Math-Net.Ru

Общероссийский математический портал

И. В. Чередник, Линейное разложение дискретных функций в терминах операции сдвиг-композиции, *Матем. вопр. криптогр.*, 2020, том 11, выпуск 1, 115–143

DOI: <https://doi.org/10.4213/mvk317>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.80.73.141

26 апреля 2023 г., 16:39:53

Линейное разложение дискретных функций в терминах операции сдвиг-композиции

И. В. Чередник

ООО «Центр сертификационных исследований», Москва

Получено 29.IV.2019

Аннотация. 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 трех 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

Linear decomposition of discrete functions in terms of shift-composition operation

I. V. Cherednik

LLC «Certification Research Center», Moscow

Abstract. We investigate the shift-composition operation on discrete functions that arise in connection with homomorphisms of shift registers. For an arbitrary function over a finite field all possible representations in the form of shift-compositions of two functions (where the right function is linear) are described. Besides, the possibility to represent an arbitrary function as a shift-composition of three functions such that both left and right functions are linear is studied. It is proved that in the case of a simple field for linear functions and quadratic functions that are linear in the extreme variable the concepts of reducibility and linear reducibility coincide.

Keywords: discrete functions, finite fields, shift register, shift-composition

Введение

Пусть Ω_q — конечное множество из q элементов. В данной работе будем использовать множество переменных $\{x_0, x_1, x_2, \dots\}$, а множество всех функций q -значной логики от переменных $x_0, x_1, x_2, \dots$ будем обозначать через F_q . Произвольную функцию $f \in F_q$ всегда можно рассматривать как функцию от соответствующего допустимого набора переменных $x_0, x_1, \dots, x_n$.

Всюду далее, если не оговорено противное, полагается, что $q = p^t$, где p — простое, $t \in \mathbb{N}$, а на множестве Ω_q задана структура поля $(\mathbb{F}_q, +, \cdot)$. При этом, как известно (см. [2]), каждая функция $f \in F_q$ представляется единственным приведенным 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 будут рассматриваться преимущественно в булевом случае, при этом операция сложения в поле $\mathbb{F}_2$ будет явным образом выделяться символом $\oplus$.

В работах отечественных криптографов К. Г. Таболова, В. А. Башева, А. Я. Прососова, В. И. Солодовникова и других была введена и исследована (преимущественно в терминах гомоморфизмов регистров сдвига) операция сдвиг-композиции на множестве всех функций F_q :

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

Нетрудно убедиться, что множество F_q образует полугруппу относительно операции $\triangleleft$ с нейтральным элементом x_0 . При этом, с одной стороны, операция сдвиг-композиции является достаточно естественным обобщением операции композиции отображений от одной переменной, а с другой стороны, данная операция имеет явно регистровую природу и, например, удачно согласуется с операцией произведения многочленов, возникающей при исследовании линейных рекуррентных последовательностей — 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 $(L_q, +, \triangleleft)$, где L_q — множество всех q -значных функций, представимых линейными, но не аффинными многочленами (см. [4–6]).

В работах перечисленных выше авторов в разной степени общности и направленности достаточно подробно исследована связь между представлением функции f в виде $f = g \triangleleft h$ и существованием гомоморфизма, отображающего регистр сдвига, соответствующий функции f ,

на меньший регистр сдвига, соответствующий функции g (все основные результаты по данной тематике единым образом изложены в книге [6]). Так, например, В. И. Солодовников [5] описал все возможные представления функции f над конечным полем $\mathbb{F}_q$ в виде $f = l \triangleleft g$, где $l \in L_q$, что позволило указать все возможные гомоморфизмы регистра сдвига с обратной связью f на линейные регистры сдвига.

В настоящей работе описаны все возможные представления произвольной функции f над конечным полем $\mathbb{F}_q$ в виде $f = g \triangleleft l$, где $l \in L_q$. Кроме того, изучена возможность представления произвольной функции f над конечным полем $\mathbb{F}_q$ в виде $f = l_1 \triangleleft g \triangleleft l_2$, где $l_1, l_2 \in L_q$. Доказано, что в случае простого поля для линейных функций, а также для квадратичных функций, линейных по крайней переменной, понятия приводимости и линейной приводимости совпадают. Случай произвольного поля планируется рассмотреть в одной из следующих работ.

1. Основные определения и обозначения

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 естественными будут производные обозначения

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

Операция сдвиг-композиции обладает определенной симметричностью, а потому для краткости формулирования результатов и удобства проведения соответствующих доказательств преимущественно будем рассматривать множества *F_q и ${}^+F_q$, хотя естественно, что все утверждения остаются верными и для множеств F_q^* и F_q^+ .

Сформулируем несколько простых, но необходимых для дальнейшего изложения фактов, которые, впрочем, легко проверить с использованием определений (см. [3]).

Утверждение 1. 1) Включение $f, g \in {}^*F_q$ эквивалентно условию $f \triangleleft g \in {}^*F_q$.

2) Если f_1, f_2 — функции от переменных $x_0, x_1, \dots, x_n$ и функция g не имеет запретов длины $n+1$, то справедлива импликация

$$f_1 \triangleleft g = f_2 \triangleleft g \implies f_1 = f_2.$$

- 3) Функция g является функцией без запретов тогда и только тогда, когда она допускает сокращение в любом равенстве $f_1 \triangleleft g = f_2 \triangleleft g$.
- 4) Функция g имеет запрет тогда и только тогда, когда она является правым делителем нуля в моноиде $(F_q, \triangleleft)$.
- 5) Функции, перестановочные со всеми функциями моноида $(F_q, \triangleleft)$, исчерпываются функциями вида $x_s, s \in \mathbb{N}_0$.

Как нетрудно убедиться, каждое из множеств ${}^+F_q \subset {}^*F_q \subset F_q$ образует полугруппу относительно операции $\triangleleft$ с нейтральным элементом x_0 . При этом, согласно утверждению 1, в первых двух полугруппах допускается левое сокращение, а простой пример

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

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

Утверждение 2. Множества ${}^*\widehat{F}_q, \widehat{F}_q^*, {}^*\widehat{F}_q^* u + \widehat{F}_q, \widehat{F}_q^+, {}^+\widehat{F}_q^+$ образуют моноиды с возможностью левого и правого сокращений.

Доказательство. На примере произвольной $g \in {}^*F_q$ докажем несколько более общие утверждения.

С одной стороны, для любых $f_1, f_2 \in F_q$ в равенстве $f_1 \triangleleft g = f_2 \triangleleft g$ допустимо правое сокращение, поскольку $g \in {}^*F_q$ является функцией без запретов.

С другой стороны, если для некоторых $f_1, f_2 \in F_q$ существуют такие элементы $a_1, \dots, a_{m+n} \in \Omega_q$, что

$$\begin{aligned} (f_1(a_1, \dots, a_{n+1}), \dots, f_1(a_m, \dots, a_{m+n})) \\ = (f_2(a_1, \dots, a_{n+1}), \dots, f_2(a_m, \dots, a_{m+n})), \end{aligned}$$

то, расписав равенство $g \triangleleft f_1 = g \triangleleft f_2$ подробно

$$\begin{aligned} g(f_1(x_0, \dots, x_n), f_1(x_1, \dots, x_{n+1}), \dots, f_1(x_m, \dots, x_{m+n})) \\ = g(f_2(x_0, \dots, x_n), f_2(x_1, \dots, x_{n+1}), \dots, f_2(x_m, \dots, x_{m+n})) \end{aligned}$$

и подставляя в него все последовательности наборов вида

$$(b_n, a_1, \dots, a_{m+n}), (b_{n-1}, b_n, a_1, \dots, a_{m+n-1}), \dots, (b_0, \dots, b_{n-1}, b_n, a_1, \dots, a_m),$$

легко убедиться в том, что $f_1 = f_2$. $\square$

Будем говорить, что *функция g делит справа функцию f* , если существует функция h , для которой выполняется равенство $f = h \triangleleft g$; такая функция h *делит функцию f слева*. Несложно понять, что для каждого $\pi \in S(\Omega_q)$ произвольная функция f всегда делится и справа и слева на $\pi(x_0)$ и $\pi(f)$. Такие делители функции f будем называть *несобственными*, а все остальные делители функции f — *собственными*. 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 $(F_q, \triangleleft)$ и приводимостью $\hat{f} = f - c_f$ в $(\hat{F}_q, \triangleleft)$:

$$f = g \triangleleft h \iff \hat{f} = (x_0 - c_f) \triangleleft g \triangleleft (x_0 + c_h) \triangleleft \hat{h} = g_1 \triangleleft \hat{h}, \quad g_1, \hat{h} \in \hat{F}_q.$$

Таким образом, исследование приводимости в моноиде $(F_q, \triangleleft)$ сводится к исследованию приводимости в подмоноиде $(\hat{F}_q, \triangleleft)$.

2. Длина функции

В этом разделе проводится первичное исследование вполне естественного понятия длины функции, которое согласуется с операцией сдвиг-композиции и позволяет упрощать рассуждения в доказательствах.

Если функция $f(x_0, \dots, x_n)$ зависит существенным образом только от переменных $x_{i_0}, \dots, x_{i_k}$, $0 \leq i_0 < \dots < i_k \leq n$, то величину $\text{len}(f) = i_k - i_0$ будем называть *длиной функции f* . Длины непостоянных функций $\pi(x_i)$ по определению полагаем равными 0, а длины постоянных функций по определению полагаем равными $-\infty$.

