МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

Научный журнал

2019 **№ 43**

Зарегистрирован в Федеральной службе по надзору
в сфере связи и массовых коммуникаций

Свидетельство о регистрации ПИ № ФС 77-33762 от 16 октября 2008 г.

Подписной индекс в объединённом каталоге «Пресса России» 38696

УЧРЕДИТЕЛЬ
Томский государственный университет

Адрес редакции и издателя: 634050, г. Томск, пр. Ленина, 36
E-mail: vestnik_pdm@mail.tsu.ru

В журнале публикуются результаты фундаментальных и прикладных научных исследований отечественных и зарубежных ученых, включая студентов и аспирантов, в области дискретной математики и её приложений в криптографии, компьютерной безопасности, кибернетике, информатике, программировании, теории надёжности, интеллектуальных системах.

Периодичность выхода журнала: 4 номера в год.

Редактор *Н. И. Шидловская*
Верстка *И. А. Панкратовой*

Подписано к печати 15.03.2019. Формат $60 \times 84\frac{1}{8}$. Усл. п. л. 14,3. Тираж 300 экз.
Заказ № 3681. Цена свободная. Дата выхода в свет 21.03.2019.

Отпечатано на оборудовании
Издательского Дома Томского государственного университета
634050, г. Томск, пр. Ленина, 36
Тел.: 8(3822)53-15-28, 52-98-49

СОДЕРЖАНИЕ

CONTENTS

THEORETICAL BACKGROUNDS OF APPLIED DISCRETE MATHEMATICS

MATHEMATICAL METHODS OF CRYPTOGRAPHY

MATHEMATICAL BACKGROUNDS OF COMPUTER AND CONTROL SYSTEM RELIABILITY

APPLIED GRAPH THEORY

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.7

АЛГОРИТМ НАХОЖДЕНИЯ МИНИМАЛЬНОЙ СТЕПЕНИ ПОЛИНОМА НАД КОНЕЧНЫМ ПОЛЕМ ДЛЯ ФУНКЦИИ НАД ВЕКТОРНЫМ ПРОСТРАНСТВОМ В ЗАВИСИМОСТИ ОТ ВЫБОРА НЕПРИВОДИМОГО МНОГОЧЛЕНА

С. А. Белов

Московский государственный университет имени М.В. Ломоносова, г. Москва, Россия

Рассматриваются преобразования над векторным пространством p-ичных векторов длины n, где p — простое число. Каждому такому преобразованию ставится в соответствие полином над конечным полем $\mathrm{GF}(p^n)$. Конечное поле представляется кольцом вычетов по модулю неприводимого многочлена. В общем случае, в зависимости от выбора неприводимого многочлена, преобразованию над векторным пространством соответствуют различные полиномы над конечным полем. Предложен алгоритм поиска минимальной степени среди таких полиномов и неприводимого многочлена, при котором эта степень достигается.

Ключевые слова: *конечное поле, неприводимый многочлен, булевы функции, блочный шифр.*

DOI 10.17223/20710410/43/1

AN ALGORITHM FOR FINDING THE MINIMUM DEGREE OF A POLYNOMIAL OVER A FINITE FIELD FOR A FUNCTION OVER A VECTOR SPACE DEPENDING ON THE CHOICE OF AN IRREDUCIBLE POLYNOMIAL

S. A. Belov

Moscow State University, Moscow, Russia

E-mail: serbel.sci@gmail.com

The transformations of the vector space of p-ary vectors of length n, where p is a prime number, are considered. Each such a transformation is assigned to a polynomial over a finite field $\mathrm{GF}(p^n)$. The finite field is represented by a residue ring modulo an irreducible polynomial. In general, depending on the choice of the irreducible polynomial, different polynomials over the finite field will correspond to the transformation over the vector space. In this paper, we propose an algorithm for finding the minimal degree of such a polynomial and an irreducible polynomial at which this degree is achieved. The algorithm is based on the calculation of expressions for polynomial coefficients through its values. In the process of the algorithm, the elements of finite fields are treated as polynomials. To compute specific irreducible polynomials, the Euclid algorithm computes the greatest common divisor of these expressions and the polynomial, which is the product of all irreducible polynomials of degree n. To work up to degree d, the algorithm requires storage of $O(p^n n)$ elements from $GF(p)$ and $O(p^n n^2 d^4 w)$ operations of addition and multiplication modulo p where w is the number of elements on which the polynomial is nonzero. Thus, the algorithm is especially effective for functions that have many zero values. The minimal degree polynomials for the S-boxes of block ciphers (GOST 28147-89, ICEBERG, LUFFA, LUCIFER, SERPENT, AES, PRESENT, GOST 34.12-2015) as well as the irreducible polynomials at which this degree is achieved have been computed.

Keywords: *finite field, irreducible polynomial, Boolean functions, block cipher.*

Введение

Пусть задано преобразование $g(x)$ над векторным пространством p-ичных векторов длины n, где p — простое число. Конечное поле $GF(p^n)$ будем рассматривать как кольцо вычетов по неприводимому многочлену $h(\theta)$. При условии, что известно соответствие между p-ичными векторами длины n и элементами конечного поля, каждому преобразованию $g(x)$ можно поставить в соответствие полином $f(x)$ над полем $GF(p^n)$. При различных неприводимых многочленах $h_1(\theta)$ и $h_2(\theta)$ преобразованию $g(x)$ соответствуют, вообще говоря, различные полиномы над конечным полем. В работе рассматривается следующая задача: необходимо найти такой неприводимый многочлен, чтобы в поле, построенном как кольцо вычетов по модулю этого неприводимого многочлена, степень полинома, соответствующего заданному преобразованию над векторным пространством, была наименьшей. Подобная задача рассматривалась в [1] для функций над полями характеристики два. Авторы показали, что полиномы $f_1(x)$ и $f_2(x)$ заданной функции $f(x)$ для пары неприводимых многочленов $R_1(x)$ и $R_2(x)$ связаны соотношением $f_2(x) = L(f_1(L^{-1}(x)))$, где L является обратимым линейным преобразованием рассматриваемого поля. В данной работе предложен иной подход к вычислению минимальной степени многочлена, представляющего функцию над векторным пространством, для различных неприводимых многочленов, который применим для полей произвольной характеристики.

1. Определения и обозначения

Введём определения и обозначения, которые использованы в дальнейшем, а также необходимые утверждения из теории конечных полей [2]:

$GF(q)$ — конечное поле из q элементов. Для конечного поля $GF(q)$ число q имеет вид $q = p^n$, где p — простое число, n — натуральное. Число p называется характеристикой конечного поля. Далее записи $GF(q)$ и $GF(p^n)$ будем считать равнозначными.

$V_n(p)$ — векторное пространство p-ичных векторов длины n с операциями поэлементного сложения векторов по модулю p и умножения вектора на скалярное значение по модулю p. Для пространства $V_1(p)$ будем использовать сокращённую запись $V(p)$.

$F_q[x]$ — множество многочленов переменной x над полем $GF(q)$. Любая функция $f : GF(q) \to GF(q)$ может быть представлена в виде многочлена одной переменной над полем $GF(q)$ степени не более $q - 1$.

Если функция $f : GF(q) \to GF(q)$ представляется полиномом $\sum\limits_{i=0}^{q-1} f_i x^i$, то f_i — коэффициент этого многочлена при степени i.

Весом функции над конечным полем будем называть количество аргументов, на которых она принимает значение, отличное от нуля. НОД двух многочленов $f(x)$ и $g(x)$

будем обозначать $\big(f(x), g(x)\big)$. Носителем булевой функции называется множество наборов, на которых она принимает значение 1.

Множество вычетов по модулю числа p^l-1 относительно операции умножения на p распадается на подмножества, называемые циклотомическими классами по модулю p^l-1 [3]. Циклотомический класс C_s, в котором s — наименьшее число, состоит из чисел

$$C_s = \{s, sp, sp^2, \ldots, sp^{k-1}\},$$

где k — наименьшее натуральное число, для которого $sp^k \equiv s \pmod{p^l-1}$. Старшим представителем циклотомического класса будем называть наибольшее число из этого класса.

Элементы конечного поля $\mathrm{GF}(p^n)$ будем представлять многочленами из $F_p[\theta]$ степени меньше n, сложение и умножение которых осуществляется по модулю заданного неприводимого многочлена. Когда операции над многочленами производятся не по модулю неприводимого многочлена, а по обычным правилам сложения и умножения многочленов в $F_p[\theta]$, будем подчёркивать это, явно записывая переменную θ в скобках. Так, для $a, b \in \mathrm{GF}(q)$ запись $c = ab$ означает умножение двух элементов конечного поля (умножение многочленов по модулю неприводимого многочлена), а запись $a(\theta)b(\theta)$ — обычное умножение многочленов $a(\theta)$ и $b(\theta)$ в кольце $F_p[\theta]$.

Вектору $c = (c_0, c_1, \ldots, c_{n-1})$ из $V_n(p)$ будем ставить в соответствие элемент $\sum\limits_{i=0}^{n-1} c_i\theta^i$ конечного поля $\mathrm{GF}(p^n)$. Для записи элементов конечного поля $\mathrm{GF}(p^n)$ и соответствующих им векторов $V_n(p)$ будем также использовать запись в виде чисел. Вектору $c = (c_0, c_1, \ldots, c_{n-1})$ из $V_n(p)$ (и соответствующему ему элементу поля $\sum\limits_{i=0}^{n-1} c_i\theta^i$) будем ставить в соответствие число $\sum\limits_{i=0}^{n-1} c_ip^i$ из интервала $[0, p^n-1]$. В дальнейшем будем записывать элементы конечного поля в виде многочленов переменной θ или в виде целых чисел, а многочлены, задающие функции над конечными полями, — как многочлены переменной x.

2. Формулы для коэффициентов многочлена над конечным полем

Пусть $\mathrm{GF}(q)$ — конечное поле, $f : \mathrm{GF}(q) \to \mathrm{GF}(q)$. Полином функции f можно записать в канонической форме $f(x) = \sum\limits_{a\in\mathrm{GF}(q)} \delta_a(x)f(a)$, где $\delta_a(x) = \begin{cases} 1, & x = a, \\ 0, & x \neq a. \end{cases}$

В конечном поле верно равенство $\delta_a(x) = 1 - (x-a)^{q-1}$. Подставим выражения для $\delta_a(x)$ и раскроем скобки:

$$\begin{aligned} f(x) &= \sum_{a\in\mathrm{GF}(q)} \delta_a(x)f(a) = \sum_{a\in\mathrm{GF}(q)} (1-(x-a)^{q-1})f(a) = \\ &= \sum_{a\in\mathrm{GF}(q)} (1-(x^{q-1}+ax^{q-2}+\ldots+a^{q-1}))f(a) = \\ &= -\sum_{a\in\mathrm{GF}(q)} (x^{q-1}+ax^{q-2}+\ldots+a^{q-2}x)f(a) + f(0). \end{aligned}$$

Получаем формулу для коэффициентов полинома $f(x)$:

$$f_j = \begin{cases} -\sum\limits_{a\in\mathrm{GF}(q)} a^{q-1-j}f(a), & \text{если } j = 1, 2, \ldots, q-1, \\ f(0), & \text{если } j = 0. \end{cases}$$

Теорема 1 [2]. Произведение $I(q,n,x)$ всех нормированных неприводимых многочленов степени n из кольца $F_q[x]$ задаётся формулой $I(q,n,x) = \prod\limits_{d|n}(x^{q^d} - x)^{\mu(n/d)} = \prod\limits_{d|n}(x^{q^{n/d}} - x)^{\mu(d)}$, где $\mu(n)$ — функция Мёбиуса:

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1, \\ (-1)^k, & \text{если } n \text{ – произведение } k \text{ различных простых чисел}, \\ 0, & \text{если } n \text{ делится на квадрат простого числа.} \end{cases}$$

Утверждение 1. Пусть $h(x)$ — многочлен из кольца $F_p[x]$. Нормированный неприводимый многочлен $g(x)$ степени n, такой, что $g(x)$ делит $h(x)$, существует тогда и только тогда, когда $\big(h(x), I(p,n,x)\big) \neq 1$.

Прежде чем представить алгоритм нахождения минимальной степени полинома, опишем его основную идею. Пусть задана функция $g : V_n(p) \to V_n(p)$. Вопрос, при каком неприводимом многочлена полином f, соответствующий функции g, будет иметь минимальную степень, равносилен вопросу, при каком неприводимом многочлене наибольшее количество коэффициентов $f_{q-1}, f_{q-2}, \ldots, f_1, f_0$, начиная со старших, будет равно нулю. Согласно полученной формуле, $f_j = -\sum\limits_{a \in \mathrm{GF}(q)} a^{q-1-j} f(a)$, $j = 1, 2, \ldots, q-1$. Чтобы установить, при каких неприводимых многочленах $f_j = 0$, достаточно выяснить, какие неприводимые многочлены степени n делят $f_j(\theta) = -\sum\limits_{a \in \mathrm{GF}(q)} a(\theta)^{q-1-j} f(a)(\theta)$. В силу утверждения 1, неприводимый многочлен делит $f_j(\theta)$ тогда и только тогда, когда $\big(f_j(\theta), I(p,n,\theta)\big) \neq 1$ в кольце $F_p[\theta]$. На этом основан алгоритм 1 поиска минимальной степени функции над конечным полем в зависимости от выбора неприводимого многочлена.

Алгоритм 1. Поиск минимальной степени функции

Вход: таблица значений функции g над $V_n(p)$.
Выход: минимальная степень многочлена f над $\mathrm{GF}(p^n)$.

1: $d(\theta) \leftarrow I(p,n,\theta)$
2: **Для** $j = q-1, q-2, \ldots, 1, 0$:
3:    **Если** $j > 0$, **то**
4:       $f_j(\theta) \leftarrow \sum\limits_{a \in \mathrm{GF}(q)} a(\theta)^{q-1-j} f(a)(\theta)$,
5:    **иначе**
6:       $f_j(\theta) \leftarrow f(0)(\theta)$.
7:    **Если** $f_j(\theta) \neq 0$, **то**
8:       $k(\theta) \leftarrow \big(d(\theta), f_j(\theta)\big)$.
9:       **Если** $k(\theta) = 1$, **то**
10:          **Вернуть** j.
11:       $d(\theta) \leftarrow k(\theta)$.
12: **Вернуть** 0.

Отметим, что алгоритм 1 может быть модифицирован таким образом, чтобы дополнительно получать и неприводимый многочлен, при котором достигается минимальная степень. Для этого необходимо на шаге 10, если степень $d(\theta)$ равна n, выдать $d(\theta)$, а если больше n, разложить $d(\theta)$ на множители и выдать любой из сомножителей.

Утверждение 2. Алгоритм 1 всегда возвращает минимальную степень $f(x)$ над $\mathrm{GF}(p^n)$ в зависимости от выбора неприводимого многочлена.

Доказательство. Чтобы показать корректность алгоритма 1, во-первых, отметим, что он всегда завершается и выдаёт ответ. В основном цикле последовательно перебираются коэффициенты полинома $f_j(\theta)$, начиная со старших. Согласно утверждению 1, на шаге 9 $k(\theta)$ является произведением всех неприводимых многочленов степени n, по модулю которых $f_j(\theta) = 0$. Если $k(\theta)$ отличен от 1, то существует неприводимый многочлен степени n, по модулю которого $f_j = 0$. Это означает, что минимальная степень $f(x)$ в зависимости от выбора неприводимого многочлена не более $j - 1$. Если $k(\theta)$ равен 1, то неприводимых многочленов степени n, по модулю которых $f_j(\theta) = 0$, не существует, следовательно, минимальная степень $f(x)$ не меньше j. Так как коэффициенты перебираются последовательно, начиная со старших, это означает, что минимальная степень в точности равна j. Особый случай — если функция $f(x)$ тождественно равна 0. Тогда $f_j(\theta)$ будет всё время равен нулю и цикл завершится, пройдя все итерации. В этом случае алгоритм 1 выдаст правильный ответ на шаге 12. ■

Утверждение 3. Сложность проверки с помощью алгоритма 1 того, что степень функции $f(x)$ веса w над полем $\mathrm{GF}(p^n)$ не превосходит d, составляет $\mathrm{O}(p^n n^2 d^4 w)$ операций сложения и умножения по модулю p. При этом необходимо хранить в памяти $\mathrm{O}(p^n n)$ значений из поля $\mathrm{GF}(p)$.

Доказательство. Рассмотрим итерацию с номером j. Обозначим $m = q - 1 - j$. Для вычисления на шаге 4 коэффициента $f_j(\theta)$ требуется вычислить сумму $\sum\limits_{a\in \mathrm{GF}(q)} a(\theta)^{q-1-j} f(a)(\theta)$. Многочлен $a(\theta)$ имеет степень не более $n-1$, для возведения его в степень m требуется не более $\mathrm{O}((mn)^2 \log m)$ операций. Количество слагаемых в сумме равно w, поэтому всего сложность шага 4 составляет $\mathrm{O}(wn^2m^2 \log m)$ операций.

Если $f_j(\theta) \neq 0$, то происходит вычисление НОД многочленов $f_j(\theta)$ и $d(\theta)$ на шаге 8. Степень многочлена $f_j(\theta)$ не превосходит mn, многочлена $d(\theta)$ — p^n. Поэтому сложность вычисления НОД равна $\mathrm{O}(p^n mn)$ [4]. Величина m меняется от 0 до d, суммируя значения сложности по m, имеем

$$\sum_{m=0}^{d} \mathrm{O}(wn^2m^2 \log m) < \sum_{m=0}^{d} \mathrm{O}(wn^2m^3) = \mathrm{O}(wn^2d^4), \quad \sum_{m=0}^{d} \mathrm{O}(p^n nm) = \mathrm{O}(p^n nd^2).$$

Таким образом, полная сложность равна $\mathrm{O}(p^n n^2 d^4 w)$.

В процессе работы алгоритма 1 необходимо хранить многочлены $d(\theta)$ и $k(\theta)$, каждый из которых является многочленом над $\mathrm{GF}(p)$ степени не более p^n, и многочлен $f_j(\theta)$ степени не более $p^n n$. Так как для хранения многочлена степени k над $\mathrm{GF}(p)$ требуется хранить в памяти $\mathrm{O}(k)$ значений из $\mathrm{GF}(p)$, всего для работы алгоритма необходимо хранить $\mathrm{O}(p^n n)$ значений из $\mathrm{GF}(p)$. ■

Замечание 1. Сравним алгоритм 1 с алгоритмом, который последовательно находит остатки от деления на все нормированные неприводимые многочлены степени n. В таком алгоритме шаги 7–11 алгоритма 1 будут заменены на последовательный перебор остатков от деления на все нормированные неприводимые многочлены степени n. Коэффициент $f_j(\theta)$ необходимо вычислить и в том и в другом случае. Степень многочлена $f_j(\theta)$ не превосходит mn. Количество нормированных многочленов степени n над полем $\mathrm{GF}(p)$ имеет порядок p^n/n. При вычислении остатков от деления на все неприводимые многочлены полинома $f_j(\theta)$ понадобится $\mathrm{O}\left(\dfrac{p^n}{n} mn \log{(mn)}\right) = \mathrm{O}(p^n m \log{(mn)})$ операций сложения и умножения по модулю p. Как показано выше, вычисление НОД на шаге 8 имеет сложность $\mathrm{O}(p^n nm)$ операций. Таким образом, при $m > p^n/n$ сложность вычисления шагов 7–11 алгоритма 1 становится меньше, чем сложность перебора остатков от деления на все неприводимые многочлены степени n.

Пример 1. Пусть $n = 3$, $g(x)$ задаётся таблицей (табл. 1).

Таблица 1

x	0	1	2	3	4	5	6	7
$g(x)$	1	3	4	0	5	6	7	2

Вычислим коэффициенты $f(x)$ согласно алгоритму 1:

$$d(\theta) = I(2, 3, \theta) = \theta^6 + \theta^5 + \theta^4 + \theta^3 + \theta^2 + \theta + 1;$$
$$f_7(\theta) = 1 + (\theta + 1) + \theta^2 + 0 + (\theta^2 + 1) + (\theta^2 + \theta) + (\theta^2 + \theta + 1) + \theta = 0;$$
$$f_6(\theta) = 0 \cdot 1 + 1 \cdot (\theta + 1) + \theta \cdot \theta^2 + (\theta + 1) \cdot 0 + \theta^2(\theta^2 + 1) + (\theta^2 + 1)(\theta^2 + \theta) + \\ + (\theta^2 + \theta)(\theta^2 + \theta + 1) + (\theta^2 + \theta + 1)\theta = \theta^4 + \theta^3 + \theta^2 + 1;$$
$$k(\theta) = \big(d(\theta), f_6(\theta)\big) = \theta^3 + \theta + 1;$$
$$d(\theta) = k(\theta) = \theta^3 + \theta + 1;$$
$$f_5(\theta) = 0^2 \cdot 1 + 1^2(\theta + 1) + \theta^2 \cdot \theta^2 + (\theta + 1)^2 \cdot 0 + (\theta^2)^2(\theta^2 + 1) + (\theta^2 + 1)^2(\theta^2 + \theta) + \\ + (\theta^2 + \theta)^2(\theta^2 + \theta + 1) + (\theta^2 + \theta + 1)^2\theta = \theta^6 + \theta^5 + \theta + 1;$$
$$k(\theta) = \big(d(\theta), f_5(\theta)\big) = 1.$$

В результате минимальная степень $f(x)$ равна 5 и достигается в поле $F_2/(\theta^3+\theta+1)$. При этом в полях с другими неприводимыми многочленами степень функции равна 6.

Пусть функция $g : V_n(p) \to V_n(p)$ задана в виде вектора функций $(g^{(0)}, \dots, g^{(n-1)})$, где $g^{(i)} : V_n(p) \to V(p)$, при этом для полинома $f(x)$ над $\mathrm{GF}(p^n)$ выполнено $f(x) = \sum\limits_{i=0}^{n-1} \theta^i f^{(i)}(x)$, где полином $f^{(i)}$ соответствует функции $g^{(i)}$, $f^{(i)} : \mathrm{GF}(p^n) \to \mathrm{GF}(p)$. В этом случае шаги 3–6 алгоритма 1 могут быть модифицированы (алгоритм 2).

Алгоритм 2. Модификация алгоритма 1

Вход: таблицы значений функций $g^{(0)}, \dots, g^{(n-1)}$.
Выход: минимальная степень многочлена f над $\mathrm{GF}(p^n)$.

1: $d(\theta) \leftarrow I(p, n, \theta)$.
2: **Для** $j = q - 1, q - 2, \dots, 1, 0$:
3: **Если** $j > 0$, **то**
4: $f_j(\theta) \leftarrow \sum\limits_{i=0}^{n-1} \theta^i \left(\sum\limits_{a \in \mathrm{GF}(q)} a(\theta)^{q-j-1} f^{(i)}(a)(\theta) \right)$,
5: **иначе**
6: $f_j(\theta) \leftarrow \sum\limits_{i=0}^{n-1} \theta^i f^{(i)}(0)(\theta)$.
7: **Если** $f_j(\theta) \neq 0$, **то**
8: $k(\theta) \leftarrow \big(d(\theta), f_j(\theta)\big)$.
9: **Если** $k(\theta) = 1$, **то**
10: **Вернуть** j.
11: $d(\theta) \leftarrow k(\theta)$.
12: **Вернуть** 0.

Отличие алгоритма 2 от алгоритма 1 состоит в способе вычисления коэффициентов $f_j(\theta)$ на шагах 3–6. Все утверждения, относящиеся к алгоритму 1, верны и для алгоритма 2.

3. Случай полей характеристики два

Рассмотрим случай полей характеристики два. Если $q = 2^n$, а $f(x)$ — булева функция от n переменных, то

$$f_j = \begin{cases} \sum\limits_{a \in \mathrm{GF}(2^n), f(a)=1} a^{2^n-1-j}, & \text{если } j = 1, 2, \ldots, 2^n - 1, \\ f(0), & \text{если } j = 0. \end{cases}$$

Следствие 1. Вне зависимости от выбора неприводимого многочлена, полином булевой функции нечётного веса имеет степень $2^n - 1$, чётного веса — не более $2^n - 2$.

Следствие 2. При $n > 2$ полином булевой функции чётного веса имеет степень меньше $2^n - 3$ тогда и только тогда, когда $\sum\limits_{a \in \mathrm{GF}(2^n), f(a)=1} a = 0$, то есть если покоординатная сумма векторов, составляющих носитель булевой функции, равна нулю. Коэффициенты f_{2^n-2} и f_{2^n-3} не зависят от выбора неприводимого многочлена.

