3. *Carlet C.* Vectorial Boolean Functions for Cryptography. Cambridge: Cambridge University Press, 2010. 93 p.
4. *Панкратова И. А.* Свойства компонент некоторых классов векторных булевых функций // Прикладная дискретная математика. 2019. № 44. С. 5–11.

УДК 519.713.2+519.714.5 DOI 10.17223/2226308X/12/21

ЛИНЕЙНОЕ РАЗЛОЖЕНИЕ ДИСКРЕТНЫХ ФУНКЦИЙ В ТЕРМИНАХ ОПЕРАЦИИ СДВИГ-КОМПОЗИЦИИ

И. В. Чередник

Исследуется операция сдвиг-композиции дискретных функций, возникающая при гомоморфизмах конечных регистров сдвига. Для произвольной функции над конечным полем описаны все возможные представления в виде сдвиг-композиции двух функций, правая из которых линейная. Кроме того, изучена возможность представления произвольной функции над конечным полем сдвиг-композицией трёх функций, в которой обе крайние функции линейные. Доказано, что в случае простого поля для линейных функций, а также для квадратичных функций, линейных по крайней переменной, понятия приводимости и линейной приводимости совпадают.

Ключевые слова: *дискретные функции, конечные поля, регистр сдвига, сдвиг-композиция.*

Введение

Пусть Ω_q — конечное множество из q элементов. В данной работе будем использовать множество переменных $\{x_0, x_1, x_2, \ldots\}$, а множество всех функций q-значной логики от переменных $x_0, x_1, x_2, \ldots$ будем обозначать через F_q. Произвольную функцию $f \in F_q$ всегда можно рассматривать как функцию от соответствующего допустимого набора переменных $x_0, x_1, \ldots, x_n$. В работах отечественных криптографов К. Г. Таболова, В. А. Башева, А. Я. Прососова, В. И. Солодовникова и др. была введена и исследована (преимущественно в терминах гомоморфизмов регистров сдвига) операция сдвиг-композиции на множестве всех функций F_q:

$$f(x_0, \ldots, x_n) \lhd g(x_0, \ldots, x_m) = f(g(x_0, \ldots, x_m), \ldots, g(x_n, \ldots, x_{n+m})).$$

В работах перечисленных авторов в разной степени общности и направленности достаточно подробно исследована связь между представлением функции f в виде сдвиг-композиции $f = g \lhd h$ и существованием гомоморфизма регистра сдвига, соответствующего функции f, на меньший регистр сдвига, соответствующий функции g (все основные результаты по данной тематике единым образом изложены в [1]). Так, например, в [2] описаны все возможные представления функции f над конечным полем $\mathbb{F}_q$ в виде $f = l \lhd g$, где l — линейная, что позволило указать все возможные гомоморфизмы регистра сдвига с обратной связью f на линейные регистры сдвига.

В настоящей работе предлагается описание всех возможных представлений произвольной функции f над конечным полем $\mathbb{F}_q$ в виде $f = g \lhd l$, где l — линейная. Кроме того, изучена возможность представления произвольной функции f над конечным полем $\mathbb{F}_q$ в виде $f = l_1 \lhd g \lhd l_2$, где l_1, l_2 — линейные. Доказано, что в случае простого поля для линейных функций, а также для квадратичных функций, линейных по крайней переменной, понятия приводимости и линейной приводимости совпадают.

1. Основные определения и обозначения

В данной работе, если не оговорено противное, полагается, что $q = p^t$, где p — простое, $t \in \mathbb{N}$, а на множестве Ω_q задана структура поля $(\mathbb{F}_q, +, \cdot)$. Известно [3], что каждая функция $f \in F_q$ представляется единственным приведённым многочленом из $\mathbb{F}_q[x_0, x_1, \dots]$, который для удобства будем отождествлять с функцией f.

Для полноты и простоты изложения примеры в данной работе рассматриваются преимущественно в булевом случае, при этом операция сложения в поле $\mathbb{F}_2$ выделяется символом «$\oplus$».

