ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Январь–март 2022. Т. 29, № 1. С. 56–73

УДК 519.712.3+512.622+510.52 DOI 10.33048/daio.2022.29.727

# О СЛОЖНОСТИ ПОИСКА ПЕРИОДОВ ФУНКЦИЙ, ЗАДАННЫХ МНОГОЧЛЕНАМИ НАД КОНЕЧНЫМ ПРОСТЫМ ПОЛЕМ

*С. Н. Селезнева*

Московский гос. университет им. М. В. Ломоносова,
Ленинские горы, 1, 119991 Москва, Россия
E-mail: selezn@cs.msu.ru

**Аннотация.** Рассматриваются многочлены над конечным простым полем $F_p = (E_p; +, \cdot)$, содержащим $p$ элементов, при этом с каждым таким многочленом $f(x_1, \ldots, x_n)$ связывается $p$-значная функция $f\colon E_p^n \to E_p$, которую этот многочлен определяет. Периодом $p$-значной функции $f(x_1, \ldots, x_n)$ называется набор $a = (a_1, \ldots, a_n)$ элементов из $E_p$ такой, что имеет место равенство $f(x_1 + a_1, \ldots, x_n + a_n) = f(x_1, \ldots, x_n)$. В работе предложен алгоритм, который для простого $p$ и произвольной $p$-значной функции $f(x_1, \ldots, x_n)$, заданной многочленом над полем $F_p$, находит базис линейного пространства всех периодов этой функции $f$, при этом сложность алгоритма равна $n^{O(d)}$, где $d$ — степень многочлена, задающего функцию $f$. Как следствие, показано, что в случае простого $p$ при каждом заданном числе $d$ задача поиска базиса линейного пространства всех периодов $p$-значной функции, заданной многочленом степени не выше $d$, может быть решена полиномиальным алгоритмом относительно числа переменных этой функции. Библиогр. 11.

**Ключевые слова:** $p$-значная функция (функция $p$-значной логики), конечное поле, простое поле, многочлен над полем, периодичность, алгоритм, сложность.

## Введение

В работе рассматриваются многочлены над конечным простым полем $F_p = (E_p; +, \cdot)$, содержащим $p$ элементов ($p$ — простое число), при этом с каждым таким многочленом $f$ связывается $p$-значная функция

Исследование выполнено при поддержке Российского фонда фундаментальных исследований (проект № 19–01–00200–а) и Минобрнауки РФ в рамках программы Московского центра фундаментальной и прикладной математики (проект № 075–15–2019–1621).

$f\colon E_p^n \to E_p$, которую этот многочлен определяет. *Периодом* $p$-значной функции $f(x_1,\dots,x_n)$ называется такой набор $a=(a_1,\dots,a_n)\in E_p^n$, что верно равенство $f(x_1+a_1,\dots,x_n+a_n)=f(x_1,\dots,x_n)$. *Периодической* называем $p$-значную функцию, для которой найдётся ненулевой период. Отметим, что наличие ненулевого периода у функции алгебры логики (т. е. при $p=2$) означает определённую слабость этой функции с криптографической точки зрения (см., например, [1, с. 107]). В ряде работ рассматривались свойства периодических функций алгебры логики (см., например, [2, 3]). В [4, 5] показано, что при простых $p$ проверить периодичность относительно заданного периода $p$-значной функции, заданной многочленом над полем $F_p$, можно с полиномиальной сложностью.

Известно, что для любой $p$-значной функции множество всех её периодов образует линейное пространство над полем $F_p$. В [6] (см. также [7]) при простых $p$ предложен вероятностный алгоритм для поиска базиса линейного пространства всех периодов $p$-значной функции, заданной многочленом над полем $F_p$. Сложность этого вероятностного алгоритма из [6, 7] равна $n^{O(d)}$, где $n$ — число переменных функции, а $d$ — степень многочлена. В [8] найден детерминированный алгоритм, который находит базис пространства всех периодов функции алгебры логики, заданной многочленом над полем $F_2$; сложность этого алгоритма равна $n^{O(d)}$, где $n$ — число переменных функции, а $d$ — степень многочлена. В настоящей работе результат из [8] обобщается на случай произвольного простого числа $p$. А именно, доказано, что при простых $p$ поиск периодов $p$-значной функции, заданной многочленом над полем $F_p$, можно свести к решению некоторой однородной системы линейных алгебраических уравнений над полем $F_p$ и такое сведение можно выполнить детерминированным алгоритмом со сложностью $n^{O(d)}$, где $n$ — число переменных функции, а $d$ — степень многочлена. Как следствие, получено, что для $p$-значных функций, которые задаются многочленами ограниченной степени, базис пространства всех периодов можно найти с полиномиальной сложностью относительно числа их переменных.

## 1. Основные определения

Сначала напомним некоторые определения, которые, в основном, относятся к дискретным функциям и многочленам над конечными полями. Не определённые здесь алгебраические понятия можно найти, например, в [9].

Если $A$ — произвольное множество, $n\geqslant 1$ и $a\in A^n$, то $i$-й разряд набора $a$ обозначаем $a_i$, $i=1,\dots,n$, т. е. $a=(a_1,\dots,a_n)$, при этом если $a_j\in A^n$, то $a_j=(a_{j,1},\dots,a_{j,n})$. Если $\circ\colon A^m\to A$ — $m$-местная операция на множестве $A$ и $a_1,\dots,a_m\in A^n$, $n\geqslant 1$, то считаем, что $\circ(a_1,\dots,a_m)=b\in A^n$, где $b_i=\circ(a_{1,i},\dots,a_{m,i})$ для всех $i=1,\dots,n$.

**1.1. Натуральные числа и наборы.** Пусть $N = \{0, 1, 2, \dots\}$ — множество натуральных чисел с нулём. Если $s \in N^n$, где $n \geqslant 1$, то положим $i(s) = \{s_i \mid s_i \neq 0\}$ и $o(s) = \{s_i \mid s_i = 0\}$. *Весом* набора $s \in N^n$ называем величину $|s| = \sum\limits_{i=1}^{n} s_i$ (здесь $+$ обозначает сложение целых чисел). Введём обозначение: $e_i = (\underbrace{0, \dots, 0}_{i-1}, 1, \underbrace{0, \dots, 0}_{n-i}) \in N^n$, $i = 1, \dots, n$.

Если $p \in N$, $p \geqslant 2$, то положим $N_p = \{0, 1, \dots, p-1\} \subseteq N$. Если $s \in N_p^n$, то *номером* набора $s$ (по основанию $p$) назовём число $\nu_p(s) = \sum\limits_{i=1}^{n} s_i \cdot p^{n-i}$. *Лексикографическим порядком* $\leqslant_p$ на множестве $N_p^n$ назовём линейное упорядочение наборов из $N_p^n$ по возрастанию их номеров (по основанию $p$). Как обычно, если $s, t \in N_p^n$, $s \leqslant_p t$ и $s \neq t$, то пишем $s <_p t$. Кроме того, если $s \leqslant_p t$, $s <_p t$, то также пишем $t \geqslant_p s$, $t >_p s$.