Доказательство. Следует из формулы для f_{2^n-2} и того, что $f_{2^n-3} = (f_{2^n-2})^2$. ■

Для булевых функций алгоритм 1 может быть оптимизирован. Так как известно, что для функции $f(x)$ над $\mathrm{GF}(2^n)$ выполнено $f_{2j \bmod (2^n-1)} = f_j^2$, $j = 1, \ldots, 2^n - 2$ [5], то если коэффициент $f_j(\theta)$ равен нулю, то все коэффициенты с номерами из того же циклотомического класса по модулю 2 также равны нулю. Поэтому в цикле достаточно рассмотреть только те j, для которых $2^n - 1 - j$ являются старшими представителями циклотомических классов.

4. Криптографические применения

Описанные алгоритмы могут быть применены в задачах криптоанализа. Они позволяют выбрать представление конечного поля таким образом, чтобы степень исследуемых отображений была как можно меньше. Поиск такого представления уменьшает сложность применения методов криптоанализа, связанных с алгебраическими характеристиками исследуемого отображения, например интерполяционного криптоанализа [6]. В качестве криптографических отображений были проанализированы S-блоки шифров ГОСТ 28147-89 [7, 8], ICEBERG [9], LUFFA [10], LUCIFER [11], SERPENT [12], AES [13], PRESENT [14], ГОСТ Р 34.12-2015 (Кузнечик) [15]. Результаты приведены в табл. 2. Для каждого S-блока вычислена минимальная степень в зависимости от выбора неприводимого многочлена. Указан многочлен, при котором достигается минимальная степень.

Таблица 2

S-box	Степени S-блоков		Многочлен
	Макс.	Мин.	
GOST-A-ParamSet S1 – S8	14	14	Любой
GOST-B-ParamSet S1	14	14	Любой
GOST-B-ParamSet S2	14	13	$\theta^4 + \theta + 1$
GOST-B-ParamSet S3 – S5	14	14	Любой
GOST-B-ParamSet S6 – S8	14	13	$\theta^4 + \theta^3 + 1$
GOST-C-ParamSet S1 – S4	14	14	Любой
GOST-C-ParamSet S5	14	13	$\theta^4 + \theta + 1$
GOST-C-ParamSet S6	14	14	Любой

Окончание табл. 2

S-box	Степени S-блоков		Многочлен
	Макс.	Мин.	
GOST-C-ParamSet S7	14	13	$\theta^4+\theta+1$
GOST-C-ParamSet S8	14	14	Любой
GOST-D-ParamSet S1	14	13	$\theta^4+\theta^3+\theta^2+\theta+1$
GOST-D-ParamSet S2 – S8	14	14	Любой
GOST-T-ParamSet S1	14	13	$\theta^4+\theta^3+1$
GOST-T-ParamSet S2	14	14	Любой
GOST-T-ParamSet S3	14	13	$\theta^4+\theta^3+\theta^2+\theta+1$
GOST-T-ParamSet S4	14	13	$\theta^4+\theta^3+\theta^2+\theta+1$
GOST-T-ParamSet S5	14	13	$\theta^4+\theta^3+1$
GOST-T-ParamSet S6 – S8	14	14	Любой
GOST-Z-ParamSet S1 – S8	14	14	Любой
ICEBERG S0, S1	13	13	Любой
LUFFA	14	14	Любой
Lucifer S0, S1	14	14	Любой
Present	14	14	Любой
Serpent S0	14	14	Любой
Serpent S1	14	13	$\theta^4+\theta^3+1$
Serpent S2 – S7	14	14	Любой
Кузнечик	254	253	$\theta^8+\theta^4+\theta^3+\theta+1$
AES	254	254	Любой

Продемонстрируем вид конкретных полиномов на примере S-блока шифра Кузнечик, который задаётся массивом значений $f=(f(0),f(1),\ldots,f(255))$ [15]:

$$f=(252,238,221,17,207,110,49,22,251,196,250,218,35,197,4,77,233,119,240,219,147,46,153,186,23,\\ 54,241,187,20,205,95,193,249,24,101,90,226,92,239,33,129,28,60,66,139,1,142,79,5,132,2,174,227,\\ 106,143,160,6,11,237,152,127,212,211,31,235,52,44,81,234,200,72,171,242,42,104,162,253,58,206,\\ 204,181,112,14,86,8,12,118,18,191,114,19,71,156,183,93,135,21,161,150,41,16,123,154,199,243,145,\\ 120,111,157,158,178,177,50,117,25,61,255,53,138,126,109,84,198,128,195,189,13,87,223,245,36,169,\\ 62,168,67,201,215,121,214,246,124,34,185,3,224,15,236,222,122,148,176,188,220,232,40,80,78,51,\\ 10,74,167,151,96,115,30,0,98,68,26,184,56,130,100,159,38,65,173,69,70,146,39,94,85,47,140,163,\\ 165,125,105,213,149,59,7,88,179,64,134,172,29,247,48,55,107,228,136,217,231,137,225,27,131,73,\\ 76,63,248,254,141,83,170,144,202,216,133,97,32,113,103,164,45,43,9,91,203,155,37,208,190,229,\\ 108,82,89,166,116,210,230,244,180,192,209,102,175,194,57,75,99,182).$$

В поле с неприводимым многочленом $\theta^8+\theta^4+\theta^3+\theta+1$ степень многочлена этой функции равна 253, и многочлен имеет следующий вид (коэффициенты полинома, являющиеся элементами конечного поля, записаны в числовом виде):

$$f(x)=158x^{253}+217x^{252}+132x^{251}+45x^{250}+90x^{249}+221x^{248}+175x^{246}+207x^{245}+8x^{244}+18x^{243}+\\ +89x^{242}+56x^{241}+162x^{240}+158x^{239}+125x^{238}+139x^{237}+137x^{236}+227x^{235}+204x^{234}+207x^{233}+\\ +41x^{232}+x^{231}+41x^{230}+83x^{229}+4x^{228}+59x^{227}+135x^{226}+163x^{225}+51x^{224}+103x^{223}+154x^{222}+\\ +249x^{221}+145x^{220}+214x^{219}+63x^{218}+198x^{217}+107x^{216}+42x^{215}+37x^{214}+194x^{212}+210x^{211}+\\ +107x^{210}+100x^{209}+202x^{208}+227x^{207}+81x^{206}+95x^{205}+77x^{204}+174x^{203}+114x^{202}+128x^{201}+\\ +233x^{200}+37x^{199}+161x^{198}+234x^{197}+15x^{196}+58x^{195}+7x^{194}+102x^{193}+70x^{192}+55x^{191}+119x^{190}+\\ +149x^{189}+77x^{188}+35x^{187}+32x^{186}+143x^{185}+30x^{184}+59x^{183}+56x^{182}+10x^{181}+217x^{180}+32x^{179}+\\ +66x^{178}+126x^{177}+224x^{176}+199x^{175}+93x^{174}+91x^{173}+134x^{172}+185x^{171}+88x^{170}+156x^{169}+\\ +233x^{168}+187x^{167}+6x^{166}+148x^{165}+231x^{164}+66x^{163}+51x^{162}+176x^{161}+84x^{160}+172x^{159}+\\ +98x^{158}+73x^{157}+132x^{156}+185x^{155}+113x^{154}+243x^{153}+111x^{152}+183x^{151}+38x^{150}+129x^{149}+$$

$$+88x^{148}+83x^{147}+236x^{146}+176x^{145}+235x^{144}+253x^{143}+158x^{142}+35x^{141}+186x^{140}+44x^{139}+$$
$$+197x^{138}+223x^{137}+133x^{136}+127x^{135}+201x^{134}+217x^{133}+70x^{132}+102x^{131}+121x^{130}+100x^{129}+$$
$$+242x^{128}+27x^{127}+84x^{126}+111x^{125}+138x^{124}+77x^{123}+123x^{122}+68x^{121}+10x^{120}+58x^{119}+$$
$$+140x^{118}+142x^{117}+16x^{116}+41x^{115}+230x^{114}+227x^{113}+96x^{112}+72x^{111}+159x^{110}+37x^{109}+$$
$$+14x^{108}+201x^{107}+5x^{106}+202x^{105}+17x^{104}+175x^{103}+105x^{102}+137x^{101}+204x^{100}+37x^{99}+64x^{98}+$$
$$+195x^{97}+185x^{96}+73x^{95}+193x^{94}+211x^{93}+28x^{92}+245x^{91}+76x^{90}+113x^{89}+238x^{88}+206x^{87}+$$
$$+88x^{86}+70x^{85}+62x^{84}+25x^{83}+167x^{82}+225x^{81}+233x^{80}+32x^{79}+241x^{78}+194x^{77}+36x^{76}+$$
$$+208x^{75}+165x^{74}+252x^{73}+171x^{72}+118x^{71}+234x^{70}+249x^{69}+23x^{68}+234x^{67}+7x^{66}+243x^{65}+$$
$$+66x^{64}+140x^{63}+142x^{62}+x^{61}+217x^{60}+87x^{59}+105x^{58}+174x^{57}+116x^{56}+228x^{55}+238x^{54}+$$
$$+236x^{53}+241x^{52}+18x^{51}+81x^{50}+221x^{49}+138x^{48}+178x^{47}+28x^{46}+160x^{45}+161x^{44}+129x^{43}+$$
$$+56x^{42}+130x^{41}+81x^{40}+207x^{39}+185x^{38}+57x^{37}+207x^{36}+22x^{35}+99x^{34}+242x^{33}+205x^{32}+$$
$$+168x^{31}+x^{30}+36x^{29}+94x^{28}+96x^{27}+158x^{26}+251x^{25}+32x^{24}+217x^{23}+58x^{22}+86x^{21}+207x^{20}+$$
$$+132x^{19}+171x^{18}+113x^{17}+199x^{16}+36x^{15}+246x^{14}+89x^{13}+5x^{12}+111x^{11}+200x^{10}+139x^{9}+$$
$$+172x^{8}+109x^{7}+163x^{6}+176x^{5}+170x^{4}+187x^{3}+110x^{2}+140x+252.$$

В полях с другими неприводимыми многочленами эта функция имеет степень 254, например для поля с неприводимым многочленом $\theta^8+\theta^4+\theta^3+\theta^2+1$ многочлен имеет следующий вид:

$$f(x)=184x^{254}+200x^{253}+124x^{252}+119x^{251}+76x^{250}+195x^{249}+74x^{248}+216x^{247}+134x^{246}+$$
$$+206x^{245}+24x^{244}+62x^{243}+174x^{242}+214x^{241}+158x^{240}+111x^{239}+228x^{238}+199x^{237}+234x^{236}+$$
$$+84x^{235}+164x^{234}+109x^{233}+174x^{232}+134x^{231}+47x^{230}+85x^{229}+182x^{228}+146x^{227}+93x^{226}+$$
$$+189x^{225}+254x^{224}+194x^{223}+205x^{222}+2x^{221}+240x^{220}+7x^{219}+166x^{218}+231x^{217}+134x^{216}+$$
$$+251x^{215}+78x^{214}+146x^{213}+204x^{212}+29x^{211}+79x^{210}+91x^{209}+111x^{208}+229x^{207}+225x^{206}+$$
$$+45x^{205}+106x^{204}+121x^{203}+36x^{202}+134x^{201}+205x^{200}+65x^{199}+210x^{198}+127x^{197}+38x^{196}+$$
$$+166x^{195}+133x^{194}+22x^{193}+253x^{192}+229x^{191}+204x^{190}+148x^{189}+224x^{188}+112x^{187}+134x^{186}+$$
$$+253x^{185}+96x^{184}+240x^{183}+195x^{182}+165x^{181}+119x^{180}+167x^{179}+7x^{178}+150x^{177}+143x^{176}+$$
$$+213x^{175}+165x^{174}+113x^{173}+107x^{172}+134x^{171}+127x^{170}+213x^{169}+109x^{168}+238x^{167}+176x^{166}+$$
$$+165x^{165}+17x^{164}+105x^{163}+78x^{162}+36x^{161}+231x^{160}+81x^{159}+34x^{158}+126x^{157}+134x^{156}+$$
$$+178x^{155}+70x^{154}+24x^{153}+138x^{152}+71x^{151}+84x^{150}+115x^{149}+145x^{148}+144x^{147}+240x^{146}+$$
$$+63x^{145}+34x^{144}+15x^{143}+224x^{142}+134x^{141}+16x^{140}+249x^{139}+255x^{138}+207x^{137}+242x^{136}+$$
$$+108x^{135}+163x^{134}+182x^{133}+132x^{132}+136x^{131}+36x^{130}+155x^{129}+189x^{128}+74x^{127}+134x^{126}+$$
$$+99x^{125}+5x^{124}+251x^{123}+118x^{122}+77x^{121}+76x^{120}+38x^{119}+15x^{118}+141x^{117}+233x^{116}+$$
$$+100x^{115}+136x^{114}+155x^{113}+17x^{112}+134x^{111}+249x^{110}+147x^{109}+74x^{108}+81x^{107}+103x^{106}+$$
$$+116x^{105}+59x^{104}+74x^{103}+174x^{102}+80x^{101}+57x^{100}+172x^{99}+153x^{98}+40x^{97}+134x^{96}+93x^{95}+$$
$$+199x^{94}+147x^{93}+169x^{92}+164x^{91}+133x^{90}+60x^{89}+46x^{88}+30x^{87}+200x^{86}+7x^{85}+75x^{84}+$$
$$+185x^{83}+87x^{82}+134x^{81}+6x^{80}+196x^{79}+243x^{78}+199x^{77}+104x^{76}+87x^{75}+84x^{74}+3x^{73}+89x^{72}+$$
$$+172x^{71}+50x^{70}+150x^{69}+56x^{68}+200x^{67}+134x^{66}+165x^{65}+238x^{64}+52x^{63}+214x^{62}+193x^{61}+$$
$$+134x^{60}+166x^{59}+191x^{58}+155x^{57}+137x^{56}+110x^{55}+227x^{54}+184x^{53}+21x^{52}+134x^{51}+21x^{50}+$$
$$+227x^{49}+234x^{48}+175x^{47}+24x^{46}+111x^{45}+23x^{44}+12x^{43}+11x^{42}+180x^{41}+183x^{40}+131x^{39}+$$
$$+69x^{38}+93x^{37}+134x^{36}+81x^{35}+42x^{34}+149x^{33}+2x^{32}+146x^{31}+157x^{30}+135x^{29}+82x^{28}+74x^{27}+$$
$$+46x^{26}+227x^{25}+145x^{24}+9x^{23}+176x^{22}+134x^{21}+114x^{20}+53x^{19}+67x^{18}+36x^{17}+156x^{16}+$$
$$+190x^{15}+103x^{14}+110x^{13}+101x^{12}+89x^{11}+162x^{10}+245x^{9}+37x^{8}+85x^{7}+134x^{6}+67x^{5}+239x^{4}+$$
$$+174x^{3}+8x^{2}+65x+252.$$

Заключение

В работе предложен алгоритм, находящий минимальную степень полинома $f(x)$ в зависимости от выбора неприводимого многочлена для отображения $g : V_n(p) \to V_n(p)$, и вариация алгоритма для случая, когда отображение задано вектором функций $g_i : V_n(p) \to V(p)$, $i = 0, \ldots, n-1$. Отдельно рассмотрен случай полей характеристики два, в котором выражения для коэффициентов полинома, соответствующего отображению над векторным пространством, имеют особенно простой вид. Для нелинейных блоков замены некоторых блочных шифров вычислены минимальные степени полиномов над конечным полем и указаны неприводимые многочлены, при которых эти минимальные степени достигаются.

ЛИТЕРАТУРА

1. *Youssef A. M. and Gong G.* On the interpolation attacks on block ciphers // Intern. Workshop on Fast Software Encryption. Berlin, Heidelberg, 2000. P. 109–120.
2. *Lidl R. and Niederreiter H.* Finite Fields. Cambridge: Cambridge University Press, 1997. V. 20.
3. *McWilliams F. J. and Sloane N. J. A.* The Theory of Error-Correcting Codes. N.Y.: Elsevier, 1977.
4. *Sorenson J.* An analysis of Lehmer's Euclidean GCD algorithm // Proc. Intern. Symp. on Symbolic and Algebraic Computation. Montreal, Canada, 1995. P. 257–397.
5. *Carlet C.* Boolean functions for cryptography and error correcting codes // Y. Crama and P. Hammer (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Cambridge: Cambridge University Press, 2010. P. 257–397.
6. *Jakobsen T. and Knudsen L. R.* The interpolation attack on block ciphers // Intern. Workshop on Fast Software Encryption. Springer, 1997. P. 28–40.
7. ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. М.: Издательство стандартов, 1989.
8. *Popov V., Kurepkin I., and Leontiev S.* RFC 4357: Additional Cryptographic Algorithms for Use with GOST 28147–89, GOST R 34.10–94, GOST R 34.10–2001 and GOST R 34.11–94 Algorithms. M.: IETF, 2006.
9. *Standaert F. X., Piret G., Rouvroy G., et al.* ICEBERG: An involutional cipher efficient for block encryption in reconfigurable hardware // Intern. Workshop on Fast Software Encryption. Berlin, Heidelberg, 2004. P. 279–298.
10. *De Canniere C., Sato H., and Watanabe D.* Hash Function Luffa: Specification. Submission to NIST SHA-3 Competition. 2008. http://www.hitachi.com/rd/yrl/crypto/luffa.
11. *Sorkin A.* Lucifer, a cryptographic algorithm // Cryptologia. 1984. V. 8. No. 1. P. 22–42.
12. *Biham E., Anderson R., and Knudsen L.* Serpent: A new block cipher proposal // Intern. Workshop on Fast Software Encryption. Berlin, Heidelberg, 1998. P. 222–238.
13. *Daemen J. and Rijmen V.* The Design of Rijndael. AES — the Advanced Encryption Standard. Berlin, Heidelberg: Springer Science & Business Media, 2013.
14. *Bogdanov A., Knudsen L. R., Leander G., et al.* PRESENT: An ultra-lightweight block cipher // Intern. Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Heidelberg, 2007. P. 450—466.
15. Информационная технология. Криптографическая защита информации. Блочные шифры. М.: Стандартинформ, 2015.

REFERENCES

1. *Youssef A. M. and Gong G.* On the interpolation attacks on block ciphers. Intern. Workshop on Fast Software Encryption. Berlin, Heidelberg, 2000, pp. 109–120.
2. *Lidl R. and Niederreiter H.* Finite Fields. Cambridge, Cambridge University Press, 1997, vol. 20.
3. *McWilliams F. J. and Sloane N. J. A.* The Theory of Error-Correcting Codes. N.Y., Elsevier, 1977.
4. *Sorenson J.* An analysis of Lehmer's Euclidean GCD algorithm. Proc. Intern. Symp. on Symbolic and Algebraic Computation, Montreal, Canada, 1995, pp. 257–397.
5. *Carlet C.* Boolean functions for cryptography and error correcting codes. Y. Crama and P. Hammer (eds.). Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Cambridge, Cambridge University Press, 2010, pp. 257–397.
6. *Jakobsen T. and Knudsen L. R.* The interpolation attack on block ciphers. Intern. Workshop on Fast Software Encryption, Springer, 1997, pp. 28–40.
7. GOST 28147–89. Sistemy obrabotki informatsii. Zashchita kriptograficheskaya. Algoritm kriptograficheskogo preobrazovaniya [GOST 28147–89. Information Processing Systems. Cryptographic Protection. Algorithm of Cryptographic Transformation.] Moscow, Standards Publ., 1989. (in Russian)
8. *Popov V., Kurepkin I., and Leontiev S.* RFC 4357: Additional Cryptographic Algorithms for Use with GOST 28147–89, GOST R 34.10–94, GOST R 34.10–2001 and GOST R 34.11–94 Algorithms. Moscow, IETF, 2006.
9. *Standaert F. X., Piret G., Rouvroy G., et al.* ICEBERG: An involutional cipher efficient for block encryption in reconfigurable hardware. Intern. Workshop on Fast Software Encryption, Berlin, Heidelberg, 2004, pp. 279—298.
10. *De Canniere C., Sato H., and Watanabe D.* Hash Function Luffa: Specification. Submission to NIST SHA-3 Competition, 2008. `http://www.hitachi.com/rd/yrl/crypto/luffa`.
11. *Sorkin A.* Lucifer, a cryptographic algorithm. Cryptologia, 1984, vol. 8, no. 1, pp. 22–42.
12. *Biham E., Anderson R., and Knudsen L.* Serpent: A new block cipher proposal. Intern. Workshop on Fast Software Encryption, Berlin, Heidelberg, 1998, pp. 222–238.
13. *Daemen J. and Rijmen V.* The Design of Rijndael. AES — the Advanced Encryption Standard. Berlin, Heidelberg, Springer Science & Business Media, 2013.
14. *Bogdanov A., Knudsen L. R., Leander G., et al.*PRESENT: An ultra-lightweight block cipher. Intern. Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Heidelberg, 2007, pp. 450–466.
15. Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Blochnyye shifry.[Information Technology. Cryptographic Protection of Information. Block Ciphers.] Moscow, Standartinform Publ., 2015. (in Russian)

УДК 519.113.3

ДИСКРЕТНЫЕ ПЕРИОДИЧЕСКИЕ ФУНКЦИИ БЕРНУЛЛИ

М. С. Беспалов

Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых, г. Владимир, Россия

В пространстве дискретных периодических функций с условием нормировки (сумма значений отсчётов по периоду равна нулю) рассматриваются операции циклической свертки, конечной разности и дискретного преобразования Фурье. Приводится обзор свойств дискретных периодических функций Бернулли, выделенных в качестве основного объекта изучаемой структуры. Дискретные периодические функции Бернулли положительного порядка практически идентичны конструкции специальных чисел и многочленов, введённых М. С. Беспаловым и Н. М. Коробовым.

Ключевые слова: *дискретное преобразование Фурье, циклическая свертка, конечная разность, производящая функция, числа и многочлены Коробова.*

DOI 10.17223/20710410/43/2

BERNOULLI'S DISCRETE PERIODIC FUNCTIONS

M. S. Bespalov

Vladimir State University named after Alexander and Nikolay Stoletovs, Vladimir, Russia

E-mail: bespalov@vlsu.ru

This paper is a survey of known and some new properties of the discrete periodic Bernoulli functions $b_n(j)$ of order n introduced by V. N. Malozemov and viewed as elements $x = x(0)x(1)\dots x(N-1) \in \mathbb{C}_0^N \subset \mathbb{C}^N$ with the normalization condition $\sum\limits_{k=0}^{N-1} x(k) = 0$. It is proved that the operator $\Delta : \mathbb{C}_0^N \to \mathbb{C}_0^N$ where $\Delta[x] = y = y(0)y(1)\dots y(N-1)$, $y(k) = x(k+1) - x(k)$, is a bijection and $\Delta[b_n] = b_{n-1}$. Moreover, according to Malozemov's result, the set of the discrete periodic Bernoulli functions is an infinite cyclic group relative to the cyclic convolution $x * y(s) = \sum\limits_{j=0}^{N-1} x(j)y(s-j)$ with a neutral element b_0, and $b_n * b_m = b_{n+m}$. It is proved that either the set of $N-1$ cyclic shifts $x^{k\rightarrow}(j) = x(j-k)$ of any discrete periodic Bernoulli function or the set $\{b_m, b_{m+1}, \dots, b_{m+N-2}\}$ yields a basis of the space $\mathbb{C}_0^N$. The generating function $\sum\limits_{n=0}^{\infty} b_n t^n$ of a sequence of discrete periodic Bernoulli functions is calculated. Formulas $\sum\limits_{k=1}^{N-1} \sin^{2m}(\pi k/N)$, $m \in \mathbb{Z}$, for calculating the sums of even degrees of sinuses at equidistant nodes of a circle are found by means of these functions and the discrete Fourier transform. It has been established that a cyclic shift by 1 and the multiplication by $-N$ transform these functions of positive order into special polynomials $P_n(k)$, which were introduced by Bespalov and Korobov and have become popular as the Korobov polynomials of the first kind in the form $K_n(x) = n!P_n(x)$.

We have calculated the Korobov numbers $K_n = -n! \cdot N \cdot b_n(1)$ up to K_{13} and the Korobov polynomials up to $K_7(x)$ for any array size (parameter) N.

Keywords: *discrete Fourier transform, cyclic convolution,finite difference, generating function, Korobov numbers and Korobov polynomials.*

Введение

Дискретные периодические функции Бернулли (далее именуются как *сигналы Бернулли*) введены в [1] и изучались в отдельных докладах семинара «Дискретный гармонический анализ и геометрическое моделирование» [2]. Полученные для них результаты собраны в учебном пособии [3]. Представление B-сплайнов на сетке через сигналы Бернулли предложено в [4]. Конструкция сигналов Бернулли положительного порядка практически идентична конструкции специальных чисел и многочленов, введённых в [5, 6] и ставших популярными (после публикации работ А. В. Устинова [7, 8]) в виде чисел и многочленов Коробова. Предложенное в [1] название объясняется тем, что дискретные периодические функции Бернулли служат аналогом на сетке чисел и многочленов Бернулли.