Пусть $f = a_0x_0 + \dots + a_nx_n$ и $g = b_0x_0 + \dots + b_mx_m$ — линейные функции длин $\text{len } f = n$ и $\text{len } g = m$ соответственно. Тогда при изоморфизме

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

им соответствуют многочлены $f = a_0x^0 + \dots + a_nx^n$ и $g = b_0x^0 + \dots + b_mx^m$ степеней $\deg f = n$ и $\deg g = m$ соответственно. Легко видеть, что равенство

$$\text{len}(f \triangleleft g) = m + n = \text{len } f + \text{len } g$$

согласуется с известным равенством

$$\deg(fg) = \deg f + \deg g.$$

На самом деле введенное понятие длины согласуется с операцией сдвиг-композиции для достаточно широких и практически значимых классов функций.

Утверждение 3. Равенство $\text{len}(f \triangleleft g) = \text{len } f + \text{len } g$ справедливо при выполнении хотя бы одного из следующих условий:

- 1) $f \in {}^*F_q^*$,
- 2) $g \in {}^*F_q^*$,
- 3) $g \in {}^+F_q$ и q — простое.

Доказательство. Произвольные функции $f, g \in F_q$ длин n и m соответственно представляются в виде

$$f = x_s \triangleleft \hat{f}(x_0, \dots, x_n), \quad s \geq 0, \quad \text{и} \quad g = x_t \triangleleft \hat{g}(x_0, \dots, x_m), \quad t \geq 0,$$

где $\hat{f}(x_0, \dots, x_n)$ и $\hat{g}(x_0, \dots, x_m)$ — функции длин n и m соответственно. При этом справедливо соотношение

$$f \triangleleft g = (x_s \triangleleft \hat{f}) \triangleleft (x_t \triangleleft \hat{g}) = x_{s+t} \triangleleft (\hat{f} \triangleleft \hat{g}).$$

Учитывая изложенное выше, не ограничивая общности, далее будем полагать, что $f = f(x_0, \dots, x_n)$ и $g = g(x_0, \dots, x_m)$ — функции длин n и m соответственно.

1) Поскольку g существенно зависит от переменной x_0 , то существуют $a_0 \neq a'_0$, $a_1, \dots, a_m \in \Omega_q$, для которых

$$g(a_0, a_1, \dots, a_m) = b_0 \neq b'_0 = g(a'_0, a_1, \dots, a_m).$$

Теперь из биективности f по первой переменной легко вывести, что для произвольных $a_{m+1}, \dots, a_{m+n} \in \Omega_q$ выполняется неравенство

$$(f \triangleleft g)(a_0, \dots, a_{m+n}) = f(b_0, \dots, b_n) \neq f(b'_0, \dots, b_n) = (f \triangleleft g)(a'_0, \dots, a_{m+n}),$$

т. е. функция $f \triangleleft g$ существенно зависит от переменной x_0 .

Существенная зависимость функции $f \triangleleft g$ от переменной x_{m+n} доказывается аналогично.

2) Если $f = \text{const}$, то равенство очевидно. Если же $f \neq \text{const}$, то по предположению f существенно зависит от переменной x_0 и, следовательно, существуют $b_0 \neq b'_0, b_1, \dots, b_n \in \Omega_q$, для которых

$$f(b_0, b_1, \dots, b_n) \neq f(b'_0, b_1, \dots, b_n).$$

Для функции g , биективной по переменной x_0 , существуют такие элементы $a_0 \neq a'_0, a_1, \dots, a_{m+n} \in \Omega_q$, что

$$\begin{aligned} (g(a_0, \dots, a_m), g(a_1, \dots, a_{m+1}), \dots, g(a_n, \dots, a_{m+n})) &= (b_0, b_1, \dots, b_n), \\ (g(a'_0, \dots, a_m), g(a_1, \dots, a_{m+1}), \dots, g(a_n, \dots, a_{m+n})) &= (b'_0, b_1, \dots, b_n). \end{aligned}$$

Теперь легко видеть, что функция $f \triangleleft g$ существенным образом зависит от переменной x_0 :

$$(f \triangleleft g)(a_0, \dots, a_{m+n}) = f(b_0, \dots, b_n) \neq f(b'_0, \dots, b_n) = (f \triangleleft g)(a'_0, \dots, a_{m+n}).$$

Существенная зависимость функции $f \triangleleft g$ от переменной x_{m+n} доказывается аналогичным образом.

3) Не ограничивая общности, будем считать, что g линейна по первой переменной: $g(x_0, x_1, \dots, x_m) = x_0 + \psi(x_1, \dots, x_m)$.

Покажем сначала, что $f \triangleleft g$ существенно зависит от переменной x_0 . В разложении

$$f = \sum_{i=0}^{q-1} x_0^i \varphi_i(x_1, \dots, x_n) = \sum_{i=0}^s x_0^i \varphi_i(x_1, \dots, x_n), \quad \varphi_s \neq 0$$

функция φ_s отлична от 0 и, следовательно, $\varphi_s \triangleleft g \neq 0$, поскольку g — функция без запретов. Поэтому функция

$$f \triangleleft g = \sum_{i=0}^s (x_0 + \psi(x_1, \dots, x_m))^i (\varphi_i \triangleleft g)(x_1, \dots, x_{n+m}) = x_0^s (\varphi_s \triangleleft g) + \dots$$

существенно зависит от переменной x_0 .

Покажем, что $f \triangleleft g$ существенно зависит от переменной x_{n+m} . Поскольку g существенно зависит от x_m , то для некоторых $a_m \neq a'_m, a_0, \dots, a_{m-1} \in \Omega_q$ выполняется неравенство $g(a_0, a_1, \dots, a_m) \neq g(a_0, a_1, \dots, a'_m)$. Учитывая линейность g по первой переменной, не ограничивая общности, можно полагать, что $g(a_0, a_1, \dots, a_m) = 0$ и $g(a_0, a_1, \dots, a'_m) = c$.

Рассмотрим теперь функцию $f(x_0, \dots, x_n)$; для нее существует такой набор $b_0, \dots, b_{n-1} \in \Omega_q$, что $f(b_0, \dots, b_{n-1}, x_n) \neq \text{const}$. Другими словами, среди значений

$$f(b_0, \dots, b_{n-1}, 0), f(b_0, \dots, b_{n-1}, 1), \dots, f(b_0, \dots, b_{n-1}, q-1)$$

существуют различные. При простом q на множестве Ω_q можно определить единственную с точностью до изоморфизма группу — циклическую группу, которая порождается любым своим ненулевым элементом, например c . Значит, указанные значения можно переписать следующим образом:

$$f(b_0, \dots, b_{n-1}, 0), f(b_0, \dots, b_{n-1}, c), \dots, f(b_0, \dots, b_{n-1}, (q-1)c),$$

и нетрудно понять, что существует $t \in \overline{0, q-1}$, для которого

$$f(b_0, \dots, b_{n-1}, tc) \neq f(b_0, \dots, b_{n-1}, (t+1)c).$$

Остается заметить, что $g(a_0 + tc, a_1, \dots, a_m) = tc$, $g(a_0 + tc, a_1, \dots, a'_m) = (t+1)c$ и потому на любой паре векторов

$$(b_{-n}, \dots, b_{-1}, b_0 + tc, b_1, \dots, b_m) \text{ и } (b_{-n}, \dots, b_{-1}, b_0 + tc, b_1, \dots, b'_m)$$

функция $f \triangleleft g$ принимает различные значения. □

Сделаем несколько замечаний относительно утверждения 3.

Замечание 2. Стоит отметить, что первые два условия являются достаточными в случае произвольного составного q , не обязательно простого.

Замечание 3. Простые примеры

$$(x_0 \oplus x_1 x_3 \oplus x_1 x_2 x_3) \triangleleft x_0 x_1 = x_0 x_1 \text{ и } (x_1 x_3 \oplus x_1 x_2 x_3 \oplus x_3) \triangleleft x_0 x_1 = x_3 x_4$$

показывают, что первое условие нельзя заменить ни на $f \in {}^*F_q$, ни на $f \in F_q^*$.

Замечание 4. Нетрудно понять, что в третьем условии функцию $g \in {}^+F_q$ можно заменить любой функцией вида

$$\pi(x_0) + \varphi(x_1, \dots, x_n), \quad \pi \in S_q.$$

Замечание 5. В булевом случае третье достаточное условие можно переформулировать как $g \in {}^*F_q$. Однако для нечетных простых q такое обобщение невозможно: уже в случае 3-значной логики функции

$$f = (x_0^2 + 2)(x_1 + x_1^2) \in F_3 \text{ и } g = x_0 + (1 + 2x_0)(x_1 + x_1^2) \in {}^*F_3,$$

но $f \triangleleft g = (2x_0 + x_0^2)(x_1 + x_1^2)$ и, соответственно, $\text{len}(f \triangleleft g) < \text{len } f + \text{len } g$. (Суть данного примера легко понять, выписав таблицы истинности функций f и g .)

Замечание 6. Простота q существенна в третьем условии, поскольку для составного q при любом определении группа $(\Omega_q, +)$ содержит собственную подгруппу $(H, +)$, и тогда возможна следующая общая конструкция.