Если $k \in N$, то $k!$ обозначает факториал числа $k$, т. е. $k! = k \cdot \ldots \cdot 1$ при $k \geqslant 1$ и $0! = 1$. Если $k, m \in N$, то $C_m^k$ — биномиальный коэффициент, т. е. $C_m^k = \frac{m!}{k!(m-k)!}$.

**1.2. Кольцо многочленов $p$-значных функций.** Пусть $p$ — простое число, $p \geqslant 2$, $E_p$ — множество из $p$ элементов, $F_p = (E_p; +, \cdot)$ — простое поле порядка $p$ с нулём 0 и единицей 1. Для простоты считаем, что $E_p = \{0, 1, \dots, p-1\}$. При этом вычитание в поле $F_p$ обозначаем знаком $-$ и обратный элемент к элементу $c \in E_p$ в поле $F_p$ обозначаем $c^{-1}$. Если $m \in N$, то иногда число $m$ будем рассматривать как элемент поля $F_p$, считая, что $m = \underbrace{1 + \ldots + 1}_{m} \in E_p$. Пусть, как обычно, $F_p[x_1, \dots, x_n]$ обозначает кольцо многочленов переменных $x_1, \dots, x_n$ над полем $F_p$.

Пусть $P_p^{(n)} = \{f \mid f \colon E_p^n \to E_p\}$ — множество всех функций $n$ переменных на множестве $E_p$, где $n \geqslant 1$, т. е. множество $n$-местных $p$-значных функций (см., например, [10, с. 43–44]). Если $f \in P_p^{(n)}$ и $f = f(x_1, \dots, x_n)$, то функцию $f$ называем функцией переменных $x_1, \dots, x_n$. Любой многочлен $f \in F_p[x_1, \dots, x_n]$ определяет некоторую функцию из $P_p^{(n)}$. Известно (см., например, [10, с. 69–71]), что любую функцию из $P_p^{(n)}$ можно представить однозначно многочленом из $F_p[x_1, \dots, x_n]$, в котором степень любой переменной не выше $p-1$. Пусть $PF_p[x_1, \dots, x_n]$ — множество всех многочленов из $F_p[x_1, \dots, x_n]$, в которых степень любой переменной не выше $p-1$. Несложно проверить, что множество $PF_p[x_1, \dots, x_n]$ с операциями сложения и умножения многочленов в кольце $F_p[x_1, \dots, x_n]$ и дальнейшим понижением степеней переменных по правилу $x^p = x$ является кольцом (коммутативным и ассоциативным кольцом с единицей). Это кольцо будем называть *кольцом многочленов $p$-значных функций* и будем также обозначать через $PF_p[x_1, \dots, x_n]$. Кольцо $PF_2[x_1, \dots, x_n]$

называем *кольцом многочленов Жегалкина*. Таким образом, между функциями из $P_p^{(n)}$ переменных $x_1, \ldots, x_n$ и многочленами из $PF_p[x_1, \ldots, x_n]$ можно установить взаимно однозначное соответствие, поэтому в дальнейшем будем отождествлять понятие $p$-значной функции из $P_p^{(n)}$ и её представление в виде многочлена из $PF_p[x_1, \ldots, x_n]$, если это не приводит к путанице. В частности, если $f \in PF_p[x_1, \ldots, x_n]$, будем писать также $f \in P_p^{(n)}$, и, наоборот, если $f(x_1, \ldots, x_n) \in P_p^{(n)}$, будем писать $f \in PF_p[x_1, \ldots, x_n]$. Кроме того, под равенством многочленов из кольца $PF_p[x_1, \ldots, x_n]$ будем понимать их равенство в кольце $PF_p[x_1, \ldots, x_n]$ (т. е. совпадение функций из $P_p^{(n)}$, которые они определяют).

Набор $a \in E_p^n$ называется *периодом* многочлена $f \in PF_p[x_1, \ldots, x_n]$ (и соответствующей функции $f \in P_p^{(n)}$), если в кольце $PF_p[x_1, \ldots, x_n]$

$$f(x_1 + a_1, \ldots, x_n + a_n) = f(x_1, \ldots, x_n).$$

Понятно, что нулевой набор $0 = (0, \ldots, 0) \in E_p^n$ является периодом любого многочлена из $PF_p[x_1, \ldots, x_n]$. Многочлен $f \in PF_p[x_1, \ldots, x_n]$ и соответствующая функция $f \in P_p^{(n)}$ называются *периодическими*, если найдётся ненулевой набор $a \in E_p^n$, являющийся их периодом. Периодический многочлен $f \in PF_p[x_1, \ldots, x_n]$ с периодом $a \in E_p^n$ называется также *инвариантным относительно смещения* (*сдвига*) $a$. Множество всех периодов многочлена $f \in PF_p[x_1, \ldots, x_n]$ обозначим через $T(f)$. Пусть $f \in PF_p[x_1, \ldots, x_n]$. Отметим, что $0 = (0, \ldots, 0) \in T(f)$. Несложно проверить, что если $a_1, a_2 \in T(f)$ и $c \in E_p$, то $a_1 + a_2 \in T(f)$ и $c \cdot a_1 \in T(f)$. Значит, множество $T(f)$ является линейным пространством над полем $F_p$. Следовательно, для любого многочлена $f \in F_p[x_1, \ldots, x_n]$ множество $T(f)$ можно определить как множество решений некоторой однородной системы линейных уравнений над полем $F_p$.

**1.3. Дополнительные определения и обозначения.** Введём соответствие между наборами $s \in N^n$ и одночленами из $F_p[x_1, \ldots, x_n]$: набор $s \in N^n$ и одночлен $x_1^{s_1} \cdot \ldots \cdot x_n^{s_n}$, где $x^m = \underbrace{x \cdot x \cdot \ldots \cdot x}_{m}$ при $m \geqslant 1$ и $x^0 = 1$, соответствуют друг другу. Для набора $s \in N^n$ соответствующий ему одночлен обозначим через $x^s$, т. е. $x^s = \prod\limits_{i \in i(s)} x_i$ при $s \neq (0, \ldots, 0)$ и $x^s = 1$ при $s = (0, \ldots, 0)$, при этом степень $d(x^s)$ одночлена $x^s$ равна весу набора $s$, т. е. $d(x^s) = |s|$.

Теперь любой многочлен $f \in PF_p[x_1, \ldots, x_n]$ можно записать как выражение вида $\sum\limits_{s \in N_p^n} a_s \cdot x^s$, где $a_s \in E_p$ — коэффициент при одночлене $x^s$ в многочлене $f$, $s \in N_p^n$. Если $f \in PF_p[x_1, \ldots, x_n]$, то коэффициент при одночлене $x^s$, $s \in N_p^n$, в многочлене $f$ обозначим через $c_f(s)$, $c_f(s) \in E_p$.