Приведённый в данной работе обзор свойств сигналов Бернулли предваряется напоминанием свойств чисел и многочленов Бернулли, описанием пространства сигналов и операций в нём. В качестве практического применения сигналов Бернулли приведён способ вычисления через них тригонометрических сумм, в п. 6 указана связь сигналов Бернулли с позднее введёнными числами и многочленами Коробова.

1. Числа и многочлены Бернулли

Числа Бернулли B_k вычисляются по рекуррентной формуле

$$\sum_{k=0}^{n-1} \mathrm{C}_n^k B_k = 0, \tag{1}$$

где $\mathrm{C}_n^k = \dfrac{n!}{k!(n-k)!}$, с начальным условием $B_0 = 1$. В частности, $B_1 = -1/2$, $B_2 = 1/6$, $B_3 = 0$, $B_4 = -1/30$. Все числа Бернулли с нечётными номерами, кроме B_1, равны нулю.

Многочлены Бернулли определяются через их разложение по степеням x, где участвуют числа Бернулли:

$$B_n(x) = \sum_{k=0}^{n} \mathrm{C}_n^k B_k x^{n-k}. \tag{2}$$

В частности, $B_0(x) \equiv 1$, $B_1(x) = x - \dfrac{1}{2}$, $B_2(x) = x^2 - x + \dfrac{1}{6}$, $B_3(x) = x^3 - \dfrac{3}{2}x^2 + \dfrac{1}{2}x$. Из (2) вытекает, что $B_n = B_n(0)$.

Приведём отдельные свойства многочленов Бернулли:

$$B_n(1-x) = (-1)^n B_n(x) \quad \text{— теорема дополнения;} \tag{3}$$

$$B_n(x+y) = \sum_{k=0}^{n} \mathrm{C}_n^k B_k(y) x^{n-k} \quad \text{— теорема сложения аргументов;} \tag{4}$$

$$B_n'(x) = nB_{n-1}(x);$$

$$\int_0^1 B_n(x)\, dx = 0 \quad \text{— нормировка;} \tag{5}$$

$$B_n(x+1) - B_n(x) = nx^{n-1} \quad \text{— вычисление конечной разности.}$$

В последнее время более удобным считается [8] определение чисел и многочленов Бернулли через экспоненциальную производящую функцию:

$$\frac{t}{e^t-1}=\sum_{n=0}^{\infty}\frac{B_n}{n!}t^n, \qquad \frac{te^{tx}}{e^t-1}=\sum_{n=0}^{\infty}\frac{B_n(x)}{n!}t^n.$$

2. Пространство сигналов

Основной класс *дискретных функций* — функции, заданные на множестве целых чисел $\mathbb{Z}$, то есть двусторонние последовательности. При цифровой обработке сигналов (ЦОС) рассматривают *дискретные периодические* (с периодом N: $x(k+N)=x(k)$) *функции*, которые для сокращения записи будем называть *сигналами*. Пространство (периодических) сигналов обозначим $\mathbb{C}^N$, выделяя основную часть сигнала $x\in\mathbb{C}^N$ вида $x=(x(0)\;x(1)\ldots x(N-1))$.

Матрицу *прямого дискретного преобразования Фурье* (ДПФ) порядка N определим поэлементно (далее N фиксируем)

$$F=F_N=(\omega^{-kj})_{k,j=0}^{N-1}, \tag{6}$$

где $\omega=\omega_N=\exp(2\pi i/N)$. При ЦОС исходный сигнал x преобразуется линейным оператором (6) в выходной сигнал (*спектр Фурье* сигнала x): $y=x\cdot F$; перепишем его в развернутом виде

$$y(s)=\sum_{j=0}^{N-1}x(j)\omega^{-sj}, \tag{7}$$

откуда вытекает периодичность сигнала y.

Оператор *обратного дискретного преобразования Фурье* определяется комплексно-сопряжённой матрицей $\overline{F_N}$:

$$F^{-1}=\frac{1}{N}\cdot\overline{F_N}=\frac{1}{N}(\omega^{kj})_{k,j=0}^{N-1}\,. \tag{8}$$

Операторная запись для (7): $y=\mathcal{F}[x]$; для восстановления: $x=\mathcal{F}^{-1}[y]$.

Другие основные операции над $x,y\in\mathbb{C}^N$:

1) линейные операции — сложение сигналов и умножение на число;
2) умножение сигналов в виде покоординатного умножения

$$x\circ y=(x(0)\cdot y(0)\quad x(1)\cdot y(1)\;\ldots\;x(N-1)\cdot y(N-1));$$

3) циклическая свертка

$$x*y\;(s)=\sum_{j=0}^{N-1}x(j)y(s-j)\;,\quad s\in\mathbb{Z};$$

4) циклический сдвиг (вправо): $x^{k\to}(j)=x(j-k)$,
   в частности, $x^{N\to}=x$, а $x^{N-1\to}=x^{\leftarrow}$ — операция обратного сдвига;
5) конечная разность Δ сигнала $x\in\mathbb{C}^N$:

$$\Delta[x](j)=x(j+1)-x(j).$$

Для второй операции использован известный [9] знак $\circ$ операции *умножения по Адамару* (покоординатного умножения) векторов.

Строки матриц F, $\overline{F}$ называются [10] *дискретными экспоненциальными функциями* (ДЭФ). Основную ДЭФ обозначим $r = (1\ \omega\ \omega^2\ \ldots \omega^{N-1}\ )$. Остальные ДЭФ (в матричной форме) следующие:

$$r^{2\circ} = r \circ r,\ r^{3\circ} = r^{2\circ} \circ r,\ r^{4\circ}, \ldots, r^{N-1\circ},\ r^{N\circ} = r^{0\circ},$$

где знак операции в показателе принято опускать. В матрице (6) ДЭФ следуют в порядке $r^0, r^{N-1}, r^{N-2}, \ldots, r^2, r$, а в матрице (8) — по возрастанию степени. Вместо обозначения $r^{0\circ}$ будем использовать символ $\mathbf{1}$ для *основного постоянного сигнала*: $\mathbf{1} = (11\ldots1)$. К основным сигналам относят *единичный импульс* $\delta = \delta_N = (1000\ldots0)$.

Двуместные операции $\circ$ и $*$ коммутативны, ассоциативны и дистрибутивны, в пространстве $\mathbb{C}^N$ обладают нейтральными элементами $\mathbf{1}$ и δ соответственно. Приведённые операции линейны.

В пространстве $\mathbb{C}^N$ введём норму $\|x\| = \sqrt{\sum\limits_{k=0}^{N-1} |x(k)|^2}$.

Утверждение 1. В обозначениях $X = \mathcal{F}[x]$, $Y = \mathcal{F}[y]$ имеем

$$\mathcal{F}[x * y] = X \circ Y, \qquad N\mathcal{F}[x \circ y] = X * Y;$$

выполняется равенство Парсеваля

$$N\|x\|^2 = \|X\|^2.$$

Это утверждение (см. доказательство в [3]) и следующие две леммы легко проверяются.

Далее рассмотрим подпространство $\mathbb{C}_0^N$ пространства $\mathbb{C}^N$, состоящее из сигналов $x \in \mathbb{C}^N$, удовлетворяющих *условию нормировки* (аналог (5)):

$$\sum_{k=0}^{N-1} x(k) = 0. \tag{9}$$

Лемма 1. Приведённые операции, за исключением умножения сигналов $\circ$ и ДПФ, замкнуты в пространстве $\mathbb{C}_0^N$.

Лемма 2. В структуре $(\mathbb{C}_0^N; *)$ единственный нейтральный элемент $\left(\delta - \dfrac{1}{N}\mathbf{1}\right)$.

Лемма 3. Если $b \in \mathbb{C}_0^N$, то решение $x \in \mathbb{C}_0^N$ разностного уравнения $\Delta[x] = b$ единственно.

Доказательство. Приведём алгоритм вычисления $x \in \mathbb{C}_0^N$. Полагаем $x(0) = C$, не определяя пока C. Уравнение $\Delta[x] = b$ перепишем в виде $x(j) = x(j-1) + b(j-1)$, откуда вытекает, что $x(j) = C + b(0) + b(1) + \ldots + b(j-1)$ для j от 1 до $N-1$. По условию нормировки (9) составляем уравнение

$$NC + \sum_{j=0}^{N-2} (N-j-1)b(j) = 0, \tag{10}$$

позволяющее однозначно вычислить C, через которое восстанавливаем все отсчёты сигнала x. ∎

Итак, в классе сигналов $\mathbb{C}_0^N$ определена обратная к операции вычисления конечной разности операция $\Delta^{-1} : \mathbb{C}_0^N \to \mathbb{C}_0^N$.

Выделим возможные специальные виды сигналов класса $\mathbb{C}_0^N$. Сигнал x назовём *симметричным* с центром в m и обозначим $x \in S(m)$, если $x(m-k) = x(m+k)$ для всех $k \in \mathbb{Z}$. Аналогично, если $x(m-k) = x(m+k+1)$, то $x \in S(m+1/2)$. Сигнал x назовём *антисимметричным* с центром в m и обозначим $x \in AS(m)$, если $x(m-k) = -x(m+k)$ для всех $k \in \mathbb{Z}$. Аналогично, $x \in AS(m+1/2)$, если имеем $x(m-k) = -x(m+k+1)$.

За счёт периодичности сигнала его центры повторяются через $N/2$: $x \in S(m)$ влечёт $x \in S(m \pm N/2)$ и т. д.

Утверждение 2. Пусть $x \in \mathbb{C}_0^N$, $t = n/2$ при $n \in \mathbb{Z}$.
Если $x \in S(t)$, то $\Delta[x] \in AS\,(t-1/2)$, $\Delta^{-1}[x] \in AS\,(t+1/2)$.
Если $x \in AS(t)$, то $\Delta[x] \in S\,(t-1/2)$, $\Delta^{-1}[x] \in S\,(t+1/2)$.

Доказательство, которое можно провести проверкой всех восьми случаев отдельно (хотя явно выписаны четыре случая, помним, что t может быть целым или дробным), продемонстрируем на примере одного из более сложных случаев.

Пусть $x \in S(0)$, $y = \Delta^{-1}[x]$. Предложим $y(0) = -x(0)/2$ как вариант начального значения. Формула $y(j+1) = y(j) + x(j)$ из леммы 3 допускает обращение в виде $y(j-1) = y(j) - x(j-1)$. По этим формулам: $y(k) = x(0)/2 + x(1) + x(2) + \ldots + x(k-1)$, $y(1-k) = -y(k)$ при $k = 2, 3, \ldots, (N+1)/2$ и $y(1) = x(0)/2$, что влечёт $y \in AS(1/2)$. Осталось доказать справедливость условия нормировки (9) для построенного y, что означает верность выбора начального значения $y(0)$.

Если N чётное, то условие (9) выполняется автоматически. Пусть N нечётное. Получили, что

$$y\left((N+1)/2\right) = x(0)/2 + x(1) + x(2) + \ldots + x\left((N+1)/2 - 1\right) \tag{11}$$

и $y((N+1)/2) = -y(1-(N+1)/2)$. По условию периодичности $y((N+1)/2) = {}$ $= y(1-(N+1)/2)$. Значит, должно быть $y((N+1)/2) = 0$. Проверим — так ли это? При $x \in S(0)$ имеем $x \in S(N/2)$, что влечёт $y((N+1)/2) = x(N-1) + \ldots +$ $+ x((N+1)/2) + x(N)/2$ из (11). Сложим эти два представления: $2y(N+1)/2) =$ $= \sum\limits_{k=0}^{N-1} x(k) = 0$ по условию $x \in \mathbb{C}_0^N$.

Ввиду периодичности считаем, что доказан случай

$$x \in S(m) \Rightarrow \Delta^{-1}[x] \in AS\,(m+1/2)\,.$$

3. Сигналы Бернулли

Основным представителем класса $\mathbb{C}_0^N$ служат *дискретные периодические функции Бернулли* [3, с. 171] порядка s, координаты которых определяются равенством

$$b_s(j) = \frac{1}{N}\sum_{k=1}^{N-1} (\omega^k - 1)^{-s} \cdot \omega^{kj}, \qquad s, j \in \mathbb{Z},\ \omega = \exp\left(\frac{2\pi i}{N}\right). \tag{12}$$

Будем называть их короче — *сигналами Бернулли* порядка s (периода N, где N считаем фиксированным). В частности, начальный сигнал Бернулли (для наглядности добавили разделительные запятые)

$$b_0 = \delta - \frac{1}{N}\mathbf{1} = \frac{1}{N}\left(N-1, -1, -1, \ldots, -1\right).$$

По свойствам корней N-й степени из единицы

$$\sum_{k=0}^{N-1} \omega^{kj} = 0 \quad \text{при всех } 1 \leqslant j < N, \qquad \sum_{k=0}^{N-1} \omega^{kN} = N \tag{13}$$

проверяется указанный вид b_0, принадлежность всех ДЭФ (кроме $\mathbf{1}$) пространству $\mathbb{C}_0^N$ и следующая лемма.

Лемма 4. Для сигналов Бернулли любого целого порядка $b_s \in \mathbb{C}_0^N$.

Лемма 5. Для сигналов Бернулли $b_s = \Delta[b_{s+1}]$ и $b_{s+1} = \Delta^{-1}[b_s]$.

Доказательство. Вычислим координаты сигнала

$$\Delta[b_{s+1}](j) = \frac{1}{N}\sum_{k=1}^{N-1}(\omega^k - 1)^{-(s+1)}\omega^{k(j+1)} - \frac{1}{N}\sum_{k=1}^{N-1}(\omega^k - 1)^{-(s+1)}\omega^{kj} =$$
$$= \frac{1}{N}\sum_{k=1}^{N-1}(\omega^k - 1)^{-(s+1)}\omega^{kj}(\omega^k - 1) = b_s(j).$$

По лемме 3 получаем второе утверждение леммы 5. ■

Замечание 1. В качестве альтернативного определения сигналов Бернулли можно предложить формулу $b_0 = \delta - \dfrac{1}{N}\mathbf{1}$ для сигнала Бернулли нулевого порядка и соотношения леммы 5.

Следствие 1. Для сдвига сигнала Бернулли верно $b_s^{\leftarrow} = b_s + b_{s-1}$.

Доказательство. В координатах доказанная формула $b_{s-1} = \Delta[b_s]$ выглядит так: $b_{s-1}(j) = b_s(j+1) - b_s(j)$ или $b_s(j+1) = b_s(j) + b_{s-1}(j)$. ■

Следствие 2. Отсчёты всех сигналов Бернулли вещественные. Более того, отсчёты всех сигналов Бернулли отрицательного порядка и координаты векторов $N^{k+1} \cdot b_k$ при неотрицательных k — целые числа.

Доказательство. Имеем $b_{-1} = \Delta[b_0] = (-1\ 0\ 0 \ldots\ 0\ 0\ 1)$. Так как отсчёты b_{-1} целые, то по лемме 5 получаем, что отсчёты каждого следующего сигнала Бернулли отрицательного порядка целые.

Координаты вектора $N \cdot b_0 = N\delta - \mathbf{1}$ суть целые числа. Для сигналов Бернулли следующих (больших) порядков, согласно формуле $b_{s+1} = \Delta^{-1}[b_s]$, вычисляем координаты по алгоритму леммы 3, решая при этом уравнение (10) для C и накапливая множитель N в знаменателе. ■

Утверждение 3. При $k \leqslant N$ имеет место следующее представление для сдвигов сигнала Бернулли: $b_{s+k}^{k\leftarrow} = \sum\limits_{m=0}^{k} \mathrm{C}_k^m b_{s+m}$. В частности, при $k = N$ получаем аналог формулы (1), который справедлив лишь для N, равного размеру сетки:

$$\sum_{m=0}^{N-1} \mathrm{C}_N^m b_{s+m} = 0. \tag{14}$$

Доказательство. Применив формулу $b_{s+1}^{\leftarrow} = b_{s+1} + b_s$ следствия 1 трижды, получаем базу индукции

$$b_{s+2}^{2\leftarrow} = b_{s+2}^{\leftarrow} + b_{s+1}^{\leftarrow} = b_{s+2} + b_{s+1} + b_{s+1} + b_s.$$

Аналогично доказываем индуктивный переход от $k-1$ к случаю k:

$$b^{k\leftarrow}_{s+k} = b^{(k-1)\leftarrow}_{s+1+k-1} + b^{(k-1)\leftarrow}_{s+k-1} = \sum_{m=0}^{k-1} \mathrm{C}^m_{k-1} b_{s+1+m} + \sum_{m=0}^{k-1} \mathrm{C}^m_{k-1} b_{s+m} =$$
$$= \sum_{j=1}^{k} \mathrm{C}^{j-1}_{k-1} b_{s+j} + \sum_{j=0}^{k-1} \mathrm{C}^{j}_{k-1} b_{s+j} = \sum_{j=0}^{k} \mathrm{C}^{j}_{k} b_{s+j},$$

где применили известное свойство биномиальных коэффициентов

$$\mathrm{C}^{j-1}_{k-1} + \mathrm{C}^{j}_{k-1} = \mathrm{C}^{j}_{k}. \tag{15}$$

Формула (14) вытекает из равенства $b^{N\leftarrow} = b$ для $b \in \mathbb{C}^N$. ■

Замечание 2. Формулу (14) при небольших N можно использовать как следующий рекуррентный способ вычисления значений сигналов Бернулли:

$$b_s = -\frac{1}{N} \sum_{k=1}^{N-1} \mathrm{C}^{k+1}_{N} b_{s-k}.$$

В частности, $b_s = -\dfrac{1}{2} b_{s-1}$ при $N = 2$, $b_s = -b_{s-1} - \dfrac{1}{3} b_{s-2}$ при $N = 3$ и т. д.

Следствие 3 (теорема сложения аргументов, аналог (4)). При $k \geqslant 0$ верно

$$b_n(j+k) = \sum_{l=0}^{k} \mathrm{C}^{l}_{k} b_{n-l}(j).$$

Замечание 3. В следствии 2 приведено утверждение о целочисленности отсчётов сигналов $N^{k+1} b_k$, которое довольно грубое. Анализ биномиальных коэффициентов в соотношении линейной зависимости (14) позволяет получить следующее утверждение:

Если $N = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, где p_j, $j = 1, \dots, k$, — простые числа, $n \geqslant 0$, то отсчёты сигналов

$$N p_1^{[\frac{n}{p_1-1}]} p_2^{[\frac{n}{p_2-1}]} \dots p_k^{[\frac{n}{p_k-1}]} b_n$$

целочисленные. Доказательство не приводим из-за его громоздкости.

Лемма 6. Дискретное преобразование Фурье сигналов Бернулли имеет вид

$$\mathcal{F}[b_n](0) = 0, \quad \mathcal{F}[b_n](j) = (\omega^j - 1)^{-n} \quad \text{при } j = 1, 2, \dots, N-1,$$

что короче записывается при $n \in \mathbb{N}$ двумя формулами:

$$\mathcal{F}[b_{-n}] = (r - \mathbf{1})^n \quad \text{и условно } \mathcal{F}[b_n] = (r - \mathbf{1})^{-n}.$$

Доказательство. По лемме 4 имеем $\mathcal{F}[b_n](0) = 0$. Для остальных отсчётов

$$\mathcal{F}[b_n](j) = \sum_{s=0}^{N-1} \frac{1}{N} \sum_{k=1}^{N-1} (\omega^k - 1)^{-n} \omega^{ks} \omega^{-sj} = \frac{1}{N} \sum_{k=1}^{N-1} (\omega^k - 1)^{-n} \sum_{s=0}^{N-1} \omega^{(k-j)s}.$$

Применяя (13), получаем $\mathcal{F}[b_n](j) = (\omega^j - 1)^{-n}$. ■

Следующее свойство сигналов Бернулли первым, по-видимому, отметил В. Н. Малоземов.

Теорема 1. Циклическая свертка сигналов Бернулли равна соответствующему сигналу Бернулли:

$$b_n * b_m = b_{n+m}.$$

Доказательство. Первый способ — проверяем непосредственно:

$$(b_n * b_m)(j) = \sum_{s=0}^{N-1} \frac{1}{N^2} \sum_{k=1}^{N-1} (\omega^k - 1)^{-n} \omega^{sk} \sum_{l=1}^{N-1} (\omega^l - 1)^{-m} \omega^{(j-s)l} =$$
$$= \frac{1}{N^2} \sum_{k=1}^{N-1} (\omega^k - 1)^{-n} \sum_{l=1}^{N-1} (\omega^l - 1)^{-m} \omega^{jl} \sum_{s=0}^{N-1} \omega^{s(k-l)}.$$

Продолжаем по формуле (13):

$$(b_n * b_m)(j) = \frac{1}{N} \sum_{k=1}^{N-1} (\omega^k - 1)^{-n} (\omega^k - 1)^{-m} \omega^{jk} = b_{n+m}(j).$$

Второй способ — через ДПФ. По утверждению 1 и лемме 6 с учётом того, что нулевой отсчёт всех спектров Фурье равен нулю, получаем

$$\mathcal{F}[b_n * b_m] = \mathcal{F}[b_n] \circ \mathcal{F}[b_m] = (r - \mathbf{1})^{-n} \circ (r - \mathbf{1})^{-m} = \mathcal{F}[b_{n+m}].$$

Теорема доказана. ■

Есть третий (более длинный) способ доказательства через итерации операторов Δ и Δ^{-1}. Его укажем в виде следствия теоремы.

Следствие 4. Для любого $m \in \mathbb{Z}$ конечная разность всех порядков и её обращение для $x \in \mathbb{C}_0^N$ представима как

$$\Delta^m[x] = b_{-m} * x.$$

Эту формулу можно переписать в виде $x = \Delta^m[x] * b_m$, полученным в [1] и применённым в [4] для анализа B-сплайнов.

Следствие 5. Сигнал Бернулли любого порядка есть соответствующая степень образующего сигнала b_1:

$$b_n = b_1^{n*}, \quad \text{где } n \in \mathbb{Z}.$$

Лемма 7 (аналог теоремы дополнения (3)). Для сигналов Бернулли верно

$$b_m(m - j) = (-1)^m b_m(j).$$

Доказательство. По определению (12) и условию $\omega^N = 1$ имеем

$$b_m(m-j) = \frac{1}{N} \sum_{k=1}^{N-1} (\omega^k - 1)^{-m} \omega^{k(m-j)} = \frac{1}{N} \sum_{k=1}^{N-1} (1 - \omega^{-k})^{-m} \omega^{-kj} =$$
$$= \frac{1}{N} \sum_{k=1}^{N-1} (1 - \omega^{N-k})^{-m} \omega^{(N-k)j} = \frac{1}{N} \sum_{k=1}^{N-1} (1 - \omega^k)^{-m} \omega^{kj} = (-1)^m b_m(j).$$

Лемма доказана. ■

Из утверждения 2 вытекает

Утверждение 4 (свойство симметрии, антисимметрии). Сигнал Бернулли чётного порядка симметричен, нечётного — антисимметричен:

$$b_{2m} \in S(m), \quad b_{2m+1} \in AS\,(m+1/2)\,.$$

Следствие 6. Для отдельных отсчётов верно $b_1(0) = -\dfrac{N-1}{2N}$ и $b_1(1) = \dfrac{N-1}{2N}$. Для остальных отсчётов $b_1(1+k) = \dfrac{N-1-2k}{2N}$.