Множество всех q-значных функций, которые биективны по первой (последней) переменной, будем обозначать через ${}^*F_q$ (F_q^*); множество всех q-значных функций, которые линейны по первой (последней) переменной, будем обозначать через ${}^+F_q$ (F_q^+); множество всех функций, сохраняющих константу 0, будем обозначать $\widehat{F}_q$. При этом естественны производные обозначения

$$ {}^*F_q^* = F_q^* \cap {}^*F_q, \quad {}^+F_q^+ = {}^+F_q \cap F_q^+, \quad {}^*\widehat{F}_q = {}^*F_q \cap \widehat{F}_q, \quad \dots $$

Как нетрудно убедиться, каждое из множеств ${}^+F_q \subset {}^*F_q \subset F_q$ образует полугруппу относительно операции $\lhd$ с нейтральным элементом x_0. При этом несложный пример

$$ (x_0 \oplus x_1) \lhd (x_0 \oplus x_1) = (x_0 \oplus x_1) \lhd (x_0 \oplus x_1 \oplus 1) $$

показывает, что даже в рамках моноида $({}^+F_q, \lhd)$ не всегда возможно производить правое сокращение в равенствах. Однако возможность правого и левого сокращений всё же присутствует в достаточно широких классах практически значимых функций.

Утверждение 1. Множества ${}^*\widehat{F}_q$, $\widehat{F}_q^*$, ${}^*\widehat{F}_q^*$ и ${}^+\widehat{F}_q$, $\widehat{F}_q^+$, ${}^+\widehat{F}_q^+$ образуют моноиды с возможностью левого и правого сокращений.

Будем говорить, что *функция g делит справа функцию f*, если существует такая функция h, для которой выполняется равенство $f = h \lhd g$. Для каждой перестановки π элементов множества Ω_q произвольная функция f всегда делится справа на $\pi(x_0), \pi(f)$ — такие делители функции f будем называть *несобственными*. Аналогичным образом определяются соответствующие понятия левой делимости. Если у функции f существует собственный правый, а следовательно, и собственный левый делители, то будем говорить, что функция f *приводима*.

Замечание 1. Пусть $f \in F_q$ и $f(0, \dots, 0) = c_f$. Существует тесная связь между приводимостью f в моноиде $(F_q, \lhd)$ и приводимостью $\hat{f} = f - c_f$ в подмоноиде $(\widehat{F}_q, \lhd)$:

$$ f = g \lhd h \iff \hat{f} = (x_0 - c_f) \lhd g \lhd (x_0 + c_h) \lhd \hat{h}, \quad \text{где } (x_0 - c_f) \lhd g \lhd (x_0 + c_h), \hat{h} \in \widehat{F}_q. $$

Таким образом, исследование приводимости в моноиде $(F_q, \lhd)$ во многом сводится к исследованию приводимости в подмоноиде $(\widehat{F}_q, \lhd)$.

2. Линейное разложение

Множество L_q всех функций, представимых линейными, но не аффинными многочленами над $\mathbb{F}_q$

$$ c_{i_0} x_{i_0} + c_{i_1} x_{i_1} + \dots + c_{i_k} x_{i_k} \ : \ i_0 < i_1 < \dots < i_k, k \in \mathbb{N}, \ c_{i_0}, c_{i_1}, \dots, c_{i_k} \in \mathbb{F}_q, $$

образует коммутативное кольцо $(L_q, +, \lhd)$, а отображение

$$ c_{i_0} x^{i_0} + c_{i_1} x^{i_1} + \dots + c_{i_k} x^{i_k} \mapsto c_{i_0} x_{i_0} + c_{i_1} x_{i_1} + \dots + c_{i_k} x_{i_k} $$

является изоморфизмом колец $(\mathbb{F}_q[x], +, \cdot)$ и $(L_q, +, \lhd)$ [1, 2, 4]. Подразумевая этот изоморфизм, далее будем формулировать известные понятия и использовать известные утверждения о делимости многочленов применительно к линейным функциям.

По понятным причинам класс L_q является важным с практической точки зрения подмоноидом в $(F_q, \lhd)$ и выделение у произвольной функции левых или правых линейных делителей представляется естественной и актуальной задачей. Функцию $f \in F_q$ будем называть *линейно приводимой справа*, если у нее существует собственный правый делитель $l \in L_q$. В противном случае функцию f будем называть *линейно неприводимой справа*. Аналогичным образом определяется левая линейная приводимость функций. Функцию будем называть *линейно неприводимой*, если она линейно неприводима и справа, и слева.

В. И. Солодовников в [2] описал все возможные левые линейные разложения для произвольной функции из $\widehat{F}_q$.

Теорема 1 [2]. Произвольная функция $f \in \widehat{F}_q$ однозначно представляется в виде

$$f = \sum_{\substack{1 \leqslant i_1 < \ldots < i_k, \\ 1 \leqslant a_0, a_1, \ldots, a_k < q}} l_{i_1,\ldots,i_k;a_0,a_1,\ldots,a_k} \lhd x_0^{a_0} x_{i_1}^{a_1} \ldots x_{i_k}^{a_k},$$

где $l_{i_1,\ldots,i_k;a_0,a_1,\ldots,a_k} \in L_q$ для всех $1 \leqslant i_1 < \ldots < i_k,\ 0 < a_0, a_1, \ldots, a_k < q$.