Тогда

$$f = \sum_{s \in N_p^n} c_f(s) \cdot x^s.$$

Если $f \in PF_p[x_1, \ldots, x_n]$, то пусть $S(f)$ — множество всех таких наборов $s \in N_p^n$, что в многочлене $f(x_1, \ldots, x_n)$ коэффициент при одночлене $x^s$ не равен нулю, т. е. $c_f(s) \neq 0$, значит,

$$f = \sum_{s \in S(f)} c_f(s) \cdot x^s.$$

Кроме того, будем говорить, что одночлен $x^s$, $s \in N_p^n$, *содержится в многочлене* $f \in PF_p[x_1, \ldots, x_n]$ (или *является слагаемым* этого многочлена), если $c_f(s) \neq 0$, т. е. $s \in S(f)$. Если $S(f) = \varnothing$, то $f = 0$ — нулевой многочлен, не содержащий ни одного слагаемого. Для многочлена $f \in PF_p[x_1, \ldots, x_n]$ его степенью $d(f)$ называется наибольшая из степеней среди его слагаемых, при этом $d(0) = -\infty$. Для многочлена $f \in PF_p[x_1, \ldots, x_n]$ его *длиной* $l(f)$ назовём число его слагаемых, т. е. $l(f) = |S(f)|$.

Многочлен $l \in F_p[x_1, \ldots, x_n]$ назовём *линейным* (или *линейной формой*), если $d(l) \leqslant 1$. Иными словами, линейная форма — многочлен вида

$$l = c_0 + c_1 x_1 + \ldots + c_n x_n,$$

где $c_0, c_1, \ldots, c_n \in E_2$. Множество всех линейных многочленов из $F_p[x_1, \ldots, x_n]$ обозначим через $LF_p[x_1, \ldots, x_n]$.

## 2. Производные многочленов $p$-значных функций

Напомним понятие производной для многочленов из кольца $F_p[x_1, \ldots, x_n]$. Если $f \in F_p[x_1, \ldots, x_n]$, причём

$$f = \sum_{m=0}^{d} x_i^m \cdot f_m,$$

где $f_m \in F_p[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$, $m = 0, 1, \ldots, d$, то *производной* $f'_{x_i}$ многочлена $f$ по переменной $x_i$ называется многочлен

$$f'_{x_i} = \sum_{m=1}^{d} m x_i^{m-1} \cdot f_m.$$

Назовём *производной* $f'_{x_i}$ многочлена $f \in PF_p[x_1, \ldots, x_n]$ по переменной $x_i$ производную по переменной $x_i$ многочлена $f$, рассматриваемого как элемент кольца $F_p[x_1, \ldots, x_n]$. Понятно, что если $f \in PF_p[x_1, \ldots, x_n]$, то $f'_{x_i} \in PF_p[x_1, \ldots, x_n]$. Отметим, что некоторые общие свойства производной сохраняются для многочленов из кольца $PF_p[x_1, \ldots, x_n]$, но некоторые из свойств нарушаются. В частности, если $f, g \in PF_p[x_1, \ldots, x_n]$

и $c \in E_p$, то

$$(f \pm g)'_{x_i} = f'_{x_i} \pm g'_{x_i}, \quad (c \cdot f)'_{x_i} = c \cdot f'_{x_i}.$$

Однако в общем случае неверно, что $(f \cdot g)'_{x_i} = f'_{x_i} \cdot g + f \cdot g'_{x_i}$. Действительно, если $f = x_1 + x_2 \in PF_2[x_1, x_2, x_3]$ и $g = x_1 + x_3 \in PF_2[x_1, x_2, x_3]$, то $f \cdot g = x_1x_2 + x_1x_3 + x_2x_3 + x_1 \in PF_2[x_1, x_2, x_3]$, поэтому $(f \cdot g)'_{x_1} = x_2 + x_3 + 1$, но

$$f'_{x_1} \cdot g + f \cdot g'_{x_1} = x_1 + x_3 + x_1 + x_2 = x_2 + x_3 \neq x_2 + x_3 + 1 = (f \cdot g)'_{x_1}.$$

Также в общем случае неверна формула производной сложной функции. Однако в частном случае, который мы будем рассматривать, она справедлива. Докажем её.

**Лемма 1.** *Пусть $p$ простое, $n, k \in N$, $n \geqslant k \geqslant 1$, $s_1, \ldots, s_k \in N_p$ и*

$$g = x_1^{s_1} \cdot \ldots \cdot x_k^{s_k} \in PF_p[x_1, \ldots, x_k],$$

$$f = g(x_1 + l_1, \ldots, x_k + l_k) = \prod_{i=1}^{k} (x_i + l_i)^{s_i} \in PF_p[x_1, \ldots, x_n],$$

*где $l_i \in LF_p[x_{k+1}, \ldots, x_n]$, $i = 1, \ldots, k$. Тогда для многочлена $f$ и любой переменной $x_i$, $i = 1, \ldots, k$, верно*

$$f'_{x_i} = g'_{x_i}(x_1 + l_1, \ldots, x_k + l_k).$$

Доказательство. Не ограничивая общности рассуждений, предположим, что $i = 1$. Сначала рассмотрим случай $k = 1$. Тогда

$$f = g(x_1 + l_1) = (x_1 + l_1)^{s_1} = \sum_{m=0}^{s_1} C_{s_1}^m x_1^m l_1^{s_1 - m},$$

поэтому, пользуясь тем, что многочлен $l_1$ не содержит переменной $x_1$, получаем

$$f'_{x_1} = (g(x_1 + l_1))'_{x_1} = ((x_1 + l_1)^{s_1})'_{x_1} = \sum_{m=1}^{s_1} C_{s_1}^m m x_1^{m-1} l_1^{s_1 - m}$$

$$= s_1 \sum_{m=0}^{s_1 - 1} C_{s_1 - 1}^m x_1^m l_1^{s_1 - 1 - m} = s_1 (x_1 + l_1)^{s_1 - 1} = g'_{x_1}(x_1 + l_1).$$

Далее, при $k \geqslant 2$ утверждение леммы верно, так как выражение $(x_2 + l_2)^{s_2} \cdot \ldots \cdot (x_k + l_k)^{s_k}$ не содержит переменной $x_1$. Лемма 1 доказана.

Из леммы 1 сразу получаем лемму 2.

