ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

**Том 56** **2020** **Вып. 4**

УДК 621.391 : 519.714.5

© 2020 г. **И.В. Чередник**

# ОСОБЕННОСТИ $p$-ЛИНЕЙНОГО РАЗЛОЖЕНИЯ $p$-ЛИНЕЙНЫХ ФУНКЦИЙ В ТЕРМИНАХ ОПЕРАЦИИ СДВИГ-КОМПОЗИЦИИ

Исследуется операция сдвиг-композиции дискретных функций, которая возникает при гомоморфизмах конечных регистров сдвига. Доказано, что при простом $p$ в классе всех функций, линейных по крайним переменным, для $p$-линейных функций совпадают понятия приводимости и $p$-линейной приводимости. Кроме того, показано, что линейная функция, неприводимая в классе всех линейных функций, не имеет $p$-линейных делителей, биективных по крайней правой переменной, а в некоторых случаях и вовсе не имеет $p$-линейных делителей.

*Ключевые слова*: регистр сдвига, гомоморфизмы регистров сдвига, сдвиг-композиция, конечные поля, $p$-линейные функции, разложение матричных многочленов, скрученные многочлены, скрученные линейные рекуррентные последовательности.

**DOI:** 10.31857/S0555292320040063

## § 1. Введение

Пусть $\mathbb{F}_q$ – конечное поле из $q = p^t$ элементов, $F_q(n) = \{f \mid f\colon \mathbb{F}_q^n \to \mathbb{F}_q\}$ – множество всех $\mathbb{F}_q$-значных функций от $n$ переменных, $F_q = \bigcup\limits_{n\geqslant 0} F_q(n)$.

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

$$\forall f \in F_q(n+1)\ \forall g \in F_q(m+1)$$
$$(f \lhd g)(x_0, \dots, x_{n+m}) = f\big(g(x_0, \dots, x_m), \dots, g(x_n, \dots, x_{n+m})\big).$$

В работах перечисленных выше авторов в разной степени общности и направленности достаточно подробно исследована связь между представлением функции $h$ в виде $h = f \lhd g$ и существованием гомоморфизма регистра сдвига, внутреннее функционирование которого определяется функцией $h$, на регистр сдвига, внутреннее функционирование которого определяется функцией $f$ (функция $g$ из разложения $h = f \lhd g$ определяет характер гомоморфизма регистров сдвига). Все основные достижения в данной области единым образом изложены в монографии [1], мы лишь кратко перечислим результаты, полученные в направлении декомпозиции функций относительно операции $\lhd$-умножения.

В работе [2] описаны все возможные представления произвольной функции $h \in F_q$ в виде $h = l \lhd g$, где $l$ – линейная над $\mathbb{F}_q$ функция. Это достижение позволяет указать все возможные гомоморфизмы произвольного регистра сдвига на регистры сдвига с линейной обратной связью.

В работе [3] описаны все возможные представления произвольной функции $h \in F_q$ в виде $h = f \lhd l$, где $l$ – линейная над $\mathbb{F}_q$ функция. Кроме того, изучена возможность представления произвольной функции $h \in F_q$ в виде $f = l_1 \lhd g \lhd l_2$, где $l_1, l_2$ – линейные над $\mathbb{F}_q$ функции.

В работе [4] в терминах операции сдвиг-композиции исследуется возможность левого линейного разложения системы функций. Как оказалось, подобные разложения кроме стандартных приложений, связанных с гомоморфизмами регистров сдвига (см. [1]), обнаруживают очень интересное применение в вычислении представления произвольной функции $h \in F_q$ в виде $h = f \lhd g$, где $f$ – $p$-линейная функция (линейная над $\mathbb{F}_p$). Здесь стоит отметить, что предложенный в работе [4] метод позволяет эффективно выделять максимальный левый $p$-линейный $\lhd$-делитель у произвольной $p$-нелинейной функции, но не пригоден для построения нетривиального $p$-линейного $\lhd$-разложения $p$-линейной функции. Последняя задача по существу является переформулировкой классической проблемы факторизации многочленов над кольцом матриц и, очевидно, крайне сложна.

В данной статье мы представляем два нетривиальных результата о $p$-линейных разложениях $p$-линейных функций, которые кроме теоретической ценности описания возможных гомоморфизмов регистров сдвига также имеют большое значение при исследовании факторизации многочленов над кольцом матриц и, соответственно, при построении практически значимых классов скрученных линейных рекуррентных последовательностей (см. [5]).

## § 2. Постановка задачи

**1.** Следуя терминологии работ [1,2,6,7], регистром сдвига длины $n$ над полем $\mathbb{F}_q$ с функцией обратной связи $\varphi \in F_q(n+1)$ и выходной функцией $\psi \in F_q(n+1)$ будем называть автомат

$$R(\varphi, \psi) = (\mathbb{F}_q, \mathbb{F}_q^n, \mathbb{F}_q, h, f),$$

у которого функции переходов и выходов определяются равенствами

$$h((x_1, \ldots, x_n), x) = (x_2, \ldots, x_n, \varphi(x_1, \ldots, x_n, x)),$$
$$f((x_1, \ldots, x_n), x) = \psi(x_1, x_2, \ldots, x_n, \varphi(x_1, \ldots, x_n, x)).$$

Нетрудно видеть, что биективность функции обратной связи $\varphi$ по первой переменной равносильна регулярности регистра сдвига $R(\varphi, \psi)$ – при любом входном символе частичная функция переходов $h_x$ автомата $R(\varphi, \psi)$ является биекцией. Кроме того, биективность каждой из функций $\varphi$ и $\psi$ по последней переменной является необходимым и достаточным условием для обратимости автомата $R(\varphi, \psi)$. В связи с отмеченными особенностями при реализации регистров сдвига на практике преимущественно используются функции обратной связи, биективные по первой и (или) последней переменным, и выходные функции, биективные по последней переменной (см. [1, 2, 7]). Здесь стоит отметить, что наиболее простыми в реализации и, соответственно, наиболее распространенными на практике функциями, биективными по какой-либо переменной, являются функции, линейные по указанной переменной.

Множество всех $\mathbb{F}_q$-значных функций, биективных по первой (последней) переменной, будем обозначать через ${}^*F_q$ ($F_q^*$), а множество всех $\mathbb{F}_q$-значных функций, линейных по первой (последней) переменной, – через ${}^+F_q$ ($F_q^+$). При этом естественными будут производные обозначения

$${}^*F_q^* = {}^*F_q \cap F_q^*, \quad {}^*F_q^+ = {}^*F_q \cap F_q^+, \quad {}^+F_q^* = {}^+F_q \cap F_q^*, \quad {}^+F_q^+ = {}^+F_q \cap F_q^+.$$

**2.** Как известно (см. [8]), каждая функция $f(x_0,\dots,x_n)\in F_q$ единственным образом представляется приведенным многочленом из $\mathbb{F}_q[x_0,x_1,\dots]$:

$$f(x_0,\dots,x_n)=\sum_{i_0,\dots,i_n\in\overline{0,q-1}} c_{i_0\dots i_n}x_0^{i_0}\dots x_n^{i_n}.$$

При проведении некоторых исследований относительно функций из $F_q$ часто бывает удобным вести изложение на языке соответствующих приведенных многочленов из $\mathbb{F}_q[x_0,x_1,\dots]$, которые в отличие от функций определяются от общего набора переменных $x_0,x_1,\dots$

Множество всех приведенных многочленов из $\mathbb{F}_q[x_0,x_1,\dots]$ относительно операций сложения и умножения с последующим приведением результата по модулю идеала $(x_i^q-x_i\mid i\in\mathbb{N}_0)$ образует коммутативное кольцо с единицей. Кроме того, на множестве всех приведенных многочленов из $\mathbb{F}_q[x_0,x_1,\dots]$ корректно определить операцию сдвиг-композиции ($\lhd$-умножения):

$$f(x_0,\dots,x_n)\lhd g(x_0,\dots,x_m)\stackrel{\text{def}}{=}$$
$$\stackrel{\text{def}}{=} f\big(g(x_0,\dots,x_m),\dots,g(x_n,\dots,x_{n+m})\big)\mod(x_i^q-x_i\mid i\in\mathbb{N}_0).$$

Нетрудно видеть, что множество всех приведенных многочленов из $\mathbb{F}_q[x_0,x_1,\dots]$ относительно операции $\lhd$-умножения образует полугруппу с нейтральным элементом $x_0$.