При этом все левые линейные делители функции f исчерпываются делителями $l = \text{НОД}(l_{i_1,\ldots,i_k;a_0,a_1,\ldots,a_k} : 1 \leqslant i_1 < \ldots < i_k,\ 0 < a_0, a_1, \ldots, a_k < q)$. В частности, функция f линейно неприводима слева в том и только в том случае, когда $l = x_0$.

Линейную функцию вида $x_0 + a_1 x_{i_1} + \ldots + a_k x_{i_k}$ будем называть *унитарной по переменной* x_0.

Следствие 1 [2]. Произвольная функция $f \in \widehat{F}_q$ однозначно представляется в виде $f = x_s \lhd l \lhd g$, где x_s — крайняя левая переменная, от которой f зависит существенным образом; $l \in L_q$ — унитарная по переменной x_0; g — линейно неприводимая слева.

Для описания правых делителей потребуются дополнительные обозначения. Известно [5, 6], что в случае $q = p^t$, где p — простое, $t > 1$, степень нелинейности приведённого одночлена $x^a \in \mathbb{F}_q[x]$, $a < q$, лучше оценивать не самим числом a, а его p-ичным весом

$$\|a\|_p = a_0 + \ldots + a_{t-1},$$

определяемым из p-ичного представления

$$a = a_0 + \ldots + a_{t-1} p^{t-1},\ 0 \leqslant a_0, \ldots, a_{t-1} < p.$$

В связи с этим одночлен x^a часто расписывают в виде $x^{a_0} \ldots x^{p^{t-1} a_{t-1}}$, а произвольный приведённый моном $\mathbf{x}^{\mathbf{a}} = x_0^{a_0} \ldots x_n^{a_n}$, где $0 \leqslant a_0, \ldots, a_n < q$ и $a_i = a_{i0} + \ldots + a_{it-1} p^{t-1}$, $i \in \{0, \ldots, n\}$, — в виде

$$\mathbf{x}^{\mathbf{a^p}} = x_0^{a_{00}} \ldots x_0^{p^{t-1} a_{0t-1}} \ldots x_n^{a_{n0}} \ldots x_n^{p^{t-1} a_{nt-1}},$$

подразумевая при этом $\mathbf{a^p} = (a_{00}, \ldots, a_{0t-1}, \ldots, a_{n0}, \ldots, a_{nt-1})$.

Отношение градуированного лексикографического порядка на $\mathbb{N}_0^{(n+1)t}$ индуцирует отношение порядка на множестве приведенных мономов из $\mathbb{F}_q[x_0, \ldots, x_n]$

$$\mathbf{x}^{\mathbf{a^p}} \geqslant \mathbf{x}^{\mathbf{b^p}} \quad \Leftrightarrow \quad \mathbf{a^p} \geqslant_{\text{grlex}} \mathbf{b^p},$$

при котором мономы сначала упорядочиваются по степени нелинейности, а мономы одной степени нелинейности упорядочиваются «лексикографически» при условии

$$x_0 > \ldots > x_0^{p^{t-1}} > \ldots > x_n > \ldots > x_n^{p^{t-1}}.$$

При простом q введённое отношение порядка совпадает со стандартным градуированным лексикографическим порядком на множестве всех приведённых мономов из $\mathbb{F}_q[x_0, \ldots, x_n]$.

Пусть

$$\mathbf{x}^{\mathbf{a^P}} = x_{i_0}^{a_{00}} \ldots x_{i_0}^{p^{t-1}a_{0t-1}} \ldots x_{i_k}^{a_{k0}} \ldots x_{i_k}^{p^{r-1}a_{kr-1}} x_{i_k}^{p^r a_{kr}}, \quad 0 < a_{kr} < p.$$

Тогда мономы

$$x_{i_0}^{a_{00}} \ldots x_{i_0}^{p^{t-1}a_{0t-1}} \ldots x_{i_k}^{a_{k0}} \ldots x_{i_k}^{p^{r-1}a_{kr-1}} x_{i_k}^{p^r(a_{kr}-1)} x_{i_k+j}^{p^r}, \quad j \geqslant 1,$$

и только их будем называть *линейно связанными с мономом* $\mathbf{x}^{\mathbf{a^P}}$.