**Лемма 2.** *Пусть $p$ простое, $n, k \in N$, $n \geqslant k \geqslant 1$, $g \in PF_p[x_1, \ldots, x_k]$ и*

$$f = g(x_1 + l_1, \ldots, x_k + l_k) \in PF_p[x_1, \ldots, x_n],$$

*где* $l_i \in LF_p[x_{k+1}, \ldots, x_n]$, $i = 1, \ldots, k$. *Тогда для многочлена* $f$ *и любой переменной* $x_i$, $i = 1, \ldots, k$, *верно*

$$f'_{x_i} = g'_{x_i}(x_1 + l_1, \ldots, x_k + l_k).$$

*В частности, если* $f \in PF_p[x_1, \ldots, x_k]$ *и* $a_1, \ldots, a_n \in E_p$, *то для любой переменной* $x_i$ *верно*

$$(f(x_1 + a_1, \ldots, x_n + a_n))'_{x_i} = f'_{x_i}(x_1 + a_1, \ldots, x_n + a_n).$$

В [6] рассматривались свойства таких периодических многочленов из кольца $F_p[x_1, \ldots, x_n]$, в которых степень любой переменной не превосходит $p - 1$. В силу того, что каждая $p$-значная функция однозначно задаётся многочленом такого вида, можно напрямую перенести эти свойства на многочлены из кольца $PF_p[x_1, \ldots, x_n]$. Для полноты изложения докажем их в лемме 3.

**Лемма 3** [6]. *Пусть* $f \in PF_p[x_1, \ldots, x_n]$ *и* $a \in E_p^n$. *Тогда если* $a \in T(f)$, *то* $a \in T(f'_{x_i})$ *для любого* $i = 1, \ldots, n$.

Доказательство. Действительно, если $a \in T(f)$, то

$$f(x_1 + a_1, \ldots, x_n + a_n) - f(x_1, \ldots, x_n) = 0,$$

поэтому

$$(f(x_1 + a_1, \ldots, x_n + a_n))'_{x_i} - (f(x_1, \ldots, x_n))'_{x_i} = 0,$$

т. е.

$$f'_{x_i}(x_1 + a_1, \ldots, x_n + a_n) - f'_{x_i}(x_1, \ldots, x_n) = 0.$$

Значит, $a \in T(f'_{x_i})$. Лемма 3 доказана.

Отметим также, что для рассматриваемой производной многочленов из $PF_p[x_1, \ldots, x_n]$ верно, что если $f \in PF_p[x_1, \ldots, x_n]$, то $(f'_{x_i})'_{x_j} = (f'_{x_j})'_{x_i}$ для любых переменных $x_i$, $x_j$. Тем самым можно говорить о производной многочлена $f$ по переменным $x_i, x_j$, не указывая их порядок. В общем случае введём обозначение: если $s \in N_p^n$ и $f \in PF_p[x_1, \ldots, x_n]$, то положим

$$f^{(|s|)}_{x^s} = (\ldots(\ldots(\ldots(f'_{\underbrace{x_1}_{s_1}})\ldots)'_{x_1}\ldots)'_{\underbrace{x_n}_{s_n}}\ldots)'_{x_n}.$$

Из леммы 3 получаем

**Следствие 1.** *Пусть* $f \in PF_p[x_1, \ldots, x_n]$ *и* $a \in E_p^n$. *Тогда если* $a \in T(f)$, *то* $a \in T\big(f^{(|s|)}_{x^s}\big)$ *для любого набора* $s \in N_p^n$.

### 3. Свойства периодических многочленов $p$-значных функций

В этом разделе установим некоторые свойства периодических многочленов из кольца $PF_p[x_1, \ldots, x_n]$.

**Лемма 4.** *Пусть $p$ — простое число, $n \geqslant 1$ и*

$$f = l + c_0 \in LF_p[x_1, \ldots, x_n],$$

*где $l \in LP_p[x_1, \ldots, x_n]$, $l(0, \ldots, 0) = 0$, $c_0 \in E_p$. Набор $a \in E_2^n$ является периодом многочлена $f$ тогда и только тогда, когда набор $a$ является решением уравнения*

$$l(x_1, \ldots, x_n) = 0,$$

*т. е. когда $l(a) = 0$.*

Доказательство. Пусть $l = c_1x_1 + \ldots + c_nx_n$, где $c_1, \ldots, c_n \in E_p$. Набор $a$ является периодом многочлена $f$ тогда и только тогда, когда

$$l(x_1 + a_1, \ldots, x_n + a_n) - l(x_1, \ldots, x_n) = c_1a_1 + \ldots + c_na_n = l(a) = 0.$$

Лемма 4 доказана.

**Лемма 5.** *Пусть $p$ — простое число, $n \geqslant 1$ и*

$$f = l^s \in PF_p[x_1, \ldots, x_n],$$

*где $l \in LF_p[x_1, \ldots, x_n]$, $l(0, \ldots, 0) = 0$, $s \in N_p$, $s \geqslant 1$. Набор $a \in E_2^n$ является периодом многочлена $f$ тогда и только тогда, когда $a$ является решением уравнения*

$$l(x_1, \ldots, x_n) = 0,$$

*т. е. когда $l(a) = 0$.*

Доказательство. Пусть $l = c_1x_1 + \ldots + c_nx_n$, где $c_1, \ldots, c_n \in E_p$.

1. В силу того, что $l(x_1+a_1, \ldots, x_n+a_n) = l(x_1, \ldots, x_n)+l(a)$, получаем, что если $l(a) = 0$, то $a \in T(f)$.

2. Пусть $a \in T(f)$. Если $l = 0$, то утверждение леммы верно. Пусть $l \neq 0$. Не ограничивая общности рассуждений, предположим, что $c_1 \neq 0$. Тогда $l = c_1x_1 + l_1$, где $l_1 = c_2x_2 + \ldots + c_nx_n \in LF_p[x_2, \ldots, x_n]$, причём $l_1(0, \ldots, 0) = 0$. Тогда $f = g\big(x_1 + c_1^{-1}l_1\big)^s$, где $g = c_1^s x_1^s \in PF_p[x_1]$. По лемме 3 верно $a \in T\big(f^{(s-1)}_{x_1^{s-1}}\big)$. По лемме 1 находим

$$f^{(s-1)}_{x_1^{s-1}} = s!c_1^s\big(x_1 + c_1^{-1}l_1\big) = s!c_1^{s-1}(c_1x_1 + l_1) = s!c_1^{s-1}l.$$

Далее, по лемме 4 заключаем, что $l(a) = 0$. Лемма 5 доказана.

**Лемма 6.** *Пусть $p$ — простое число, $n \geqslant 1$, $s \in N_p^n$, $|s| \geqslant 1$ и*

$$f = \prod_{i \in i(s)} (x_i + l_i)^{s_i} \in PF_p[x_1, \ldots, x_n],$$

*где $l_i \in LF_p[x_{i+1}, \ldots, x_n]$, $l_i(0, \ldots, 0) = 0$, $i \in i(s)$. Набор $a \in E_p^n$ является периодом многочлена $f$ тогда и только тогда, когда $a$ является решением следующей системы уравнений:*

$$\begin{cases} x_{i_1} + l_{i_1} = 0, \\ \ldots, \\ x_{i_k} + l_{i_k} = 0, \end{cases} \tag{1}$$

*где $i(s) = \{i_1, \ldots, i_k\}$.*

Доказательство. 1. По лемме 5, если набор $a \in E_p^n$ является решением уравнения $x_i + l_i = 0$, то набор $a$ является периодом многочлена $(x_i + l_i)^{s_i}$, $i \in i(s)$, поэтому любое решение системы (1) является периодом многочлена $f$.