**3.** Как известно, существует несколько подходов к определению степени нелинейности отображения над конечным полем $\mathbb{F}_q$ (см. [9, 10]). Наиболее простой состоит в том, что под степенью нелинейности функции $f\in F_q$ понимается степень соответствующего приведенного многочлена из $\mathbb{F}_q[x_0,x_1,\dots]$. При таком подходе линейными называют функции, приведенные многочлены которых имеют вид

$$\beta_0x_0+\dots+\beta_nx_n\in\mathbb{F}_q[x_0,x_1,\dots].$$

Однако в случае $q=p^t$ на практике зачастую гораздо более плодотворным оказывается другой подход к определению степени нелинейности, который учитывает более общую линейность отображения $f\in F_q$ над подполем $\mathbb{F}_p$.

Если функция $f(x_0,\dots,x_n)\in F_q$ задана приведенным многочленом

$$f(x_0,\dots,x_n)=\sum_{i_0,\dots,i_n\in\overline{0,q-1}} c_{i_0\dots i_n}x_0^{i_0}\dots x_n^{i_n},$$

то *индексом p-нелинейности функции* $f$ называют величину

$$\operatorname{ind}_p f=\max\big\{\|i_0\|_p+\dots+\|i_n\|_p:\ i_0,\dots,i_n=\overline{0,q-1},\ c_{i_0\dots i_n}\neq0\big\},\tag{1}$$

где $\|j\|_p=j_0+j_1+\dots+j_{t-1}$ – $p$-ичный вес числа $j=j_0+pj_1+\dots+p^{t-1}j_{t-1}\in\overline{0,q-1}$.

С другой стороны, если зафиксировать некоторый базис $\alpha_1,\dots,\alpha_t$ пространства $\mathbb{F}_q$ над $\mathbb{F}_p$, то каждый аргумент $x_i$ функции $f(x_0,\dots,x_n)$ можно представить в виде

$$x_i=\alpha_1x_{i1}+\dots+\alpha_tx_{it},\quad x_{ij}\in\mathbb{F}_p,$$

а саму функцию $f(x_0,\dots,x_n)$ отождествить с набором $p$-значных *координатных* функций

$$f_1(x_{01},\dots,x_{0t},\dots,x_{n1},\dots,x_{n,t}),$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$
$$f_t(x_{01},\dots,x_{0t},\dots,x_{n1},\dots,x_{n,t}),$$

который удовлетворяет соотношению $f = \alpha_1 f_1 + \ldots + \alpha_t f_t$. В таком случае индекс $p$-нелинейности функции $f$ согласно [9] можно вычислить по формуле

$$\operatorname{ind}_p f = \max\{\deg f_1, \ldots, \deg f_t\}. \tag{2}$$

Здесь стоит отметить, что в случае простого $p$ индекс $p$-нелинейности функции $f \in F_q$ совпадает с ее аддитивным показателем нелинейности $\operatorname{dl} f$. Изящное аксиоматическое изложение аддитивного подхода к измерению степени нелинейности, а также сравнение данного подхода с классическим, можно найти в работах [10, 11]. Так, в работе [10] доказано, что при простом $p$ аддитивный показатель $\operatorname{dl} f$ степени нелинейности функции $f \in F_p$ совпадает с классическим показателем $\deg f$, а для произвольной функции $f \in F_q$ ее аддитивный показатель нелинейности можно вычислять различными способами в зависимости от представления функции $f$:

$$\operatorname{dl} f = \max\{\operatorname{dl} f_1, \ldots, \operatorname{dl} f_t\} = \max\{\deg f_1, \ldots, \deg f_t\} = \operatorname{ind}_p f.$$

Функцию $f \in F_q$ будем называть *$p$-линейной*, если $\operatorname{ind}_p f = 1$ и $f(0, \ldots, 0) = 0$. Согласно (1) функция $f(x_0, \ldots, x_n) \in F_q$ является $p$-линейной в том и только том случае, когда она представляется приведенным многочленом вида

$$\left(\beta_{01}x_0 + \ldots + \beta_{0t}x_0^{p^{t-1}}\right) + \ldots + \left(\beta_{n1}x_n + \ldots + \beta_{nt}x_n^{p^{t-1}}\right) \in \mathbb{F}_q[x_0, x_1, \ldots],$$

при этом ее координатные функции $f_1, \ldots, f_t$ ввиду (2) представляются многочленами вида

$$\begin{gathered}
a_{01}^{(1)}x_{01} + \ldots + a_{0t}^{(1)}x_{0t} + \ldots + a_{n1}^{(1)}x_{n1} + \ldots + a_{n,t}^{(1)}x_{n,t} \in \mathbb{F}_p[x_{01}, \ldots, x_{0t}, x_{11}, \ldots], \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
a_{01}^{(t)}x_{01} + \ldots + a_{0t}^{(t)}x_{0t} + \ldots + a_{n1}^{(t)}x_{n1} + \ldots + a_{n,t}^{(t)}x_{n,t} \in \mathbb{F}_p[x_{01}, \ldots, x_{0t}, x_{11}, \ldots].
\end{gathered}$$

Множество всех $p$-линейных функций из $F_q$ будем обозначать через $L_q^p$. Заметим, что в данной терминологии классические линейные функции из $F_q$ являются $q$-линейными, т.е. $L_q = L_q^q$. Напомним, что многочлены вида $\beta_1 x + \ldots + \beta_t x^{p^{t-1}} \in \mathbb{F}_q[x]$ описывают все линейные преобразования пространства $\mathbb{F}_q$ над полем $\mathbb{F}_p$ и называются *$p$-линеаризованными* многочленами (см. [8]). Соответственно, все $p$-линеаризованные многочлены вида

$$\left(\beta_{01}x_0 + \ldots + \beta_{0t}x_0^{p^{t-1}}\right) + \ldots + \left(\beta_{n1}x_n + \ldots + \beta_{n,t}x_n^{p^{t-1}}\right) \in \mathbb{F}_q[x_0, x_1, \ldots, x_n]$$

описывают все отображения пространства $\mathbb{F}_q^{n+1}$ в $\mathbb{F}_q$, линейные над $\mathbb{F}_p$.

**4.** Множество $L_q[x_0, x_1, \ldots]$ всех линейных, но не аффинных многочленов над $\mathbb{F}_q$

$$\beta_0 x_0 + \ldots + \beta_n x_n \in \mathbb{F}_q[x_0, x_1, \ldots]$$

относительно операций сложения и $\lhd$-умножения образует коммутативное кольцо, а отображение

$$\beta_0 x_0 + \ldots + \beta_n x_n \mapsto \beta_0 x^0 + \ldots + \beta_n x^n$$

является изоморфизмом колец $(L_q[x_0, x_1, \ldots], +, \lhd) \cong (\mathbb{F}_q[x], +, \cdot)$ (см. [1, 2, 7]).

Рассмотрим теперь множество $L_q^p[x_0, x_1, \ldots]$ всех $p$-линеаризованных многочленов из $\mathbb{F}_q[x_0, x_1, \ldots]$. Множество всех $p$-линеаризованных многочленов из $\mathbb{F}_q[x]$ относительно операций сложения и композиции образует кольцо, изоморфное кольцу $\operatorname{End}_{\mathbb{F}_p}\mathbb{F}_q$ всех линейных преобразований пространства $\mathbb{F}_q$ над $\mathbb{F}_p$. Указанный изо-

морфизм

$$\beta_1 x + \ldots + \beta_t x^{p^{t-1}} \mapsto B$$

естественным образом индуцирует отображение

$$\left(\beta_{01} x_0 + \ldots + \beta_{0t} x_0^{p^{t-1}}\right) + \ldots + \left(\beta_{n1} x_n + \ldots + \beta_{n,t} x_n^{p^{t-1}}\right) \mapsto B_0 + \ldots + B_n X^n,$$

являющееся изоморфизмом колец $(L_q^p[x_0, x_1, \ldots], +, \lhd) \cong ((\mathrm{End}_{\mathbb{F}_p} \mathbb{F}_q)[X], +, \cdot\,)$. Отметим, что кольцо $((\mathrm{End}_{\mathbb{F}_p} \mathbb{F}_q)[X], +, \cdot\,)$ известно как кольцо *скрученных* многочленов и является базовым объектом исследований в теории скрученных линейных рекуррентных последовательностей (см. [5, 12]).