Доказательство. Имеем $b_0 \in S(0)$, $b_1 \in AS(1/2)$, $b_0(0) = \dfrac{N-1}{N}$; обозначим $2C = \dfrac{N-1}{N}$. Тогда $b_1(0) = -C$ и $b_1(1) = C$; далее по лемме 3. ■

При $1 \leqslant k < N$ следующая формула для b_{-k} даёт явный вид начальных отрицательных сигналов Бернулли в виде сдвинутого набора биномиальных коэффициентов с чередующимися знаками. Её частные случаи:

$$b_{-1} = (-1\;0\;0\ldots\;0\;0\;1), \quad b_{-2} = (1\;0\;0\ldots\;0\;0\;1\;\;-2),$$
$$b_{-3} = (-1\;0\;\ldots\;0\;1\;\;-3\;3), \quad b_{-4} = (1\;0\;\ldots\;0\;1\;\;-4\;6\;\;-4) \quad \text{и т. д.}$$

Утверждение 5. Для сигналов Бернулли отрицательного порядка имеет место

$$b_{-k} = \sum_{j=0}^{k} (-1)^j \mathrm{C}_k^j \delta^{(k-j)\leftarrow}; \tag{16}$$

$$\|b_{-k}\|^2 = \frac{4^k(2k-1)!!}{(2k)!!}. \tag{17}$$

Доказательство. Следствие 1 влечёт базу индукции для (16):

$$b_{-1} = b_0^{\leftarrow} - b_0 = \delta^{\leftarrow} - \delta - \frac{1}{N}(\mathbf{1}^{\leftarrow} - \mathbf{1}) = \delta^{\leftarrow} - \delta, \quad b_{-2} = b_{-1}^{\leftarrow} - b_{-1} = \delta^{2\leftarrow} - 2\delta^{\leftarrow} + \delta.$$

Индуктивный переход (во второй сумме заменяем $s = j+1$, переобозначаем символом j и применяем (15)):

$$b_{-k} = b_{-k+1}^{\leftarrow} - b_{-k+1} = \sum_{j=0}^{k-1} (-1)^j \mathrm{C}_{k-1}^j \delta^{(k-j)\leftarrow} - \sum_{j=0}^{k-1} (-1)^j \mathrm{C}_{k-1}^j \delta^{(k-1-j)\leftarrow} =$$
$$= \delta^{k\leftarrow} + \sum_{j=1}^{k-1} (-1)^j (\mathrm{C}_{k-1}^j + \mathrm{C}_{k-1}^{j-1}) \delta^{(k-j)\leftarrow} + (-1)^k \delta = \sum_{j=0}^{k} (-1)^j \mathrm{C}_k^j \delta^{(k-j)\leftarrow}.$$

Из (16) вытекает приведённый явный вид сигналов и квадрат нормы:

$$\|b_{-k}\|^2 = \sum_{j=0}^{k} \left(\mathrm{C}_k^j\right)^2.$$

По тождеству Вандермонда [11, с. 27]

$$\sum_{j=0}^{k} \left(\mathrm{C}_k^j\right)^2 = \mathrm{C}_{2k}^k = \frac{(2k)!}{(k!)^2} = \frac{(2k)!!(2k-1)!!}{(k!)(k!)} = \frac{2^k(2k-1)!!}{k!} = \frac{4^k(2k-1)!!}{(2k)!!}.$$

Утверждение доказано. ■

Следствие 7. Набор из $N-1$ сигналов Бернулли подряд идущих порядков составляет базис пространства $\mathbb{C}_0^N$.

Доказательство. Подпространство $\mathbb{C}_0^N$ N-мерного пространства $\mathbb{C}^N$ имеет размерность $N-1$. Если отсчёты с номером 0 временно удалим, как допускающие восстановление по свойству нормировки (9), то заметим, что векторы $b_{-1}, b_{-2}, \ldots, b_{-N+1}$ линейно независимы, как обладающие диагональной структурой. Значит, они составляют базис пространства $\mathbb{C}_0^N$. По формуле (14) линейной зависимости этот базис можно сдвигать на одну позицию в любую сторону. ■

Замечание 4. Очевидно, что для любого $x \in \mathbb{C}_0^N$ полный набор его сдвигов линейно зависим: $\sum\limits_{k=0}^{N-1} x^{k\to} = 0$. Зато набор из $(N-1)$-го сдвига любого сигнала Бернулли составляет базис пространства $\mathbb{C}_0^N$. Для сигнала Бернулли порядка -1 это легко проверяется, а далее доказывается по лемме 3.

Рассмотрим простейшие частные случаи сигналов Бернулли.

С л у ч а й $N=2$. Пространство $\mathbb{C}_0^2$ одномерно и при всех целых s

$$b_s = \frac{(-1)^s}{2^{s+1}}\,(1\ \ -1) = \left(-\frac{1}{2}\right)^s b_0.$$

С л у ч а й $N=3$. Пространство $\mathbb{C}_0^3$ двумерно с базисом

$$b_0 = \frac{1}{3}(2\ \ -1\ \ -1) \quad \text{и} \quad b_{-1} = (-1\ 0\ 1)$$

и соотношением $b_{k+2} = -\dfrac{1}{3} b_k^{\to}$.

С л у ч а й $N=4$. Хотя пространство $\mathbb{C}_0^4$ трёхмерно, сигналы Бернулли группируются не по тройкам, а по парам (чётные и нечётные порядки), а именно (отделили координаты запятыми):

$$b_{2s} = \frac{(-1)^s}{2^{2s+2}}\left(2^{s+1}+1,\ \ -1,\ \ -2^{s+1}+1,\ \ -1\right)^{s\to},$$

$$b_{2s-1} = \frac{(-1)^{s-1}}{2^{2s+1}}\left(2^s+1,\ \ 2^s-1,\ \ -2^s+1,\ \ -2^s-1\right)^{s\to}.$$

Для остальных N общих формул представления всех сигналов Бернулли нет.

По теореме 1 в кольце $(\mathbb{C}_0^N; +, *)$ легко вычисляется обратный элемент к сигналам Бернулли. Для произвольного обратимого $x \in \mathbb{C}_0^N$ есть две стандартные схемы вычисления обратного, то есть такого $y \in \mathbb{C}_0^N$, что $x * y = b_0$. Один приём «в лоб» методом неопределённых коэффициентов — составление и решение системы N-го порядка. С использованием циркулянтной матрицы $C(x)$ для сигнала x (её определение см. в [9, с. 40]) уравнение записывается в матричном виде $y \cdot C(x) = b_0$.

Второй приём покажем на примере сигнала $x = (1, 0, 3, -4)$. Вычислим ДПФ от него: $X = \mathcal{F}[x] = (0, -2-4i, 8, -2+4i)$. Найдём Y, такой, что $X \circ Y = \mathbf{1} - \delta = (0, 1, 1, 1)$: $Y = \left(0, \dfrac{-1+2i}{10}, \dfrac{1}{8}, \dfrac{-1-2i}{10}\right)$. Через обратное ДПФ от Y найдём искомый $y = \dfrac{1}{160}(-3, -21, 13, 11)$.

Предложим третий приём. Произвольный $x \in \mathbb{C}_0^N$ легко раскладывается по базису $\{b_{-1}, b_{-2}, \ldots, b_{-N+1}\}$. В случае $x = (1, 0, 3, -4)$ имеем $x = 2b_{-1} + 3b_{-2}$. Искомый $y \in \mathbb{C}_0^4$, такой, что $x * y = b_0$, будем искать в сдвинутом базисе в виде $y = \alpha b_1 + \beta b_0 + \gamma b_{-1}$. По линейности циклической свертки и теореме 1 имеем

$$x * y = 2\alpha b_0 + (3\alpha + 2\beta) b_{-1} + (3\beta + 2\gamma) b_{-2} + 3\gamma b_{-3}.$$

Здесь на помощь приходит соотношение (14) линейной зависимости, которое добавим с некоторым неопределённым коэффициентом s:

$$x * y = b_0 + s(4b_0 + 6b_{-1} + 4b_{-2} + b_{-3}).$$

Приравняв коэффициенты, получаем систему, которая решается последовательно:

$$\gamma = \frac{s}{3},\ \beta = \frac{10}{9}s,\ \alpha = \frac{34}{27}s,\ s = -\frac{27}{40} \quad \to \quad \alpha = -\frac{17}{20},\ \beta = -\frac{3}{4},\ \gamma = -\frac{9}{40}.$$

При $N \geqslant 5$ первые два приёма слишком сложны для использования без привлечения компьютера, а с помощью третьего можно решать и вручную.

4. Производящая функция сигналов Бернулли

Производящей функцией последовательности $a = \{a_k\}_{k=0}^{\infty}$ называется [11]

$$\varphi(x) = \sum_{k=0}^{\infty} a_k x^k.$$

Введём производящие функции для N отсчётов последовательности сигналов Бернулли (12) неотрицательного порядка:

$$\varphi_k(x) = \sum_{s=0}^{\infty} b_s(k) x^s, \quad k = 0, 1, \ldots, N-1.$$

Теорема 2. Производящая вектор-функция $\Phi(x) = \sum\limits_{s=0}^{\infty} b_s x^s$ для всех отсчётов сигналов Бернулли неотрицательного порядка равна

$$\Phi(x) = \delta + \varphi(x; N)\left((1+x)^{N-1}, 1, (1+x), (1+x)^2, \ldots, (1+x)^{N-2}\right),$$

где $\varphi(x; N) = \dfrac{x}{1-(1+x)^N}$.

Доказательство. По формуле $b_s(k) = b_s(k-1) + b_{s-1}(k-1)$ из следствия 1 имеем

$$\varphi_k(x) = b_0(k) + \sum_{s=1}^{\infty} b_s(k) x^s = b_0(k) + \sum_{s=1}^{\infty} (b_s(k-1)x^s + b_{s-1}(k-1)x^s).$$

При $2 \leqslant k \leqslant N-1$ получим

$$\varphi_k(x) = -\frac{1}{N} + \sum_{s=1}^{\infty} b_s(k-1)x^s + x\sum_{s=0}^{\infty} b_s(k-1)x^s = \varphi_{k-1}(x) + x\varphi_{k-1}(x).$$

Небольшое отличие при $k = 1$ и $k = N$:

$$\varphi_1(x) = b_0(1) + \sum_{s=1}^{\infty} (b_s(0)x^s + b_{s-1}(0)x^s) = b_0(1) - b_0(0) + (1+x)\varphi_0(x),$$
$$\varphi_N(x) = b_0(N) - b_0(N-1) + (1+x)\varphi_{N-1}(x).$$

Получили формулы

$$\varphi_1(x) = -1 + (1+x)\varphi_0(x), \quad \varphi_0(x) = \varphi_N(x) = 1 + (1+x)\varphi_{N-1}(x).$$

Выразим все рассмотренные производящие функции через одну:

$$\varphi_k(x) = (1+x)^{k-1}\varphi_1(x) \quad \text{при } 1 \leqslant k \leqslant N-1,$$
$$\varphi_0(x) = \frac{1+\varphi_1(x)}{x+1}, \quad \varphi_0(x) = 1 + (1+x)^{N-1}\varphi_1(x).$$

Приравняв две последние, получим

$$\varphi(x;N) = \varphi_1(x) = \frac{x}{1-(1+x)^N}.$$

Теорема доказана. ■

Следствие 8. Отсчёт сигналов Бернулли с номером 1 порядков $s \geqslant 2$ как функция от размера сетки N есть многочлен нечётного порядка; гарантируется, что среди его корней присутствуют корни $N = \pm 1$.

Доказательство. Для $\varphi(x;N) = \varphi_1(x) = \dfrac{x}{1-(1+x)^N}$ вычислим

$$\varphi(x;-N) = \frac{x}{1-(1+x)^{-N}} = x - \varphi(x;N),$$

что влечёт первое утверждение. Более того, из доказательства следствия 2 вытекает наличие N в знаменателях всех отсчётов сигналов Бернулли положительного порядка.

Рассмотрим величины $-Nb_s(1)$ как чётные многочлены степени s от переменной N. Из условия $\varphi(x;1) = -1$ вытекает, что при $s \geqslant 2$ числа $N = \pm 1$ служат корнями этого многочлена. ■

5. Тригонометрические суммы

Через производящую функцию теоремы 2, взятую в виде $-N\varphi(x;N)$, в [5, 12] вычисляются суммы чётных отрицательных степеней синусов в равноотстоящих узлах окружности. В. Н. Малоземов в [2] предложил более красивое изложение этих результатов с распространением на положительные степени. Эти суммы имеют практическое применение [13].

Теорема 3. Суммы чётных степеней синусов в равноотстоящих узлах выражаются через нормы сигналов Бернулли ($s > 0$):

$$\sum_{k=1}^{N-1} \sin^{2s}\frac{\pi k}{N} = \frac{N}{4^s}\|b_{-s}\|^2, \qquad \sum_{k=1}^{N-1} \frac{1}{\sin^{2s}(\pi k/N)} = 4^s N \|b_s\|^2.$$

В частности, при $s < N$ имеем

$$\sum_{k=1}^{N-1} \sin^{2s}\tfrac{\pi k}{N} = N\,\frac{(2s-1)!!}{(2s)!!}. \tag{18}$$

Сумма $\displaystyle\sum_{k=1}^{N-1} \frac{1}{\sin^{2s}(\pi k/N)}$ при натуральном s равна чётному многочлену от N степени $2s$, содержащему множитель (N^2-1). В качестве формулы для вычисления этих многочленов предлагается

$$\sum_{k=1}^{N-1} \frac{1}{\sin^{2s}(\pi k/N)} = \frac{4^s N}{(s!)^2} \lim_{z\to 1}\lim_{t\to 1} \frac{\partial^{2s}}{\partial z^s\,\partial t^s}\left(\frac{(z-1)(t-1)((zt)^N-1)}{(z^N-1)(t^N-1)(zt-1)}\right). \tag{19}$$

Доказательство. По равенству Парсеваля (утверждение 1) $N\|b_s\|^2 = \|\mathcal{F}[b_s]\|^2$. Правую часть вычислим согласно результатам леммы 6:

$$\|\mathcal{F}[b_s]\|^2 = \|(r-\mathbf{1})^{-s}\|^2 = \sum_{k=1}^{N-1} |\omega^k - 1|^{-2s} = \sum_{k=1}^{N-1} |\omega^{k/2} - \omega^{-k/2}|^{-2s} \cdot |\omega|^{-sk}.$$

По формуле Эйлера $\mathrm{e}^{i\varphi} = \cos\varphi + i\sin\varphi$ получим

$$\|\mathcal{F}[b_s]\|^2 = \sum_{k=1}^{N-1} \left|2\sin\frac{\pi k}{N}\right|^{-2s}.$$

Далее считаем $s > 0$ и запишем две формулы:

$$N\|b_{-s}\|^2 = 4^s \sum_{k=1}^{N-1} \sin^{2s}\frac{\pi k}{N}, \qquad N\|b_s\|^2 = 4^{-s} \sum_{k=1}^{N-1} \sin^{-2s}\frac{\pi k}{N}.$$

Для первой из них по формуле (17) при $s < N$ получаем (18). Сигналы Бернулли положительного порядка восстанавливаются через производящую вектор-функцию теоремы 2: $b_s = \frac{1}{s!}\,(\Phi(x))^{(s)}\,|_{x=0}$, а для отдельных отсчётов

$$b_s(k) = \frac{1}{s!}\lim_{u\to 0}\left(\frac{d^s}{du^s}\varphi_k(u)\right) = \frac{1}{s!}\lim_{z\to 1}\left(\frac{d^s}{dz^s}\frac{z^{k-1}(z-1)}{1-z^N}\right).$$

При вычислении квадрата нормы вместо нулевого отсчёта берем отсчёт с номером N:

$$\|b_s\|^2 = \left(\frac{1}{s!}\right)^2 \sum_{k=1}^{N} \lim_{z\to 1}\lim_{t\to 1} \frac{\partial^{2s}}{\partial z^s\,\partial t^s}\left(\frac{z^{k-1}(z-1)t^{k-1}(t-1)}{(z^N-1)(t^N-1)}\right),$$

что равносильно (19).

Так как при замене N на $-N$ в правой части (19) ничего не меняется, эта функция чётная. К тому же эта функция является многочленом, что нетрудно проверить (в [5] это доказано для очень близкой конструкции). Один из корней этого многочлена $N = 1$, так как при $N = 1$ правая часть (19) обращается в нуль. Из чётности многочлена вытекает, что и $N = -1$ есть корень. ■

Приведём частные случаи результатов теоремы 3:

$$\sum_{k=1}^{N-1}\sin^2\frac{\pi k}{N} = \frac{N}{2} \text{ при } N \geqslant 2, \quad \sum_{k=1}^{N-1}\sin^4\frac{\pi k}{N} = \frac{3N}{8} \text{ при } N \geqslant 3,$$
$$\sum_{k=1}^{N-1}\sin^6\frac{\pi k}{N} = \frac{5N}{16} \text{ при } N \geqslant 4, \quad \sum_{k=1}^{N-1}\sin^8\frac{\pi k}{N} = \frac{35N}{128} \text{ при } N \geqslant 5.$$

Из курса математического анализа известно [14, с. 434], что

$$\int_0^\pi \sin^{2s} x\,dx = \sqrt{\pi}\frac{\Gamma(\frac{2s+1}{2})}{\Gamma(s+1)} = \pi\,\frac{(2s-1)!!}{(2s)!!}. \tag{20}$$

Сравнивая (20) с формулой (18), замечаем, что для интеграла $\int_0^\pi \sin^{2s} x\,dx$ обе формулы прямоугольников (при $\Delta x = \pi/N$) точны при достаточном ($N \geqslant s+1$) числе узлов:

$$\Delta x\sum_{k=0}^{N-1}\sin^{2s}(k\Delta x) = \Delta x\sum_{k=1}^{N}\sin^{2s}(k\Delta x) = \int_0^\pi \sin^{2s} x\,dx.$$

Верны следующие частные случаи:

$$\sum_{k=1}^{N-1}\frac{1}{\sin^2(\pi k/N)}=\frac{N^2-1}{3},\qquad \sum_{k=1}^{N-1}\frac{1}{\sin^4(\pi k/N)}=\frac{(N^2-1)(N^2+11)}{45},$$
$$\sum_{k=1}^{N-1}\frac{1}{\sin^6(\pi k/N)}=\frac{(N^2-1)(2N^4+23N^2+191)}{945},$$
$$\sum_{k=1}^{N-1}\frac{1}{\sin^8(\pi k/N)}=\frac{(N^2-1)(3N^6+43N^4+337N^2+2497)}{14175},$$
$$\sum_{k=1}^{N-1}\frac{1}{\sin^{10}(\pi k/N)}=\frac{(N^2-1)(2N^8+35N^6+321N^4+2125N^2+14797)}{93555}.$$

Из этого набора формул легко вычисляются участимммы чётных степеней котангенсов в равноотстоящих узлах, приведённые в [15] и востребованные в механике.

По алгоритму леммы 3 и формуле теоремы 3 составлена программа [16] вычисления $\sum\limits_{k=1}^{N-1}\dfrac{1}{\sin^{2s}(\pi k/N)}$ по произвольным заданным N и s.

6. Связь с числами и многочленами Коробова

При построении производящей функции в теореме 2 более удобный вид получается при рассмотрении обратного сдвига. Поэтому далее рассмотрим следующую последовательность дискретных периодических функций (называемых сигналами):

$$-N\cdot b_0^{\leftarrow},\ -N\cdot b_1^{\leftarrow},\ -N\cdot b_2^{\leftarrow},\ldots,-N\cdot b_s^{\leftarrow},\ldots$$

Будем использовать предложенные в [6] названия и обозначения:

— *специальные числа* P_s для начальных отсчётов этих сигналов:

$$P_s=-N\cdot b_s^{\leftarrow}(0)=-N\cdot b_s(1);$$

— *специальные многочлены* $P_s(k)$ для остальных отсчётов этих сигналов (за одним исключением: последняя координата начального сигнала выпадает из общей конструкции, $P_0(x)\equiv 1$):

$$P_s(k)=-N\cdot b_s(k+1),\quad k=0,1,\ldots,N-1.$$

Специальные числа P_s и специальные многочлены $P_s(x)$, а также производящие функции для них

$$\psi(u)=\sum_{s=0}^{\infty}P_su^s,\quad \Psi(u,x)=\sum_{s=0}^{\infty}P_s(x)u^s$$

введены и вычислены в [5, 6]. В [5] обозначения другие. После естественного видоизменения эти специальные числа и многочлены приобрели вид *чисел Коробова* и *многочленов Коробова* первого рода [8]

$$K_s=s!P_s,\quad K_s(x)=s!P_s(x)$$

с теми же экспоненциальными (термин из [11]) производящими функциями

$$\psi(u)=\sum_{s=0}^{\infty}\frac{K_s}{s!}u^s,\quad \Psi(u,x)=\sum_{s=0}^{\infty}\frac{K_s(x)}{s!}u^s.$$

Из теоремы 2 вытекает

Утверждение 6. Экспоненциальные производящие функции чисел и многочленов Коробова первого рода имеют следующий вид:

$$\psi(u) = \psi(u;N) = \frac{Nu}{(u+1)^N - 1}, \quad \Psi(u,x) = \Psi(u,x;N) = \frac{Nu(u+1)^x}{(u+1)^N - 1}.$$

Основной результат работы [5] сформулируем в принятых обозначениях, используя понятие *обобщённой степени* $k^{(s)} = k(k-1)\dots(k-s+1)$.

Теорема 4. Решение бесконечной (так как $s \in \mathbb{N}$) системы разностных уравнений

$$\Delta[P_s] = P_{s-1}$$

с условием нормировки $\sum\limits_{k=0}^{N-1} P_s(k) = 0$ и начальным условием $P_0(k) \equiv 1$ имеет следующий вид:

$$P_s(k) = P_0\frac{k^{(s)}}{s!} + P_1\frac{k^{(s-1)}}{(s-1)!} + \ldots + P_{s-1}\frac{k^{(1)}}{1!} + P_s. \tag{21}$$

Здесь специальные числа P_s имеют вид многочленов степени s от параметра N со старшим коэффициентом $B_s/s!$, где B_s — числа Бернулли. Начиная с $s=2$, это чётные многочлены (то есть многочлены от N^2), для которых числа 1 и -1 служат корнями.

Рекуррентная формула для вычисления чисел P_s как многочленов от N имеет следующий вид:

$$P_0\frac{N^{(s+1)}}{(s+1)!} + P_1\frac{N^{(s)}}{s!} + \ldots + P_{s-1}\frac{N^{(2)}}{2!} + P_sN = 0. \tag{22}$$

Доказательство. По условию нормировки из соображений симметрии имеем $P_1(k) = k - \dfrac{N-1}{2}$, что можно представить в виде $P_1(k) = P_0k^{(1)} + P_1$, где $P_1 = -\dfrac{N-1}{2}$. Это база индукции для доказательства (21) и (22).

Предположим, что

$$P_{s-1}(k) = P_0\frac{k^{(s-1)}}{(s-1)!} + P_1\frac{k^{(s-2)}}{(s-2)!} + \ldots + P_{s-2}\frac{k^{(1)}}{1!} + P_{s-1}.$$

Так как $\Delta[k^{(n)}] = nk^{(n-1)}$, решение уравнения $\Delta[P_s] = P_{s-1}$, согласно лемме 3, имеет вид (21), где P_s пока не найдено. Ищем его методом прогонки:

$$P_s(0) = P_s, \quad P_s(1) = P_s + P_{s-1}, \quad P_s(2) = P_s + 2P_{s-1} + P_{s-2}, \ldots$$

Общий вид формулы для $0 \leqslant k \leqslant N-1$:

$$P_s(k) = \sum_{j=0}^{k} \mathrm{C}_k^j P_{s-j}.$$

По условию нормировки $\sum\limits_{k=0}^{N-1} P_s(k) = \sum\limits_{k=0}^{N-1}\sum\limits_{j=0}^{k} \mathrm{C}_k^j P_{s-j} = 0$. Отделим старшее слагаемое и поменяем пределы суммирования:

$$NP_s + \sum_{j=1}^{N-1}\left(\sum_{i=j}^{N-1} \mathrm{C}_i^j\right) P_{s-j} = 0.$$

Согласно [11, задача 1.2], получили $\sum\limits_{j=1}^{N-1} \mathrm{C}_N^{j+1} P_{s-j} + NP_s = 0$. Запись этого выражения в виде многочлена от N приводит к (22).

Теперь рассмотрим специальные числа P_s как многочлены от N степени s, где старший коэффициент при N^s может оказаться нулём. Этот коэффициент найдём анализом старших слагаемых.

База индукции: $P_0 = B_0 = 1$, $P_1 = B_1 N + \mathrm{O}(N^{1-1})$, где $B_0 = 1$, $B_1 = -1/2$ — числа Бернулли.

Индуктивное предположение: $P_k = \dfrac{B_k}{k!} n^k + \mathrm{O}(N^{k-1})$ при всех k от 1 до $n-1$. Так как формулу (22) анализируем для всех N, отмечаем, что с ростом N она обрывается на n:

$$P_n = -\frac{1}{N} \sum_{j=1}^{n} \frac{N^{(j+1)}}{(j+1)!} P_{n-j}.$$

Следим только за старшим коэффициентом:

$$P_n = -\sum_{j=1}^{n} \frac{(N-1)^{(j)}}{(j+1)!} \left(\frac{B_{n-j}}{(n-j)!} N^{n-j} + \mathrm{O}(N^{n-j-1}) \right) = \left(\sum_{j=1}^{n} \frac{-B_{n-j}}{(j+1)!(n-j)!} \right) N^n +$$

$$+\mathrm{O}(N^{n-1}) = \left(\frac{-1}{n!} \sum_{j=1}^{n} \frac{n!}{(j+1)!(n-j)!} B_{n-j} \right) N^n + \mathrm{O}(N^{n-1}) = \frac{B_n}{n!} + \mathrm{O}(N^{n-1})$$

по свойству (1).

Чётность P_n как многочлена от N и наличие множителя $(N^2 - 1)$ (при $n \geqslant 2$) доказаны в следствии 8. ■

В [12] отмечено, что решение данной системы разностных уравнений уже получено, найдены производящие функции для них и приведена формула (19) для тригонометрических сумм.