2. Пусть набор $a \in E_p^n$ является периодом многочлена $f$. Пусть $1 \leqslant i_1 < \ldots < i_k \leqslant n$. Докажем индукцией по $k$, что набор $a$ является решением системы $(*)$. Базис индукции $k = 1$ следует из леммы 5. Индуктивный переход: пусть $k \geqslant 2$. По следствию 1 для $i_1 \in i(s)$ верно $a \in T\left(f^{(s_{i_1})}_{x_{i_1}^{s_{i_1}}}\right)$. По лемме 1 находим

$$f^{(s_{i_1})}_{x_{i_1}^{s_{i_1}}} = s_{i_1}! \prod_{\substack{j \in i(s), \\ j \neq i_1}} (x_j + l_j)^{s_j}.$$

По предположению индукции заключаем, что набор $a$ является решением системы уравнений

$$\begin{cases} x_{i_2} + l_{i_2} = 0, \\ \ldots, \\ x_{i_k} + l_{i_k} = 0. \end{cases}$$

Согласно следствию 1 для $i_1 \in i(s)$ верно $a \in T\left(f^{(s_{i_1}-1)}_{x_{i_1}^{s_{i_1}-1}}\right)$. По лемме 1 находим

$$f^{(s_{i_1}-1)}_{x_{i_1}^{s_{i_1}-1}} = s_{i_1}!(x_{i_1} + l_{i_1}) \prod_{\substack{j \in i(s), \\ j \neq i_1}} (x_j + l_j)^{s_j}.$$

Теперь если предположить, что набор $a$ не является решением уравнения $x_{i_1} + l_{i_1} = 0$, то $a \notin T\left(f^{(s_{i_1}-1)}_{x_{i_1}^{s_{i_1}-1}}\right)$, что неверно, поэтому $a$ является

решением уравнения $x_{i_1} + l_{i_1} = 0$. Значит, набор $a$ является решением системы (1). Лемма 6 доказана.

## 4. Основная теорема

В этом разделе докажем теорему 1, на основе которой построим алгоритм. Сначала обоснуем вспомогательные утверждения.

**Лемма 7.** *Пусть $p$ — простое число, $n \geqslant 1$, $f \in PF_p[x_1, \ldots, x_n]$, $d(f) \geqslant 1$ и $s \in S(f)$ — наибольший набор в лексикографическом порядке среди всех наборов веса $d(f)$ в множестве $S(f)$, причём $c_f(s) = 1 \in E_p$. Пусть*

$$l_{i,0} = \sum_{j \in o(s)} c_f(s - e_i + e_j) \cdot x_j \in LF_p[x_1, \ldots, x_n],$$

$$l_{i,1} = \sum_{\substack{j \in i(s), \\ j > i}} (s_j + 1) c_f(s - e_i + e_j) \cdot x_j \in LF_p[x_1, \ldots, x_n],$$

$$l_i = l_{i,0} + l_{i,1} \in LF_p[x_1, \ldots, x_n],$$

*где $i \in i(s)$. Тогда если набор $a \in E_p^n$ является периодом многочлена $f$, то $a$ является решением следующей системы уравнений:*

$$\begin{cases} x_{i_1} + s_{i_1}^{-1} l_{i_1} = 0, \\ \ldots, \\ x_{i_k} + s_{i_k}^{-1} l_{i_k} = 0, \end{cases} \tag{2}$$

*где $i(s) = \{i_1, \ldots, i_k\}$.*

Доказательство. По следствию 1 если $a \in T(f)$, то $a \in T\big(f_{x^{s-e_i}}^{(|s-e_i|)}\big)$ для каждого $i \in i(s)$.

Заметим, что если $t \in S(f)$, $t \neq s$ и для некоторого набора $u_i \in N_p^n$ верно $s - e_i + u_i = t$, где $i \in i(s)$, то $u_i = e_j$ для некоторого $j > i$ (в силу того, что $|t| = |s| = d(f)$ и $s$ — наибольший набор в лексикографическом порядке среди наборов веса $d(f)$ в $S(f)$).

Положим $c = \prod\limits_{i \in i(s)} s_i! \in E_p$. Отметим, что $c \neq 0$. Пусть $i \in i(s)$. Тогда

$$(x^s)_{x^{s-e_i}}^{(|s|-1)} = c \cdot x_i.$$

Если $j \in o(s)$, то

$$(x^{s-e_i+e_j})_{x^{s-e_i}}^{(|s|-1)} = c \cdot s_i^{-1} \cdot x_j.$$

Если же $j \in i(s)$ и $j > i$, то

$$(x^{s-e_i+e_j})_{x^{s-e_i}}^{(|s|-1)} = c \cdot s_i^{-1} \cdot (s_j + 1) \cdot x_j.$$

Значит, $f_{x^{s-e_i}}^{(|s-e_i|)} = c \cdot \big(x_i + s_i^{-1} l_i\big) + c_i$ для каждого $i \in i(s)$, где $c_i \in E_p$.

Итак, для каждого $i \in i(s)$ верно, что набор $a$ — период линейного многочлена $c \cdot \left(x_i + s_i^{-1} l_i\right) + c_i$. По лемме 4 получаем, что $a$ — решение уравнения $x_i + s_i^{-1} l_i = 0$, $i \in i(s)$, поэтому заключаем, что если $a \in T(f)$, то набор $a$ является решением системы (2). Лемма 7 доказана.

**Лемма 8.** *Пусть $p$ — простое число, $n \geqslant 1$, $s \in N_p^n$, $|s| = k \geqslant 1$ и*

$$g = \prod_{i \in i(s)} (x_i + l_i)^{s_i} \in PF_p[x_1, \ldots, x_n],$$

*где $l_i \in LF_p[x_{i+1}, \ldots, x_n]$, $l_i(0, \ldots, 0) = 0$, $i \in i(s)$. Тогда для любого набора $t \in S(g)$ верно, что если $|t| = |s|$ и $t \neq s$, то набор $t$ строго меньше набора $s$ в лексикографическом порядке, т. е. $t <_g s$.*

Доказательство. Рассмотрим случай, когда $i(s) = \{1, \ldots, k\}$, где $k \geqslant 1$. Заметим, что

$$g = \prod_{i=1}^{k} (x_i + l_i)^{s_i} = \prod_{i=1}^{k} \sum_{r_i=0}^{s_i} C_{s_i}^{r_i} x_i^{s_i - r_i} l_i^{r_i}$$

$$= \sum_{r_1=0}^{s_1} \ldots \sum_{r_k=0}^{s_k} c_{r_1,\ldots,r_k} x_1^{s_1 - r_1} \ldots x_k^{s_k - r_k} l_1^{r_1} \ldots l_k^{r_k},$$

где $c_{r_1,\ldots,r_k} = C_{s_1}^{r_1} \ldots C_{s_k}^{r_k}$.