Элементы кольца $\mathrm{End}_{\mathbb{F}_p} \mathbb{F}_q$ наиболее естественно представлять матрицами размера $t \times t$ над полем $\mathbb{F}_p$. Поэтому всюду далее в данной статье мы будем рассматривать кольцо скрученных многочленов $((\mathrm{End}_{\mathbb{F}_p} \mathbb{F}_q)[X], +, \cdot\,)$ в матричном представлении $((\mathbb{F}_p)_{t\times t}[X], +, \cdot\,)$, подразумевая при этом известный изоморфизм

$$((\mathbb{F}_p)_{t\times t}[X], +, \cdot\,) \cong ((\mathbb{F}_p[x])_{t\times t}, +, \cdot\,).$$

**5.** Будем говорить, что *функция $g$ делит справа функцию $h$*, если существует функция $f$, для которой выполняется равенство $h = f \lhd g$; при этом будем говорить, что *функция $f$ делит функцию $h$ слева*. Произвольная $h \in F_q$ делится слева и справа на обратимые элементы моноида $(F_q, \lhd)$:

$$h = g \lhd (g^{-1} \lhd h), \quad h = (h \lhd g^{-1}) \lhd g,$$

подобные разложения будем называть *несобственными*. Если функция $h$ допускает собственное разложение $h = f \lhd g$, то будем говорить, что $h$ *приводима*, а функции $f$ и $g$ будем называть *собственными левым и правым делителями функции $h$*.

Следуя [3], определим один параметр, который естественным образом характеризует размер функции. Если функция $f(x_0, \ldots, x_n)$ зависит существенным образом только от переменных $x_{i_0}, \ldots, x_{i_k}$, $0 \leqslant i_0 < \ldots < i_k \leqslant n$, то величину $\operatorname{len} f = i_k - i_0$ будем называть *длиной функции $f$*. Длины постоянных функций по определению полагаем равными $-\infty$. Введенный параметр удачно согласуется с операцией сдвиг-композиции:

$$\operatorname{len}(f \lhd g) \leqslant \operatorname{len} f + \operatorname{len} g;$$

более того, при естественных с практической точки зрения ограничениях $f \in {}^*F_q^*$ или $g \in {}^*F_q^*$ указанное неравенство обращается в равенство (см. [3, утверждение 3]).

Разложение $h = f \lhd g$, в котором $\operatorname{len} f < \operatorname{len} h$ и $\operatorname{len} g < \operatorname{len} h$, будем называть *существенным*, при этом функции $f$ и $g$ будем называть *существенными левым и правым делителями функции $h$*.

С практической точки зрения исследования гомоморфизмов регистров сдвига существенность соответствующих разложений (см. [2, теорема 1]) означает, что гомоморфный образ регистра сдвига является регистром сдвига меньшей длины. Здесь стоит отметить также, что наличие собственных разложений еще не гарантирует возможность их применения при решении практической задачи построения гомоморфизма регистра сдвига на регистр сдвига меньшей длины. Так, например, над полем $\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$ линейная функция $x_0 + x_1$ допускает собственное разложение

$$x_0 + x_1 = \left(x_0 + (\alpha + 1)x_1 + \alpha x_1^2\right) \lhd \left(x_0 + \alpha x_1 + \alpha x_1^2\right),$$

в котором длины компонент разложения совпадают с длиной исходной функции.

*Замечание* 1. Вообще говоря, существенное разложение необязательно является собственным и, наоборот, собственное разложение не всегда существенно. Однако при рассмотрении класса ${}^*F_q^*$, который относительно операции сдвиг-композиции образует полугруппу, понятия собственного и существенного разложений совпадают, поскольку множество всех обратимых элементов моноида $({}^*F_q^*, \lhd)$ совпадает с множеством всех его элементов длины 0.

*Замечание* 2. Нетрудно видеть, что множество $\widehat{F}_q$ всех функций из $F_q$, сохраняющих константу 0, замкнуто относительно операции сдвиг-композиции и образует полугруппу. Для произвольной функции $f \in F_q$, $f(0,\dots,0) = c_f$ существует тесная связь между приводимостью $f$ в $F_q$ и приводимостью $\widehat{f} = f - c_f$ в $\widehat{F}_q$:

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

Таким образом, исследование приводимости в моноиде $(F_q, \lhd)$ сводится к исследованию приводимости в подмоноиде $(\widehat{F}_q, \lhd)$. В дальнейшем в данной статье без ограничения общности рассматривается приводимость в рамках $\widehat{F}_q$, даже если это не оговаривается явным образом.

**6.** В работе [4] предложен эффективный алгоритм выделения максимального левого существенного $p$-линейного делителя у произвольной $p$-нелинейной функции $h$:

$$h = f \lhd g, \quad f \in L_q^p, \quad \operatorname{len} g \text{ минимально возможная.}$$

К сожалению, указанный алгоритм не пригоден даже для вычисления собственного разложения $p$-линейной функции – результатом применения данного метода к $p$-линейной функции $h$ будет тривиальное разложение $h = h \lhd x_0$. Задача нахождения $p$-линейных разложений $p$-линейных функций по существу эквивалентна построению $\lhd$-разложений $p$-линеаризованных многочленов в кольце $(L_q^p[x_0, x_1, \dots], +, \lhd)$ и фактически является переформулировкой классической проблемы о факторизации многочленов над кольцом матриц – по-видимому, на текущий момент данная проблема не имеет простого алгебраического решения.

В данной статье представлены два нетривиальных результата о $p$-линейных разложениях $p$-линейных функций, которые кроме теоретической ценности также имеют большое значение при исследовании и построении практически значимых классов скрученных линейных рекуррентных последовательностей (см. [5]). Исследование приводимости проводится в естественных практических рамках поиска существенных разложений, в которых обе компоненты линейны (биективны) по крайней правой переменной.

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

## § 3. $p$-линейная приводимость линейных функций

Как было отмечено выше, множество всех линейных многочленов $L_q[x_0, x_1, \dots]$ относительно операций сложения и сдвиг-композиции образует кольцо, изоморфное кольцу многочленов $\mathbb{F}_q[x]$. Таким образом, исследование приводимости классической линейной функции в классе $L_q$ эквивалентно известной проблеме факторизации многочленов над конечным полем $\mathbb{F}_q$ (см., например, [8]).

Поскольку $L_q \subsetneq L_q^p$, то очевидно, что для классической линейной функции понятие $p$-линейной приводимости в классе $L_q^p$ является более широким по сравнению с линейной приводимостью в классе $L_q$. Для удобства и наглядности исследование

$p$-линейной приводимости классических линейных функций будем проводить в матричном представлении, подразумевая ранее отмеченные изоморфизмы

$$(L_q^p[x_0, x_1, \ldots], \lhd, +) \cong ((\mathrm{End}_{\mathbb{F}_p} \mathbb{F}_q)[X], +, \cdot) \cong ((\mathbb{F}_p)_{t\times t}[X], +, \cdot) \cong ((\mathbb{F}_p[x])_{t\times t}, +, \cdot).$$

В матричной терминологии исследование $p$-линейной приводимости классической линейной функции $h \in L_q$ фактически означает исследование приводимости соответствующего многочлена $h(x) \in \mathbb{F}_q[x]$ в кольце многочленов $(\mathbb{F}_p)_{t\times t}[X]$.

Напомним, как устроено естественное вложение $\mathbb{F}_q[x] \to (\mathbb{F}_p)_{t\times t}[X]$. Выберем произвольный неприводимый над $\mathbb{F}_p$ многочлен $\chi(x) \in \mathbb{F}_p[x]$ степени $t$. Как известно, многочлен $\chi(x)$ имеет в поле $\mathbb{F}_q$ корень $\alpha$ и $\mathbb{F}_q = \mathbb{F}_p(\alpha)$. При выборе произвольной матрицы $S \in (\mathbb{F}_p)_{t\times t}$ с характеристическим многочленом $\chi(x)$ корректно определить отображение

$$r_0 + r_1\alpha + \ldots + r_{t-1}\alpha^{t-1} \mapsto r_0E + r_1S + \ldots + r_{t-1}S^{t-1}, \tag{3}$$

являющееся изоморфизмом полей

$$\mathbb{F}_q = \mathbb{F}_p(\alpha) \cong \mathbb{F}_p(S) = \{r_0E + r_1S + \ldots + r_{t-1}S^{t-1} : r_0, r_1, \ldots, r_{t-1} \in \mathbb{F}_p\}.$$

Данный изоморфизм полей естественным образом продолжается до изоморфизма колец многочленов $\mathbb{F}_p(\alpha)[x] \cong \mathbb{F}_p(S)[X]$, при котором многочлену

$$h(x) = h_0 + \ldots + h_{n-1}x^{n-1} + h_nx^n \in \mathbb{F}_p(\alpha)[x], \quad h_i = \sum_{j=0}^{t-1} r_{ij}\alpha^j, \quad 0 \leqslant i \leqslant n,$$

ставится в соответствие многочлен

$$H(X) = H_0 + \ldots + H_{n-1}X^{n-1} + H_nX^n \in \mathbb{F}_p(S)[X], \quad H_i = \sum_{j=0}^{t-1} r_{ij}S^j, \quad 0 \leqslant i \leqslant n.$$

Таким образом, установлено вложение $\mathbb{F}_q[x] \to (\mathbb{F}_p)_{t\times t}[X]$ (здесь стоит отметить, что данное вложение не является единственным, но все подобные вложения сопряжены).