В [6] специальные числа P_s вводятся формулой (22) с начальным условием $P_0 = 1$, а специальные многочлены $P_s(x)$, для которых $P_s(k) = -Nb_s(k+1)$ на сетке, — формулой (21) с начальным условием $P_0(x) \equiv 1$, без мотивировки происхождения этих формул. В [8] предложен подход к определению P_s и $P_s(x)$ через производящие функции.

Утверждение 7. Три следующих способа определения специальных чисел P_s и специальных многочленов $P_s(x)$ (а следовательно, также чисел и многочленов Коробова первого рода) эквивалентны:

1) в виде решения системы разностных уравнений с нормировкой (9);
2) формулами (21), (22);
3) через производящие функции $\psi(u) = \dfrac{Nu}{(u+1)^N - 1}$ и $\Psi(u,x) = \dfrac{Nu(u+1)^x}{(u+1)^N - 1}$ соответственно.

Переходы $1 \to 2$, $1 \to 3$ доказаны в [5] (см. также теорему 4 и утверждение 6), переход $2 \to 3$ — в [6], а переход $3 \to 1$ — в [8].

Замечание 5. Существует четвёртый (рекуррентный) способ определения специальных многочленов $P_n(k)$ (от целочисленного аргумента k на сетке) с помощью формулы (14). Этот способ аналогичен формуле (22) для вычисления специальных чисел. Однако для него нужно слегка поправить определение $P_0(k)$: оставляем неизменным $P_0(k) = 1$ при $0 \leqslant k \leqslant N-2$ и изменяем один отсчёт $P_0(N-1) = 1-N$. За счёт этой поправки, которая не влияет на вычисление последующих многочленов $P_n(k)$, добились того, что и для начального многочлена верно условие нормировки

$$\sum_{k=0}^{N-1} P_n(k) = 0. \tag{23}$$

Введение поправки позволяет определить и вычислять, применяя операцию Δ, «специальные многочлены отрицательного порядка» по аналогии с сигналами Бернулли. В качестве начальных данных предлагаемого четвёртого способа достаточно вычислить $N-2$ таких «многочленов», начиная от P_{-1} до $P_{-(N-2)}$. Формулы для вычисления их отсчётов, удовлетворяющих условию (23): $P_{-k}(j) = 0$ при $0 \leqslant j \leqslant N-k-2$, $P_{-k}(N-k-1+s) = (-1)^{s+1} N \mathrm{C}_k^s$ при $0 \leqslant s \leqslant k$.

Наличие величин, которые названы «многочленами», позволяет запустить процесс вычисления специальных многочленов по формуле

$$P_s(j) = -\frac{1}{N} \sum_{k=1}^{N-1} \mathrm{C}_N^{k-1} P_{s-k}(j) = 0, \quad s = 1, 2, 3, \ldots \tag{24}$$

Приведём несколько начальных чисел Коробова, вычисленных по формуле (22) и соотношению $K_s = s! P_s$ (отметим, что в [6–8] вычисления выполнены до третьего порядка):

$$K_1 = -\frac{N-1}{2},\ K_2 = \frac{N^2-1}{6},\ K_3 = -\frac{N^2-1}{4},\ K_4 = -\frac{1}{30}(N^2-1)(N^2-19),$$
$$K_5 = \frac{(N^2-1)(N^2-9)}{4},\ K_6 = \frac{1}{84}(N^2-1)(2N^4-145N^2+863),$$
$$K_7 = -\frac{5}{24}(N^2-1)(N^2-25)(2N^2-11).$$

Следующие числа Коробова вычислены методом неопределённых коэффициентов с использованием результатов теоремы 4:

$$K_8 = -\frac{1}{90}(N^2-1)(3N^6-497N^4+9247N^2-33953),$$
$$K_9 = \frac{7}{20}(N^2-1)(N^2-49)(3N^4-50N^2+167),$$
$$K_{10} = \frac{5}{660}(N^2-1)(10N^8-2993N^6+114597N^4-1184767N^2+3250433),$$
$$K_{11} = -\frac{15}{8}(N^2-1)(N^2-9)(N^2-81)(2N^4-49N^2+173),$$
$$K_{12} = -\frac{N^2-1}{5460}(1382N^{10}-653818N^8+42418211N^6-845983589N^4+6117468907N^2-$$
$$-13695779093),$$
$$K_{13} = \frac{11}{840}(N^2-1)(N^2-121)(1382N^8-77096N^6+1336965N^4-8756954N^2+18382103).$$

Из наблюдения за видом чисел Коробова вытекает

Гипотеза 1.

$$\lim_{N\to\infty} \frac{K_{2n+1}}{K_{2n}} = \frac{1-4n^2}{2}.$$

Если гипотеза верна, то нам известны старшие ненулевые коэффициенты всех чисел Коробова. В качестве упражнения можно попробовать методом неопределённых коэффициентов продолжить вычисления чисел Коробова, общий вид которых (при верности гипотезы) следующий:

$$K_{14} = \frac{7}{6}(N^2-1)T_{12}(N), \quad K_{15} = -\frac{455}{4}(N^2-1)(N^2-169)T_{10}(N),$$

$$K_{16} = \frac{-3617}{510}(N^2-1)T_{14}(N), \; K_{17} = \frac{3617}{4}(N^2-1)(N^2-9)(N^2-25)(N^2-225)T_8(N).$$

Здесь $T_n(N)$ — чётный многочлен степени n со старшим коэффициентом 1, коэффициенты которого и следует вычислить. Для применения метода неопределённых коэффициентов предлагается таблица значений отдельных специальных чисел $P_n = K_n/n!$ в зависимости от размера сетки N.

n	N					
	2	3	4	5	6	7
14	$1/2^{14}$	$2/2187$	$-255/16384$	$8/125$	$71698571/35831808$	$445/49$
15	$-1/2^{15}$	$-1/2187$	$255/32768$	$-21/125$	$-71698571/71663616$	$357/49$
16	$1/2^{16}$	$1/6561$	$1/65536$	$76/625$	$-429909599/429981696$	$-948/49$
17	$-1/2^{17}$	0	$-513/131072$	0	$262143/131072$	$474/49$

Для вычисления K_{16} добавим недостающее значение $P_{16} = -6684671/2^{16}$ при $N = 8$. Приведем также вид начальных многочленов Коробова:

$$K_0(x) = 1, \; K_1(x) = x - \frac{N-1}{2}, \; K_2(x) = x^2 - Nx + \frac{N^2-1}{6},$$

$$K_3(x) = x^3 - \frac{3(N+1)}{2}x^2 + \frac{N(N+3)}{2}x - \frac{N^2-1}{4},$$

$$K_4(x) = x^4 - (2N+4)x^3 + (N^2+6N+4)x^2 - 2N(N+2)x - \frac{(N^2-1)(N^2-19)}{30},$$

$$K_5(x) = x^5 - \frac{5}{2}(N+3)x^4 + \frac{5}{3}(N^2+9N+11)x^3 - \frac{5}{2}(3N^2+11N+6)x^2 -$$
$$- \frac{1}{6}(N^4-55N^2-90N)x + \frac{1}{4}(N^2-1)(N^2-9),$$

$$K_6(x) = x^6 - 3(N+4)x^5 + \frac{5}{2}(N^2+12N+21)x^4 - 5(4N^2+21N+20)x^3 +$$
$$+ \frac{1}{2}(-N^4+105N^2+300N+144)x^2 + (2N^4-50N^2-72N)x + K_6,$$

$$K_7(x) = x^7 - \frac{7}{2}(N+5)x^6 + \frac{7}{2}(N^2+15N+34)x^5 - \frac{35}{4}(5N^2+34N+45)x^4 +$$
$$+ \frac{7}{6}(-N^4+170N^2+675N+548)x^3 + \frac{7}{4}(5N^4-225N^2-548N-240)x^2 +$$
$$+ \frac{1}{6}(N^6-119N^4+1918N^2+2520N)x + K_7.$$

По свойству многочленов Коробова первого рода $\Delta K_s(x) = sK_{s-1}(x)$ и числам Коробова $K_s = K_s(0)$ в качестве начальных условий вычисляется следующий общий вид старших коэффициентов многочленов Коробова первого рода:

$$K_n(x) = x^n - \frac{n(N+n-2)}{2}x^{n-1} + \mathrm{C}_n^2 \frac{2N^2+6(n-2)N+3n^2-13n+12}{12}x^{n-2} -$$
$$- \mathrm{C}_n^3 \frac{(2n-4)N^2+(3n^2-13n+12)N+(n^3-7n^2+14n-8)}{8}x^{n-3} + \ldots$$

При фиксированном N численное значение чисел и многочленов Коробова на сетке удобнее вычислять не по этим формулам, а с помощью леммы 3 или формулы (24).

В [8] предложен метод вывода многочленов Бернулли из многочленов Коробова $\lim\limits_{N\to\infty} \dfrac{K_n(Nx)}{N^n} = B_n(x)$.

Заключение

Дискретные периодические функции Бернулли служат естественным и достаточно удобным аппаратом при более подробном изложении теории дискретного преобразования Фурье. Поэтому не случайно на них практически одновременно и независимо друг от друга вышли проф. В. Н. Малоземов и автор работы. В рамках теории чисел дискретные периодические функции Бернулли представлены в виде многочленов Коробова и активно исследуются. Например, работа [17] в течение 2017 г. процитирована 5 раз. Кроме возможных приложений в технике, их востребованность обусловлена ещё и тем, что числа и многочлены Коробова служат одним из основных примеров для изложения теневого исчисления, развитого в работах Рота и его последователей [18]. В рамках теневого исчисления изучаются [8] также числа и многочлены Коробова второго рода, которые в данной работе не затрагиваются. Близким объектом служат многочлены Карлица.

ЛИТЕРАТУРА

1. *Бер М. Г., Малоземов В. Н.* Наилучшие формулы для приближенного вычисления дискретного преобразования Фурье // Ж. вычислит. матем. и матем. физики. 1992. Т. 32. № 11. С. 1709–1719.
2. Избранные главы дискретного гармонического анализа и геометрического моделирования. Ч. 2 / под ред. В. Н. Малоземова. СПб.: Изд-во ВВМ, 2014. 605 с.
3. *Малоземов В. Н., Машарский С. М.* Основы дискретного гармонического анализа. СПб.: Лань, 2012. 304 с.
4. *Малоземов В. Н., Певный А. Б.* Дискретные периодические сплайны и их вычислительные применения // Ж. вычислит. матем. и матем. физики. 1998. Т. 38. № 8. С. 1235–1246.
5. *Беспалов М. С.* Представление для сумм четных отрицательных степеней синусов в равноотстоящих узлах // Изв. вузов. Математика. 1996. Т. 8 (411). С. 6–12.
6. *Коробов Н. М.* Специальные полиномы и их приложения // Диофантовы приближения. Математические записки. 1996. Т. 2. С. 77–89.
7. *Устинов А. В.* О формулах суммирования и интерполяции // Чебышевский сб. 2001. Т. 1. № 1. С. 52–71.
8. *Устинов А. В.* Полиномы Коробова и теневой анализ // Чебышевский сб. 2003. Т. 4. № 4(8). С. 137–152.
9. *Хорн Р., Джонсон Ч.* Матричный анализ. М.: Мир, 1989. 655 с.
10. *Трахтман А. М., Трахтман В. А.* Основы теории дискретных сигналов на конечных интервалах. М.: Сов. радио, 1975. 208 с.
11. Комбинаторный анализ. Задачи и упражнения / под ред. К. А. Рыбникова. М.: Наука, 1982. 368 с.
12. *Беспалов М. С.* О производящих функциях для некоторых тригонометрических сумм // Научные исследования института — техническому и культурному прогрессу. Материалы XXV научн. конф. ВПИ. Ч. 1. Владимир: ВПИ, 1990. С. 40.
13. *Гузев М. А., Устинов А. В.* Механические характеристики модели молекулярной динамики и полиномы Коробова // Дальневост. матем. журн. 2016. Т. 16. № 2. С. 39–43.

14. *Зорич В. А.* Математический анализ. Ч. II. М.: Наука, 1984. 640 с.
15. *Беспалов М. С.* Тригонометрические суммы для задач молекулярной динамики // Междунар. конф. по матем. теории управления и механике. Тез. докл. Суздаль, 7–11 июля 2017. Владимир: ООО «Аркаим», 2017. С. 36–37.
16. *Беспалов М. С., Панина Н. А.* Программа вычисления точного значения сумм четных отрицательных степеней синусов в равноотстоящих узлах окружности. Зарегистрированная программа для ЭВМ. Свидетельство о гос. регистрации программ для ЭВМ № 2011616549 от 22 августа 2011 г.
17. *Долгий Д. В., Ким Д. С., Ким Т.* О полиномах Коробова первого рода // Матем. сб. 2017. Т. 206. № 1. С. 65–79.
18. *Roman S. M. and Rota G.-C.* The umbral calculus // Adv. Math. 1978. V. 27. P. 95–188.

REFERENCES

1. *Ber M. G. and Malozemov V. N.* The best formulas for approximate calculastion of a discrete Fourier transform. Comput. Math. and Math. Physics, 1992, vol. 32, no. 11. pp. 1533–1544.
2. Izbrannye glavy discretnogo garmonicheskogo analiza i geometricheskogo modelirovaniya. Ch. 2. [Selected Chapters of Discrete Harmonic Analysis and Geometric Modeling. P. 2]. Ed. V. N. Malozemov. St. Petersburg, VVM Publ., 2014. 605 p. (in Russian)
3. *Malozemov V. N. and Macharskiy S. M.* Osnovy discretnogo garmonicheskogo analiza [Basics of Discrete Harmonic Analysis]. St. Petersburg, Lane Publ., 2012. 304 p. (in Russian)
4. *Malozemov V. N. and Pevniy A. B.* Discrete periodic splines and their computational application. Comput. Math. and Math. Physics, 1998, vol. 38, no. 8. pp. 1181–1192.
5. *Bespalov M. S.* Representation for sums of even negative degrees of sines in equivdistant nodes. Russian Mathematics, 1996, vol. 40, no. 8, pp. 4–10.
6. *Korobov N. M.* Special'nye polinomy i ikh prilojeniya [Special polynomials and its application]. Diofantovy Pribligeniya. Matematicheskie Zapiski, 1996, vol. 2, pp. 77–89. (in Russian)
7. *Ustinov A. V.* O formulakh summirovaniya i interpolyacii [On summation and interpolation formulas]. Chebyshevskii Sbornik, 2001, vol. 1, no. 1, pp. 52–71. (in Russian)
8. *Ustinov A. V.* Polynomy Korobova i tenevoi analis [Polynomials of Korobov and umbral analysis]. Chebyshevskii Sbornik, 2003, vol. 4, no. 4(8), pp. 137–152. (in Russian)
9. *Horn R. A. and Johnson C. R.* Matrix Analysis. Cambridge, Cambridge University Press, 1986. 662 p.
10. *Trakhman A. M., Trakhman V. A.* Osnovy teorii signalov na konechnikh intervalakh [Fundamentals of the Theory of Signals of Finite Intervals]. Moscow, Soviet Radio Publ., 1975. 208 p. (in Russian)
11. Kombinatorniy analis. Zadzchi i upragneniya [Combinatorial Analysis. Tasks and Exercises]. Ed. K. A. Rybnikov. Moscow, Nauka Publ., 1982. 368 p. (in Russian)
12. *Bespalov M. S.* O proizvodyachikh funkciyakh dlia nekotorikh trigonometricheskikh summ [On generating functions for same trigonometric sums]. Proc. XXV Sci. Conf. VPI. P. 1. Vladimir, VPI Publ., 1990, p. 40. (in Russian)
13. *Guzev M. A. and Ustinov A. V.* Mechanical characteristics of molecular dynamics model and Korobov polynomials. Dal'nevostochnyi Matematicheskii Zhurnal, 2016, vol. 16, no. 2, pp. 39–43. (in Russian)
14. *Zorich V. A.* Matematicheskii analis [Mathematical Analysis]. P. 2. Moscow, Nauka Publ., 1984. 640 p. (in Russian)
15. *Bespalov M. S.* Trigonometricheskie summy dlia zadach molekuliarnoy dinamiki [Trigonometric sums for problems of molecular dynamics]., Intern. Conf. Math. Control Theory and Mechanics. Vladimir, Arcaim Publ., 2017, pp. 36–37. (in Russian)

16. *Bespalov M. S. and Panina N. A.* Program calculation exact value for sums of even negative degrees of sines in equivdistant nodes. Program for computation no. 2011616549. 22.08.2011.
17. *Dolgy D. V., Kim D. S., and Kim T.* Korobov polynomials of the first kind. Sb. Math. 2017, vol. 208, no. 1. pp. 60–74.
18. *Roman S. M. and Rota G.-C.* The umbral calculus. Adv. Math., 1978, vol. 27, pp. 95–188.

UDC 512.53 DOI 10.17223/20710410/43/3

CHARACTERIZATIONS OF NON ASSOCIATIVE ORDERED SEMIGROUPS BY THE PROPERTIES OF THEIR FUZZY IDEALS WITH THRESHOLDS $(\alpha, \beta]$

K. Nasreen

Quaid-i-Azam University, Islamabad, Pakistan

E-mail: kausar.nasreen57@gmail.com

In this paper, we give the characterizations of regular (intra-regular, both regular and intra-regular) ordered AG-groupoids by the properties of fuzzy (left, right, quasi-, bi-, generalized bi-) ideals with thresholds $(\alpha, \beta]$.

Keywords: *fuzzy left (right, interior, quasi-, bi-, generalized bi-) ideals with thresholds $(\alpha, \beta]$, regular (intra-regular) ordered AG-groupoids.*

Introduction

In 1972, a generalization of commutative semigroups has been established by Kazim et al [1]. In ternary commutative law: $abc = cba$, they introduced the braces on the left side of this law and explored a new pseudo associative law, that is $(ab)c = (cb)a$. This law is called the left invertive law. A groupoid S is said to be a left almost semigroup (abbreviated as LA-semigroup) if it satisfies the left invertive law. This structure is also known as Abel—Grassmann's groupoid (abbreviated as AG-groupoid) [2]. An AG-groupoid is a midway structure between an abelian semigroup and a groupoid. Mushtaq et al [3] investigated the concept of ideals of AG-groupoids.

In [4] (resp. [5]), a groupoid S is said to be medial (resp. paramedial) if $(ab)(cd) = (ac)(bd)$ (resp. $(ab)(cd) = (db)(ca)$). In [1], an AG-groupoid is medial, but in general an AG-groupoid needs not to be paramedial. Every AG-groupoid with left identity is paramedial by Protic et al [2] and also satisfies $a(bc) = b(ac)$, $(ab)(cd) = (dc)(ba)$.

Algebraic structures play a prominent role in mathematics with wide ranging applications in many disciplines such as theoretical physics, computer sciences, control engineering, information sciences, coding theory, topological spaces and the like.

Although semigroups concentrate on theoretical aspects, they also include applications in error-correcting codes, control engineering, formal language, computer science and information science.

Algebraic structures especially ordered semigroups play a prominent role in mathematics with wide ranging applications in many disciplines such as control engineering, computer arithmetics, coding theory, sequential machines and formal languages.

In [6], if $(S, \cdot, \leqslant)$ is an ordered semigroup and $\varnothing \neq A \subseteq S$, we define a subset of S as follows: $(A] = \{s \in S : s \leqslant a \text{ for some } a \in A\}$. A non-empty subset A of S is called a subsemigroup of S if $A^2 \subseteq A$.

A non-empty subset A of S is called a left (resp. right) ideal of S if the following conditions hold: (1) $SA \subseteq A$ (resp. $AS \subseteq A$); (2) if $a \in A$ and $b \in S$ such that $b \leqslant a$ implies $b \in A$. Equivalent definition: A is called a left (resp. right) ideal of S if $(A] \subseteq A$ and $SA \subseteq A$ (resp. $AS \subseteq A$).

In [6, 7], an ordered semigroup S is said to be a regular if for every $a \in S$, there exists an element $x \in S$ such that $a \leqslant axa$. Equivalent definitions are as follows: (1) $A \subseteq (ASA]$

for every $A \subseteq S$; (2) $a \in (aSa]$ for every $a \in S$. In [7, 8], an ordered semigroup S is said to be an intra-regular if for every $a \in S$ there exist elements $x, y \in S$ such that $a \leqslant xa^2y$. Equivalent definitions are as follows: (1) $A \subseteq (SA^2S]$ for every $A \subseteq S$; (2) $a \in (Sa^2S]$ for every $a \in S$.

We will define the concept of fuzzy left (resp. right, interior, quasi-, bi-, generalized bi-) ideals with thresholds $(\alpha, \beta]$ of an ordered AG-groupoid S. We will establish a study by discussing the different properties of such ideals. We will also characterize regular (resp. intra-regular, both regular and intra-regular) ordered AG-groupoids by the properties of fuzzy left (right, quasi-, bi-, generalized bi-) ideals with thresholds $(\alpha, \beta]$.

1. Fuzzy ideals with thresholds $(\alpha, \beta]$ in ordered AG-groupoids

An ordered AG-groupoid S is a partially ordered set, at the same time an AG-groupoid such that $a \leqslant b$ implies $ac \leqslant bc$ and $ca \leqslant cb$ for all $a, b, c \in S$. Two conditions are equivalent to the one condition $(ca)d \leqslant (cb)d$ for all $a, b, c, d \in S$.

Let S be an ordered AG-groupoid and $\varnothing \neq A \subseteq S$, we define a subset $(A] = \{s \in S : s \leqslant a \text{ for some } a \in A\}$ of S, obviously $A \subseteq (A]$. If $A = \{a\}$, then we write $(a]$ instead of $(\{a\}]$. For $\varnothing \neq A, B \subseteq S$, then $AB = \{ab : a \in A, b \in B\}$, $((A]] = (A]$, $(A](B] \subseteq (AB]$, $((A](B]] = (AB]$, if $A \subseteq B$, then $(A] \subseteq (B]$, $(A \cap B] \neq (A] \cap (B]$ in general.

For $\varnothing \neq A \subseteq S$, A is called an ordered AG-subgroupoid of S if $A^2 \subseteq A$; A is called a left (resp. right) ideal of S if the following hold: (1) $SA \subseteq A$ (resp. $AS \subseteq A$); (2) if $a \in A$ and $b \in S$ such that $b \leqslant a$ implies $b \in A$. Equivalent definition: A is called a left (resp. right) ideal of S if $(A] \subseteq A$ and $SA \subseteq A$ (resp. $AS \subseteq A$). A is called an ideal of S if A is both a left ideal and a right ideal of S. In particular, if A and B are any types of ideals of S, then $(A \cap B] = (A] \cap (B]$.

We denote by $L(a), R(a), I(a)$ the left ideal, the right ideal and the ideal of S respectively, generated by a. We have $L(a) = \{s \in S : s \leqslant a \text{ or } s \leqslant xa \text{ for some } x \in S\} = (a \cup Sa]$, $S(a) = (a \cup aS]$, $I(a) = (a \cup Sa \cup aS \cup (Sa)S]$.

First time, Zadeh introduced the concept of fuzzy set in his classical paper [9] of 1965. This concept has provided a useful mathematical tool for describing the behavior of systems that are too complex to admit precise mathematical analysis by classical methods and tools. Extensive applications of fuzzy set theory have been found in various fields such as artificial intelligence, computer science, management science, expert systems, finite state machines, languages, robotics, coding theory and others.

Since then, many papers on fuzzy sets appeared showing the importance of the concept and its applications to logic, set theory, groupoids, semigroup, ordered semigroup, group theory, real analysis, measure theory, topology, etc.

Rosenfeld [10] was the first, who introduced the concept of fuzzy set in a group. The study of fuzzy set in semigroups was established by Kuroki [11, 12]. He studied fuzzy ideals and fuzzy interior (resp. quasi-, bi-, generalized bi-, semiprime, semiprime quasi-) ideals of semigroups. A systematic exposition of fuzzy semigroups appeared by Mordeson et al [13], where one can find the theoretical results on fuzzy semigroups and their use in fuzzy finite state machines and languages. Fuzzy sets in ordered semigroups/ordered groupoids were first explored by Kehayopulu et al [14, 15]. They also studied fuzzy ideals and fuzzy interior (resp. quasi-, bi-, generalized bi-) ideals in ordered semigroups.

By a fuzzy subset μ of an ordered AG-groupoid S, we mean a function $\mu : S \to [0, 1]$, the complement of μ is denoted by μ', is a fuzzy subset of S defined by $\mu'(x) = 1 - \mu(x)$ for all $x \in S$.

A fuzzy subset μ of S is called a fuzzy ordered AG-subgroupoid of S if $\mu(xy) \geqslant \mu(x) \wedge \mu(y)$ for all $x, y \in S$; μ is called a fuzzy left (resp. right) ideal of S if (1) $\mu(xy) \geqslant \mu(y)$ (resp. $\mu(xy) \geqslant \mu(x)$); (2) $x \leqslant y$ implies $\mu(x) \geqslant \mu(y)$ for all $x, y \in S$; μ is a fuzzy ideal of S if μ is both a fuzzy left and a fuzzy right ideal of S. Every fuzzy ideal (whether left, right, two-sided) is a fuzzy AG-subgroupoid of S but the converse is not true in general.