Значит,

$$g = \sum_{r_1=0}^{s_1} \ldots \sum_{r_k=0}^{s_k} c_{r_1,\ldots,r_k} x^{s - r_1 e_1 - \ldots - r_k e_k} l_1^{r_1} \ldots l_k^{r_k},$$

или

$$g = x^s + \sum_{r_1 + \ldots + r_k \geqslant 1} c_{r_1,\ldots,r_k} x^{s - r_1 e_1 - \ldots - r_k e_k} l_1^{r_1} \ldots l_k^{r_k},$$

где $0 \leqslant r_1 \leqslant s_1, \ldots, 0 \leqslant r_k \leqslant s_k$. Тогда $g = g_1 + g_2$, где $g_1 = x^s \in PF_p[x_1, \ldots, x_n]$ и

$$g_2 = \sum_{r_1 + \ldots + r_k \geqslant 1} c_{r_1,\ldots,r_k} x^{s - r_1 e_1 - \ldots - r_k e_k} l_1^{r_1} \ldots l_k^{r_k} \in PF_p[x_1, \ldots, x_n],$$

причём $0 \leqslant r_1 \leqslant s_1, \ \ldots, \ 0 \leqslant r_k \leqslant s_k$.

Рассмотрим такое слагаемое $x^t$, $t \in N_p^n$, многочлена $g_2$ с ненулевым коэффициентом, что $|t| = |s|$ и $t \neq s$. Перед возможными понижениями степеней некоторых переменных по правилу $x^p = x$ оно имело вид

$$x^{s - r_1 e_1 - \ldots - r_k e_k} \cdot \prod_{i=1}^{k} x_{j_{i,1}} \cdot \ldots \cdot x_{j_{i,r_i}},$$

где $j_{i,1}, \ldots, j_{i,r_i} > i$ для всех $i = 1, \ldots, k$. Затем, если необходимо, нужно было выполнить все возможные понижения степеней переменных по правилу $x^p = x$ и тем самым получить одночлен из кольца $PF_p[x_1, \ldots, x_n]$. Однако, если предположить, что какая-то переменная $x_j$, $1 \leqslant j \leqslant n$, в выражении выше имеет степень выше $p-1$, то степень одночлена $x^t$ (как одночлена из кольца $PF_p[x_1, \ldots, x_n]$) не может быть равной $|s|$, поэтому степень любой переменной $x_j$, $j = 1, \ldots, n$, в выражении выше не превосходит $p-1$. Это означает, что

$$t = s - r_1 e_1 - \ldots - r_k e_1 + \sum_{i=1}^{k} (e_{j_{i,1}} + \ldots + e_{j_{i,r_i}}) \in N_p^n.$$

Получаем

$$\nu_p(s) - \nu_p(t) = \sum_{i=1}^{k} (r_i p^{n-i} - p^{n-j_{i,1}} - \ldots - p^{n-j_{i,r_i}}) > 0,$$

так как $i < j_{i,1}, \ldots, j_{i,r_i}$ для всех $i = 1, \ldots, k$.

Заметим, что приведённое выше доказательство, можно провести и для набора $s \in N_p^n$ общего вида. Лемма 8 доказана.

**Теорема 1.** *Пусть $p$ — простое число, $n \geqslant 1$, $f \in PF_p[x_1, \ldots, x_n]$, $d(f) \geqslant 1$ и $s \in S(f)$ — наибольший набор в лексикографическом порядке среди всех наборов веса $d(f)$ в множестве $S(f)$, причём $c_f(s) = 1 \in E_p$. Пусть*

$$l_{i,0} = \sum_{j \in o(s)} c_f(s - e_i + e_j) \cdot x_j \in LF_p[x_1, \ldots, x_n],$$

$$l_{i,1} = \sum_{\substack{j \in i(s), \\ j > i}} (s_j + 1) c_f(s - e_i + e_j) \cdot x_j \in LF_p[x_1, \ldots, x_n],$$

$$l_i = l_{i,0} + l_{i,1} \in LF_p[x_1, \ldots, x_n],$$

*где $i \in i(s)$, и*

$$g = \prod_{i \in i(s)} \left(x_i + s_i^{-1} l_i\right)^{s_i} \in PF_p[x_1, \ldots, x_n],$$

$$h = f - g \in PF_p[x_1, \ldots, x_n].$$

*Тогда*

1) *если $t \in S(h)$ и $|t| = |s|$, то набор $t$ строго меньше набора $s$ в лексикографическом порядке, т. е. $t <_g s$;*

2) *набор $a \in E_p^n$ является периодом многочлена $f$ в том и только том случае, когда $a$ является периодом как для каждого линейного многочлена $x_i + s_i^{-1} l_i$, $i \in i(s)$, так и многочлена $h$.*

Доказательство. 1) Если $t \in S(h)$ и $|t| = |s|$, то по лемме 8 набор $t$ строго меньше набора $s$ в лексикографическом порядке.

2.1) Если набор $a \in E^n$ является периодом каждого линейного многочлена $x_i + s_i^{-1} l_i$, $i \in i(s)$, и является периодом многочлена $h$, то $a$ является периодом многочлена $f$, так как $f = g + h$.

2.2) Пусть $a \in E^n$ является периодом многочлена $f$. Тогда по лемме 7 набор $a$ является периодом каждого линейного многочлена $x_i + s_i^{-1} l_i$, $i \in i(s)$. Далее, по лемме 6 набор $a$ является периодом многочлена $g$, значит, $a$ является периодом многочлена $h$, так как $h = f - g$. Теорема 1 доказана.

## 5. Алгоритм поиска периодов многочленов $p$-значных функций

В этом разделе опишем алгоритм поиска базиса линейного пространства всех периодов $p$-значной функции, заданной многочленом из кольца $PF_p[x_1, \ldots, x_n]$, обоснуем его правильность и оценим его сложность. В описании алгоритма знак $:=$ означает присваивание, т. е. переменной слева от этого знака присваивается значение выражения справа от этого знака.

**Алгоритм** $A_p$. Поиск всех периодов многочлена $f \in PF_p[x_1, \ldots, x_n]$.

**Вход:** Многочлен $f \in PF_p[x_1, \ldots, x_n]$, где $p$ — простое число, $n \geqslant 1$.
**Выход:** Однородная система линейных уравнений $T$ над полем $F_p$.