Пусть $\varphi: \Omega_q \rightarrow H$ — произвольная функция, отличная от константы. Тогда $g(x_0, x_1) = x_0 + \varphi(x_1)$ существенно зависит от обеих переменных и

$$g(x_0, x_1) \in H \iff x_0 \in H.$$

Теперь заметим, что функция $f(x_0, x_1) = \text{Ind}\{x_0 = 0, x_1 \in H\}$ существенно зависит от обеих переменных и выполняется равенство

$$\begin{aligned} (f \triangleleft g)(x_0, x_1, x_2) &= \text{Ind}\{g(x_0, x_1) = 0, g(x_1, x_2) \in H\} \\ &= \text{Ind}\{g(x_0, x_1) = 0, x_1 \in H\}. \end{aligned}$$

Проиллюстрируем изложенную конструкцию явным примером: для функций $f(x_0, x_1) = (1 + x_0^3)(1 + x_1 + x_1^2)$ и $g(x_0, x_1) = x_0 + (x_1 + x_1^2)$ над полем $\mathbb{F}_4$ выполняется равенство

$$f \triangleleft g = (1 + x_0 + x_1 + x_1^2)(1 + x_1 + x_1^2).$$

Следствие 1. При простом q обратимыми элементами моноида $({}^+F_q, \triangleleft)$ являются линейные перестановки от переменной x_0 и только они.

Доказательство. Пусть f — обратимый элемент моноида $({}^+F_q, \triangleleft)$. Тогда $f \triangleleft g = x_0$ для некоторого $g \in {}^+F_q$ и при вычислении длин левой и правой частей получим, что $\text{len } f + \text{len } g = \text{len } x_0 = 0$. Отсюда необходимо следует, что $\text{len } f = \text{len } g = 0$ и, следовательно, $f(x_0) = ax_0 + b$, $a \neq 0$ — перестановка. $\square$

Замечание 7. В двоичном случае ${}^+F_2 = {}^*F_2$, и следствие 1 дает описание вообще всех обратимых элементов в F_q : x_0 и $x_0 \oplus 1$. Однако ${}^+F_q \neq {}^*F_q$ при простом $q > 2$, и уже в случае 3-значной логики можно указать пример:

$$(x_0 + (1 + 2x_0)(x_1 + x_1^2)) \triangleleft (x_0 + (1 + 2x_0)(x_1 + x_1^2)) = x_0.$$

(Суть данного примера легко понять, выписав таблицу истинности функции g .)

Также отметим, что следствие 1 нельзя дословно обобщить на случай составного q . Например, если φ — линейное преобразование пространства $\mathbb{F}_q$, удовлетворяющее условию $\varphi^t = 0$, то очевидно, что

$$(x_0 - \varphi(x_1)) \triangleleft (x_0 + \varphi(x_1) + \dots + \varphi^t(x_1)) = x_0 - \varphi^t(x_1) = x_0.$$

3. Линейные разложения

Легко видеть, что 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 $(L_q, +, \triangleleft)$, 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 $(L_q, +, \triangleleft)$ (данный факт без доказательства отмечался в [4–6]). Подразумевая указанный 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 $(F_q, \triangleleft)$, 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.

Замечание 8. Мы сознательно рассматриваем понятия линейной приводимости, но не аффинной, поскольку:

- во-первых, аффинная приводимость произвольной функции не содержит ничего качественно нового по сравнению с ее линейной приводимостью:

$$\begin{aligned} f = g \triangleleft (l + c) &\iff f = g \triangleleft (x_0 + c) \triangleleft l, \\ f = (l + c) \triangleleft g &\iff f - c = l \triangleleft g, \end{aligned}$$

— во-вторых, в классе аффинных функций не выполняются перестановочность:

$$(x_0 \oplus x_1) \triangleleft (x_0 \oplus x_1 \oplus 1) = x_0 \oplus x_2 \neq x_0 \oplus x_2 \oplus 1 = (x_0 \oplus x_1 \oplus 1) \triangleleft (x_0 \oplus x_1),$$

и однозначность разложения на множители:

$$(x_0 \oplus x_1) \triangleleft (x_0 \oplus x_1 \oplus 1) = (x_0 \oplus x_1) \triangleleft (x_0 \oplus x_1),$$

в то время как в коммутативном моноиде $(L_q, \triangleleft)$ имеет место однозначное разложение на множители.

В. И. Солодовников в [5] описал все возможные левые линейные разложения произвольной функции из $\widehat{F}_q$.

Теорема 4 (теорема 5 в [5]). *Произвольная функция $f \in \widehat{F}_q$ однозначно представляется в виде*

$$f = \sum_{\substack{1 \leq i_1 < \dots < i_k \\ 1 \leq a_0, a_1, \dots, a_k < q}} l_{i_1, \dots, i_k; a_0, a_1, \dots, a_k} \triangleleft x_0^{a_0} x_{i_1}^{a_1} \dots x_{i_k}^{a_k},$$

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

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

Следствие 2 (теорема 6 в [5]). *Произвольная функция $f \in \widehat{F}_q$ однозначно представляется в виде $f = l \triangleleft g$, где $l \in L_q$ — функция, унитарная по крайней переменной, а g — линейно неприводимая слева.*

В данном разделе предлагается описание всех возможных правых линейных разложений произвольной функции над полем $\mathbb{F}_q$. Для удобства изложения сначала рассмотрим случай простого поля.

3.1. Правое линейное разложение над простым полем

Для удобства произвольный вектор из $\mathbb{N}_0^t$ будем обозначать $\mathbf{a} = (a_1, \dots, a_t)$, а величину $a_1 + \dots + a_t$ — через $\|\mathbf{a}\|$. Напомним, что отношение $\geq_{\text{lex}}$, определенное на множестве $\mathbb{N}_0^t$ по правилу

$$\mathbf{a} \geq_{\text{lex}} \mathbf{b} \iff \mathbf{a} = \mathbf{b} \text{ или } \mathbf{a} - \mathbf{b} = (0, \dots, 0, c, \dots), c > 0,$$

называется отношением лексикографического порядка, а отношение $\geq_{\text{grlex}}$, определенное на множестве $\mathbb{N}_0^t$ по правилу

$$\mathbf{a} \geq_{\text{grlex}} \mathbf{b} \iff \|\mathbf{a}\| > \|\mathbf{b}\| \text{ или } \mathbf{a} \geq_{\text{lex}} \mathbf{b},$$

называется отношением градуированного лексикографического порядка.

Всюду далее произвольный приведенный моном $x_0^{a_0} \dots x_n^{a_n}$ из $\mathbb{F}_q[x_0, \dots, x_n]$ кратко будем обозначать через $\mathbf{x}^{\mathbf{a}}$, а если потребуется явное указание входящих в него переменных, то будем писать $\mathbf{x}^{\mathbf{a}} = x_{i_0}^{a_{i_0}} \dots x_{i_k}^{a_{i_k}}$, $0 < a_{i_0}, \dots, a_{i_k} < q$. Отношение градуированного лексикографического порядка на $\mathbb{N}_0^{n+1}$ естественным образом индуцирует отношение порядка на множестве приведенных мономов из $\mathbb{F}_q[x_0, \dots, x_n]$:

$$\mathbf{x}^{\mathbf{a}} \geq \mathbf{x}^{\mathbf{b}} \iff \mathbf{a} \geq_{\text{grlex}} \mathbf{b},$$

при котором мономы сначала упорядочиваются по степени, а мономы одной степени упорядочиваются лексикографически при условии $x_0 > \dots > x_n$.

Пусть

$$\mathbf{x}^{\mathbf{a}} = x_{i_0}^{a_{i_0}} \dots x_{i_{k-1}}^{a_{i_{k-1}}} x_{i_k}^{a_{i_k}}, \quad 0 < a_{i_0}, \dots, a_{i_{k-1}}, a_{i_k} < q.$$

Тогда следующие мономы

$$x_{i_0}^{a_{i_0}} \dots x_{i_{k-1}}^{a_{i_{k-1}}} x_{i_k}^{a_{i_k}-1} x_{i_{k+1}} > x_{i_0}^{a_{i_0}} \dots x_{i_{k-1}}^{a_{i_{k-1}}} x_{i_k}^{a_{i_k}-1} x_{i_{k+2}} > \dots$$

и только их будем называть *линейно связанными по последней переменной с мономом $\mathbf{x}^{\mathbf{a}}$ над $\mathbb{F}_q$* или кратко *линейно связанными с $\mathbf{x}^{\mathbf{a}}$* . При этом будем говорить, что моном $\mathbf{x}^{\mathbf{a}}$ *существенно больше* монома $\mathbf{x}^{\mathbf{b}}$, если $\mathbf{x}^{\mathbf{a}} > \mathbf{x}^{\mathbf{b}}$ и $\mathbf{x}^{\mathbf{b}}$ линейно не связан с $\mathbf{x}^{\mathbf{a}}$. Конечную последовательность мономов $\mathbf{x}^{\mathbf{a}_0} > \dots > \mathbf{x}^{\mathbf{a}_m}$ будем называть *существенно убывающей*, если моном $\mathbf{x}^{\mathbf{a}_i}$ существенно больше $\mathbf{x}^{\mathbf{a}_{i+1}}$ для каждого $i \in \{0, \dots, m-1\}$.

Теорема 5. Пусть q — простое. Тогда произвольная функция $f \in F_q$ однозначно представляется в виде

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

где $c \in \Omega_q$, $\mathbf{x}^{\mathbf{a}_0} > \dots > \mathbf{x}^{\mathbf{a}_m}$ — существенно убывающая последовательность мономов, и для каждого $i \in \{0, \dots, m\}$ коэффициент $c_i \in \Omega_q$

отличен от 0, а $l_i(x_0, \dots)$ — 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 $(l_0, \dots, l_m)$ и, в частности, функция f линейно неприводима справа в том и только в том случае, когда $(l_0, \dots, l_m) = x_0$.