We denote by $F(S)$ the set of all fuzzy subsets of S. For $\varnothing \neq A \subseteq S$, the characteristic function of A is denoted by χ_A and defined by

$$\chi_A(a) = \begin{cases} 1, & \text{if } a \in A, \\ 0, & \text{if } a \notin A. \end{cases}$$

Let $\mu, \gamma \in F(S)$; by the symbols $\mu \wedge \gamma$ and $\mu \vee \gamma$ we mean the following fuzzy subsets:

$$(\mu \wedge \gamma)(x) = \min\{\mu(x), \gamma(x)\} \text{ and } (\mu \vee \gamma)(x) = \max\{\mu(x), \gamma(x)\}.$$

An ordered AG-groupoid S can be considered a fuzzy subset of itself and we write $S = \chi_S$, i.e., $S(x) = \chi_S(x) = 1$ for all $x \in S$. This implies that $S(x) = 1$ for all $x \in S$.

Let $x \in S$, we define a set $A_x = \{(y, z) \in S \times S : x \leqslant yz\}$. Let μ and γ be two fuzzy subsets of S, then product of μ and γ is denoted by $\mu \circ \gamma$ and defined by:

$$(\mu \circ \gamma)(x) = \begin{cases} \bigvee\limits_{(y,z) \in A_x} \min\{\mu(y), \gamma(z)\}, & \text{if } A_x \neq \varnothing, \\ 0, & \text{if } A_x = \varnothing. \end{cases}$$

A fuzzy subset μ of S is called a fuzzy interior ideal of S if: (1) $\mu\left((xy)z\right) \geqslant \mu(y)$; (2) $x \leqslant y$ implies $\mu(x) \geqslant \mu(y)$ for all $x, y, z \in S$. A fuzzy subset μ of S is called a fuzzy quasi-ideal of S if: (1) $(\mu \circ S) \cap (S \circ \mu) \subseteq \mu$; (2) $x \leqslant y$ implies $\mu(x) \geqslant \mu(y)$ for all $x, y \in S$. A fuzzy AG-subgroupoid μ of S is called a fuzzy bi-ideal of S if: (1) $\mu((xa)y) \geqslant \min\{\mu(x), \mu(y)\}$; (2) $x \leqslant y$ implies $\mu(x) \geqslant \mu(y)$ for all $x, a, y \in S$. A fuzzy subset μ of S is called a fuzzy generalized bi-ideal of S if: (1) $\mu((xa)y) \geqslant \min\{\mu(x), \mu(y)\}$; (2) $x \leqslant y$ implies $\mu(x) \geqslant \mu(y)$ for all $x, a, y \in S$.

Every fuzzy bi-ideal of S is a fuzzy generalized bi-ideal of S, but the converse is not true. A fuzzy ideal μ of S is called a fuzzy idempotent of S if $\mu \circ \mu = \mu$.

Now we define fuzzy ordered AG-subgroupoid with thresholds $(\alpha, \beta]$ and fuzzy left (resp. right, interior, quasi-, bi-, generalized bi-) ideals with thresholds $(\alpha, \beta]$ of an ordered AG-groupoid S.

A fuzzy subset μ of an ordered AG-groupoid S is called a fuzzy ordered AG-subgroupoid with thresholds $(\alpha, \beta]$ of S if $\max\{\mu(xy), \alpha\} \geqslant \min\{\mu(x), \mu(y), \beta\}$. A fuzzy subset μ of S is called a fuzzy left ideal with thresholds $(\alpha, \beta]$ of S if: (1) $\max\{\mu(xy), \alpha\} \geqslant \min\{\mu(y), \beta\}$; (2) $x \leqslant y$ implies $\mu(x) \geqslant \mu(y)$ for all $x, y \in S$ and $\alpha, \beta \in (0, 1]$ such that $\alpha < \beta$. A fuzzy subset μ of S is called a fuzzy right ideal with thresholds $(\alpha, \beta]$ of S if: (1) $\max\{\mu(xy), \alpha\} \geqslant$ $\geqslant \min\{\mu(x), \beta\}$; (2) $x \leqslant y$ implies $\mu(x) \geqslant \mu(y)$ for all $x, y \in S$ and $\alpha, \beta \in (0, 1]$ such that $\alpha < \beta$.

A fuzzy subset μ of S is called a fuzzy ideal with thresholds $(\alpha, \beta]$ of S if it is both a fuzzy left and a fuzzy right ideal with thresholds $(\alpha, \beta]$. Every fuzzy ideal (whether left, right, two-sided) with thresholds $(\alpha, \beta]$ is a fuzzy ordered AG-subgroupoid of S but the converse is not true in general.

A fuzzy subset μ of S is called a fuzzy interior ideal with thresholds $(\alpha, \beta]$ of S if: (1) $\max\{\mu((xy)z), \alpha\} \geqslant \min\{\mu(y), \beta\}$; (2) $x \leqslant y$ implies $\mu(x) \geqslant \mu(y)$ for all $x, y, z \in S$

and $\alpha, \beta \in (0, 1]$ such that $\alpha < \beta$. A fuzzy subset μ of S is called a fuzzy quasi-ideal with thresholds $(\alpha, \beta]$ of S if: (1) $\max\{\mu(x), \alpha\} \geqslant \min\{(\mu \circ S)(x), (S \circ \mu)(x), \beta\}$; (2) $x \leqslant y$ implies $\mu(x) \geqslant \mu(y)$ for all $x, y \in S$ and $\alpha, \beta \in (0, 1]$ such that $\alpha < \beta$.

A fuzzy ordered AG-subgroupoid μ with thresholds $(\alpha, \beta]$ of S is called a fuzzy bi-ideal with thresholds $(\alpha, \beta]$ of S if: (1) $\max\{\mu((xy)z), \alpha\} \geqslant \min\{\mu_A(x), \mu_A(z), \beta\}$; (2) $x \leqslant y$ implies $\mu(x) \geqslant \mu(y)$ for all $x, y, z \in S$ and $\alpha, \beta \in (0, 1]$ such that $\alpha < \beta$.

A fuzzy subset μ of S is called a fuzzy generalized bi-ideal with thresholds $(\alpha, \beta]$ of S if: (1) $\max\{\mu((xy)z), \alpha\} \geqslant \min\{\mu(x), \mu(z), \beta\}$; (2) $x \leqslant y$ implies $\mu(x) \geqslant \mu(y)$ for all $x, y, z \in S$ and $\alpha, \beta \in (0, 1]$ such that $\alpha < \beta$.

Every fuzzy bi-ideal with thresholds $(\alpha, \beta]$ of S is a fuzzy generalized bi-ideal with thresholds $(\alpha, \beta]$ of S, but the converse is not true.

Let μ be a fuzzy set of an ordered AG-groupoid S and $\alpha, \beta \in (0, 1]$ such that $\alpha < \beta$. We define a fuzzy subset μ_α^β of S as follow: $\mu_\alpha^\beta(x) = (\mu_A(x) \wedge \beta) \vee \alpha$ for all $x \in S$.

Let μ and γ be two fuzzy subsets of an ordered AG-groupoid S. We define fuzzy sets $\mu \wedge_\alpha^\beta \gamma$, $\mu \vee_\alpha^\beta \gamma$, $\mu \circ_\alpha^\beta \gamma$ and $\mu -_\alpha^\beta \gamma$ of S as follows:

$$(\mu_A \wedge_\alpha^\beta \mu_B)(x) = \{(\mu_A \wedge \mu_B)(x) \wedge \beta\} \vee \alpha,$$
$$(\mu_A \vee_\alpha^\beta \mu_B)(x) = \{(\mu_A \vee \mu_B)(x) \wedge \beta\} \vee \alpha,$$
$$(\mu_A \circ_\alpha^\beta \mu_B)(x) = \{(\mu_A \circ \mu_B)(x) \wedge \beta\} \vee \alpha,$$
$$(\mu_A -_\alpha^\beta \mu_B)(x) = \{(\mu_A - \mu_B)(x) \wedge \beta\} \vee \alpha$$

for all $x \in S$. Now we are giving the central properties of such ideals of an S, which will be very helpful for further sections.

Lemma 1. Let S be an ordered AG-groupoid. Then the following properties hold:

(1) $(\mu \circ_\alpha^\beta \gamma) \circ_\alpha^\beta \delta = (\delta \circ_\alpha^\beta \gamma) \circ_\alpha^\beta \mu$;
(2) $(\mu \circ_\alpha^\beta \gamma) \circ_\alpha^\beta (\delta \circ_\alpha^\beta \lambda) = (\mu \circ_\alpha^\beta \delta) \circ_\alpha^\beta (\gamma \circ_\alpha^\beta \lambda)$

for all fuzzy subsets μ, γ, δ and λ of S.

Proof. Let μ, γ and δ be fuzzy subsets of an ordered AG-groupoid S. We have to show that $(\mu \circ_\alpha^\beta \gamma) \circ_\alpha^\beta \delta = (\delta \circ_\alpha^\beta \gamma) \circ_\alpha^\beta \mu$. Now

$$((\mu \circ_\alpha^\beta \gamma) \circ_\alpha^\beta \delta)(x) = \{((\mu \circ \gamma) \circ \delta)(x) \wedge \beta\} \vee \alpha = \{((\delta \circ \gamma) \circ \mu)(x) \wedge \beta\} \vee \alpha = \\ = ((\delta \circ_\alpha^\beta \gamma) \circ_\alpha^\beta \mu)(x).$$

In same lines, we can prove (2). ■

Proposition 1. Let S be an ordered AG-groupoid with left identity e. Then the following assertions hold:

(1) $\mu \circ_\alpha^\beta (\gamma \circ_\alpha^\beta \delta) = \gamma \circ_\alpha^\beta (\mu \circ_\alpha^\beta \delta)$;
(2) $(\mu \circ_\alpha^\beta \gamma) \circ_\alpha^\beta (\delta \circ_\alpha^\beta \lambda) = (\lambda \circ_\alpha^\beta \gamma) \circ_\alpha^\beta (\delta \circ_\alpha^\beta \mu)$;
(3) $(\mu \circ_\alpha^\beta \gamma) \circ_\alpha^\beta (\delta \circ_\alpha^\beta \lambda) = (\lambda \circ_\alpha^\beta \delta) \circ_\alpha^\beta (\gamma \circ_\alpha^\beta \mu)$

for all fuzzy subsets μ, γ, δ and λ of S.

Proof. Same as Lemma 1. ■

Theorem 1. Let A and B be two non-empty subsets of an ordered AG-groupoid S. Then the following conditions hold:

(1) $\chi_A \circ_\alpha^\beta \chi_B = (\chi_{(AB]})_\alpha^\beta$;
(2) $\chi_A \vee_\alpha^\beta \chi_B = (\chi_{A \cup B})_\alpha^\beta$;
(3) $\chi_A \wedge_\alpha^\beta \chi_B = (\chi_{A \cap B})_\alpha^\beta$.

Proof. Straight forward. ■

Theorem 2. Let A be a non-empty subset of an ordered AG-groupoid S. Then the following properties hold:

(1) A is an AG-subgroupoid of S if and only if χ_A is a fuzzy AG-subgroupoid with thresholds $(\alpha, \beta]$ of S;

(2) A is a left (resp. right, two-sided) ideal of S if and only if χ_A is a fuzzy left (resp. right, two-sided) ideal with thresholds $(\alpha, \beta]$ of S.

Proof.

(1) Let A be an AG-subgroupoid of an ordered AG-groupoid S and $x, y \in S$. If $x, y \notin A$, then by definition of characteristic function $\chi_A(x) = 0 = \chi_A(y)$. Thus

$$\chi_A(xy) \geqslant \min\{\chi_A(x), \chi_A(y)\} = \min\{\chi_A(x), \chi_A(y), \beta\} \Rightarrow$$
$$\Rightarrow \chi_A(xy) \geqslant \min\{\chi_A(x), \chi_A(y), \beta\} \Rightarrow \max\{\chi_A(xy), \alpha\} \geqslant \min\{\chi_A(x), \chi_A(y), \beta\}.$$

In same lines, we have $\max\{\chi_A(xy), \alpha\} \geqslant \min\{\chi_A(x), \chi_A(y), \beta\}$, when $x, y \in A$. Hence the characteristic function χ_A of A is a fuzzy AG-subgroupoid with thresholds $(\alpha, \beta]$of S.

Conversely, suppose that the characteristic function $\chi_A$of A is a fuzzy AG-subgroupoid with thresholds $(\alpha, \beta]$ of an ordered AG-groupoid S. Let $x, y \in A$, then by definition $\chi_A(x) = 1 = \chi_A(y)$. Since $\max\{\chi_A(xy), \alpha\} \geqslant \min\{\chi_A(x), \chi_A(y), \beta\} = \beta$, χ_A being a fuzzy AG-subgroupoid with thresholds $(\alpha, \beta]$ of S. Thus $\max\{\chi_A(xy), \alpha\} \geqslant \beta$, this implies that $\chi_A(xy) = 1$, i.e., $xy \in A$. Hence A is an AG-subgroupoid of S.

(2) Let A be a left ideal of an ordered AG-groupoid S and $x, y \in S$. If $y \notin A$, then by definition of characteristic function $\chi_A(y) = 0$. Thus

$$\chi_A(xy) \geqslant \chi_A(y) = \min\{\chi_A(y), \beta\} \Rightarrow$$
$$\Rightarrow \chi_A(xy) \geqslant \min\{\chi_A(y), \beta\} \Rightarrow \max\{\chi_A(xy), \alpha\} \geqslant \min\{\chi_A(y), \beta\}.$$

Similarly, we have $\max\{\chi_A(xy), \alpha\} \geqslant \min\{\chi_A(y), \beta\}$, when $y \in A$. Therefore the characteristic function χ_A of A is a fuzzy left ideal with thresholds $(\alpha, \beta]$ of S.

Conversely, assume that the characteristic function $\chi_A$of A is a fuzzy left ideal with thresholds $(\alpha, \beta]$ of an ordered AG-groupoid S. Let $y \in A$and $z \in S$, then by definition $\chi_A(y) = 1$.Since $\max\{\chi_A(zy), \alpha\} \geqslant \min\{\chi_A(y), \beta\} = \beta$, χ_A being a fuzzy left ideal with thresholds $(\alpha, \beta]$ of S. Thus $\max\{\chi_A(zy), \alpha\} \geqslant \beta$. This implies that $\chi_A(zy) = 1$, i.e., $zy \in A$. Therefore A is a left ideal of S. ■

Theorem 3. Let μ be a fuzzy subset of an ordered AG-groupoid S. Then the following assertions hold:

(1) μ is a fuzzy ordered AG-subgroupoid with thresholds $(\alpha, \beta]$ of S if and only if $\mu \circ_\alpha^\beta \mu \subseteq \mu_\alpha^\beta$;

(2) μ is a fuzzy left (resp. right) ideal with thresholds $(\alpha, \beta]$ of S if and only if $S \circ_\alpha^\beta \mu \subseteq \mu_\alpha^\beta$ (resp. $\mu \circ_\alpha^\beta S \subseteq \mu_\alpha^\beta$).

Proof.

(1) Suppose that μ is a fuzzy AG-subgroupoid with thresholds $(\alpha, \beta]$ of an ordered AG-groupoid S and $x \in S$. If $(\mu \circ_\alpha^\beta \mu)(x) = 0$, then obvious $\mu \circ_\alpha^\beta \mu \subseteq \mu_\alpha^\beta$, otherwise we have

$$(\mu \circ_\alpha^\beta \mu)(x) = \{(\mu \circ \mu)(x) \wedge \beta\} \vee \alpha = \left\{\Big(\bigvee_{(y,z) \in A_x} \min\{\mu(y), \mu(z)\}\Big) \wedge \beta\right\} \vee \alpha \leqslant$$
$$\leqslant \left\{\bigvee_{(y,z) \in A_x} \min\{\mu(yz)\} \wedge \beta\right\} \vee \alpha = \{\mu(x) \wedge \beta\} \vee \alpha = \mu_\alpha^\beta(x) \Rightarrow \mu \circ_\alpha^\beta \mu \subseteq \mu_\alpha^\beta.$$

Conversely, assume that $\mu \circ_{\alpha}^{\beta} \mu \subseteq \mu_{\alpha}^{\beta}$. Let $x, y \in S$ such that $a \leqslant xy$. Now

$$\max\{\mu(xy), \alpha\} \geqslant \max\{\mu(a), \alpha\} = \max\{\min\{\mu(a), \beta\}, \alpha\} = \mu_{\alpha}^{\beta}(a) \geqslant (\mu \circ_{\alpha}^{\beta} \mu)(a) =$$
$$= \{(\mu \circ \mu)(a) \wedge \beta\} \vee \alpha = \Big\{\Big(\bigvee_{(s,t)\in A_a} \min\{\mu(s), \mu(t)\}\Big) \wedge \beta\Big\} \vee \alpha \geqslant$$
$$\geqslant \{\mu(x) \wedge \mu(y) \wedge \beta\} \vee \alpha = \mu(x) \wedge \mu(y) \wedge \beta = \min\{\mu(x), \mu(y), \beta\} \Rightarrow$$
$$\Rightarrow \max\{\mu(xy), \alpha\} \geqslant \min\{\mu(x), \mu(y), \beta\}.$$

Hence μ is a fuzzy AG-subgroupoid with thresholds $(\alpha, \beta]$ of S.

(2) Suppose that μ is a fuzzy left ideal with thresholds $(\alpha, \beta]$ of an ordered AG-groupoid S and $x \in S$. If $(S \circ_{\alpha}^{\beta} \mu)(x) = 0$, then obvious $S \circ_{\alpha}^{\beta} \mu \subseteq \mu_{\alpha}^{\beta}$, otherwise we have

$$(S \circ_{\alpha}^{\beta} \mu)(x) = \{(S \circ \mu)(x) \wedge \beta\} \vee \alpha = \Big\{\Big(\bigvee_{(y,z)\in A_x} \min\{S(y), \mu(z)\}\Big) \wedge \beta\Big\} \vee \alpha =$$
$$= \Big\{\Big(\bigvee_{(y,z)\in A_x} \min\{1, \mu(z)\}\Big) \wedge \beta\Big\} \vee \alpha = \Big\{\Big(\bigvee_{(y,z)\in A_x} \min\{\mu(z)\}\Big) \wedge \beta\Big\} \vee \alpha \leqslant$$
$$\leqslant \Big\{\Big(\bigvee_{(y,z)\in A_x} \min\{\mu(yz)\}\Big) \wedge \beta\Big\} \vee \alpha = (\mu(x) \wedge \beta) \vee \alpha = \mu_{\alpha}^{\beta}(x) \Rightarrow S \circ_{\alpha}^{\beta} \mu \subseteq \mu_{\alpha}^{\beta}.$$

Conversely, assume that $S \circ_{\alpha}^{\beta} \mu \subseteq \mu_{\alpha}^{\beta}$. Let $y, z \in S$ such that $x \leqslant yz$. Now

$$\max\{\mu(yz), \alpha\} \geqslant \max\{\mu(x), \alpha\} = \max\{\min\{\mu(x), \beta\}, \alpha\} = \mu_{\alpha}^{\beta}(x) \geqslant (S \circ_{\alpha}^{\beta} \mu)(x) =$$
$$= \{(S \circ \mu)(x) \wedge \beta\} \vee \alpha = \Big\{\Big(\bigvee_{(s,t)\in A_x} \min\{S(s), \mu(t)\}\Big) \wedge \beta\Big\} \vee \alpha \geqslant ((S(y) \wedge \mu(z)) \wedge \beta) \vee \alpha =$$
$$= (1 \wedge \mu(z)) \wedge \beta = \min\{\mu(z), \beta\} \Rightarrow \max\{\mu(yz), \alpha\} \geqslant \min\{\mu(z), \beta\}.$$

Therefore μ is a fuzzy left ideal with thresholds $(\alpha, \beta]$ of S. ■

Lemma 2. If μ and γ are two fuzzy AG-subgroupoid (resp. (left, right, two-sided) ideals) with thresholds $(\alpha, \beta]$ of an ordered AG-groupoid S, then $\mu \wedge_{\alpha}^{\beta} \gamma$ is also a fuzzy AG-subgroupoid (resp. (left, right, two-sided) ideal) with thresholds $(\alpha, \beta]$ of S.

Proof. Let μ and γ be two fuzzy AG-subgroupoids with thresholds $(\alpha, \beta]$ of an ordered AG-groupoid S. We have to show that $\mu \wedge_{\alpha}^{\beta} \gamma$ is also a fuzzy AG-subgroupoid with thresholds $(\alpha, \beta]$ of S. Now

$$\max\{(\mu \wedge_{\alpha}^{\beta} \gamma)(xy), \alpha\} = \max\{\{\{(\mu \wedge \gamma)(xy) \wedge \beta\} \vee \alpha\}, \alpha\} = \{(\mu \wedge \gamma)(xy) \wedge \beta\} \vee \alpha =$$
$$= \{\mu(xy) \wedge \gamma(xy) \wedge \beta\} \vee \alpha \geqslant \{\mu(x) \wedge \mu(y) \wedge \gamma(x) \wedge \gamma(y) \wedge \beta\} \vee \alpha =$$
$$= \{\mu(x) \wedge \gamma(x) \wedge \mu(y) \wedge \gamma(y) \wedge \beta\} \vee \alpha = \{(\mu \wedge \gamma)(x) \wedge (\mu \wedge \gamma)(y) \wedge \beta \wedge \beta \wedge \beta\} \vee \alpha =$$
$$= \{((\mu \wedge \gamma)(x) \wedge \beta) \wedge ((\mu \wedge \gamma)(y) \wedge \beta) \wedge \beta\} \vee \alpha =$$
$$= (\{(\mu \wedge \gamma)(x) \wedge \beta\} \vee \alpha) \wedge (\{(\mu \wedge \gamma)(y) \wedge \beta\} \vee \alpha) \wedge (\beta \vee \alpha) =$$
$$= (\mu \wedge_{\alpha}^{\beta} \gamma)(x) \wedge (\mu \wedge_{\alpha}^{\beta} \gamma)(y) \wedge \beta = \min\{(\mu \wedge_{\alpha}^{\beta} \gamma)(x), (\mu \wedge_{\alpha}^{\beta} \gamma)(y), \beta\}.$$

Thus $\max\{(\mu \wedge_{\alpha}^{\beta} \gamma)(xy), \alpha\} \geqslant \min\{(\mu \wedge_{\alpha}^{\beta} \gamma)(x), (\mu \wedge_{\alpha}^{\beta} \gamma)(y), \beta\}$. Hence $\mu \wedge_{\alpha}^{\beta} \gamma$ is a fuzzy AG-subgroupoid with thresholds $(\alpha, \beta]$ of S. ■

Lemma 3. If μ and γ are two fuzzy AG-subgroupoids with thresholds $(\alpha, \beta]$ of an ordered AG-groupoid S, then $\mu \circ_{\alpha}^{\beta} \gamma$ is also a fuzzy AG-subgroupoid with thresholds $(\alpha, \beta]$ of S.

Proof. Suppose that μ and γ are two fuzzy AG-subgroupoids with thresholds $(\alpha,\beta]$ of an ordered AG-groupoid S. We have to show that $\mu\circ_\alpha^\beta\gamma$ is also a fuzzy AG-subgroupoid with thresholds $(\alpha,\beta]$ of S. Now

$$(\mu\circ_\alpha^\beta\gamma)^2=(\mu\circ_\alpha^\beta\gamma)\circ_\alpha^\beta(\mu\circ_\alpha^\beta\gamma)=(\mu\circ_\alpha^\beta\mu)\circ_\alpha^\beta(\gamma\circ_\alpha^\beta\gamma)\subseteq\mu_\alpha^\beta\circ_\alpha^\beta\gamma_\alpha^\beta=\mu\circ_\alpha^\beta\gamma.$$

Therefore $\mu\circ_\alpha^\beta\gamma$ is a fuzzy AG-subgroupoid with thresholds $(\alpha,\beta]$ of S. ■

Remark 1. If μ is a fuzzy AG-subgroupoid with thresholds $(\alpha,\beta]$ of an ordered AG-groupoid S, then $\mu\circ_\alpha^\beta\mu$ is also a fuzzy AG-subgroupoid with thresholds $(\alpha,\beta]$ of S.

Lemma 4. Let S be an ordered AG-groupoid with left identity e. Then every fuzzy right ideal with thresholds $(\alpha,\beta]$ of S is a fuzzy ideal with thresholds $(\alpha,\beta]$ of S.