1. Положим $T := \varnothing$, $k := 1$, $f_k := f$, $S_k := S(f_k)$.
2. **while** $d(f_k) \geqslant 1$ **do**

2.1) выберем среди наборов наибольшего веса в множестве $S_k$ наибольший в лексикографическом порядке набор; пусть это набор $s_k \in S_k$,

2.2) положим

$$c_k := c_{f_k}(s),$$
$$f_{k,0} := c_k^{-1} \cdot f_k,$$

2.3) для всех $i \in i(s_k)$ положим

$$l_{k,i,0} := \sum_{j \in o(s_k)} c_{f_{k,0}}(s_k - e_i + e_j) \cdot x_j,$$
$$l_{k,i,1} := \sum_{\substack{j \in i(s_k), \\ j > i}} (s_{k,j} + 1) c_{f_{k,0}}(s_k - e_i + e_j) \cdot x_j,$$
$$l_{k,i} := l_{k,i,0} + l_{k,i,1},$$

2.4) положим

$$g_k := c_k \cdot \prod_{i \in i(s_k)} \left(x_i + s_{k,i}^{-1} l_{k,i}\right)^{s_{k,i}},$$
$$h_k := f_k - g_k,$$

2.5) добавим к системе $T$ однородную систему линейных уравнений $T_k$, а именно, положим

$$T_k := \left\{x_i + s_{k,i}^{-1} l_{k,i} = 0 \mid i \in i(s_k)\right\},$$
$$T := T \cup T_k,$$

2.6) положим $k := k + 1$, $f_k := h_k$, $S_k := S(f_k)$.

**end while**

3. Алгоритм останавливается и выдаёт однородную систему линейных уравнений $T$.

**Теорема 2.** *Пусть $p$ — простое число. Для любого многочлена $f \in PF_p[x_1, \ldots, x_n]$ алгоритм $A_p$ останавливается, выдаёт однородную систему линейных уравнений $T$, определяющую $T(f)$, и при этом цикл в нём выполняется $O(n^{d(f)})$ раз.*

Доказательство. Пусть на вход алгоритма $A_p$ подаётся многочлен $f \in PF_p[x_1, \ldots, x_n]$. Сначала заметим, что для любого $k = 1, 2, \ldots$, если $d(f_k) \geqslant 1$, то для многочленов $f_k, g_k, h_k \in PF_p[x_1, \ldots, x_n]$, где $f_k = g_k + h_k$, выполняется теорема 1.

1) Покажем, что алгоритм $A_p$ останавливается на входе $f$ и цикл в нём повторяется $O(n^{d(f)})$ раз. Пусть при работе алгоритма последовательно выбираются наборы $s_1, s_2, \ldots, s_k, \ldots \in E_2^n$. По теореме 1 для любого $k = 1, 2, \ldots$ верно, что либо $|s_k| > |s_{k+1}|$, либо $|s_k| = |s_{k+1}|$, но набор $s_{k+1}$ меньше набора $s_k$ в лексикографическом порядке. Значит, последовательность наборов $s_1, s_2, \ldots, s_k, \ldots$ конечна, и пусть она состоит из $m$ наборов, $m \geqslant 1$. В последовательности $s_1, s_2, \ldots, s_m$ могут встречаться только наборы веса, не превосходящего $d(f)$, поэтому $m = O(n^{d(f)})$.

2) Покажем, что после завершения работы алгоритма верно, что система $T$ определяет множество $T(f)$. По теореме 1 получаем, что для каждого $k = 1, 2, \ldots, m$ верно $T(f_k) = T(g_k) \cap T(h_k)$. Кроме того, по теореме 1 множество $T(g_k)$ совпадает с множеством решений однородной системы линейных уравнений $T_k$. Алгоритм завершается, когда получен постоянный многочлен $f_m = c \in PF_p[x_1, \ldots, x_n]$, где $c \in E_p$. Несложно заметить, что периодом многочлена $f_m$ является любой набор из $E_p^n$. Теорема 2 доказана.

Далее докажем теорему о сложности задачи поиска базиса линейного пространства всех периодов $p$-значной функции, заданной многочленом

из кольца $PF_p[x_1, \ldots, x_n]$. Входом этой задачи считаем многочлен $f \in PF_p[x_1, \ldots, x_n]$, а выходом — базис линейного пространства $T(f)$.

Сначала опишем, как задаются многочлены из кольца $PF_p[x_1, \ldots, x_n]$ в памяти вычислителя и как понимается сложность алгоритма. Считаем, что многочлен $f \in PF_p[x_1, \ldots, x_n]$ подаётся на вход алгоритму как множество $S(f)$. Следовательно, длина слова, которое подаётся на вход алгоритму, равна $O(n \cdot l(f))$. При работе алгоритма в памяти хранится некоторое множество наборов из $E_p^n$ и доступ к ним последовательный, в начале работы алгоритма — это множество $S(f)$. Сложность алгоритма $A$, которому на вход подаются многочлены $f \in PF_p[x_1, \ldots, x_n]$, рассматриваем как функцию $L_A(N)$, где $N = n \cdot l(f)$. Под простейшим действием алгоритма понимаем вычисление значения некоторой двухместной операции или некоторого двухместного предиката на множестве $E_p^n$ или переход к следующему набору из $E_p^n$ в памяти. При этом считаем, что сложность любого простейшего действия алгоритма равна $O(n)$ битовых операций. Как обычно, под сложностью $L_A(N)$ алгоритма $A$ понимаем наибольшее число битовых операций, которые выполнит алгоритм до завершения работы, среди всех входов длины $N$. Более подробно об алгоритмах и их сложности см., например, [11].

**Теорема 3.** *Пусть $p$ — простое число. Задача поиска базиса линейного пространства всех периодов многочлена $f \in PF_p[x_1, \ldots, x_n]$ может быть решена детерминированным алгоритмом со сложностью $n^{O(d(f))}$.*

Доказательство. Опишем алгоритм $A$ решения этой задачи с указанной сложностью. Пусть $f \in PF_p[x_1, \ldots, x_n]$. Применим алгоритм $A_p$ к многочлену $f$, получим систему линейных уравнений $T$ над полем $F_p$. По теореме 2 множество решений системы $T$ совпадает с множеством $T(f)$. Решим систему $T$ методом исключения неизвестных, найдём базис линейного пространства $T(f)$. Правильность этого алгоритма следует из теоремы 2.

Оценим сложность описанного алгоритма $A$. При выполнении цикла в алгоритме $A_p$ осуществляются преобразования многочленов из $PF_p[x_1, \ldots, x_n]$ степени не выше $d(f)$, а именно, перемножение скобок, понижение степени переменной по правилу $x^p = x$ и приведение подобных слагаемых, поэтому сложность выполнения каждого цикла равна $n^{O(d(f))}$. По теореме 2 цикл выполняется $O(n^{d(f)})$ раз. Значит (с учётом сложности решения системы линейных уравнений методом исключения неизвестных), сложность алгоритма $A$ равна $n^{O(d(f))}$. Теорема 3 доказана.