Теперь можно сформулировать и доказать центральный результат данного параграфа.

Теорема 1. *Пусть многочлен $h(x) \in \mathbb{F}_q[x]$ неприводим над $\mathbb{F}_q$. Тогда $H(X)$ не имеет собственных унитарных делителей в кольце $(\mathbb{F}_p)_{t\times t}[X]$. Если к тому же $h(x) \notin \mathbb{F}_{p^l}[x]$ при всех $l < t$, то $H(X)$ вообще не имеет собственных делителей в $(\mathbb{F}_p)_{t\times t}[X]$.*

Доказательство. Для удобства будем полагать, что $h(x) \in \mathbb{F}_q[x]$ – унитарный многочлен степени $n$. При проведении доказательства будем использовать вложение $\mathbb{F}_q[x] \to (\mathbb{F}_p)_{t\times t}[X]$, которое определялось ранее с помощью отображения (3).

Неприводимый многочлен $\chi(x) \in \mathbb{F}_p[x]$ в расширении $\mathbb{F}_q = \mathbb{F}_p(\alpha)$ имеет $t$ различных корней $\alpha, \ldots, \alpha^{p^{t-1}}$, и как известно из курса линейной алгебры, существует обратимая матрица $C \in (\mathbb{F}_q)_{t\times t}$, такая что $C^{-1}SC = \mathrm{diag}(\alpha, \ldots, \alpha^{p^{t-1}})$. На самом деле сопряжение указанной матрицей $C$ приводит к диагональному виду все матрицы из $\mathbb{F}_p(S)$:

$$\begin{aligned}
&C^{-1}(r_0E + r_1S + \ldots + r_{t-1}S^{t-1})C = \ldots = \\
&= \mathrm{diag}\big(r_0 + r_1\alpha + \ldots + r_{t-1}\alpha^{t-1}, \ldots, r_0 + r_1\alpha^{p^{t-1}} + \ldots + r_{t-1}(\alpha^{p^{t-1}})^{t-1}\big) = \\
&= \mathrm{diag}\big(\beta, \ldots, \beta^{p^{t-1}}\big) \in (\mathbb{F}_q)_{t\times t}.
\end{aligned}$$

Предположим, что многочлен $H(X)$ допускает в кольце $(\mathbb{F}_p)_{t\times t}[X]$ собственное разложение:

$$H(X) = F(X)\cdot G(X), \quad \det F(x) \neq 1, \quad \det G(x) \neq 1.$$

Тогда при сопряжении обеих частей данного равенства матрицей $C$ получим соотношение

$$\begin{aligned}
&F_1(X)\cdot G_1(X) = (C^{-1}F(X)C)\cdot(C^{-1}G(X)C) = C^{-1}h(X)C = \\
&= C^{-1}\left(\left(\sum_{j=0}^{t-1} r_{0j}S^j\right) + \ldots + \left(\sum_{j=0}^{t-1} r_{n-1j}S^j\right)X^{n-1} + X^n\right)C = \\
&= \left(\sum_{j=0}^{t-1} r_{0j}, \operatorname{diag}\bigl(\alpha^j, \ldots, \alpha^{p^{t-1}j}\bigr)\right) + \ldots + \\
&+ \left(\sum_{j=0}^{t-1} r_{n-1j}\operatorname{diag}\bigl(\alpha^j, \ldots, \alpha^{p^{t-1}j}\bigr)\right)X^{n-1} + X^n = \\
&= \operatorname{diag}\Bigl(h_0 + \ldots + h_{n-1}x^{n-1} + x^n, \ldots, h_0^{p^{t-1}} + \ldots + h_{n-1}^{p^{t-1}}x^{n-1} + x^n\Bigr) = \\
&= \operatorname{diag}\Bigl(h(x), \ldots, h^{(p^{t-1})}(x)\Bigr).
\end{aligned}$$

Если $l \in \mathbb{N}$ – наименьшее со свойством $h(x) \in \mathbb{F}_{p^l}[x]$, то $t = lm$ и $(m,n) = 1$. Кроме того, $h^{(p^{l+s})} = h^{(p^s)}$, $s \in \mathbb{N}_0$, и следовательно,

$$\operatorname{diag}\Bigl(h(x), \ldots, h^{(p^{t-1})}(x)\Bigr) = \operatorname{diag}\Bigl(h(x), \ldots, h^{(p^{l-1})}(x), \ldots, h(x), \ldots, h^{(p^{l-1})}(x)\Bigr).$$

Теперь в равенстве

$$F_1(x)\cdot G_1(x) = \operatorname{diag}\Bigl(h(x), \ldots, h^{(p^{l-1})}(x), \ldots, h(x), \ldots, h^{(p^{l-1})}(x)\Bigr)$$

вычислим определители обеих частей:

$$\det F_1(x)\cdot\det G_1(x) = h(x)^m\cdot\ldots\cdot h^{(p^{l-1})}(x)^m.$$

Из единственности канонического разложения следует, что

$$\det G_1(x) = h(x)^{m_0}\cdot\ldots\cdot h^{(p^{l-1})}(x)^{m_{l-1}}.$$

Поскольку $\det G_1(x) = \det G(x) \in \mathbb{F}_p[x]$, а $h(x), \ldots, h^{(p^{l-1})}(x) \in \mathbb{F}_{p^l}[x]$ – все многочлены, сопряженные с $h(x)$ над $\mathbb{F}_p$, то на самом деле $m_0 = \ldots = m_{l-1}$:

$$\det G_1(x) = \Bigl(h(x)\cdot\ldots\cdot h^{(p^{l-1})}(x)\Bigr)^{m_0}, \quad \deg\bigl(\det G_1(x)\bigr) = nlm_0.$$

Если $G(X)$ – унитарный многочлен степени $k$, то $G_1(X) = C^{-1}G(X)C$ – унитарный многочлен той же степени $k$, и следовательно, $\det G_1(x)$ – унитарный многочлен степени $kt$. В таком случае справедливы равенства

$$\deg\bigl(\det G_1(x)\bigr) = kt = klm = nlm_0,$$

из которых ввиду взаимной простоты $(m,n) = 1$ следует, что $n \mid k$. Таким образом, $\deg G(X) = k = n = \deg H(X)$, и соответственно, $G(X) = H(X)$.

Если $h(x) \notin \mathbb{F}_{p^l}[x]$ при всех $l < t$, то многочлен $h(x) \cdot \ldots \cdot h^{(p^{t-1})}(x)$ является неприводимым над $\mathbb{F}_p$ многочленом (степени $nt$), что противоречит системе условий

$$\det F_1(x) \cdot \det G_1(x) = h(x) \cdot \ldots \cdot h^{(p^{t-1})}(x), \quad \det F_1(x) \neq 1, \quad \det G_1(x) \neq 1. \quad \blacktriangle$$

Напомним, что произвольная $p$-линейная функция $f(x_0, \ldots, x_n) \in L_q^p$ задается соответствующим $p$-линеаризованным многочленом

$$\left(\beta_{01}x_0 + \ldots + \beta_{0t}x_0^{p^{t-1}}\right) + \ldots + \left(\beta_{n1}x_n + \ldots + \beta_{n,t}x_n^{p^{t-1}}\right),$$

которому при изоморфизме $(L_q^p[x_0, x_1, \ldots], \lhd, +) \cong ((\mathbb{F}_p)_{t\times t}[X], +, \cdot)$ сопоставляется многочлен $B_0 + \ldots + B_nX^n$. При этом, очевидно, линейным по крайней правой переменной функциям из $L_q^p$ соответствуют унитарные многочлены из $(\mathbb{F}_p)_{t\times t}[X]$.

Следствие 1. *Пусть $h \in L_q$ – функция, неприводимая в классе $L_q$. Тогда $h$ не допускает собственного (и следовательно, существенного) разложения в сдвиг-композицию $p$-линейных функций, одна из которых линейна по крайней правой переменной.*

*Если к тому же $h \notin L_{p^l}$ при всех $l < t$, то $h(x)$ вообще не допускает собственного разложения в сдвиг-композицию $p$-линейных функций.*

В заключение параграфа приведем несколько примеров, наглядно демонстрирующих качественное расширение понятия $p$-линейной приводимости по сравнению с классической линейной приводимостью. Для простоты изложения в примерах предварительно будет рассмотрено матричное представление.