Proof. Suppose that μ is a fuzzy right ideal with thresholds $(\alpha,\beta]$ of an ordered AG-subgroupoid S and $x,y\in S$. Thus

$$\max\{\mu(xy),\alpha\}=\max\{\mu((ex)y),\alpha\}=\max\{\mu((yx)e),\alpha\}\geqslant$$
$$\geqslant\min\{\mu(yx),\beta\}\geqslant\min\{\mu(y),\beta\}.$$

Therefore μ is a fuzzy ideal with thresholds $(\alpha,\beta]$ of S. ■

Lemma 5. If μ and γ are two fuzzy left (resp. right) ideals with thresholds $(\alpha,\beta]$ of an ordered AG-groupoid S with left identity e, then $\mu\circ_\alpha^\beta\gamma$ is also a fuzzy left (resp. right) ideal with thresholds $(\alpha,\beta]$ of S.

Proof. Let μ and γ be two fuzzy left ideals with thresholds $(\alpha,\beta]$ of an ordered AG-groupoid S. We have to show that $\mu\circ_\alpha^\beta\gamma$ is also a fuzzy left ideal with thresholds $(\alpha,\beta]$ of S. Now

$$S\circ_\alpha^\beta(\mu\circ_\alpha^\beta\gamma)=(S\circ_\alpha^\beta S)\circ_\alpha^\beta(\mu\circ_\alpha^\beta\gamma)=(S\circ_\alpha^\beta\mu)\circ_\alpha^\beta(S\circ_\alpha^\beta\gamma)\subseteq\mu\circ_\alpha^\beta\gamma.$$

Hence $\mu\circ_\alpha^\beta\gamma$ is a fuzzy left ideal with thresholds $(\alpha,\beta]$ of S. Similarly, we can prove for right ideals. ■

Remark 2. If μ is a fuzzy left (resp. right) ideal with thresholds $(\alpha,\beta]$ of an ordered AG-groupoid S with left identity e, then $\mu\circ_\alpha^\beta\mu$ is a fuzzy ideal with thresholds $(\alpha,\beta]$ of S.

Lemma 6. If μ and γ are two fuzzy ideals with thresholds $(\alpha,\beta]$ of an ordered AG-groupoid S, then $\mu\circ_\alpha^\beta\gamma\subseteq\mu\wedge_\alpha^\beta\gamma$.

Proof. Let μ and γ be two fuzzy ideals with thresholds $(\alpha,\beta]$ of an ordered AG-groupoid S and $x\in S$. If $(\mu\circ_\alpha^\beta\gamma)(x)=0$, then obvious $\mu\circ_\alpha^\beta\gamma\subseteq\mu\wedge_\alpha^\beta\gamma$, otherwise we have

$$(\mu\circ_\alpha^\beta\gamma)(x)=\{(\mu\circ\gamma)(x)\wedge\beta\}\vee\alpha=\Big\{\Big(\bigvee_{(y,z)\in A_x}\min\{\mu(y),\gamma(z)\}\Big)\wedge\beta\Big\}\vee\alpha\leqslant$$
$$\leqslant\Big\{\Big(\bigvee_{(y,z)\in A_x}\min\{\mu(yz),\gamma(yz)\}\Big)\wedge\beta\Big\}\vee\alpha=\Big\{\Big(\bigvee_{(y,z)\in A_x}\min\{(\mu\wedge\gamma)(yz)\}\Big)\wedge\beta\Big\}\vee\alpha=$$
$$=\{(\mu\wedge\gamma)(x)\wedge\beta\}\vee\alpha=(\mu\wedge_\alpha^\beta\gamma)(x).$$

Therefore $\mu\circ_\alpha^\beta\gamma\subseteq\mu\wedge_\alpha^\beta\gamma$. ■

Remark 3. If μ is a fuzzy ideal with thresholds $(\alpha,\beta]$ of an ordered AG-groupoid S, then $\mu\circ_\alpha^\beta\mu\subseteq\mu_\alpha^\beta$.

Lemma 7. Let S be an ordered AG-groupoid. Then $\mu \circ_{\alpha}^{\beta} \gamma \subseteq \mu \wedge_{\alpha}^{\beta} \gamma$ for every fuzzy right ideal μ with thresholds $(\alpha, \beta]$ and for every fuzzy left ideal γ with thresholds $(\alpha, \beta]$ of S.

Proof. Same as Lemma 6. ■

Theorem 4. Let A be a non-empty subset of an ordered AG-groupoid S. Then the following conditions are true:

(1) A is an interior ideal of S if and only if χ_A is a fuzzy interior ideal with thresholds $(\alpha, \beta]$ of S;
(2) A is a quasi-ideal of S if and only if χ_A is a fuzzy quasi-ideal with thresholds $(\alpha, \beta]$ of S;
(3) A is a bi-ideal of S if and only if χ_A is a fuzzy bi-ideal with thresholds $(\alpha, \beta]$ of S;
(4) A is a generalized bi-ideal of S if and only if χ_A is a fuzzy generalized bi-ideal with thresholds $(\alpha, \beta]$ of S.

Proof.

(1) Let A be an interior ideal of an ordered AG-groupoid S. Let $x, y, a \in S$. If $a \notin A$, then by definition of characteristic function $\chi_A(a) = 0$. Thus

$$\chi_A((xa)y) \geqslant \chi_A(a) = \min\{\chi_A(a), \beta\} \Rightarrow \chi_A((xa)y) \geqslant \min\{\chi_A(a), \beta\} \Rightarrow \\ \Rightarrow \max\{\chi_A((xa)y), \alpha\} \geqslant \min\{\chi_A(a), \beta\}.$$

Similarly, we have $\max\{\chi_A((xa)y), \alpha\} \geqslant \min\{\chi_A(a), \beta\}$, when $a \in A$. Hence the characteristic function χ_A of A is a fuzzy interior ideal with thresholds $(\alpha, \beta]$ of S.

Conversely, suppose that the characteristic function $\chi_A$of A is a fuzzy interior ideal with thresholds $(\alpha, \beta]$ of S. Let $t \in (SA)S$, so $t = (xa)y$, where $a \in A$ and $x, y \in S$. Then by definition $\chi_A(a) = 1$. Since $\max\{\chi_A((xa)y), \alpha\} \geqslant \min\{\chi_A(a), \beta\} = \beta$, χ_A being a fuzzy interior ideal with thresholds $(\alpha, \beta]$ of S. This implies that $\chi_A((xa)y) \geqslant \beta$, thus $\chi_A((xa)y) = 1$, i.e., $(xa)y \in A$. Hence A is an interior ideal of S.

(2) Let A be a quasi-ideal of S. Let $x \in S$ and $x \notin A$, then $x \notin SA$ or $x \notin AS$. If $x \notin SA$, then by definition of characteristic function $(S \circ \chi_A)(x) = 0$. Thus $\max\{\chi_A(x), \alpha\} \geqslant 0 = = \min\{(\chi_A \circ S)(x), (S \circ \chi_A)(x), \beta\}$. If $x \in A$, then $\max\{\chi_A(x), \alpha\} = 1 \geqslant \min\{(\chi_A \circ S)(x), S \circ \chi_A(x), \beta\}$. Therefore the characteristic function χ_A of A is a fuzzy quasi-ideal with thresholds $(\alpha, \beta]$ of S.

Conversely, assume that the characteristic function χ_A of A is a fuzzy quasi-ideal with thresholds $(\alpha, \beta]$ of S. Let x be an element of $AS \cap SA$, this means that $x \in AS$ and SA. Since

$$\max\{\chi_A(x), \alpha\} \geqslant \min\{(\chi_A \circ S)(x), (S \circ \chi_A)(x), \beta\} = \min\{(\chi_A \circ \chi_S)(x), (\chi_S \circ \chi_A)(x), \beta\} = \\ = \min\{\chi_{AS}(x), \chi_{SA}(x), \beta\} = \beta \Rightarrow \max\{\chi_A(x), \alpha\} \geqslant \beta.$$

Thus $\chi_A(x) = 1$, i.e., $x \in A$. Therefore A is a quasi-ideal of S.

(3) Let A be a bi-ideal of S. Let $x, y, a \in S$. If $x, y \notin A$, then by definition of characteristic function $\chi_A(x) = \chi_A(y) = 0$. Thus

$$\chi_A((xa)y) \geqslant \chi_A(x) \wedge \chi_A(y) = \min\{\chi_A(x), \chi_A(y), \beta\} \Rightarrow \chi_A((xa)y) \geqslant \min\{\chi_A(x), \chi_A(y), \beta\} \Rightarrow \\ \Rightarrow \max\{\chi_A((xa)y), \alpha\} \geqslant \min\{\chi_A(x), \chi_A(y), \beta\}.$$

Similarly, we have $\max\{\chi_A((xa)y), \alpha\} \geqslant \min\{\chi_A(x), \chi_A(y), \beta\}$, when $x, y \in A$. Hence the characteristic function χ_A of A is a fuzzy bi-ideal with thresholds $(\alpha, \beta]$ of S.

Conversely, suppose that the characteristic function $\chi_A$of A is a fuzzy bi-ideal with thresholds $(\alpha, \beta]$ of S. Let $t \in (AS)A$, so $t = (xa)y$, where $x, y \in A$ and $a \in S$. Then by definition $\chi_A(x) = \chi_A(y) = 1$. As $\max\{\chi_A((xa)y), \alpha\} \geqslant \min\{\chi_A(x), \chi_A(y), \beta\} = \beta$, χ_A being a fuzzy bi-ideal with thresholds $(\alpha, \beta]$ of S. This implies that $\chi_A((xa)y) \geqslant \beta$, thus $\chi_A((xa)y) = 1$, i.e., $(xa)y \in A$. Hence A is bi-ideal of S. Similarly, we can prove (4). ■

Theorem 5. Let μ be a fuzzy subset of an ordered AG-groupoid S. Then μ is a fuzzy interior ideal with thresholds $(\alpha, \beta]$ of S if and only if $(S \circ_\alpha^\beta \mu) \circ_\alpha^\beta S \subseteq \mu_\alpha^\beta$.

Proof. Suppose that μ is a fuzzy interior ideal with thresholds $(\alpha, \beta]$ of an ordered AG-groupoid S and $x \in S$. If $((S \circ_\alpha^\beta \mu) \circ_\alpha^\beta S)(x) = 0$, then obvious $(S \circ_\alpha^\beta \mu) \circ_\alpha^\beta S \subseteq \mu_\alpha^\beta$, otherwise there exist $a, b, c, d \in S$ such that $x \leqslant ab$ and $a \leqslant cd$. Since μ is a fuzzy interior ideal with thresholds $(\alpha, \beta]$ of S, this implies that $\max\{\mu((cd)b), \alpha\} \geqslant \min\{\mu(d), \beta\}$. Now

$$((S \circ_\alpha^\beta \mu) \circ_\alpha^\beta S)(x) = \{((S \circ \mu) \circ S)(x) \wedge \beta\} \vee \alpha =$$
$$= \Big\{\Big(\bigvee_{(a,b)\in A_x} \min\{(S \circ \mu)(a), S(b)\}\Big) \wedge \beta\Big\} \vee \alpha = \Big\{\Big(\bigvee_{(a,b)\in A_x} \min\{(S \circ \mu)(a), 1\}\Big) \wedge \beta\Big\} \vee \alpha =$$
$$= \Big\{\Big(\bigvee_{(a,b)\in A_x} \min\{(S \circ \mu)(a)\}\Big) \wedge \beta\Big\} \vee \alpha =$$
$$= \Big\{\Big(\bigvee_{(a,b)\in A_x} \min\Big\{\Big(\bigvee_{(c,d)\in A_a} \min\{S(c), \mu(d)\}\Big)\Big\}\Big) \wedge \beta\Big\} \vee \alpha =$$
$$= \Big\{\Big(\bigvee_{(a,b)\in A_x} \min\Big\{\Big(\bigvee_{(c,d)\in A_a} \min\{1, \mu(d)\}\Big)\Big\}\Big) \wedge \beta\Big\} \vee \alpha =$$
$$= \Big\{\Big(\bigvee_{(a,b)\in A_x} \min\Big\{\Big(\bigvee_{(c,d)\in A_a} \min\{\mu(d)\}\Big)\Big\}\Big) \wedge \beta\Big\} \vee \alpha = \Big\{\Big(\bigvee_{((c,d),b)\in A_x} \min\{\mu(d)\}\Big) \wedge \beta\Big\} \vee \alpha \leqslant$$
$$\leqslant \Big\{\Big(\bigvee_{((c,d),b)\in A_x} \min\{\mu((cd)b)\}\Big) \wedge \beta\Big\} \vee \alpha = \{\mu(x) \wedge \beta\} \vee \alpha = \mu_\alpha^\beta(x) \Rightarrow (S \circ_\alpha^\beta \mu) \circ_\alpha^\beta S \subseteq \mu_\alpha^\beta.$$

Conversely, assume that $(S \circ_\alpha^\beta \mu) \circ_\alpha^\beta S \subseteq \mu_\alpha^\beta$ and $x, y, z \in S$ such that $a \leqslant (xy)z$. Now

$$\max\{\mu((xy)z), \alpha\} = \max\{\min\{\mu((xy)z), \beta\}, \alpha\} \geqslant \max\{\min\{\mu(a), \beta\}, \alpha\} = \mu_\alpha^\beta(a) \geqslant$$
$$\geqslant ((S \circ_\alpha^\beta \mu) \circ_\alpha^\beta S)(a) = \{((S \circ \mu) \circ S)(a) \wedge \beta\} \vee \alpha =$$
$$= \Big\{\Big(\bigvee_{(s,t)\in A_a} \min\{(S \circ \mu)(s), S(t)\}\Big) \wedge \beta\Big\} \vee \alpha \geqslant \{((S \circ \mu)(xy) \wedge S(z)) \wedge \beta\} \vee \alpha =$$
$$= \{((S \circ \mu)(xy) \wedge 1) \wedge \beta\} \vee \alpha = \{(S \circ \mu)(xy) \wedge \beta\} \vee \alpha =$$
$$= \Big\{\Big(\bigvee_{(m,n)\in A_{xy}} \min\{S(m), \mu(n)\}\Big) \wedge \beta\Big\} \vee \alpha \geqslant \{(S(x) \wedge \mu(y)) \wedge \beta\} \vee \alpha =$$
$$= \{(1 \wedge \mu(y)) \wedge \beta\} \vee \alpha = \mu(y) \wedge \beta = \min\{\mu(y), \beta\} \Rightarrow \max\{\mu((xy)z), \alpha\} \geqslant \min\{\mu(y), \beta\}.$$

Therefore μ is a fuzzy interior ideal with thresholds $(\alpha, \beta]$ of S. ■

Theorem 6. Let μ be a fuzzy ordered AG-subgroupoid with thresholds $(\alpha, \beta]$ of an ordered AG-groupoid S. Then μ is a fuzzy bi-ideal with thresholds $(\alpha, \beta]$ of S if and only if $(\mu \circ_\alpha^\beta S) \circ_\alpha^\beta \mu \subseteq \mu_\alpha^\beta$.

Proof. Same as Theorem 5. ■

Theorem 7. Let μ be a fuzzy subset of an ordered AG-groupoid S. Then μ is a fuzzy generalized bi-ideal with thresholds $(\alpha, \beta]$ of S if and only if $(\mu \circ_\alpha^\beta S) \circ_\alpha^\beta \mu \subseteq \mu_\alpha^\beta$.

Proof. Same as Theorem 5. ■

Lemma 8. If μ and γ are two fuzzy bi- (resp. generalized bi-, quasi-, interior) ideals with thresholds $(\alpha,\beta]$ of an ordered AG-groupoid S, then $\mu\wedge_\alpha^\beta\gamma$ is also a fuzzy bi- (resp. generalized bi-, quasi-, interior) ideal with thresholds $(\alpha,\beta]$ of S.

Proof. Let μ and γ be two fuzzy bi-ideals with thresholds $(\alpha,\beta]$ of an ordered AG-groupoid S. We have to show that $\mu\wedge_\alpha^\beta\gamma$ is also a fuzzy bi-ideal with thresholds $(\alpha,\beta]$ of S. Since μ and γ are fuzzy AG-subgroupoids with thresholds $(\alpha,\beta]$ of S then $\mu\wedge_\alpha^\beta\gamma$ is also a fuzzy AG-subgroupoid with thresholds $(\alpha,\beta]$ of S by the Lemma 2. We have to show that $\max\{(\mu\wedge_\alpha^\beta\gamma)((xa)y),\alpha\}\geqslant\min\{(\mu\wedge_\alpha^\beta\gamma)(x),(\mu\wedge_\alpha^\beta\gamma)(y),\beta\}$. Now

$$\max\{(\mu\wedge_\alpha^\beta\gamma)((xa)y),\alpha\}=\max\{\{\{(\mu\wedge\gamma)((xa)y)\wedge\beta\}\vee\alpha\},\alpha\}=$$
$$=\{(\mu\wedge\gamma)((xa)y)\wedge\beta\}\vee\alpha=\{\mu((xa)y)\wedge\gamma((xa)y)\wedge\beta\}\vee\alpha\geqslant$$
$$\geqslant\{\mu(x)\wedge\mu(y)\wedge\gamma(x)\wedge\gamma(y)\wedge\beta\}\vee\alpha=\{\mu(x)\wedge\gamma(x)\wedge\mu(y)\wedge\gamma(y)\wedge\beta\}\vee\alpha=$$
$$=\{(\mu\wedge\gamma)(x)\wedge(\mu\wedge\gamma)(y)\wedge\beta\wedge\beta\wedge\beta\}\vee\alpha=\{((\mu\wedge\gamma)(x)\wedge\beta)\wedge((\mu\wedge\gamma)(y)\wedge\beta)\wedge\beta\}\vee\alpha=$$
$$=(\{(\mu\wedge\gamma)(x)\wedge\beta\}\vee\alpha)\wedge(\{(\mu\wedge\gamma)(y)\wedge\beta\}\vee\alpha)\wedge(\beta\vee\alpha)=$$
$$=(\mu\wedge_\alpha^\beta\gamma)(x)\wedge(\mu\wedge_\alpha^\beta\gamma)(y)\wedge\beta=\min\{(\mu\wedge_\alpha^\beta\gamma)(x),(\mu\wedge_\alpha^\beta\gamma)(y),\beta\}.$$

Thus $\max\{(\mu\wedge_\alpha^\beta\gamma)((xa)y),\alpha\}\geqslant\min\{(\mu\wedge_\alpha^\beta\gamma)(x),(\mu\wedge_\alpha^\beta\gamma)(y),\beta\}$. Hence $\mu\wedge_\alpha^\beta\gamma$ is a fuzzy bi-ideal with thresholds $(\alpha,\beta]$ of S. ■

Lemma 9. If μ and γ are two fuzzy bi- (resp. generalized bi-, interior) ideals with thresholds $(\alpha,\beta]$ of an ordered AG-groupoid S with left identity e, then $\mu\circ_\alpha^\beta\gamma$ is also a fuzzy bi- (resp. generalized bi-, interior) ideal with thresholds $(\alpha,\beta]$ of S.

Proof. Let μ and γ be two fuzzy bi-ideals with thresholds $(\alpha,\beta]$ of an ordered AG-groupoid S. We have to show that $\mu\circ_\alpha^\beta\gamma$ is also a fuzzy bi-ideal with thresholds $(\alpha,\beta]$ of S. Since μ and γ are fuzzy AG-subgroupoids with thresholds $(\alpha,\beta]$ of S, then $\mu\circ_\alpha^\beta\gamma$ is also a fuzzy AG-subgroupoid with thresholds $(\alpha,\beta]$ of S by the Lemma 3. Now

$$((\mu\circ_\alpha^\beta\gamma)\circ_\alpha^\beta S)\circ_\alpha^\beta(\mu\circ_\alpha^\beta\gamma)=((\mu\circ_\alpha^\beta\gamma)\circ_\alpha^\beta(S\circ_\alpha^\beta S))\circ_\alpha^\beta(\mu\circ_\alpha^\beta\gamma)=$$
$$=((\mu\circ_\alpha^\beta S)\circ_\alpha^\beta(\gamma\circ_\alpha^\beta S))\circ_\alpha^\beta(\mu\circ_\alpha^\beta\gamma)=((\mu\circ_\alpha^\beta S)\circ_\alpha^\beta\mu)\circ_\alpha^\beta((\gamma\circ_\alpha^\beta S)\circ_\alpha^\beta\gamma)\subseteq\mu_\alpha^\beta\circ_\alpha^\beta\gamma_\alpha^\beta=\mu\circ_\alpha^\beta\gamma.$$

Therefore $\mu\circ_\alpha^\beta\gamma$ is a fuzzy bi-ideal with thresholds $(\alpha,\beta]$ of S. ■

Lemma 10. Every fuzzy ideal with thresholds $(\alpha,\beta]$ of an ordered AG-groupoid S is a fuzzy interior ideal with thresholds $(\alpha,\beta]$ of S. The converse is not true in general.

Proof. Let μ be a fuzzy ideal with thresholds $(\alpha,\beta]$ of an ordered AG-groupoid S and $x,y,z\in S$. Thus $\max\{\mu\left((xy)z\right),\alpha\}\geqslant\min\{\mu\left(xy\right),\beta\}\geqslant\min\{\mu\left(y\right),\beta\}$. Hence μ is a fuzzy interior ideal with thresholds $(\alpha,\beta]$ of S. ■

Proposition 2. Let μ be a fuzzy subset of an ordered AG-groupoid S with left identity e. Then μ is a fuzzy ideal with thresholds $(\alpha,\beta]$ of S if and only if μ is a fuzzy interior ideal with thresholds $(\alpha,\beta]$ of S.

Proof. Suppose that μ is a fuzzy interior ideal with thresholds $(\alpha,\beta]$ of an ordered AG-groupoid S and $x,y\in S$. Thus $\max\{\mu(xy),\alpha\}=\max\{\mu((ex)y),\alpha\}\geqslant\min\{\mu(x),\beta\}$. So μ is a fuzzy right ideal with thresholds $(\alpha,\beta]$ of S. Therefore μ is a fuzzy ideal with thresholds $(\alpha,\beta]$ of S by the Lemma 4. Converse is true by the Lemma 10. ■

Lemma 11. Every fuzzy left (resp. right, two-sided) ideal with thresholds $(\alpha,\beta]$ of an ordered AG-groupoid S is a fuzzy bi-ideal with thresholds $(\alpha,\beta]$ of S. The converse is not true in general.

Proof. Assume that μ is a fuzzy right ideal with thresholds $(\alpha, \beta]$ of an ordered AG-groupoid S and $x, y, z \in S$. Thus $\max\{\mu\left((xy)z\right), \alpha\} \geqslant \min\{\mu\left(xy\right), \beta\} \geqslant \min\{\mu\left(x\right), \beta\}$ and $\max\{\mu\left((xy)z\right), \alpha\} = \max\{\mu\left((zy)x\right), \alpha\} \geqslant \min\{\mu\left(zy\right), \beta\} \geqslant \min\{\mu\left(z\right), \beta\}$.

This implies that $\max\{\mu((xy)z), \alpha\} \geqslant \min\{\mu(x), \mu(z), \beta\}$. So μ is a fuzzy bi-ideal with thresholds $(\alpha, \beta]$ of S. ■

Lemma 12. Every fuzzy bi-ideal with thresholds $(\alpha, \beta]$ of an ordered AG-groupoid S is a fuzzy generalized bi-ideal with thresholds $(\alpha, \beta]$ of S. The converse is not true in general.

Proof. Obvious. ■

Lemma 13. Every fuzzy left (resp. right, two-sided) ideal with thresholds $(\alpha, \beta]$ of an ordered AG-groupoid S is a fuzzy quasi-ideal with thresholds $(\alpha, \beta]$ of S. The converse is not true in general.

Proof. Let μ be a fuzzy left ideal with thresholds $(\alpha, \beta]$ of an ordered AG-groupoid S. Thus

$$\max\{\mu(x), \alpha\} \geqslant \min\{(S \circ \mu)(x), \beta\} \geqslant \min\{(\mu \circ S)(x), (S \circ \mu)(x), \beta\}.$$

Hence μ is a fuzzy quasi-ideal with thresholds $(\alpha, \beta]$ of S. ■

Proposition 3. Every fuzzy quasi-ideal with thresholds $(\alpha, \beta]$ of an ordered AG-groupoid S is a fuzzy AG-subgroupoid with thresholds $(\alpha, \beta]$ of S.

Proof. Suppose that μ is a fuzzy quasi-ideal with thresholds $(\alpha, \beta]$ of an ordered AG-groupoid S. Since $\mu \circ_\alpha^\beta \mu \subseteq \mu \circ_\alpha^\beta S$ and $\mu \circ_\alpha^\beta \mu \subseteq S \circ_\alpha^\beta \mu$, this implies that $\mu \circ_\alpha^\beta \mu \subseteq \mu \circ_\alpha^\beta S \wedge S \circ_\alpha^\beta \mu \subseteq \mu_\alpha^\beta$. Therefore μ is a fuzzy AG-subgroupoid with thresholds $(\alpha, \beta]$ of S. ■

Proposition 4. Let μ be a fuzzy right ideal with thresholds $(\alpha, \beta]$ and γ be a fuzzy left ideal with thresholds $(\alpha, \beta]$ of an ordered AG-groupoid S, respectively. Then $\mu \wedge_\alpha^\beta \gamma$ is a fuzzy quasi-ideal with thresholds $(\alpha, \beta]$ of S.

