образует арифметическую прогрессию, $\psi(x) = \alpha \varkappa_{n-1}^{K_{a,d}}(x)$, $\alpha \in P \backslash \{0\}$, $f \in D(F, \psi)$. Тогда верно неравенство

$$C(f) \leqslant \left(\frac{2}{\pi} \ln(p^{n-1}) + \frac{13}{40} p + \frac{7}{20} \right) (p^{n-1} - 1) p^{m/2}.$$

Заметим, что у бент-функции f от m переменных над $\mathbb{Z}_p$ значение $C(f)$ равно $p^{m/2}$. Это позволяет говорить, что при малых n и $\psi(x) = \alpha \varkappa_{n-1}^{K_{a,d}}(x)$, $\alpha \in P \backslash \{0\}$ класс функций $D(F, \psi)$ достаточно удалён от класса аффинных функций от m переменных над $\mathbb{Z}_p$.

3.4. Автоматная реализация

Таблицы значений функций исследуемого класса можно вырабатывать с помощью конечного автомата, в основе которого лежит регистр сдвига над кольцом R. Пусть $R = \mathbb{Z}_{2^n}$, $u = (\bar{v}, x\bar{v}, \ldots, x^{m-1}\bar{v})$, тогда таблицу функции $f_{u,v,\psi}$ можно выработать с помощью автомата (рис. 1).

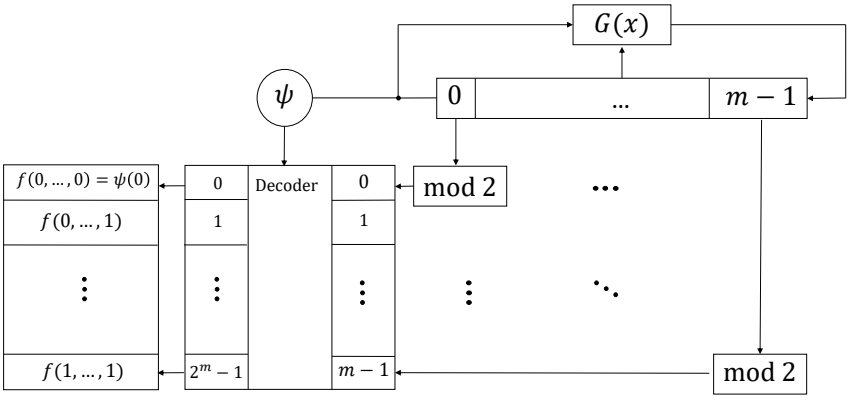

Рис. 1

Автомат состоит из регистра сдвига над кольцом $\mathbb{Z}_{2^n}$ с характеристическим многочленом $G(x)$, элементов «mod 2», которые вычисляют младший бит элемента кольца,

элемента «ψ», который вычисляет значение функции ψ от элемента кольца, дешифратора (декодера), который записывает значение, полученное сверху, по адресу, полученному справа. Столбец значений функции $f_{u,v,\psi}$ полностью заполняется за 2^m-1 тактов работы регистра сдвига.

ЛИТЕРАТУРА

1. *Былков Д. Н.* Об одном классе булевых функций, построенных с использованием старших разрядных последовательностей линейных рекуррент // Прикладная дискретная математика. Приложение. 2014. № 7. С. 59–60.
2. *Былков Д. Н., Камловский О. В.* Параметры булевых функций, построенных с использованием старших координатных последовательностей линейных рекуррент // Математические вопросы криптографии. 2012. Т. 3. № 4. С. 25–53.
3. *Нечаев А. А.* Цикловые типы линейных подстановок над конечными коммутативными кольцами // Матем. сборник. 1993. Т. 184. № 3. С. 21–56.
4. *Нечаев А. А.* Код Кердока в циклической форме // Дискретная математика. 1989. Т. 1. № 4. С. 123–139.
5. *Погорелов Б. А., Сачков В. Н.* Словарь криптографических терминов. М.: МЦНМО, 2006.
6. *Кузьмин А. С., Нечаев А. А.* Линейные рекуррентные последовательности над кольцами Галуа // Алгебра и логика. 1995. Т. 34. № 2. С. 169–189.
7. *Камловский О. В.* Частотные характеристики разрядных последовательностей линейных рекуррент над кольцами Галуа // Изв. РАН. Сер. матем. 2013. Т. 77. № 6. С. 71–96.

УДК 519.7 DOI 10.17223/2226308X/11/11

ВЕКТОРНЫЕ 2-В-1 ФУНКЦИИ КАК ПОДФУНКЦИИ ВЗАИМНО ОДНОЗНАЧНЫХ APN-ФУНКЦИЙ[1]

В. А. Идрисова

Работа посвящена проблеме существования взаимно однозначных APN-функций от чётного числа переменных. Рассматриваются свойства подфункций взаимно однозначных APN-функций. Доказано, что любая $(n-1)$-подфункция произвольной взаимно однозначной APN-функции может быть получена при помощи специальных символьных последовательностей. Данные результаты позволяют предложить новый алгоритм построения взаимно однозначных APN-функций из 2-в-1 функций и соответствующих координатных булевых функций. Получена нижняя оценка на число таких булевых функций.

Ключевые слова: *векторная булева функция, APN-функция, взаимно однозначная функция, 2-в-1 функция, перестановка.*

Векторной булевой функцией F называется произвольное отображение $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$. Рассмотрим векторную булеву функцию F из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$. Для векторов $a, b \in \mathbb{F}_2^n$, где $a \neq \mathbf{0}$, определим величину

$$\delta(a,b) = \big|\{x \in \mathbb{F}_2^n : F(x+a) + F(x) = b\}\big|.$$

Обозначим за Δ_F следующий параметр:

$$\Delta_F = \max_{a \neq \mathbf{0}, b \in \mathbb{F}_2^n} \delta(a,b).$$

[1]Работа поддержана грантом РФФИ, проект № 17-41-543364.