Пример 1. Рассмотрим неприводимый над полем $\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}$ многочлен $h(x) = 1 + x + x^3$. Согласно доказанной теореме 1 многочлен $H(X) = E + X + X^3$ не имеет унитарных делителей в кольце $(\mathbb{F}_2)_{2\times 2}[X]$. Однако $H(X)$ допускает собственное разложение в кольце $(\mathbb{F}_2)_{2\times 2}[X]$:

$$\begin{aligned}
&H(X) = E + X + X^3 = \begin{pmatrix}1&0\\0&1\end{pmatrix} + \begin{pmatrix}1&0\\0&1\end{pmatrix}X + \begin{pmatrix}1&0\\0&1\end{pmatrix}X^3 = \\
&= \begin{pmatrix}1+x+x^3 & 0\\ 0 & 1+x+x^3\end{pmatrix} = \begin{pmatrix}1 & x\\ x^2 & 1+x\end{pmatrix} \cdot \begin{pmatrix}1+x & x\\ x^2 & 1\end{pmatrix} = \\
&= \left(\begin{pmatrix}1&0\\0&1\end{pmatrix} + \begin{pmatrix}0&1\\0&1\end{pmatrix}X + \begin{pmatrix}0&0\\1&0\end{pmatrix}X^2\right) \cdot \left(\begin{pmatrix}1&0\\0&1\end{pmatrix} + \begin{pmatrix}1&1\\0&0\end{pmatrix}X + \begin{pmatrix}0&0\\1&0\end{pmatrix}X^2\right).
\end{aligned}$$

Таким образом, линейная функция $x_0 + x_1 + x_3$, неприводимая в классе $L_4$, допускает над $\mathbb{F}_4$ существенное и собственное 2-линейное разложение

$$\begin{aligned}
&x_0 + x_1 + x_3 = \left(x_0 + (\alpha+1)x_1 + (\alpha+1)x_1^2 + x_2 + (\alpha+1)x_2^2\right) \lhd \\
&\lhd \left(x_0 + \alpha x_1 + (\alpha+1)x_1^2 + x_2 + (\alpha+1)x_2^2\right).
\end{aligned}$$

Пример 2. Многочлен $h(x) = 1 + x^2 + x^4$ над полем $\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}$ раскладывается на линейные множители:

$$h(x) = (\alpha + x)^2 \cdot ((\alpha+1) + x)^2.$$

При этом для многочлена $H(X) = E + X^2 + X^4$ в кольце $(\mathbb{F}_2)_{2\times 2}[X]$ можно указать разложение

$$H(X) = \left(E + \begin{pmatrix}1&1\\0&1\end{pmatrix}X + X^2\right) \cdot \left(E + \begin{pmatrix}1&1\\0&1\end{pmatrix}X + X^2\right),$$

в котором каждый сомножитель не имеет корней в $(\mathbb{F}_2)_{2\times 2}$, и следовательно, не имеет унитарных делителей в $(\mathbb{F}_2)_{2\times 2}[X]$.

Таким образом, для линейной функции $x_0 + x_2 + x_4$ над полем $\mathbb{F}_4$ в дополнение к каноническому линейному разложению

$$x_0 + x_2 + x_4 = (\alpha x_0 + x_1) \lhd (\alpha x_0 + x_1) \lhd \big((\alpha+1)x_0 + x_1\big) \lhd \big((\alpha+1)x_0 + x_1\big)$$

можно указать нетривиальное 2-линейное разложение

$$x_0 + x_2 + x_4 = (x_0 + x_1^2 + x_2) \lhd (x_0 + x_1^2 + x_2),$$

в котором каждая из компонент не имеет 2-линейных делителей, линейных по крайней правой переменной.

Пример 3. Многочлен $h(x) = 1 + x + x^3 + x^4$ над полем $\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}$ раскладывается на линейные множители:

$$h(x) = (1+x)^2 \cdot (\alpha + x) \cdot ((\alpha+1) + x).$$

При этом для многочлена $H(X) = E + X + X^3 + X^4$ в кольце $(\mathbb{F}_2)_{2\times 2}[X]$ можно указать дополнительные разложения:

$$H(X) = \left(E + \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}X + X^2\right) \cdot \left(E + \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}X + X^2\right) =$$
$$= \begin{pmatrix}1+x+x^2 & 0\\ 0 & 1+x^2\end{pmatrix} \cdot \begin{pmatrix}1+x^2 & 0\\ 0 & 1+x+x^2\end{pmatrix},$$
$$H(X) = \left(E + \begin{pmatrix}1 & 0\\ 1 & 0\end{pmatrix}X + X^2\right) \cdot \left(E + \begin{pmatrix}0 & 0\\ 1 & 1\end{pmatrix}X + X^2\right) =$$
$$= \begin{pmatrix}1+x+x^2 & 0\\ x & 1+x^2\end{pmatrix} \cdot \begin{pmatrix}1+x^2 & 0\\ x & 1+x+x^2\end{pmatrix},$$

в которых каждый из сомножителей не имеет корней в $(\mathbb{F}_2)_{2\times 2}$, и следовательно, не имеет унитарных делителей в $(\mathbb{F}_2)_{2\times 2}[X]$.

Таким образом, над полем $\mathbb{F}_4$ линейная функция $x_0 + x_1 + x_3 + x_4$ в дополнение к каноническому линейному разложению

$$x_0 + x_1 + x_3 + x_4 = (x_0 + x_1) \lhd (x_0 + x_1) \lhd (\alpha x_0 + x_1) \lhd \big((\alpha+1)x_0 + x_1\big)$$

обладает нетривиальными 2-линейными разложениями

$$x_0 + x_1 + x_3 + x_4 = \big(x_0 + (\alpha+1)x_1 + \alpha x_1^2 + x_2\big) \lhd \big(x_0 + \alpha x_1 + \alpha x_1^2 + x_2\big),$$
$$x_0 + x_1 + x_3 + x_4 = \big(x_0 + \alpha x_1 + x_1^2 + x_2\big) \lhd \big(x_0 + (\alpha+1)x_1 + x_1^2 + x_2\big),$$

в которых каждая из компонент не имеет 2-линейных делителей, линейных по крайней правой переменной.

## § 4. Приводимость $p$-линейных функций

В работе [3] доказывается несколько практически значимых результатов о степени нелинейности сдвиг-композиции функций. Наиболее интересными, на наш взгляд, являются следующие утверждения.

Теорема 2 [3, теорема 10]. *Если $p$ – простое число, то для композиции $f \lhd g$ произвольных функций $f \in F_p$ и $g \in {}^+F_p$ справедливы следующие утверждения*:

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

Здесь стоит отметить, что ядром доказательства теоремы 2 является следующая лемма, которая и сама по себе представляет интерес.

Л е м м а 1 [3, лемма 12]. *При простом $p$ для любого $f \in F_p$, $\deg f \geqslant 2$, и любого $g \in {}^+F_p$ выполняется неравенство*

$$\deg(f \lhd g) \geqslant \deg g + 1.$$

В работе [3] приведены примеры, показывающие невозможность продолжения результатов теоремы 2 и леммы 1 на случай непростого поля $\mathbb{F}_q$ при использовании классического подхода к определению степени нелинейности. В данном параграфе исследуется возможность распространения результатов теоремы 2 и леммы 1 на случай непростого поля $\mathbb{F}_q$ при использовании индекса $p$-нелинейности, определенного выше (см. (1) и (2)).

Как показывает следующий пример, результат леммы 1 не допускает обобщения на случай непростого поля $\mathbb{F}_q$ даже при использовании параметра $\operatorname{ind}_p$ вместо deg.