Теорема 2. Произвольная функция $f \in F_q$ однозначно представляется в виде

$$f = c + \sum_{i=0}^{m} c_i \, \mathbf{x}^{\mathbf{a}_i^{\mathbf{P}}} \lhd l_i(x_0, \ldots),$$

где $c \in \Omega_q$; $\mathbf{x}^{\mathbf{a}_0^{\mathbf{P}}} > \ldots > \mathbf{x}^{\mathbf{a}_m^{\mathbf{P}}}$ — убывающая последовательность линейно несвязанных мономов, и для каждого $i \in \{0, \ldots, m\}$ коэффициент $c_i \in \Omega_q$ отличен от 0, а $l_i(x_0, \ldots)$ — линейная функция, унитарная по переменной x_0.

При этом если f существенно зависит от переменной x_0, то все правые линейные делители функции f исчерпываются делителями НОД$\,(l_0, \ldots, l_m)$. В частности, функция f линейно неприводима справа в том и только в том случае, когда НОД$\,(l_0, \ldots, l_m) = x_0$.

Следствие 2. Произвольная функция $f \in F_q$ однозначно представляется в виде $f = x_s \lhd g \lhd l$, где x_s — крайняя левая переменная, от которой f зависит существенным образом; g — линейно неприводимая справа; $l \in L_q$ — унитарная по переменной x_0.

Замечание 2. Представление, доказанное в теореме 2, существенным образом зависит от условий $x_0 > \ldots > x_0^{p^{t-1}} > \ldots\ldots > x_n > \ldots > x_n^{p^{t-1}}$. Так, для функции

$$f = x_0^3 + x_0^2 x_2 + x_0 x_1^2 + x_0 x_2^2$$

над полем $\mathbb{F}_4$ при условии $x_0 > x_0^2 > x_1 > x_1^2 > x_2 > x_2^2$ справедливо разложение

$$f = x_0 x_0^2 \lhd (x_0 + x_1 + x_2) + x_1 x_1^2 \lhd (x_0 + x_1) + x_0^2 x_1 \lhd x_0,$$

а при условии $x_0^2 > x_0 > x_1^2 > x_1 > x_2^2 > x_2$ — разложение

$$f = x_0^2 x_0 \lhd (x_0 + x_2) + x_0 x_1^2 \lhd x_0 + x_2^2 x_2 \lhd x_0.$$

3. Особенности двустороннего линейного разложения

Теорема 3. Пусть q простое и функция $f \in F_q$ делится слева на $l_1 \in L_q$, а справа на $l_2 \in L_q$. Тогда если l_1 и l_2 взаимно просты, то справедливо разложение

$$f = l_1 \lhd g \lhd l_2.$$

Если, дополнительно, l_1 и l_2 — максимальные левый и правый делители функции f, то g — линейно неприводимая.

Замечание 3. Условие простоты q является существенным в теореме 3. Так, например, если $q = p^t$, $t \geqslant 2$ и $\alpha \in \mathbb{F}_q \backslash \mathbb{F}_p$, то $\alpha^p \neq \alpha$ и, очевидно, линейные функции $x_0 + \alpha x_1$, $x_0 + \alpha^p x_1$ взаимно просты. Однако при этом справедливы разложения

$$(x_0 + \alpha^p x_1^p) \lhd x_0^p = x_0^p + \alpha^p x_1^p = x_0^p \lhd (x_0 + \alpha x_1)$$

и легко убедиться в невозможности представления

$$x_0^p + \alpha^p x_1^p = (x_0 + \alpha^p x_1^p) \lhd g \lhd (x_0 + \alpha x_1).$$

Замечание 4. Условие взаимной простоты левого и правого линейных делителей является существенным в теореме 3. Так, например, для булевой функции

$$f = (x_0 \oplus x_1) \lhd x_0 x_1 \lhd (x_0 \oplus x_1) \oplus (x_0 \oplus x_1)$$

справедливы разложения

$$f = (x_0 \oplus x_1) \lhd (x_0 x_1 \oplus x_0 x_2 \oplus x_1 x_2 \oplus x_0 \oplus x_1) = (x_0 \oplus x_1) \lhd g_1,$$
$$f = (x_0 x_1 \oplus x_1 x_2 \oplus x_0) \lhd (x_0 \oplus x_1) = g_2 \lhd (x_0 \oplus x_1),$$

но при этом g_1 — линейно неприводимая справа, g_2 — линейно неприводимая слева, а потому невозможно представление

$$f = (x_0 \oplus x_1) \lhd g \lhd (x_0 \oplus x_1).$$

4. Квадратичные функции над простым полем

Ввиду изоморфизма колец $(L_q, +, \lhd)$ и $(\mathbb{F}_q, +, \cdot)$ описание всех линейных делителей произвольной функции $f \in L_q$ равносильно определению канонического разложения соответствующего многочлена.