Доказательство. Докажем первое утверждение индукцией по старшему (относительно градуированного лексикографического порядка) моному приведенного многочлена $f(x_0, \dots, x_n)$. База при $f = \text{const}$ очевидна. Перейдем к доказательству индуктивного перехода.

Пусть старший член функции f имеет вид

$$c_0 \mathbf{x}^{\mathbf{a}_0} = c_0 x_{i_0}^{a_0} \dots x_{i_k}^{a_k}, \quad 0 < a_0, \dots, a_k < q,$$

и все члены функции f , линейно связанные с $c_0 \mathbf{x}^{\mathbf{a}_0}$, суть

$$h_1 x_{i_0}^{a_0} \dots x_{i_k}^{a_k-1} x_{i_k+j_1}, \dots, h_s x_{i_0}^{a_0} \dots x_{i_k}^{a_k-1} x_{i_k+j_s}.$$

Тогда функцию f можно представить в виде

$$f = c_0 x_{i_0}^{a_0} \dots x_{i_k}^{a_k} + h_1 x_{i_0}^{a_0} \dots x_{i_k}^{a_k-1} x_{i_k+j_1} + \dots + h_s x_{i_0}^{a_0} \dots x_{i_k}^{a_k-1} x_{i_k+j_s} + \psi,$$

где каждый моном многочлена $\psi(x_0, \dots, x_n)$ существенно меньше $\mathbf{x}^{\mathbf{a}_0}$.

Поскольку q — простое, то существует $a_k^{-1} \in \mathbb{F}_q$, и легко видеть, что для

$$l_0(x_0, \dots, x_{j_s}) = x_0 + a_k^{-1} c_0^{-1} h_1 x_{j_1} + \dots + a_k^{-1} c_0^{-1} h_s x_{j_s} = x_0 + u_1 x_{j_1} + \dots + u_s x_{j_s}$$

многочлен функции $c_0 \mathbf{x}^{\mathbf{a}_0} \triangleleft l_0(x_0, \dots, x_{j_s})$ имеет вид

$$\begin{aligned} c_0 \mathbf{x}^{\mathbf{a}_0} \triangleleft l_0(x_0, \dots, x_{j_s}) &= c_0 x_{i_0}^{a_0} \dots x_{i_k}^{a_k} \triangleleft (x_0 + u_1 x_{j_1} + \dots + u_s x_{j_s}) \\ &= c_0 (x_{i_0} + u_1 x_{i_0+j_1} + \dots + u_s x_{i_0+j_s})^{a_0} \dots (x_{i_k} + u_1 x_{i_k+j_1} + \dots + u_s x_{i_k+j_s})^{a_k} \\ &= c_0 x_{i_0}^{a_0} \dots x_{i_{k-1}}^{a_{k-1}} (x_{i_k}^{a_k} + a_k x_{i_k}^{a_k-1} (u_1 x_{i_k+j_1} + \dots + u_s x_{i_k+j_s}) + \dots) + \dots \\ &= c_0 x_{i_0}^{a_0} \dots x_{i_k}^{a_k} + h_1 x_{i_0}^{a_0} \dots x_{i_k}^{a_k-1} x_{i_k+j_1} + \dots + h_s x_{i_0}^{a_0} \dots x_{i_k}^{a_k-1} x_{i_k+j_s} + \varphi, \end{aligned}$$

где каждый моном многочлена $\varphi(x_0, \dots, x_n)$ существенно меньше $\mathbf{x}^{\mathbf{a}_0}$. Теперь очевидно, что

$$f = c_0 \mathbf{x}^{\mathbf{a}_0} \triangleleft l_0(x_0, \dots, x_{j_s}) + (\psi(x_0, \dots, x_n) - \varphi(x_0, \dots, x_n)),$$

где каждый моном многочлена $\psi - \varphi$ существенно меньше $\mathbf{x}^{\mathbf{a}_0}$ и, следовательно, по предположению индукции функция $\psi - \varphi$ однозначно

представляется в виде

$$\psi - \varphi = c + \sum_{i=1}^m c_i \mathbf{x}^{\mathbf{a}_i} \triangleleft l_i(x_0, \dots),$$

где $c \in \Omega_q$, $\mathbf{x}^{\mathbf{a}_1} > \dots > \mathbf{x}^{\mathbf{a}_m}$ — существенно убывающая последовательность мономов, и для каждого $i \in \{1, \dots, m\}$ коэффициент c_i отличен от 0, а $l_i(x_0, \dots)$ — линейная функция, унитарная по переменной x_0 .

Таким образом, для функции f справедливо разложение

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

где $c \in \Omega_q$ и для каждого $i \in \{0, \dots, m\}$ коэффициент c_i отличен от 0, а $l_i(x_0, \dots)$ — линейная функция, унитарная по переменной x_0 . При этом последовательность мономов $\mathbf{x}^{\mathbf{a}_0} > \dots > \mathbf{x}^{\mathbf{a}_m}$ является существенно убывающей, поскольку $\mathbf{x}^{\mathbf{a}_0}$ существенно больше $\mathbf{x}^{\mathbf{a}_1}$ по построению $\psi - \varphi$, а $\mathbf{x}^{\mathbf{a}_1} > \dots > \mathbf{x}^{\mathbf{a}_m}$ существенно убывает по предположению индукции.

Единственность указанного разложения следует из того, что:

- коэффициент c_0 и моном $\mathbf{x}^{\mathbf{a}_0}$ однозначно определяются старшим членом функции f ,
- линейная функция $l_0(x_0, \dots)$ однозначно определяется совокупностью

$$h_1 x_{i_0}^{a_0} \dots x_{i_k}^{a_k-1} x_{i_k+j_1}, \dots, h_s x_{i_0}^{a_0} \dots x_{i_k}^{a_k-1} x_{i_k+j_s}$$

- всех одночленов приведенного многочлена f , линейно связанных с $\mathbf{x}^{\mathbf{a}_0}$,
- сумма $c + \sum_{i=1}^m c_i \mathbf{x}^{\mathbf{a}_i} \triangleleft l_i(x_0, \dots)$ определена однозначно по предположению индукции как соответствующее разложение функции $f - c_0 \mathbf{x}^{\mathbf{a}_0} \triangleleft l_0$.

Для завершения доказательства остается описать правые линейные делители функции f , существенным образом зависящей от переменной x_0 . В таком случае из разложения $f = g \triangleleft l$, $g \in F_q$, $l \in L_q$ необходимо следует, что l линейна по переменной x_0 и, не ограничивая общности, можно полагать l унитарной по переменной x_0 .

Согласно доказанному функция g обладает разложением

$$g = c' + \sum_{i=0}^{m'} c'_i \mathbf{x}^{\mathbf{a}'_i} \triangleleft l'_i(x_0, \dots),$$

где $c' \in \Omega_q$, $\mathbf{x}^{\mathbf{a}'_0} > \dots > \mathbf{x}^{\mathbf{a}'_{m'}}$ — существенно убывающая последовательность, и для каждого $i \in \{0, \dots, m'\}$ коэффициент c'_i отличен от 0,

а $l'_i(x_0, \dots)$ — линейная функция, унитарная по переменной x_0 . Однако в таком случае получаем, что функция f обладает разложением

$$f = g \triangleleft l = c' + \sum_{i=0}^{m'} c'_i \mathbf{x}^{\mathbf{a}'_i} \triangleleft (l'_i \triangleleft l)(x_0, \dots),$$

которое в силу единственности должно совпадать с

$$f = c + \sum_{i=0}^m c_i \mathbf{x}^{\mathbf{a}_i} \triangleleft l_i(x_0, \dots).$$

Значит, $m = m'$ и $c_i = c'_i$, $l_i = l'_i \triangleleft l$ для каждого $i \in \{0, \dots, m\}$. $\square$

3.2. Правое линейное разложение в общем случае

В случае $q = p^t$, где p — простое, как известно (см. [1, 7]), степень нелинейности приведенного одночлена $x^a \in \mathbb{F}_q[x]$, $a < q$, лучше оценивать не самим числом a , но его p -ичным весом

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

определяемым из p -ичного представления

$$a = a_0 + \dots + a_{t-1}p^{t-1}, \quad 0 \leq a_0, \dots, a_{t-1} < p.$$

В связи с этим одночлен x^a часто записывают в виде $x^{a_0} \dots x^{p^{t-1}a_{t-1}}$, а произвольный приведенный моном $\mathbf{x}^{\mathbf{a}} = x_0^{a_0} \dots x_n^{a_n}$, где $0 \leq a_0, \dots, a_n < q$ и

$$a_i = a_{i0} + \dots + a_{it-1}p^{t-1}, \quad i \in \{0, \dots, n\},$$

записывают в виде

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

где $\mathbf{a}^p = (a_{00}, \dots, a_{0t-1}, \dots, a_{n0}, \dots, a_{nt-1})$.

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

$$\mathbf{x}^{\mathbf{a}^p} \geq \mathbf{x}^{\mathbf{b}^p} \iff \mathbf{a}^p \geq_{\text{grlex}} \mathbf{b}^p,$$

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

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

Нетрудно видеть, что при простом q введенное отношение порядка совпадает с рассмотренным в предыдущем подразделе стандартным градуированным лексикографическим порядком на множестве всех приведенных мономов из $\mathbb{F}_q[x_0, \dots, x_n]$.