П р и м е р 4. Пусть $q = p^3$. Зафиксируем произвольный базис $\alpha_1, \alpha_2, \alpha_3$ поля $\mathbb{F}_q$ над $\mathbb{F}_p$. Рассмотрим функцию $f \in {}^+F_q^+$, определяемую в базисе $\alpha_1, \alpha_2, \alpha_3$ набором координатных функций

$$\begin{aligned} f_1 &= x_{01} + x_{12}x_{k+1,2} + x_{13}x_{k+1,3} + x_{k+2,1},\\ f_2 &= x_{02} + x_{k+1,2},\\ f_3 &= x_{03} + x_{k+1,3}, \end{aligned}$$

и функцию $g \in {}^+F_q^+$, которая в том же базисе $\alpha_1, \alpha_2, \alpha_3$ определяется набором координатных функций

$$\begin{aligned} g_1 &= x_{01} + x_{21} \cdot \ldots \cdot x_{2k+1,1} + x_{2k+3,1},\\ g_2 &= x_{02} + x_{11} \cdot \ldots \cdot x_{k1} + x_{2k+3,2},\\ g_3 &= x_{02} + x_{k+3,1} \cdot \ldots \cdot x_{2k+2,1} + x_{2k+3,3}. \end{aligned}$$

Согласно формулам (2) справедливы равенства

$$\begin{aligned} \operatorname{ind}_p f &= \max\{\deg f_1, \deg f_2, \deg f_3\} = 2,\\ \operatorname{ind}_p g &= \max\{\deg g_1, \deg g_2, \deg g_3\} = 2k. \end{aligned}$$

При этом нетрудно проверить, что степени координатных функций сдвиг-композиции $f \lhd g$ удовлетворяют соотношениям

$$\deg(f \lhd g)_1 = k + 1, \quad \deg(f \lhd g)_2 = k, \quad \deg(f \lhd g)_3 = k,$$

и следовательно, $\operatorname{ind}_p(f \lhd g) = k + 1$.

Рассмотренный пример наглядно демонстрирует, что величины

$$\operatorname{ind}_p f = \max\{\deg f_1, \ldots, \deg f_t\}, \quad \operatorname{ind}_p g = \max\{\deg g_1, \ldots, \deg g_t\}$$

невозможно использовать для точной оценки параметра $\operatorname{ind}_p(f \lhd g)$, поскольку значение $\operatorname{ind}_p(f \lhd g)$ зависит не от максимума степеней координатных функций $f$ и $g$, а от сочетаний мономов этих координатных функций.

Кроме того, нетрудно видеть, что пример 4 опровергает возможность непосредственного продолжения результатов леммы 1 и утверждения 2 теоремы 2 (при $k = 1$) на случай непростого поля $\mathbb{F}_q$ при использовании параметра $\operatorname{ind}_p$. С учетом отмеченного еще более неожиданным представляется тот факт, что утверждение 1 теоремы 2 допускает независимое обобщение на случай непростого поля $\mathbb{F}_q$.

Теорема 3. *Пусть $q = p^t$, где $p$ – простое. Тогда для сдвиг-композиции $f \lhd g$ функций $f \in {}^*F_q$ и $g \in {}^+F_q^*$ равенство* $\operatorname{ind}_p(f \lhd g) = 1$ *выполняется в том и только том случае, когда* $\operatorname{ind}_p f = \operatorname{ind}_p g = 1$.

Доказательство. Содержательную часть доказательства утверждения представим в виде двух отдельных результатов, которые сами по себе представляют практический интерес.

Для удобства будем считать, что функции $f(x_0, \ldots, x_n)$ и $g(x_0, \ldots, x_m)$ имеют длины $n$ и $m$ соответственно.

Лемма 2. *Пусть $q = p^t$. Для произвольных $f \in L_q^p$ и $g \in F_q$ справедливы следующие утверждения*:

1. $\operatorname{ind}_p(f \lhd g) \leqslant \operatorname{ind}_p g$;
2. $\operatorname{ind}_p(g \lhd f) \leqslant \operatorname{ind}_p g$;
3. *Если к тому же $f \in {}^*L_q^p$, то* $\operatorname{ind}_p(g \lhd f) = \operatorname{ind}_p g = \operatorname{ind}_p(f \lhd g)$.

Доказательство. Доказательство утверждений 1 и 2 представляется очевидным при использовании представления функций $f, g$ наборами координатных функций.

Докажем утверждение 3. Пусть

$$f(x_0, \ldots, x_n) = f_{00}x_0 + \ldots + f_{0,t-1}x_0^{p^{t-1}} + \ldots + f_{n0}x_n + \ldots + f_{n,t-1}x_n^{p^{t-1}},$$
$$g(x_0, \ldots, x_m) = \sum_{i_0, \ldots, i_m \in \overline{0,q-1}} c_{i_0 \ldots i_m} x_0^{i_0} \ldots x_m^{i_m}.$$

Условие $f \in {}^*L_q^p$ означает, что $\pi(x_0) = f_{00}x_0 + \ldots + f_{0,t-1}x_0^{p^{t-1}}$ – перестановочный $p$-линеаризованный многочлен. При этом очевидны разложения

$$f = f' \lhd \pi, \quad f = \pi \lhd f'', \quad f', f'' \in {}^+L_q^p.$$

Пусть $x_0^{j_0} \ldots x_m^{j_m}$ – наименьший относительно стандартного лексикографического порядка моном функции $g$ со свойством

$$\operatorname{ind}_p g = \operatorname{ind}_p x_0^{j_0} \ldots x_m^{j_m} = \|j_0\|_p + \ldots + \|j_m\|_p, \quad c_{j_0 \ldots j_m} \neq 0.$$

Нетрудно понять, что приведенные многочлены функций $g \lhd f'$ и $f'' \lhd g$ также содержат одночлен $c_{j_0 \ldots j_m} x_0^{j_0} \ldots x_m^{j_m}$. Тогда с учетом утверждений 1 и 2 можно выписать следующие цепочки неравенств:

$$\operatorname{ind}_p g \leqslant \operatorname{ind}_p(g \lhd f') = \operatorname{ind}_p(g \lhd f \lhd \pi^{-1}) \leqslant \operatorname{ind}_p(g \lhd f) \leqslant \operatorname{ind}_p g,$$
$$\operatorname{ind}_p g \leqslant \operatorname{ind}_p(f'' \lhd g) = \operatorname{ind}_p(\pi^{-1} \lhd f \lhd g) \leqslant \operatorname{ind}_p(f \lhd g) \leqslant \operatorname{ind}_p g. \quad \blacktriangle$$

Легко видеть, что достаточность условия, сформулированного в теореме 3, следует из утверждения 3 доказанной леммы 2.

Для доказательства необходимости нам потребуется еще один вспомогательный результат.

Лемма 3. *Пусть $q = p^t$, где $p$ – простое, а сдвиг-композиция функций $f \in F_q$ и $g \in {}^+F_q^*$ удовлетворяет условию* $\operatorname{ind}_p(f \lhd g) = 1$. *Тогда* $\operatorname{ind}_p f = 1$.

Доказательство. Если $\operatorname{ind}_p g = 1$, то по лемме 2 имеем $\operatorname{ind}_p f = \operatorname{ind}_p(f \lhd g) = 1$ – все доказано. Поэтому далее будем полагать, что $\operatorname{ind}_p g > 1$ и справедливо представление

$$g = x_0 + l_g(x_1, \ldots, x_{s-1}) + \varphi(x_s, \ldots, x_m),$$

в котором $\operatorname{ind}_p l_g = 1$, а функция $\varphi$ существенным и $p$-нелинейным образом зависит от переменной $x_s$, $s \leqslant m$.

Доказательство проведем методом от противного. Предположим, что $\operatorname{ind}_p f > 1$. Представим функцию $f$ в виде

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

где $\operatorname{ind}_p l_f = 1$, а функция

$$\psi(x_r, \ldots, x_n) = \sum_{i=0}^{q-1} x_r^i \psi_i(x_{r+1}, \ldots, x_n)$$

существенным и $p$-нелинейным образом зависит от переменной $x_r$, $r \leqslant n$.

Во введенных обозначениях рассмотрим соотношение $f \lhd g$ подробнее:

$$f \lhd g = (l_f \lhd g)(x_0, \ldots, x_{r+m-1}) + \\ + \sum_{i=0}^{q-1} \big(x_r + \tau(x_{r+1}, \ldots, x_{r+m})\big)^i (\psi_i \lhd g)(x_{r+1}, \ldots, x_{n+m}),$$

где

$$\tau(x_{r+1}, \ldots, x_{r+m}) = l_g(x_{r+1}, \ldots, x_{r+s-1}) + \varphi(x_{r+s}, \ldots, x_{r+m}).$$

Теперь заметим, что равенство $\operatorname{ind}_p(f \lhd g) = 1$ возможно только лишь в случае, когда функция $l_f \lhd g$ зависит $p$-линейным образом от переменных $x_0, \ldots, x_{r-1}$:

$$(l_f \lhd g)(x_0, \ldots, x_{r+m-1}) = \\ = l(x_0, \ldots, x_{r-1}) + \sum_{i=0}^{q-1} x_r^i \varphi_i(x_{r+1}, \ldots, x_{r+m-1}), \quad \operatorname{ind}_p l = 1.$$