Для описания линейных делителей произвольной квадратичной функции можно использовать результаты теорем 2 и 3 и, как показывает следующий результат, в случае линейных по крайней переменной квадратичных функций над простым полем это позволяет описать вообще все возможные делители.

Теорема 4. Если q — простое число, то для композиции $f \lhd g$ произвольных функций $f \in F_q$ и $g \in {}^+F_q \cup F_q^+$ справедливы следующие утверждения:

1) $\deg(f \lhd g) = 0$ тогда и только тогда, когда $\deg f = 0$;
2) $\deg(f \lhd g) = 1$ тогда и только тогда, когда $\deg f = \deg g = 1$;
3) $\deg(f \lhd g) = 2$ тогда и только тогда, когда либо $\deg f = 1$ и $\deg g = 2$, либо $\deg f = 2$ и $\deg g = 1$.

Замечание 5. Пункт 2 теоремы 4 в частном случае $q = 2$ был доказан В. И. Солодовниковым в 1978 г. [1].

Замечание 6. Простой пример

$$(x_1 x_4 \oplus x_2 x_3 x_4) \lhd (x_0 \oplus x_1 x_2 \oplus x_2) = x_1 x_4 \oplus x_1 x_5 x_6 \oplus x_1 x_6 \oplus x_3 x_4 \oplus x_3 x_5 x_6 \oplus x_3 x_6$$

показывает, что уже в случае кубических функций понятие приводимости становится шире понятия линейной приводимости.

ЛИТЕРАТУРА

1. *Солодовников В. И.* Регистры сдвига и криптоалгоритмы на их основе. LAP LAMBERT Academic Publishing, 2017.
2. *Солодовников В. И.* Гомоморфизмы регистров сдвига в линейные автоматы // Дискретная математика. 2008. № 4. С. 87–101.
3. *Лидл Р., Нидеррайтер Г.* Конечные поля. М.: Мир, 1988.
4. *Солодовников В. И.* Гомоморфизмы двоичных регистров сдвига // Дискретная математика. 2005. № 1. С. 73–88.
5. *Кузьмин А. С., Нечаев А. А., Шишкин В. А.* Бент- и гипербент-функции над конечным полем // Труды по дискретной математике. 2007. № 10. С. 97–122.
6. *Черемушкин А. В.* Аддитивный подход к определению степени нелинейности дискретной функции // Прикладная дискретная математика. 2010. № 2. С. 22–33.

УДК 519.7 DOI 10.17223/2226308X/12/22

О ВЗАИМОСВЯЗИ МЕЖДУ КВАТЕРНАРНЫМИ И БУЛЕВЫМИ БЕНТ-ФУНКЦИЯМИ[1]

А. С. Шапоренко

Исследуются кватернарные бент-функции вида $f : \mathbb{Z}_4^n \to \mathbb{Z}_4$. Показано представление коэффициентов Уолша — Адамара кватернарной функции через коэффициенты двух булевых функций. Получено, что любая кватернарная бент-функция является регулярной. Изучается связь кватернарных бент-функций от одной и двух переменных с булевыми бент-функциями от двух и четырёх переменных соответственно.

Ключевые слова: *кватернарные функции, булевы функции, регулярные бент-функции.*

Пусть $\langle x, y\rangle$ — скалярное произведение векторов, где суммирование производится по модулю 2, а $x.y$ — скалярное произведение векторов с суммированием по модулю 4.

Преобразованием Уолша — Адамара булевой функции f от n переменных называется целочисленная функция $W_f(x)$, заданная на множестве $\mathbb{Z}_2^n$ равенством

$$W_f(x) = \sum_{y \in \mathbb{Z}_2^n} (-1)^{\langle x,y\rangle \oplus f(y)}.$$

Булева функция f от n (n — чётное) переменных называется *бент-функцией*, если $|W_f(x)| = 2^{n/2}$ для любого $x \in \mathbb{Z}_2^n$.

Функция $g : \mathbb{Z}_4^n \to \mathbb{Z}_4$ называется *кватернарной функцией* от n переменных [1]. *Преобразование Уолша — Адамара кватернарной функции* g определяется следующим образом:

$$W_g(x) = \sum_{y \in \mathbb{Z}_4^n} i^{x.y+g(y)}.$$

Здесь «+» означает сложение по модулю 4.

Кватернарная функция g от n переменных называется *бент-функцией*, если $|W_g(x)| = 4^{n/2}$ для любого $x \in \mathbb{Z}_4^n$.

[1]Работа выполнена при финансовой поддержке РФФИ (проект № 18-07-01394), Министерства образования и науки (Задание № 1.13559.2019/13.1 и Программа 5-100).