Пусть

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

Тогда мономы

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

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

Теорема 6. *Произвольная функция $f \in F_q$ однозначно представляется в виде*

$$f = c + \sum_{i=0}^m c_i \mathbf{x}^{\mathbf{a}^i} \triangleleft l_i(x_0, \dots),$$

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

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

Доказательство. Докажем первое утверждение индукцией по старшему относительно введенного выше порядка моному приведенного многочлена функции $f(x_0, \dots, x_n)$. База при $f = \text{const}$ очевидна. Перейдем к доказательству индуктивного перехода.

Пусть старший член функции f имеет вид

$$c_0 \mathbf{x}^{\mathbf{a}^0} = c_0 x_{i_0}^{a_{00}} \dots x_{i_0}^{p^{t-1}a_{0t-1}} \dots x_{i_k}^{a_{k0}} \dots x_{i_k}^{p^{r-1}a_{kr-1}} x_{i_k}^{p^r a_{kr}}, \quad 0 < a_{kr} < p,$$

и все члены функции f , линейно связанные с $c_0 \mathbf{x}^{\mathbf{a}_0^P}$, суть

$$h_l x_{i_0}^{a_{00}} \dots x_{i_0}^{p^{t-1}a_{0t-1}} \dots x_{i_k}^{a_{k0}} \dots x_{i_k}^{p^{r-1}a_{kr-1}} x_{i_k}^{p^r(a_{kr}-1)} x_{i_k+j_l}^{p^r}, \quad l \in \{1, \dots, s\}.$$

Тогда функцию f можно записать в виде

$$f = c_0 x_{i_0}^{a_{00}} \dots x_{i_0}^{p^{t-1}a_{0t-1}} \dots x_{i_k}^{a_{k0}} \dots x_{i_k}^{p^{r-1}a_{kr-1}} x_{i_k}^{p^r a_{kr}} + \sum_{l=1}^s h_l x_{i_0}^{a_{00}} \dots x_{i_0}^{p^{t-1}a_{0t-1}} \dots x_{i_k}^{a_{k0}} \dots x_{i_k}^{p^{r-1}a_{kr-1}} x_{i_k}^{p^r(a_{kr}-1)} x_{i_k+j_l}^{p^r} + \psi,$$

где у многочлена $\psi(x_0, \dots, x_n)$ все мономы меньше $\mathbf{x}^{\mathbf{a}_0^P}$ и линейно не связаны с $\mathbf{x}^{\mathbf{a}_0^P}$.

Поскольку $0 < a_{kr} < p$, то существует $a_{kr}^{-1} \in \mathbb{F}_q$, и легко видеть, что для

$$\begin{aligned} l_0(x_0, \dots, x_{j_s}) &= x_0 + (a_{kr}^{-1} c_0^{-1} h_1)^{p^{t-r}} x_{j_1} + \dots + (a_{kr}^{-1} c_0^{-1} h_s)^{p^{t-r}} x_{j_s} \\ &= x_0 + u_1 x_{j_1} + \dots + u_s x_{j_s} \end{aligned}$$

многочлен функции $c_0 \mathbf{x}^{\mathbf{a}_0^P} \triangleleft l_0(x_0, \dots, x_{j_s})$ имеет вид

$$\begin{aligned} c_0 x_{i_0}^{a_{00}} \dots x_{i_0}^{p^{t-1}a_{0t-1}} \dots x_{i_k}^{a_{k0}} \dots x_{i_k}^{p^{r-1}a_{kr-1}} x_{i_k}^{p^r a_{kr}} &\triangleleft (x_0 + u_1 x_{j_1} + \dots + u_s x_{j_s}) \\ &= c_0 \prod_{l=0}^{t-1} (x_{i_0}^{p^l} + u_1 x_{i_0+j_1}^{p^l} + \dots + u_s x_{i_0+j_s}^{p^l})^{a_{0l}} \dots \\ &\quad \cdot \prod_{l=0}^r (x_{i_k}^{p^l} + u_1 x_{i_k+j_1}^{p^l} + \dots + u_s x_{i_k+j_s}^{p^l})^{a_{kl}} = \\ &= c_0 x_{i_0}^{a_{00}} \dots x_{i_k}^{p^{r-1}a_{kr-1}} (x_{i_k}^{p^r a_{kr}} + a_{kr} x_{i_k}^{p^r(a_{kr}-1)} (u_1^{p^r} x_{i_k+j_1}^{p^r} + \dots + u_s^{p^r} x_{i_k+j_s}^{p^r}) + \dots \\ &= c_0 x_{i_0}^{a_{00}} \dots x_{i_k}^{p^{r-1}a_{kr-1}} x_{i_k}^{p^r a_{kr}} + \sum_{l=1}^s h_l x_{i_0}^{a_{00}} \dots x_{i_k}^{p^{r-1}a_{kr-1}} x_{i_k}^{p^r(a_{kr}-1)} x_{i_k+j_l}^{p^r} + \varphi, \end{aligned}$$

где каждый моном многочлена $\varphi(x_0, \dots, x_n)$ меньше $\mathbf{x}^{\mathbf{a}_0^P}$ и линейно не связан с $\mathbf{x}^{\mathbf{a}_0^P}$. Теперь легко видеть, что

$$f = c_0 \mathbf{x}^{\mathbf{a}_0^P} \triangleleft l_0(x_0, \dots, x_{j_s}) + (\psi(x_0, \dots, x_n) - \varphi(x_0, \dots, x_n)),$$

где каждый моном многочлена $\psi(x_0, \dots, x_n) - \varphi(x_0, \dots, x_n)$ меньше $\mathbf{x}^{\mathbf{a}_0^P}$ и линейно не связан с $\mathbf{x}^{\mathbf{a}_0^P}$. По предположению индукции функция $\psi - \varphi$

однозначно представляется в виде

$$\psi - \varphi = c + \sum_{i=1}^m c_i \mathbf{x}^{\mathbf{a}_i^{\mathbf{p}}} \triangleleft l_i(x_0, \dots),$$

где $c \in \Omega_q$, $\mathbf{x}^{\mathbf{a}_1^{\mathbf{p}}} > \dots > \mathbf{x}^{\mathbf{a}_m^{\mathbf{p}}}$ — убывающая последовательность линейно не связанных мономов, и для каждого $i \in \{1, \dots, m\}$ коэффициент c_i отличен от 0, а $l_i(x_0, \dots)$ — линейная функция, унитарная по переменной x_0 .

Таким образом, для функции f справедливо разложение

$$f = c + \sum_{i=0}^m c_i \mathbf{x}^{\mathbf{a}_i^{\mathbf{p}}} \triangleleft l_i(x_0, \dots),$$

где $c \in \Omega_q$ и для каждого $i \in \{0, \dots, m\}$ коэффициент c_i отличен от 0, а $l_i(x_0, \dots)$ — линейная функция, унитарная по переменной x_0 . При этом последовательность мономов $\mathbf{x}^{\mathbf{a}_0^{\mathbf{p}}} > \dots > \mathbf{x}^{\mathbf{a}_m^{\mathbf{p}}}$ является строго убывающей, поскольку $\mathbf{x}^{\mathbf{a}_0^{\mathbf{p}}}$ строго больше $\mathbf{x}^{\mathbf{a}_1^{\mathbf{p}}}$ по построению $\psi - \varphi$, а $\mathbf{x}^{\mathbf{a}_1^{\mathbf{p}}} > \dots > \mathbf{x}^{\mathbf{a}_m^{\mathbf{p}}}$ убывает по предположению индукции. Кроме того, по предположению индукции $\mathbf{x}^{\mathbf{a}_1^{\mathbf{p}}} > \dots > \mathbf{x}^{\mathbf{a}_m^{\mathbf{p}}}$ — последовательность линейно не связанных мономов. Для доказательства того, что каждый из мономов $\mathbf{x}^{\mathbf{a}_1^{\mathbf{p}}}, \dots, \mathbf{x}^{\mathbf{a}_m^{\mathbf{p}}}$ линейно не связан с $\mathbf{x}^{\mathbf{a}_0^{\mathbf{p}}}$, нам потребуется вспомогательное утверждение.

Лемма 7. *Если $\mathbf{x}^{\mathbf{a}^{\mathbf{p}}} > \mathbf{x}^{\mathbf{b}^{\mathbf{p}}}$ и для некоторой линейной l многочлен $\mathbf{x}^{\mathbf{b}^{\mathbf{p}}} \triangleleft l$ содержит моном, который линейно связан с $\mathbf{x}^{\mathbf{a}^{\mathbf{p}}}$, то $\mathbf{x}^{\mathbf{b}^{\mathbf{p}}}$ линейно связан с $\mathbf{x}^{\mathbf{a}^{\mathbf{p}}}$.*

Доказательство. Для $\mathbf{x}^{\mathbf{a}^{\mathbf{p}}} > \mathbf{x}^{\mathbf{b}^{\mathbf{p}}}$ выполняется соотношение $\|\mathbf{a}^{\mathbf{p}}\|_p \geq \|\mathbf{b}^{\mathbf{p}}\|_p$, и нетрудно понять, что $\mathbf{x}^{\mathbf{b}^{\mathbf{p}}} \triangleleft l$ может содержать моном, который линейно связан с $\mathbf{x}^{\mathbf{a}^{\mathbf{p}}}$, только при условии $\|\mathbf{a}^{\mathbf{p}}\|_p = \|\mathbf{b}^{\mathbf{p}}\|_p$ и, соответственно, $\mathbf{a}^{\mathbf{p}} >_{\text{lex}} \mathbf{b}^{\mathbf{p}}$.