Если $r = n$, то очевидно, что $\psi_i \in \mathbb{F}_q$ при всех $i \in \{0, \ldots, q-1\}$. Рассмотрим случай, когда $r < n$, и предположим, что существует такой $i \in \{1, \ldots, q-1\}$, для которого $\psi_i \notin \mathbb{F}_q$. Тогда выберем наибольшее $k$ со свойством $\psi_k \notin \mathbb{F}_q$ и продолжим расписывать соотношение $f \lhd g$ подробнее:

$$f \lhd g = l(x_0, \ldots, x_{r-1}) + \sum_{i=0}^{q-1} x_r^i \varphi_i(x_{r+1}, \ldots, x_{r+m-1}) + \\ + \sum_{i=0}^{k-1} \big(x_r + \tau(x_{r+1}, \ldots, x_{r+m})\big)^i (\psi_i \lhd g)(x_{r+1}, \ldots, x_{n+m}) + \\ + \big(x_r + \tau(x_{r+1}, \ldots, x_{r+m})\big)^k (\psi_k \lhd g)(x_{r+1}, \ldots, x_{n+m}) + \\ + \sum_{i=k+1}^{q-1} \big(x_r + \tau(x_{r+1}, \ldots, x_{r+m})\big)^i \psi_i = \\ = l(x_0, \ldots, x_{r-1}) + \sum_{i=0}^{q-1} x_r^i \varphi_i(x_{r+1}, \ldots, x_{r+m-1}) + \\ + \sum_{i=0}^{k-1} \big(x_r + \tau(x_{r+1}, \ldots, x_{r+m})\big)^i (\psi_i \lhd g)(x_{r+1}, \ldots, x_{n+m}) +$$

$$+\sum_{i=0}^{k-1} x_r^i \binom{k}{i} \tau(x_{r+1},\dots,x_{r+m})^{k-i}(\psi_k \lhd g)(x_{r+1},\dots,x_{n+m}) +$$
$$+ x_r^k(\psi_k \lhd g)(x_{r+1},\dots,x_{n+m}) + \sum_{i=0}^{q-1} x_r^i v_i(x_{r+1},\dots,x_{r+m}).$$

Из полученного представления $f \lhd g$ легко видеть, что равенство $\mathrm{ind}_p(f \lhd g) = 1$ с необходимостью влечет за собой включение

$$\varphi_k(x_{r+1},\dots,x_{r+m-1}) + (\psi_k \lhd g)(x_{r+1},\dots,x_{n+m}) + v_k(x_{r+1},\dots,x_{r+m}) \in \mathbb{F}_q,$$

которое невозможно ввиду того, что

$$\mathrm{len}\big(\varphi_k(x_{r+1},\dots,x_{r+m-1}) + v_k(x_{r+1},\dots,x_{r+m})\big) \leqslant m-1 <$$
$$< m = \mathrm{len}\, g \leqslant \mathrm{len}\,\psi_k + \mathrm{len}\, g = \mathrm{len}(\psi_k \lhd g)(x_{r+1},\dots,x_{n+m}).$$

Таким образом, показали, что независимо от $r \leqslant n$ для всех $i \in \{1,\dots,q-1\}$ выполняется включение $\psi_i \in \mathbb{F}_q$, а сдвиг-композиция $f \lhd g$ на самом деле имеет вид

$$f \lhd g = l(x_0,\dots,x_{r-1}) + \sum_{i=0}^{q-1} x_r^i \varphi_i(x_{r+1},\dots,x_{r+m-1}) +$$
$$+ (\psi_0 \lhd g)(x_{r+1},\dots,x_{n+m}) + \sum_{i=1}^{q-1} \psi_i \cdot \big(x_r + \tau(x_{r+1},\dots,x_{r+m})\big)^i. \qquad (4)$$

Поскольку функция $f$ существенным и $p$-нелинейным образом зависит от переменной $x_r$, то существует такое $i \in \{1,\dots,q-1\}$, что $\psi_i \neq 0$ и $\|i\|_p \neq 1$. Выберем наибольшее $k$, у которого $\psi_k \neq 0$ и $\|k\|_p$ – максимально возможный. Пусть $k = k_l p^l + \dots + k_{t-1}p^{t-1},\ k_l \geqslant 1$. Обозначим

$$k^{(l)} = 0 + \dots + 0 + k_l p^l + \dots + k_{t-1}p^{t-1} = k,$$
$$k^{(l-1)} = 0 + \dots + p^{l-1} + (k_l - 1)p^l + \dots + k_{t-1}p^{t-1},$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$
$$k^{(0)} = p^0 + \dots + 0 + (k_l - 1)p^l + \dots + k_{t-1}p^{t-1},$$
$$k^* = 0 + \dots + 0 + (k_l - 1)p^l + \dots + k_{t-1}p^{t-1} \neq 0$$

и выделим в сумме $\sum\limits_{i=1}^{q-1} \psi_i \cdot \big(x_r + \tau(x_{r+1},\dots,x_{r+m})\big)^i$ коэффициент при $x_r^{k^*}$:

$$\sum_{i=1}^{q-1} \psi_i \cdot \big(x_r + \tau(x_{r+1},\dots,x_{r+m})\big)^i = \sum_{i=1}^{q-1} \psi_i \cdot (x_r + \tau)^{i_0 + p i_1 + \dots + p^{t-1} i_{t-1}} =$$
$$= \sum_{i=1}^{q-1} \psi_i \cdot (x_r + \tau)^{i_0} \cdot (x_r^p + \tau^p)^{i_1} \cdot \dots \cdot \left(x_r^{p^{t-1}} + \tau^{p^{t-1}}\right)^{i_{t-1}} =$$
$$= \psi_{k^{(l)}} \cdot \left(x_r^{p^l} + \tau^{p^l}\right)^{k_l} \cdot \dots \cdot \left(x_r^{p^{t-1}} + \tau^{p^{t-1}}\right)^{k_{t-1}} +$$
$$+ \psi_{k^{(l-1)}} \cdot \left(x_r^{p^{l-1}} + \tau^{p^{l-1}}\right) \cdot \left(x_r^{p^l} + \tau^{p^l}\right)^{k_l - 1} \cdot \dots \cdot \left(x_r^{p^{t-1}} + \tau^{p^{t-1}}\right)^{k_{t-1}} +$$
$$+ \dots + \psi_{k^{(0)}} \cdot (x_r + \tau) \cdot \left(x_r^{p^l} + \tau^{p^l}\right)^{k_l - 1} \cdot \dots \cdot \left(x_r^{p^{t-1}} + \tau^{p^{t-1}}\right)^{k_{t-1}} +$$

$$+\psi_{k^*}\cdot\left(x_r^{p^l}+\tau^{p^l}\right)^{k_l-1}\cdot\ldots\cdot\left(x_r^{p^{t-1}}+\tau^{p^{t-1}}\right)^{k_{t-1}}+t(x_r,\ldots,x_{r+m})=$$
$$=\psi_{k^{(l)}}\cdot\left(x_r^{k^{(l)}}+k_l x_r^{k^*}\tau^{p^l}+\ldots\right)+\psi_{k^{(l-1)}}\cdot\left(x_r^{k^{(l-1)}}+x_r^{k^*}\tau^{p^{l-1}}+\ldots\right)+$$
$$+\ldots+\psi_{k^{(0)}}\cdot\left(x_r^{k^{(0)}}+x_r^{k^*}\tau^{p^0}+\ldots\right)+\psi_{k^*}\cdot\left(x_r^{k^*}+\ldots\right)+t(x_r,\ldots,x_{r+m})=$$
$$=\psi_{k^{(l)}}x_r^{k^{(l)}}+\psi_{k^{(l-1)}}x_r^{k^{(l-1)}}+\ldots+\psi_{k^{(0)}}x_r^{k^{(0)}}+$$
$$+\left(k_l\psi_{k^{(l)}}\cdot\tau^{p^l}+\psi_{k^{(l-1)}}\cdot\tau^{p^{l-1}}+\ldots+\psi_{k^{(0)}}\cdot\tau^{p^0}+\psi_{k^*}\right)x_r^{k^*}+v(x_r,\ldots,x_{r+m})=$$
$$=\left(k_l\psi_{k^{(l)}}\cdot\tau^{p^l}+\psi_{k^{(l-1)}}\cdot\tau^{p^{l-1}}+\ldots+\psi_{k^{(0)}}\cdot\tau^{p^0}+\psi_{k^*}\right)x_r^{k^*}+w(x_r,\ldots,x_{r+m})$$

(здесь многочлены $t(x_r,\ldots,x_{r+m})$, $v(x_r,\ldots,x_{r+m})$ и $w(x_r,\ldots,x_{r+m})$ не содержат мономов с переменной $x_r$ в степени $k^*$).