Из теоремы 3 сразу следует

**Теорема 4.** *Пусть $p$ — простое число и $d \geqslant 1$ — заданное число. Задача поиска базиса линейного пространства всех периодов $p$-значных*

*функций $f(x_1, \ldots, x_n) \in P_p$ степени не выше $d$, заданных многочленами из кольца $PF_p[x_1, \ldots, x_n]$, может быть решена детерминированным полиномиальным алгоритмом относительно числа их переменных.*

## ЛИТЕРАТУРА


1. **Логачёв О. А., Сальников А. А., Смышляев С. В., Ященко В. В.** Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2012. 584 с.
2. **Dawson E., Wu C.-K.** On the linear structure of symmetric Boolean functions // Australas. J. Comb. 1997. V. 16. P. 239–243.
3. **Леонтьев В. К.** О некоторых задачах, связанных с булевыми полиномами // Журн. вычисл. математики и мат. физики. 1999. Т. 39, вып. 6. С. 1045–1054.
4. **Селезнева С. Н.** О сложности распознавания полноты множеств булевых функций, реализованных полиномами Жегалкина // Дискрет. математика. 1997. Т. 9, вып. 4. С. 24–31.
5. **Селезнева С. Н.** Полиномиальный алгоритм для распознавания принадлежности реализованной полиномом функции $k$-значной логики предполным классам самодвойственных функций //Дискрет. математика. 1998. Т. 10, вып. 3. С. 64–72.
6. **Grigoriev D. Yu.** Testing shift-equivalence of polynomials by deterministic, probabilistic and quantum machines // Theor. Comput. Sci. 1997. V. 180, No. 1–2. P. 217–228.
7. **Григорьев Д. Ю.** Распознавание эквивалентности многочленов с точностью до сдвига: детерминированные, вероятностные и квантовые вычисления // Итоги науки и техники. Сер. Соврем. математика. и её прил. 1996. Т. 34. С. 98–116.
8. **Селезнева С. Н.** О поиске периодов многочленов Жегалкина // Дискрет. математика. 2021. Т. 33, вып. 3. С. 107–120.
9. **Лидл Р., Нидеррайтер Г.** Конечные поля. Т. 1. М.: Мир, 1988. 430 с.
10. **Яблонский С. В.** Введение в дискретную математику. М.: Высшая школа, 2001. 384 с.
11. **Гэри М., Джонсон Д.** Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982. 416 с.


*Селезнева Светлана Николаевна*

Статья поступила
14 ноября 2021 г.
После доработки —
14 ноября 2021 г.
Принята к публикации
26 ноября 2021 г.

DISKRETNYI ANALIZ I ISSLEDOVANIE OPERATSII
/DISCRETE ANALYSIS AND OPERATIONS RESEARCH/
January–March 2022. Vol. 29, No. 1. P. 56–73

UDC 519.712.3+512.622+510.52 DOI 10.33048/daio.2022.29.727

# ON COMPLEXITY OF SEARCHING FOR PERIODS OF FUNCTIONS GIVEN BY POLYNOMIALS OVER A PRIME FIELD

*S. N. Selezneva*

Lomonosov Moscow State University,
1 Leninskie Gory, 119991 Moscow, Russia
E-mail: selezn@cs.msu.ru

**Abstract.** We consider polynomials over the prime field $F_p = (E_p; +, \cdot)$ of $p$ elements. With each polynomial $f(x_1, \ldots, x_n)$ under consideration, we associate a $p$-valued function $f\colon E_p^n \to E_p$ that the polynomial defines. A period of a $p$-valued function $f(x_1, \ldots, x_n)$ is a tuple $a = (a_1, \ldots, a_n)$ of elements from $E_p$ such that $f(x_1+a_1, \ldots, x_n+a_n) = f(x_1, \ldots, x_n)$. In the paper, we propose an algorithm that, for $p$ prime and an arbitrary $p$-valued function $f(x_1, \ldots, x_n)$ given by a polynomial over the field $F_p$, finds a basis of the linear space of all periods of $f$. Moreover, the complexity of the algorithm is equal to $n^{O(d)}$, where $d$ is the degree of the polynomial that defines $f$. As a consequence, we show that for $p$ prime and each fixed number $d$ the problem of searching for a basis of the linear space of all periods of a function $f$ given by a polynomial of the degree at most $d$ can be solved by a polynomial-time algorithm with respect to the number of variables of the function. Bibliogr. 11.

**Keywords:** $p$-valued function (function of $p$-valued logic), finite field, prime field, polynomial over a field, periodicity, algorithm, complexity.

## REFERENCES

1. **O. A. Logachyov, A. A. Sal'nikov, S. V. Smyshlyaev,** and **V. V. Yashchenko,** *Boolean Functions in Coding Theory and Cryptology* (MTsNMO, Moscow, 2012) [Russian].

This research is supported by Russian Foundation for Basic Research (Project 19–01–00200–a) and by Ministry of Education and Science of Russian Federation as a part of the program of Moscow Center for Fundamental and Applied Mathematics (Project 075–15–2019–1621).

English version: Journal of Applied and Industrial Mathematics **16** (1) (2022).

2. **E. Dawson** and **C.-K. Wu,** On the linear structure of symmetric Boolean functions, *Australas. J. Comb.* **16**, 239–243 (1997).
3. **V. K. Leont'ev,** Certain problems associated with Boolean polynomials, *Zh. Vychisl. Mat. Mat. Fiz.* **39** (6), 1045–1054 (1999) [Russian] [*Comput. Math. Math. Phys.* **39** (6), 1006–1015 (1999)].
4. **S. N. Selezneva,** On the complexity of completeness recognition of systems of Boolean functions realized in the form of Zhegalkin polynomials, *Diskretn. Mat.* **9** (4), 24–31 (1997) [Russian] [*Discrete Math. Appl.* **7** (6), 565–572 (1997)].
5. **S. N. Selezneva,** A polynomial algorithm for the recognition of belonging a function of $k$-valued logic realized by a polynomial to precomplete classes of self-dual functions, *Diskretn. Mat.* **10** (3), 64–72 (1998) [Russian] [*Discrete Math. Appl.* **8** (5), 483–492 (1998)].
6. **D. Yu. Grigoriev,** Testing shift-equivalence of polynomials by deterministic, probabilistic and quantum machines, *Theor. Comput. Sci.* **180** (1–2), 217–228 (1997).
7. **D. Yu. Grigoriev,** Testing the shift-equivalence of polynomials using quantum machines, *Itogi Nauki Tekh., Ser. Sovrem. Mat. Pril.* **34**, 98–116 (1996) [Russian] [*J. Math. Sci* **82** (1), 3184–3193 (1996)].
8. **S. N. Selezneva,** On searching periods of Zhegalkin polynomials, *Diskretn. Mat.* **33** (3), 107–120 (2021) [Russian].
9. **R. Lidl** and **H. Niederreiter,** *Finite Fields* (Camb. Univ. Press, Cambridge, 1985; Mir, Moscow, 1988 [Russian]).
10. **S. V. Yablonskii,** *Introduction to Discrete Mathematics* (Vysshaya Shkola, Moscow, 2001) [Russian].
11. **M. R. Garey** and **D. S. Johnson,** *Computers and Intractability: A Guide to the Theory of NP-Completeness* (Freeman, San Francisco, 1979; Mir, Moscow, 1982 [Russian]).


*Svetlana N. Selezneva*

Received November 14, 2021
Revised November 14, 2021
Accepted November 26, 2021