Пусть

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

и $s j_s$ — первый номер, для которого $a_{s j_s} > b_{s j_s}$. Тогда очевидно, что при $s < k$ или $s = k$, $j_s < r$ многочлен $\mathbf{x}^{\mathbf{b}^{\mathbf{p}}} \triangleleft l$ не содержит мономов вида

$$x_{i_0}^{a_{00}} \dots x_{i_0}^{p^{t-1}a_{0t-1}} \dots x_{i_s}^{a_{s0}} \dots x_{i_s}^{p^{j_s} a_{s j_s}} \dots$$

и, следовательно, не содержит мономов, которые линейно связаны с $\mathbf{x}^{\mathbf{a}^p}$. Значит, $s = k$, $j_s = r$ и

$$\mathbf{x}^{\mathbf{b}^p} = x_{i_0}^{a_{00}} \dots x_{i_0}^{p^{t-1}a_{0t-1}} \dots x_{i_k}^{a_{k0}} \dots x_{i_k}^{p^{r-1}a_{kr-1}} x_{i_k}^{p^r b_{kr}} \dots$$

Теперь легко видеть, что $\mathbf{x}^{\mathbf{b}^p} \triangleleft l$ может содержать моном, который линейно связан с $\mathbf{x}^{\mathbf{a}^p}$, только при $b_{kr} = a_{kr} - 1$. Таким образом, моном $\mathbf{x}^{\mathbf{b}^p}$ имеет вид

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

и по определению линейно связан с $\mathbf{x}^{\mathbf{a}^p}$. $\square$

Если предположить, что $\mathbf{x}^{\mathbf{a}^p_s}$ — наибольший из мономов $\mathbf{x}^{\mathbf{a}^p_1} > \dots > \mathbf{x}^{\mathbf{a}^p_m}$, который линейно связан с $\mathbf{x}^{\mathbf{a}^p_0}$, то согласно доказанной лемме многочлены

$$\mathbf{x}^{\mathbf{a}^p_1} \triangleleft l_1(x_0, \dots), \dots, \mathbf{x}^{\mathbf{a}^p_{s-1}} \triangleleft l_{s-1}(x_0, \dots)$$

не содержат мономов, которые линейно связаны с $\mathbf{x}^{\mathbf{a}^p_0}$, и, следовательно, многочлен $\psi - \varphi$ содержит линейно связанный с $\mathbf{x}^{\mathbf{a}^p_0}$ моном $\mathbf{x}^{\mathbf{a}^p_s}$, что противоречит предположению. Таким образом, доказали, что $\mathbf{x}^{\mathbf{a}^p_0} > \dots > \mathbf{x}^{\mathbf{a}^p_m}$ — последовательность линейно не связанных мономов.

Единственность указанного разложения следует из того, что:

- коэффициент c_0 и моном $\mathbf{x}^{\mathbf{a}^p_0}$ однозначно определяются старшим членом функции f ,
- линейная функция $l_0(x_0, \dots)$ однозначно определяется совокупностью

$$h_l x_{i_0}^{a_{i_0 0}} \dots x_{i_0}^{p^{t-1}a_{i_0 t-1}} \dots x_{i_k}^{a_{i_k 0}} \dots x_{i_k}^{p^{r-1}a_{i_k r-1}} x_{i_k}^{p^r(a_{i_k r}-1)} x_{i_k+j_l}^{p^r}, \quad l \in \{1, \dots, s\},$$

всех одночленов f , линейно связанных с $\mathbf{x}^{\mathbf{a}^p_0}$,

- сумма $c + \sum_{i=1}^m c_i \mathbf{x}^{\mathbf{a}^p_i} \triangleleft l_i(x_0, \dots)$ определена однозначно по предположению индукции как соответствующее разложение функции $f - c_0 \mathbf{x}^{\mathbf{a}^p_0} \triangleleft l_0$.

Для завершения доказательства остается описать правые линейные делители функции f , существенно зависящей от переменной x_0 . В таком случае из разложения $f = g \triangleleft l$, $g \in F_q$, $l \in L_q$, необходимо следует, что l линейна по переменной x_0 и, не ограничивая общности, можно полагать l унитарной по переменной x_0 .

Согласно доказанному функция g обладает разложением

$$g = c' + \sum_{i=0}^{m'} c'_i \mathbf{x}^{\mathbf{a}'^p_i} \triangleleft l'_i(x_0, \dots),$$

где $c' \in \Omega_q$, $\mathbf{x}^{\mathbf{a}'_0} > \dots > \mathbf{x}^{\mathbf{a}'_{m'}}$ — убывающая последовательность линейно не связанных мономов, и для каждого $i \in \{0, \dots, m'\}$ коэффициент c'_i отличен от 0, а $l'_i(x_0, \dots)$ — линейная функция, унитарная по переменной x_0 . Однако в таком случае получаем, что функция f обладает разложением

$$f = g \triangleleft l = c' + \sum_{i=0}^{m'} c'_i \mathbf{x}^{\mathbf{a}'_i} \triangleleft (l'_i \triangleleft l)(x_0, \dots),$$

которое в силу единственности должно совпадать с

$$f = c + \sum_{i=0}^m c_i \mathbf{x}^{\mathbf{a}_i} \triangleleft l_i(x_0, \dots).$$

Значит, $m = m'$ и $c_i = c'_i$, $l_i = l'_i \triangleleft l$ для каждого $i \in \{0, \dots, m\}$. $\square$

Следствие 3. Произвольная функция $f \in F_q$ однозначно представляется в виде $f = x_s \triangleleft g \triangleleft l$, где x_s — крайняя левая переменная, от которой f зависит существенным образом, функция g — линейно неприводимая справа, $l \in L_q$ — унитарная по переменной x_0 .

Замечание 9. Представление, доказанное в теореме 6, существенно зависит от условий

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

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

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

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

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

3.3. Особенности двустороннего линейного разложения

Теорема 8. Пусть q — простое и функция $f \in F_q$ делится слева на $m_1 \in L_q$:

$$f = m_1 \triangleleft g_1,$$

а справа на $m_2 \in L_q$:

$$f = g_2 \triangleleft m_2.$$

Тогда если m_1 и m_2 взаимно просты, то справедливо разложение

$$f = m_1 \triangleleft g \triangleleft m_2.$$

Если дополнительно m_1 и m_2 — максимальные левый и правый линейные делители функции f , то g — линейно неприводимая.

Доказательство. Докажем утверждение индукцией по старшему относительно градуированного лексикографического порядка моному приведенного многочлена $\tilde{f}$. Не ограничивая общности, для удобства будем полагать, что $f \in \hat{F}_q$, а m_1, m_2 — унитарные по крайней левой переменной.

База при $f \in L_q$ вполне очевидна: изоморфизм колец $(\mathbb{F}_q[x], +, \cdot)$ и $(L_q, +, \triangleleft)$ позволяет использовать свойства взаимно простых многочленов применительно к линейным функциям, а потому из условия леммы необходимо следует, что

$$f = (m_1 \triangleleft m_2) \triangleleft g = m_1 \triangleleft g \triangleleft m_2, \quad g \in L_q.$$

Докажем индуктивный переход. Не ограничивая общности, полагаем длину функции $f(x_0, \dots, x_n)$ равной n — в таком случае f существенно зависит от переменной x_0 и, как следствие, m_1 линейна по переменной x_0 . Пусть старший член функции f имеет вид $cx^{\mathbf{a}} = cx_{i_0}^{a_0} \dots x_{i_k}^{a_k}$ и все члены приведенного многочлена f , линейно связанные с $cx^{\mathbf{a}}$, суть

$$h_1 x_{i_0}^{a_0} \dots x_{i_k}^{a_k-1} x_{i_k+j_1}, \dots, h_s x_{i_0}^{a_0} \dots x_{i_k}^{a_k-1} x_{i_k+j_s}.$$

Согласно теореме 5 унитарная по переменной x_0 линейная функция l_2 , которая связывает указанные члены с $cx^{\mathbf{a}}$, делится на m_2 .

Поскольку моном $\mathbf{x}^{\mathbf{a}}$ является старшим среди мономов многочлена f , то нетрудно понять, что в многочлене f могут содержаться только неотрицательные сдвиги монома $\mathbf{x}^{\mathbf{b}} = x_{i_0}^{a_{i_0}} \dots x_{i_k}^{a_{i_k}-1} x_{i_k+j_s}$:

$$x_j \triangleleft \mathbf{x}^{\mathbf{b}} = x_{j+i_0}^{a_0} \dots x_{j+i_k}^{a_k-1} x_{j+i_k+j_s}, \quad j \geq 0.$$

Значит, многочлен f содержит все сдвиги монома $\mathbf{x}^{\mathbf{b}}$ в виде $l_b \triangleleft \mathbf{x}^{\mathbf{b}}$, $l_b \in L_q$. Согласно теореме 4 функция l_b делится на m_1 и, как следствие, справедливы соотношения

$$\text{len } m_1 \triangleleft \mathbf{x}^{\mathbf{b}} = \text{len } m_1 + \text{len } \mathbf{x}^{\mathbf{b}} \leq \text{len } l_b + \text{len } \mathbf{x}^{\mathbf{b}} = \text{len } l_b \triangleleft \mathbf{x}^{\mathbf{b}} \leq n.$$