Теперь легко видеть, что условие $\mathrm{ind}_p(f\lhd g)=1$ накладывает на компоненты представления (4) следующее ограничение:

$$\varphi_{k^*}(x_{r+1},\ldots,x_m)+\left(k_l\psi_{k^{(l)}}x_0^{p^l}+\ldots+\psi_{k^{(0)}}x_0^{p^0}+\psi_{k^*}\right)\lhd\tau(x_{r+1},\ldots,x_{r+m})\in\mathbb{F}_q.$$

Однако данное включение невозможно ввиду того, что $k_l\psi_{k^{(l)}}\neq 0$ и $\tau\in F_q^*$, а следовательно, композиция

$$\left(k_l\psi_{k^{(l)}}x_0^{p^l}+\ldots+\psi_{k^{(0)}}x_0^{p^0}+\psi_{k^*}\right)\lhd\tau(x_{r+1},\ldots,x_{r+m})$$

существенным образом зависит от $x_{r+m}$.

Таким образом, $\psi_i\in\mathbb{F}_q$ для всех $i\in\{1,\ldots,q-1\}$ и неравенство $\psi_i\neq 0$ возможно только при $\|i\|_p=1$ – пришли к противоречию с тем, что функция $\psi$ существенным и $p$-нелинейным образом зависит от переменной $x_r$. ▲

Теперь можно доказать необходимость условия, сформулированного в теореме 3.

Так как $p$ – простое, то согласно доказанной лемме 3 из условия $\mathrm{ind}_p(f\lhd g)=1$ следует, что $\mathrm{ind}_p f=1$. А поскольку $f\in {}^*F_q$, то согласно утверждению 3 леммы 2 имеем равенство $\mathrm{ind}_p g=\mathrm{ind}_p(f\lhd g)=1$. ▲

Следствие 2. *При простом $p$ регистр сдвига $R(\varphi,\psi)$ с $p$-линейной функцией обратной связи $\varphi\in {}^*(L_q^p)^+$ может допускать гомоморфизм на регистр сдвига $R(\varphi',\psi')$, $\varphi'\in {}^*F_q^+$, только если $\varphi'$ – $p$-линейная; при этом данный гомоморфизм с необходимостью является $p$-линейным отображением.*

Доказательство очевидным образом следует из [2, теорема 1] и теоремы 3. ▲

Следствие 3. *Неавтономный линейный регистр сдвига с неприводимым характеристическим многочленом не допускает собственных гомоморфизмов на регулярные регистры сдвига, функции обратной связи которых линейны по входной переменной.*

Доказательство очевидным образом следует из [2, теорема 1], доказанной теоремы 3 и следствия 1. ▲

*Замечание* 3. Ранее отмечалось, что при простом $p$ для произвольной функции $f\in F_q$ ее индекс $p$-нелинейности $\mathrm{ind}_p f$ совпадает с аддитивным показателем нелинейности $\mathrm{dl}\, f$. Следовательно, теорема 3 – центральный результат данного параграфа – допускает формулировку в терминах показателя dl, не зависящего от числа $p$. Таким образом, можно сделать вывод, что аддитивный показатель нелинейности при исследовании сдвиг-композиции является более органичным продолжением классического понятия нелинейности отображения deg на случай непростого поля $\mathbb{F}_q$ по сравнению с индексом $p$-нелинейности.

В заключение параграфа приведем ряд примеров, которые демонстрируют существенность каждого из условий теоремы 3 и леммы 3.

Пример 5. Пусть $q = p^2$ и $\mathbb{F}_q = \mathbb{F}_p(\alpha)$. Рассмотрим проекцию $\pi\colon \mathbb{F}_q \to \mathbb{F}_p$, определенную в базисе $e, \alpha$ по правилу

$$\pi(x_1 + x_2\alpha) = x_2.$$

Выберем произвольный нелинейный многочлен $\sigma \in \mathbb{F}_p[x_1, \ldots, x_n]$. Нетрудно понять, что функция $\varphi = \sigma \lhd \pi \in F_q$ в базисе $e, \alpha$ имеет координатные функции

$$\varphi_1(x_{11}, x_{12}, \ldots, x_{n1}, x_{n2}) = \sigma(x_{12}, \ldots, x_{n2}), \quad \varphi_2(x_{11}, x_{12}, \ldots, x_{n1}, x_{n2}) = 0,$$

и следовательно, выполняется равенство $\operatorname{ind}_p \varphi = \deg \sigma > 1$.

Сдвиг-композиция

$$\pi \lhd \big(x_0 + \varphi(x_1, \ldots, x_n) + x_{n+1}\big) = \pi(x_0) + \pi(x_{n+1})$$

доказывает существенность условия $f \in {}^*F_q$ в теореме 3.

Пример 6. В обозначениях примера 5 сдвиг-композиция

$$\begin{aligned}
&\big(x_0 + \varphi(x_1, \ldots, x_n)\big) \lhd \big(x_0 - \varphi(x_1, \ldots, x_n)\big) = \\
&= x_0 - \sigma(x_{12}, \ldots, x_{n2}) + \sigma \lhd \pi\big(x_1 - \varphi(x_2, \ldots, x_{n+1})\big) = \\
&= x_0 - \sigma(x_{12}, \ldots, x_{n2}) + \sigma(x_{12}, \ldots, x_{n2}) = x_0
\end{aligned}$$

подтверждает существенность условия $g \in F_q^*$ в лемме 3 и теореме 3.

Кроме того, данный пример показывает, что при составном $q$ обратимые элементы множества ${}^+F_q$ могут иметь произвольные длину и степень нелинейности (см. следствие 2 в работе [3]).

Пример 7. Условие $g \in {}^+F_q$ в лемме 3 и теореме 3 нельзя заменить даже на близкое $g \in {}^*F_q$. Для любого $q > 2$ существует перестановочный полином $f(x_0) \in F_q$, $\operatorname{ind}_p f > 1$. Нетрудно понять, что обратный перестановочный полином $g(x_0)$ также удовлетворяет условию $\operatorname{ind}_p g > 1$. При этом справедливо равенство $f \lhd g = x_0$.

## СПИСОК ЛИТЕРАТУРЫ


1. *Солодовников В.И.* Регистры сдвига и криптоалгоритмы на их основе: теоретико-автоматные свойства и их приложения. Saarbrücken: Lambert Acad. Publ., 2017.
2. *Солодовников В.И.* Гомоморфизмы регистров сдвига в линейные автоматы // Дискрет. матем. 2008. Т. 20. № 4. С. 89–101.
3. *Чередник И.В.* Линейное разложение дискретных функций в терминах операции сдвиг-композиции // Матем. вопр. криптогр. 2020. Т. 11. № 1. С. 115–143.
4. *Чередник И.В.* Линейное разложение системы дискретных функций в терминах операции сдвиг-композиции // Матем. вопр. криптогр. (в печати).
5. *Гольтваница М.А.* Методы построения скрученных линейных рекуррентных последовательностей максимального периода, базирующиеся на факторизации многочленов Галуа в кольце матричных многочленов // Матем. вопр. криптогр. 2019. Т. 10. № 4. С. 25–51.
6. *Башев В.А.* Теоретико-групповая характеризация неавтономных линейных регистров сдвига // Тр. по дискр. матем. Т. 8. М.: Физматлит, 2004. С. 52–68.
7. *Солодовников В.И.* Гомоморфизмы двоичных регистров сдвига // Дискрет. матем. 2005. Т. 17. № 1. С. 73–88.
8. *Лидл Р., Нидеррайтер Г.* Конечные поля. Т. 1, 2. М.: Мир, 1988.
9. *Кузьмин А.С., Нечаев А.А., Шишкин В.А.* Бент- и гипербент-функции над конечным полем // Тр. по дискр. матем. Т. 10. М.: Физматлит, 2007. С. 97–122.

10. *Черемушкин А.В.* Аддитивный подход к определению степени нелинейности дискретной функции // Прикл. дискр. матем. 2010. № 2 (8). С. 22–33.
11. *Черемушкин А.В.* Аддитивный подход к определению степени нелинейности дискретной функции на циклической группе примарного порядка // Прикл. дискр. матем. 2013. № 2 (20). С. 26–38.
12. *Гольтваница М.А., Зайцев С.Н., Нечаев А.А.* Скрученные линейные рекурренты максимального периода над кольцами Галуа // Фундамент. и прикл. матем. 2012. Т. 17. № 3. С. 5–23.

*Чередник Игорь Владимирович*
МИРЭА – Российский технологический университет
(РТУ МИРЭА), Москва
p.n.v.k.s@mail.ru

Поступила в редакцию
04.06.2020
После доработки
07.11.2020
Принята к публикации
08.11.2020