Рассмотрим теперь функцию $c m_1 \triangleleft \mathbf{x}^a \triangleleft l_2$, которая по построению делится слева на m_1 , а справа на m_2 . Легко видеть, что

$$\text{len}(m_1 \triangleleft \mathbf{x}^a \triangleleft l_2) = \text{len } m_1 + \text{len}(\mathbf{x}^a \triangleleft l_2) = \text{len } m_1 + \text{len } \mathbf{x}^b = \text{len}(m_1 \triangleleft \mathbf{x}^b) \leq n,$$

а кроме того, старший член функции $c m_1 \triangleleft \mathbf{x}^a \triangleleft l_2$ очевидно равен $c \mathbf{x}^a$. Значит, функция

$$f - c m_1 \triangleleft \mathbf{x}^a \triangleleft l_2$$

также зависит от переменных $x_0, \dots, x_n$, делится слева на m_1 , справа на m_2 , но при этом ее старший моном меньше $\mathbf{x}^a$ и, следовательно, к ней применимо предположение индукции:

$$f - c m_1 \triangleleft \mathbf{x}^a \triangleleft l_2 = m_1 \triangleleft g' \triangleleft m_2,$$

что и дает требуемое разложение

$$f = m_1 \triangleleft \mathbf{x}^a \triangleleft l_2 + m_1 \triangleleft g' \triangleleft m_2 = m_1 \triangleleft g \triangleleft m_2.$$

□

Замечание 10. Условие простоты q является существенным в теореме 8. Так, например, если $q = p^t$, $t \geq 2$ и $\alpha \in \mathbb{F}_q \setminus \mathbb{F}_p$, то $\alpha^p \neq \alpha$ и линейные функции $x_0 + \alpha x_1$, $x_0 + \alpha^p x_1$ взаимно просты. Однако при этом справедливы разложения

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

и легко видеть (учитывая параметр len), что представление

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

невозможно.

Замечание 11. Условие взаимной простоты левого и правого линейных делителей является существенным в теореме 8. Так, например, для булевой функции

$$f = (x_0 \oplus x_1) \triangleleft x_1 x_2 \triangleleft (x_0 \oplus x_1) \oplus (x_0 \oplus x_1)$$

справедливы представления

$$f = (x_0 \oplus x_1) \triangleleft (x_1 x_2 \oplus x_1 x_3 \oplus x_2 x_3 \oplus x_2 \oplus x_0) = (x_0 \oplus x_1) \triangleleft g_1,$$

$$f = (x_1 x_2 \oplus x_2 x_3 \oplus x_0) \triangleleft (x_0 \oplus x_1) = g_2 \triangleleft (x_0 \oplus x_1).$$

При этом g_1 — линейно неприводимая справа, а g_2 — линейно неприводимая слева, и потому невозможно разложение

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

Забегая вперед, отметим, что (согласно п. 3 теоремы 10) представления

$$f = (x_0 \oplus x_1) \triangleleft g_1 \quad \text{и} \quad g_2 \triangleleft (x_0 \oplus x_1)$$

на самом деле суть два различных разложения функции $f \in {}^+F_2$ в виде сдвиг-композиции неприводимых элементов моноида $({}^+F_2, \triangleleft)$.

4. Квадратичные функции над простым полем

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

Для полного описания всех линейных делителей произвольной квадратичной функции можно использовать результаты теорем 4 и 6, которые оформим в виде следующего утверждения.

Утверждение 9. 1) Квадратичная функция $f \in \widehat{F}_q$ однозначно представляется в виде

$$f = l(x_0, \dots) + l_0(x_{s_0}, \dots) \triangleleft x_0^2 + l_1(x_{s_1}, \dots) \triangleleft x_0 x_1 + \dots + l_r(x_{s_r}, \dots) \triangleleft x_0 x_n,$$

где $s_0 < s_1 < \dots < s_r$ (в случае $q = 2$ слагаемое $l_0(x_{s_0}, \dots) \triangleleft x_0^2$ отсутствует). При этом все левые линейные делители функции f исчерпываются делителями $(l, l_0, l_1, \dots, l_r)$.

2) Если q — четное, то квадратичная функция f однозначно представляется в виде

$$f = l(x_{s_0}, \dots) + c_0 x_{s_0}^2 \triangleleft l_0(x_0, \dots) + c_1 x_{s_1} x_{t_1} \triangleleft l_1(x_0, \dots) + \dots + c_k x_{s_k} x_{t_k} \triangleleft l_k(x_0, \dots),$$

где $s_1 < \dots < s_k$ (в случае $q = 2$ слагаемое $c_0 x_{s_0}^2 \triangleleft l_0(x_0, \dots)$ отсутствует) и для каждого $i \in \{1, \dots, k\}$: $s_i < t_i$, коэффициент c_i отличен от 0, а $l_i(x_0, \dots)$ — линейная функция, унитарная по переменной x_0 . Если при этом f существенно зависит от переменной x_0 , то все правые линейные делители функции f исчерпываются делителями $(l, l_0, l_1, \dots, l_k)$.

3) Если q — нечетное, то квадратичная функция f однозначно представляется в виде

$$f = l(x_{s_0}, \dots) + c_1 x_{s_1} x_{t_1} \triangleleft l_1(x_0, \dots) + \dots + c_k x_{s_k} x_{t_k} \triangleleft l_k(x_0, \dots),$$

где $s_1 < \dots < s_k$ и для каждого $i \in \{1, \dots, k\}$: $s_i \leq t_i$, коэффициент c_i отличен от 0, а $l_i(x_0, \dots)$ — линейная функция, унитарная по переменной x_0 . Если при этом f существенно зависит от переменной x_0 , то все правые линейные делители функции f исчерпываются делителями $(l, l_1, \dots, l_k)$.

Как показывает следующее утверждение, в случае простого поля для линейных функций, а также квадратичных функций, линейных по крайним переменным, понятия приводимости и линейной приводимости совпадают.

Теорема 10. Если q — простое число, то для композиции $f \triangleleft g$ произвольных функций $f \in F_q$ и $g \in {}^+F_q$ справедливы утверждения:

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

Доказательство. Не ограничивая общности, будем полагать, что функции $f(x_0, \dots, x_n)$ и $g(x_0, \dots, x_m)$ имеют длины n и m соответственно.

1) Поскольку произвольная $g \in {}^+F_q$ является функцией без запретов, то, как уже отмечалось ранее, она не может быть правым делителем нуля.

Для доказательства пп. 2) и 3) потребуются вспомогательные утверждения, которые позволяют оценивать степень сдвиг-композиции $f \triangleleft g$ и сами по себе представляют интерес.

Лемма 11. Если $\deg l = 1$, то для любой $f \in F_q$ выполняются равенства

$$\deg(f \triangleleft l) = \deg(l \triangleleft f) = \deg f.$$

Доказательство. Не ограничивая общности, будем считать, что l — линейная по переменной x_0 . В таком случае нетрудно понять, что старший относительно лексикографического порядка моном $\mathbf{x}^{\mathbf{a}}$ приведенного многочлена f будет также старшим мономом в приведенных многочленах функций $l \triangleleft f$ и $f \triangleleft l$. $\square$

Лемма 12. При простом q для любых $f \in F_q$, $\deg f \geq 2$, и $g \in {}^+F_q$ выполняется неравенство

$$\deg(f \triangleleft g) \geq \deg g + 1.$$

Доказательство. Ввиду леммы утверждение очевидно для ненулевой аффинной g :

$$\deg(f \triangleleft g) = \deg f \geq 2 \geq \deg g + 1.$$

Поэтому далее полагаем, что

$$g = x_0 + \psi(x_1, \dots, x_m), \quad \deg g = \deg \psi \geq 2.$$

Докажем утверждение индукцией по параметру $\text{len } f$. База при $\text{len } f = 0$:

$$f(x_0) = \sum_{i=0}^{q-1} c_i x_0^i = \sum_{i=0}^s c_i x_0^i, \quad c_s \neq 0, \quad s \geq 2.$$

В таком случае справедливо разложение

$$\begin{aligned} f \triangleleft g &= \sum_{i=0}^s c_i (x_0 + \psi(x_1, \dots, x_m))^i = c_s x_0^s \\ &\quad + s c_s x_0^{s-1} \psi(x_1, \dots) + c_{s-1} x_0^{s-1} + h(x_0, \dots), \end{aligned}$$

где $h(x_0, \dots, x_m)$ содержит переменную x_0 в степени не выше $s - 2$, и легко видеть, что

$$\begin{aligned} \deg(f \triangleleft g) &\geq \deg(c_s x_0^s + s c_s x_0^{s-1} \psi(x_1, \dots) + c_{s-1} x_0^{s-1}) \\ &\geq \deg(x_0^{s-1} (s c_s \psi(x_1, \dots) + c_{s-1})) \\ &= \deg(s c_s \psi(x_1, \dots) + c_{s-1}) + s - 1 \\ &= \deg \psi(x_1, \dots) + s - 1 = \deg g + s - 1 \geq \deg g + 1. \end{aligned}$$

Докажем индуктивный переход при $\text{len } f > 0$. Пусть

$$f = l_f(x_0, \dots, x_{r-1}) + \varphi(x_r, \dots, x_n),$$

где l_f — линейная, а $\varphi(x_r, \dots, x_n)$ зависит существенно и нелинейно от переменной x_r . Тогда функция φ представима многочленом

$$\sum_{i=0}^{q-1} x_r^i \varphi_i(x_{r+1}, \dots) = \sum_{i=0}^s x_r^i \varphi_i(x_{r+1}, \dots), \quad \varphi_s \neq 0,$$

и соотношение $f \triangleleft g$ можно переписать подробнее

$$\begin{aligned} f \triangleleft g &= l_f \triangleleft g + (x_r^s + s x_r^{s-1} \psi(x_{r+1}, \dots) + \dots) \cdot (\varphi_s \triangleleft g)(x_{r+1}, \dots) \\ &+ (x_r^{s-1} + (s-1) x_r^{s-2} \psi(x_{r+1}, \dots) + \dots) \cdot (\varphi_{s-1} \triangleleft g)(x_{r+1}, \dots) + \dots \end{aligned}$$

Рассмотрим все возможные случаи.

1. Если $s \geq 2$ и $\deg \varphi_s \geq 2$, то к композиции $\deg(\varphi_s \triangleleft g)$ применимо предположение индукции

$$\deg(x_r^s (\varphi_s \triangleleft g)(x_{r+1}, \dots)) \geq s + \deg g + 1 > \deg(l_f \triangleleft g),$$

и тогда

$$\begin{aligned} \deg(f \triangleleft g) &\geq \deg(l_f \triangleleft g + x_r^s (\varphi_s \triangleleft g)(x_{r+1}, \dots)) \\ &\geq \deg(x_r^s (\varphi_s \triangleleft g)) \geq s + \deg g + 1 \geq \deg g + 3. \end{aligned}$$

2. Если $s \geq 2$ и $\deg \varphi_s = 1$, то

$$\deg(x_r^s (\varphi_s \triangleleft g)(x_{r+1}, \dots)) = s + \deg g > \deg(l_f \triangleleft g),$$

и тогда

$$\begin{aligned} \deg(f \triangleleft g) &\geq \deg(l_f \triangleleft g + x_r^s (\varphi_s \triangleleft g)(x_{r+1}, \dots)) \\ &\geq \deg(x_r^s (\varphi_s \triangleleft g)) = s + \deg g \geq \deg g + 2. \end{aligned}$$

3. Если $s \geq 2$, $\varphi_s = c_s \in P \setminus 0$ и $\deg \varphi_{s-1} \geq 2$, то по предположению индукции

$$\deg(\varphi_{s-1} \triangleleft g) \geq \deg g + 1 > \deg g = \deg \psi,$$

и тогда

$$\begin{aligned} \deg(f \triangleleft g) &\geq \deg(l_f \triangleleft g + s c_s x_r^{s-1} \psi(x_{r+1}, \dots) + x_r^{s-1} (\varphi_{s-1} \triangleleft g)(x_{r+1}, \dots)) \\ &= \deg(x_r^{s-1} (\varphi_{s-1} \triangleleft g)) \geq \deg g + 1 + s - 1 \geq \deg g + 2. \end{aligned}$$

4. Если $s \geq 2$, $\varphi_s = c_s \in P \setminus 0$ и $\deg \varphi_{s-1} = 1$, то

$$(\varphi_{s-1} \triangleleft g)(x_{r+1}, \dots) = c_{s-1} (x_{r+1} + \psi(x_{r+2}, \dots)) + \dots,$$

и тогда

$$\begin{aligned} \deg(f \triangleleft g) &\geq \deg(l_f \triangleleft g + s c_s x_r^{s-1} \psi(x_{r+1}, \dots) + x_r^{s-1} (\varphi_{s-1} \triangleleft g)(x_{r+1}, \dots)) \\ &\geq \deg(s c_s x_r^{s-1} \psi) = \deg \psi + s - 1 \geq \deg g + 1. \end{aligned}$$

5. Если $s \geq 2$, $\varphi_s = c_s \in P \setminus 0$ и $\varphi_{s-1} = c_{s-1} \in P$, то

$$\begin{aligned} \deg(f \triangleleft g) &\geq \deg(l_f \triangleleft g + s c_s x_r^{s-1} \psi(x_{r+1}, \dots) + c_{s-1} x_r^{s-1}) \\ &\geq \deg(s c_s x_r^{s-1} \psi(x_{r+1}, \dots)) = \deg \psi + s - 1 \geq \deg g + 1. \end{aligned}$$

6. Если $s = 1$ и $\deg \varphi_s \geq 2$, то к композиции $\deg(\varphi_s \triangleleft g)$ применимо предположение индукции

$$\deg(x_r (\varphi_s \triangleleft g)(x_{r+1}, \dots)) \geq 1 + \deg g + 1 > \deg(l_f \triangleleft g),$$

и тогда

$$\deg(f \triangleleft g) \geq \deg(l_f \triangleleft g + x_r (\varphi_s \triangleleft g)) = \deg(x_r (\varphi_s \triangleleft g)) \geq \deg g + 2.$$

7. Если $s = 1$ и $\deg \varphi_s = 1$, то

$$\deg(x_r (\varphi_s \triangleleft g)) = \deg g + 1 > \deg(l_f \triangleleft g),$$

и тогда

$$\deg(f \triangleleft g) \geq \deg(l_f \triangleleft g + x_r (\varphi_s \triangleleft g)) = \deg(x_r (\varphi_s \triangleleft g)) = \deg g + 1.$$

□

2) Согласно лемме 12 равенство $\deg(f \triangleleft g) = 1$ возможно только в случае, когда $\deg f = 1$ и, следовательно, $\deg g = 1$ по лемме 11.

Достаточность сформулированного условия следует из леммы 11.

3) Если $\deg f \geq 2$, то согласно лемме 12 из равенства $\deg(f \triangleleft g) = 2$ необходимо следует, что $\deg g = 1$ и, следовательно, $\deg f = 2$ по лемме 11.

Если же $\deg f = 1$, то $\deg g = 2$ согласно лемме 11.

Достаточность сформулированного условия следует из леммы 11.

□

Сделаем ряд замечаний относительно доказанных утверждений.

Замечание 12. Пункт 2) теоремы 10 в частном случае $q = 2$ был доказан Вл. И. Солодовниковым в 1978 году (см. [6]).

Замечание 13. Простой пример

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

показывает, что уже в случае кубических функций понятие приводимости становится шире понятия линейной приводимости. Кроме того, этот пример показывает неулучшаемость доказанной оценки

$\deg(f \triangleleft g) \geq \deg g + 1$ даже для двоичных функций $f \in F_2$, $\deg f \geq 2$, и $g \in {}^+F_2$.

Рассмотренный пример также опровергает предположение о схожей оценке $\deg(f \triangleleft g) \geq \deg f + 1$ при простом q , $f \in F_q$, $\deg f \geq 2$, и $g \in {}^+F_q$. Отметим, что до сих пор не удалось построить пример, который опровергает оценку $\deg(f \triangleleft g) \geq \deg f$ при простом q , $f \in F_q$, $\deg f \geq 2$, и $g \in {}^+F_q$. (В случае составного q такой пример указан в замечании 16.)

Замечание 14. Пункты 2), 3) теоремы 10 не допускают дословного обобщения на случай составного q даже для функций, биективных по обоим крайним переменным. Так, например, над полем $\mathbb{F}_4$ справедливы разложения

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

Замечание 15. В двоичном случае в п. 2) теоремы 10 можно отказаться от условия $g \in {}^+F_2$, заменив его условием $g \in F_2$: из линейности $f \triangleleft g$ по переменной x_0 необходимо следует линейность обеих функций f и g по переменной x_0 . Однако при нечетном простом q в п. 2) нельзя отказаться от условия $g \in {}^+F_q$: даже довольно сильное условие $g \in {}^*F_q$ не является достаточным. Так, если $f(x_0)$ — нелинейный перестановочный полином (такие полиномы существуют при всех $q > 2$) и $g(x_0)$ — обратный к нему перестановочный полином, то $f \triangleleft g = x_0$.

Замечание 16. Условие $g \in {}^+F_q$ является существенным в п. 3) теоремы 10 и в лемме 12. Так, например, в простейшем двоичном случае

$$(x_0 \oplus x_1x_3 \oplus x_1x_2x_3) \triangleleft x_0x_1 = x_0x_1.$$

В случае нечетного простого q условие $g \in {}^+F_q$ нельзя заменить условием $g \in {}^*F_q$. Так, для нечетного q выполняется равенство $(q-1, q+1) = 2$ и, соответственно, $(q-1, \frac{q+1}{2^k}) = 1$ при некотором k . В таком случае функция $x_0^{\frac{q+1}{2^k}}$ является биективной и справедливо равенство

$$x_0^{2^k} \triangleleft x_0^{\frac{q+1}{2^k}} = x_0^{q+1} = x_0^2.$$

Список литературы

- [1] Кузьмин А. С., Нечаев А. А., Шишкин В. А., “Бент- и гипербент-функции над конечным полем”, *Труды по дискретной математике*, **10** (2007), 97–122.
- [2] Лидл Р., Нидеррайтер Г., *Конечные поля*, **1, 2**, М.: Мир, 1988, 822 с.

- [3] Солодовников В.И., “О полугруппе, порожденной автоматными отображениями обратимого автомата”, *Труды по дискретной математике*, **4** (2001), 231–242.
- [4] Солодовников В.И., “Гомоморфизмы двоичных регистров сдвига”, *Дискретная математика*, **17**:1 (2005), 73–88.
- [5] Солодовников В.И., “Гомоморфизмы регистров сдвига в линейные автоматы”, *Дискретная математика*, **20**:4 (2008), 87–101.
- [6] Солодовников В.И., *Регистры сдвига и криптоалгоритмы на их основе*, LAP LAMBERT Academic Publishing, 2017, 112 с.
- [7] Черемушкин А.В., “Аддитивный подход к определению степени нелинейности дискретной функции”, *Прикладная дискретная математика*, 2010, № 2, 22–33.