Proof. We have to show that $\mu \wedge_\alpha^\beta \gamma$ is a fuzzy quasi-ideal with thresholds $(\alpha, \beta]$ of an ordered AG-subgroupoid S. Now

$$((\mu \wedge_\alpha^\beta \gamma) \circ_\alpha^\beta S) \wedge (S \circ_\alpha^\beta (\mu \wedge_\alpha^\beta \gamma)) \subseteq (\mu \circ_\alpha^\beta S) \wedge (S \circ_\alpha^\beta \gamma) \subseteq \mu_\alpha^\beta \wedge \gamma_\alpha^\beta = \mu \wedge_\alpha^\beta \gamma.$$

Thus $\mu \wedge_\alpha^\beta \gamma$ is a fuzzy quasi-ideal with thresholds $(\alpha, \beta]$ of S. ■

Lemma 14. Let S be an ordered AG-groupoid with left identity e, such that $(xe)S = xS$ for all $x \in S$. Then every fuzzy quasi-ideal with thresholds $(\alpha, \beta]$ of S is a fuzzy bi-ideal with thresholds $(\alpha, \beta]$ of S.

Proof. Assume that μ is a fuzzy quasi-ideal with thresholds $(\alpha, \beta]$ of an ordered AG-subgroupoid S. This implies that μ is a fuzzy AG-subgroupoid with thresholds $(\alpha, \beta]$ of S. We have to show that $(\mu \circ_\alpha^\beta S) \circ_\alpha^\beta \mu \subseteq \mu_\alpha^\beta$. Now

$$(\mu \circ_\alpha^\beta S) \circ_\alpha^\beta \mu \subseteq (S \circ_\alpha^\beta S) \circ_\alpha^\beta \mu \subseteq S \circ_\alpha^\beta \mu$$
$$\text{and } (\mu \circ_\alpha^\beta S) \circ_\alpha^\beta \mu \subseteq (\mu \circ_\alpha^\beta S) \circ_\alpha^\beta S = (\mu \circ_\alpha^\beta S) \circ_\alpha^\beta (e \circ_\alpha^\beta S) = (\mu \circ_\alpha^\beta e) \circ_\alpha^\beta (S \circ_\alpha^\beta S) \subseteq$$
$$\subseteq (\mu \circ_\alpha^\beta e) \circ_\alpha^\beta S_\alpha^\beta = \mu_\alpha^\beta \circ_\alpha^\beta S_\alpha^\beta = \mu \circ_\alpha^\beta S \Rightarrow (\mu \circ_\alpha^\beta S) \circ_\alpha^\beta \mu \subseteq \mu \circ_\alpha^\beta S \wedge S \circ_\alpha^\beta \mu \subseteq \mu_\alpha^\beta.$$

So μ is a fuzzy bi-ideal with thresholds $(\alpha, \beta]$ of S. ■

Proposition 5. If μ and γ are two fuzzy quasi-ideals with thresholds $(\alpha, \beta]$ of an ordered AG-groupoid S with left identity e, such that $(xe)S = xS$ for all $x \in S$, then $\mu \circ_\alpha^\beta \gamma$ is a fuzzy bi-ideal with thresholds $(\alpha, \beta]$ of S.

Proof. Let μ and γ be two fuzzy quasi-ideals with thresholds $(\alpha, \beta]$ of an ordered AG-groupoid S, this implies that μ and γ be two fuzzy bi-ideals with thresholds $(\alpha, \beta]$ of S, by the Lemma 14. Then $\mu \circ_{\alpha}^{\beta} \gamma$ is also a fuzzy bi-ideal with thresholds $(\alpha, \beta]$ of S by the Lemma 9. ∎

2. Regular Ordered AG-groupoids

An ordered AG-groupoid S will be called a regular if, for every $x \in S$, there exists an element $a \in S$ such that $x \leqslant (xa)x$. Equivalent definitions are as follows:

(1) $A \subseteq ((AS)A]$ for every $A \subseteq S$;

(2) $x \in ((xS)x]$ for every $x \in S$.

In this section, we give the characterizations of regular ordered AG-groupoids by the properties of fuzzy left (right, quasi-, bi-, generalized bi-) ideals with thresholds $(\alpha, \beta]$.

Lemma 15. Every fuzzy right ideal with thresholds $(\alpha, \beta]$ of a regular ordered AG-groupoid S is a fuzzy ideal with thresholds $(\alpha, \beta]$ of S.

Proof. Suppose that μ is a fuzzy right ideal with thresholds $(\alpha, \beta]$ of S. Let $x, y \in S$, this implies that there exists $a \in S$, such that $x \leqslant (xa)x$. Thus

$$\max\{\mu(xy), \alpha\} \geqslant \max\{\mu(((xa)x)y), \alpha\} = \max\{\mu((yx)(xa)), \alpha\} \geqslant \\ \geqslant \min\{\mu(yx), \beta\} \geqslant \min\{\mu(y), \beta\}.$$

Hence μ is a fuzzy ideal with thresholds $(\alpha, \beta]$ of S. ∎

Lemma 16. Every fuzzy ideal with thresholds $(\alpha, \beta]$ of a regular ordered AG-groupoid S is a fuzzy idempotent with thresholds $(\alpha, \beta]$.

Proof. Assume that μ is a fuzzy ideal with thresholds $(\alpha, \beta]$ of S and $\mu \circ_{\alpha}^{\beta} \mu \subseteq \mu_{\alpha}^{\beta}$. We have to show that $\mu_{\alpha}^{\beta} \subseteq \mu \circ_{\alpha}^{\beta} \mu$. Let $x \in S$, this means that there exists $a \in S$ such that $x \leqslant (xa)x$. Thus

$$(\mu \circ_{\alpha}^{\beta} \mu)(x) = \{(\mu \circ \mu)(x) \wedge \beta\} \vee \alpha = \left\{\Big(\bigvee_{(y,z)\in A_x} \min\{\mu(y), \mu(z)\}\Big) \wedge \beta\right\} \vee \alpha \geqslant \\ \geqslant \{\mu(xa) \wedge \mu(x) \wedge \beta\} \vee \alpha = (\mu(xa) \vee \alpha) \wedge (\mu(x) \vee \alpha) \wedge (\beta \vee \alpha) \geqslant \\ \geqslant (\mu(x) \wedge \beta) \wedge \mu(x) \wedge \beta = \mu(x) \wedge \beta = (\mu(x) \wedge \beta) \vee \alpha = \mu_{\alpha}^{\beta}(x) \Rightarrow \mu_{\alpha}^{\beta} \subseteq \mu \circ_{\alpha}^{\beta} \mu.$$

Therefore $\mu_{\alpha}^{\beta} = \mu \circ_{\alpha}^{\beta} \mu$. ∎

Remark 4. Every fuzzy right ideal with thresholds $(\alpha, \beta]$ of a regular ordered AG-groupoid S is a fuzzy idempotent with thresholds $(\alpha, \beta]$.

Proposition 6. Let μ be a fuzzy subset of a regular ordered AG-groupoid S. Then μ is a fuzzy ideal with thresholds $(\alpha, \beta]$ of S if and only if μ is a fuzzy interior ideal with thresholds $(\alpha, \beta]$ of S.

Proof. Consider that μ is a fuzzy interior ideal with thresholds $(\alpha, \beta]$ of S. Let $x, y \in S$, then there exists an element $a \in S$, such that $x \leqslant (xa)x$. Thus

$$\max\{\mu(xy), \alpha\} \geqslant \max\{\mu(((xa)x)y), \alpha\} = \max\{\mu((yx)(xa)), \alpha\} \geqslant \min\{\mu(x), \beta\}.$$

Consequently μ is a fuzzy right ideal with thresholds $(\alpha, \beta]$ of S. So μ is a fuzzy ideal with thresholds $(\alpha, \beta]$ of S by the Lemma 15. Converse is true by the Lemma 10. ∎

Remark 5. The concept of fuzzy (two-sided, interior) ideals with thresholds $(\alpha, \beta]$ coincides in regular ordered AG-groupoids.

Proposition 7. Let S be a regular ordered AG-groupoid. Then $(\mu \circ_\alpha^\beta S) \wedge (S \circ_\alpha^\beta \mu) = \mu_\alpha^\beta$ for every fuzzy right ideal μ with thresholds $(\alpha, \beta]$ of S.

Proof. Suppose that μ is a fuzzy right ideal with thresholds $(\alpha, \beta]$ of S. This implies that $(\mu \circ_\alpha^\beta S) \wedge (S \circ_\alpha^\beta \mu) \subseteq \mu_\alpha^\beta$, because every fuzzy right ideal with thresholds $(\alpha, \beta]$ of S is a fuzzy quasi-ideal with thresholds $(\alpha, \beta]$ of S by the Lemma 13. Let $x \in S$, this implies that there exists $a \in S$, such that $x \leqslant (xa)x$. Thus

$$(\mu \circ_\alpha^\beta S)(x) = \{(\mu \circ S)(x) \wedge \beta\} \vee \alpha = \left\{ \Big(\bigvee_{(y,z) \in A_x} \min\{\mu(y), S(z)\} \Big) \wedge \beta \right\} \vee \alpha \geqslant$$
$$\geqslant \{\mu\,(xa) \wedge S\,(x) \wedge \beta\} \vee \alpha = \{\mu\,(xa) \wedge \beta\} \vee \alpha = (\mu\,(xa) \vee \alpha) \wedge (\beta \vee \alpha) \geqslant (\mu\,(x) \wedge \beta) \wedge \beta =$$
$$= \mu\,(x) \wedge \beta = (\mu\,(x) \wedge \beta) \vee \alpha = \mu_\alpha^\beta(x) \Rightarrow \mu_\alpha^\beta \subseteq \mu \circ_\alpha^\beta S.$$

Similarly, we have $\mu_\alpha^\beta \subseteq S \circ_\alpha^\beta \mu$, i.e., $\mu_\alpha^\beta \subseteq (\mu \circ_\alpha^\beta S) \wedge (S \circ_\alpha^\beta \mu)$. Hence $(\mu \circ_\alpha^\beta S) \wedge (S \circ_\alpha^\beta \mu) = \mu_\alpha^\beta$. ∎

Lemma 17. Let S be a regular ordered AG-groupoid. Then $\mu \circ_\alpha^\beta \gamma = \mu \wedge_\alpha^\beta \gamma$ for every fuzzy right ideal μ with thresholds $(\alpha, \beta]$ and every fuzzy left ideal γ with thresholds $(\alpha, \beta]$ of S.

Proof. Since $\mu \circ_\alpha^\beta \gamma \subseteq \mu \wedge_\alpha^\beta \gamma$, for every fuzzy right ideal μ with thresholds $(\alpha, \beta]$ and every fuzzy left ideal γ with thresholds $(\alpha, \beta]$ of S by the Lemma 7. Let $x \in S$, this means that there exists $a \in S$ such that $x \leqslant (xa)x$. Thus

$$(\mu \circ_\alpha^\beta \gamma)(x) = \{(\mu \circ \gamma)(x) \wedge \beta\} \vee \alpha = \left\{ \Big(\bigvee_{(y,z) \in A_x} \min\{\mu(y), \gamma(z)\} \Big) \wedge \beta \right\} \vee \alpha \geqslant$$
$$\geqslant \{\mu\,(xa) \wedge \gamma\,(x) \wedge \beta\} \vee \alpha = (\mu\,(xa) \vee \alpha) \wedge (\gamma\,(x) \vee \alpha) \wedge (\beta \vee \alpha) \geqslant$$
$$\geqslant (\mu\,(x) \wedge \beta) \wedge \gamma\,(x) \wedge \beta = \mu\,(x) \wedge \gamma\,(x) \wedge \beta = (\mu \wedge \gamma)\,(x) \wedge \beta =$$
$$= \{(\mu \wedge \gamma)\,(x) \wedge \beta\} \vee \alpha = (\mu \wedge_\alpha^\beta \gamma)(x) \Rightarrow \mu \wedge_\alpha^\beta \gamma \subseteq \mu \circ_\alpha^\beta \gamma.$$

Therefore $\mu \circ_\alpha^\beta \gamma = \mu \wedge_\alpha^\beta \gamma$. ∎

Lemma 18. Let S be an ordered AG-groupoid with left identity e. Then Sa is a smallest left ideal of S containing a.

Proof. Let $x \in Sa$ and $s \in S$, this implies that $x = s_1 a$, $s_1 \in S$. Now

$$sx = s(s_1 a) = (es)(s_1 a) = ((s_1 a)s)e = ((s_1 a)(es))e =$$
$$= ((s_1 e)(as))e = (e(as))(s_1 e) = (as)(s_1 e) = ((s_1 e)s)a \in Sa.$$

Hence $sx \in Sa$ and $(Sa] \subseteq Sa$. Now $a = ea \in Sa$, so Sa is a left ideal of S containing a. Let I be another left ideal of S containing a. Since $sa \in I$, because I is a left ideal of S. But $sa \in Sa$, this means that $Sa \subseteq I$. Therefore Sa is a smallest left ideal of S containing a. ∎

Lemma 19. Let S be an ordered AG-groupoid with left identity e. Then aS is a left ideal of S.

Proof. Straight forward. ∎

Proposition 8. Let S be an ordered AG-groupoid with left identity e. Then $aS \cup Sa$ is a smallest right ideal of S containing a.

Proof. We have to show that $aS \cup Sa$ is a smallest right ideal of S containing a. Now

$$(aS \cup Sa)S = (aS)S \cup (Sa)S = (SS)a \cup (Sa)(eS) \subseteq Sa \cup (Se)(aS) = Sa \cup S(aS) =$$
$$= Sa \cup a(SS) \subseteq Sa \cup aS = aS \cup Sa.$$

Thus $(aS \cup Sa)S \subseteq aS \cup Sa$ and also $(aS \cup Sa] \subseteq aS \cup Sa$. Therefore $aS \cup Sa$ is a right ideal of S. Since $a \in Sa$, i.e., $a \in aS \cup Sa$. Let I be another right ideal of S containing a. Now $aS \in IS \subseteq I$ and $Sa = (SS)a = (aS)S \in (IS)S \subseteq IS \subseteq I$, i.e., $aS \cup Sa \subseteq I$. Hence $aS \cup Sa$ is a smallest right ideal of S containing a. ■

Theorem 8. Let S be an ordered AG-groupoid with left identity e, such that $(xe)S = xS$ for all $x \in S$. Then the following conditions are equivalent:

(1) S is a regular;

(2) $\mu \wedge_\alpha^\beta \gamma = \mu \circ_\alpha^\beta \gamma$ for every fuzzy right ideal μ with thresholds $(\alpha, \beta]$ and every fuzzy left ideal γ with thresholds $(\alpha, \beta]$ of S;

(3) $\delta_\alpha^\beta = (\delta \circ_\alpha^\beta S) \circ \delta_\alpha^\beta$ for every fuzzy quasi-ideal δ with thresholds $(\alpha, \beta]$ of S.

Proof. Consider that (1) holds and δ be a fuzzy quasi-ideal with thresholds $(\alpha, \beta]$ of S. This implies that $(\delta \circ_\alpha^\beta S) \circ_\alpha^\beta \delta \subseteq \delta_\alpha^\beta$, because every fuzzy quasi-ideal with thresholds $(\alpha, \beta]$ of S is a fuzzy bi-ideal with thresholds $(\alpha, \beta]$ of S by the Lemma 14. Let $x \in S$, then there exists an element $a \in S$ such that $x \leqslant (xa)x$. Thus

$$((\delta \circ_\alpha^\beta S) \circ_\alpha^\beta \delta)(x) = \{((\delta \circ S) \circ \delta)(x) \wedge \beta\} \vee \alpha = \left\{ \Big(\bigvee_{(y,z) \in A_x} \in \{(\delta \circ S)(y), \delta(z)\} \Big) \wedge \beta \right\} \vee \alpha \geqslant$$

$$\geqslant \{(\delta \circ S)\,(xa) \wedge \delta\,(x) \wedge \beta\} \vee \alpha = ((\delta \circ S)\,(xa) \vee \alpha) \wedge (\delta\,(x) \vee \alpha) \wedge (\beta \vee \alpha) =$$
$$= ((\delta \circ S)\,(xa) \vee \alpha) \wedge \delta(x) \wedge \beta = \bigg(\Big(\bigvee_{(s,t) \in A_{xa}} \min\{\delta(s), S(t)\} \Big) \vee \alpha \bigg) \wedge \delta(x) \wedge \beta \geqslant$$

$$\geqslant (\{\delta(x) \wedge S(a)\} \vee \alpha) \wedge \delta(x) \wedge \beta = (\{\delta(x) \wedge 1\} \vee \alpha) \wedge \delta(x) \wedge \beta = (\delta(x) \vee \alpha) \wedge \delta(x) \wedge \beta =$$
$$= \delta(x) \wedge \beta = (\delta(x) \wedge \beta) \vee \alpha = \delta_\alpha^\beta(x) \Rightarrow \delta_\alpha^\beta \subseteq (\delta \circ_\alpha^\beta S) \circ_\alpha^\beta \delta.$$

So $\delta_\alpha^\beta = (\delta \circ_\alpha^\beta S) \circ_\alpha^\beta \delta$, i.e., (1) implies (3). Suppose that (3) holds. Let μ be a fuzzy right ideal with thresholds $(\alpha, \beta]$ and γ be a fuzzy left ideal with thresholds $(\alpha, \beta]$ of S. This implies that μ and γ be fuzzy quasi-ideals with thresholds $(\alpha, \beta]$ of S by the Lemma 13, so $\mu \wedge_\alpha^\beta \gamma$ be also a fuzzy quasi-ideal with thresholds $(\alpha, \beta]$ of S. Then by our supposition, $\mu \wedge_\alpha^\beta \gamma = ((\mu \wedge_\alpha^\beta \gamma) \circ_\alpha^\beta S) \circ_\alpha^\beta (\mu \wedge_\alpha^\beta \gamma) \subseteq (\mu \circ_\alpha^\beta S) \circ_\alpha^\beta \gamma \subseteq \mu \circ_\alpha^\beta \gamma$, i.e., $\mu \wedge_\alpha^\beta \gamma \subseteq \mu \circ_\alpha^\beta \gamma$. Since $\mu \circ_\alpha^\beta \gamma \subseteq \mu \wedge_\alpha^\beta \gamma$, so $\mu \circ_\alpha^\beta \gamma = \mu \wedge_\alpha^\beta \gamma$, i.e., (3) $\Rightarrow$ (2). Assume that (2) is true and $a \in S$. Then Sa is a left ideal of S containing a by the Lemma 18 and $aS \cup Sa$ is a right ideal of S containing a by the Proposition 8. This means that χ_{Sa} is a fuzzy left ideal with thresholds $(\alpha, \beta]$ and $\chi_{aS \cup Sa}$ is a fuzzy right ideal with thresholds $(\alpha, \beta]$ of S by the Theorem 2. Then by our assumption $\chi_{aS \cup Sa} \wedge_\alpha^\beta \chi_{Sa} = \chi_{aS \cup Sa} \circ_\alpha^\beta \chi_{Sa}$, i.e., $(\chi_{(aS \cup Sa) \cap Sa})_\alpha^\beta = (\chi_{((aS \cup Sa)Sa]})_\alpha^\beta$ by the Theorem 1. Thus $(aS \cup Sa) \cap Sa = ((aS \cup Sa)Sa]$. Since $a \in (aS \cup Sa) \cap Sa$, i.e., $a \in ((aS \cup Sa)Sa]$, so $a \in ((aS)(Sa) \cup (Sa)(Sa)]$. Now $(Sa)(Sa) = ((Se)a)(Sa) = ((ae)S)(Sa) = (aS)(Sa)$. This implies that

$$((aS)(Sa) \cup (Sa)(Sa)] = ((aS)(Sa) \cup (aS)(Sa)] = ((aS)(Sa)].$$

Thus $a \in ((aS)(Sa)]$. Then

$$a \leqslant (ax)(ya) = ((ya)x)a = (((ey)a)x)a = (((ay)e)x)a =$$
$$= ((xe)(ay))a = (a((xe)y))a \in (aS)a, \text{ for any } x, y \in S.$$

This means that $a \in ((aS)a]$, i.e., a is regular. Hence S is a regular, i.e., (2) $\Rightarrow$ (1). ■

Theorem 9. Let S be an ordered AG-groupoid with left identity e, such that $(xe)S = xS$ for all $x \in S$. the following conditions are equivalent:

(1) S is a regular;
(2) $\mu_\alpha^\beta = (\mu \circ_\alpha^\beta S) \circ_\alpha^\beta \mu$ for every fuzzy quasi-ideal μ with thresholds $(\alpha, \beta]$ of S;
(3) $\gamma_\alpha^\beta = (\gamma \circ_\alpha^\beta S) \circ_\alpha^\beta \gamma$ for every fuzzy bi-ideal γ with thresholds $(\alpha, \beta]$ of S;
(4) $\delta_\alpha^\beta = (\delta \circ_\alpha^\beta S) \circ_\alpha^\beta \delta$ for every fuzzy generalized bi-ideal δ with thresholds $(\alpha, \beta]$ of S.

Proof.
(1) $\Rightarrow$ (4) is obvious.
(4) $\Rightarrow$ (3), since every fuzzy bi-ideal with thresholds $(\alpha, \beta]$ of S is a fuzzy generalized bi-ideal with thresholds $(\alpha, \beta]$ of S by the Lemma 12.
(3) $\Rightarrow$ (2), since every fuzzy quasi-ideal with thresholds $(\alpha, \beta]$ of S is a fuzzy bi-ideal with thresholds $(\alpha, \beta]$ of S by the Lemma 14.
(2) $\Rightarrow$ (1) by the Theorem 8. ■

Theorem 10. Let S be an ordered AG-groupoid with left identity e, such that $(xe)S = xS$ for all $x \in S$. Then the following conditions are equivalent:

(1) S is a regular;
(2) $\mu \wedge_\alpha^\beta \nu = (\mu \circ_\alpha^\beta \nu) \circ_\alpha^\beta \mu$ for every fuzzy quasi-ideal μ with thresholds $(\alpha, \beta]$ and every fuzzy ideal ν with thresholds $(\alpha, \beta]$ of S;
(3) $\gamma \wedge_\alpha^\beta \nu = (\gamma \circ_\alpha^\beta \nu) \circ_\alpha^\beta \gamma$ for every fuzzy bi-ideal γ with thresholds $(\alpha, \beta]$ and every fuzzy ideal ν with thresholds $(\alpha, \beta]$ of S;
(4) $\delta \wedge_\alpha^\beta \nu = (\delta \circ_\alpha^\beta \nu) \circ_\alpha^\beta \delta$ for every fuzzy generalized bi-ideal δ with thresholds $(\alpha, \beta]$ and every fuzzy ideal ν with thresholds $(\alpha, \beta]$ of S.

Proof. Suppose that (1) holds. Let δ be a fuzzy generalized bi-ideal with thresholds $(\alpha, \beta]$ and ν be a fuzzy ideal with thresholds $(\alpha, \beta]$ of S. Now $(\delta \circ_\alpha^\beta \nu) \circ_\alpha^\beta \delta \subseteq (S \circ_\alpha^\beta \nu) \circ_\alpha^\beta S \subseteq \subseteq \nu \circ_\alpha^\beta S \subseteq \nu_\alpha^\beta$ and $(\delta \circ_\alpha^\beta \nu) \circ_\alpha^\beta \delta \subseteq (\delta \circ_\alpha^\beta S) \circ_\alpha^\beta \delta \subseteq \delta_\alpha^\beta$, i.e., $(\delta \circ_\alpha^\beta \nu) \circ_\alpha^\beta \delta \subseteq \delta_\alpha^\beta \wedge \nu_\alpha^\beta = \delta \wedge_\alpha^\beta \nu$. Let $x \in S$, this implies that there exists $a \in S$ such that $x \leqslant (xa)x$. Now $xa \leqslant ((xa)x)a = = (ax)(xa) = x((ax)a)$. Thus

$$
\begin{aligned}
((\delta \circ_\alpha^\beta \nu) \circ_\alpha^\beta \delta)(x) = \{((\delta \circ \nu) \circ \delta)(x) \wedge \beta\} \vee \alpha = \left\{\Big(\bigvee_{(y,z)\in A_x} \min\{(\delta \circ \nu)(y), \delta(z)\}\Big) \wedge \beta\right\} \vee \alpha \geqslant \\
\geqslant \{(\delta \circ \nu)(xa) \wedge \delta(x) \wedge \beta\} \vee \alpha = ((\delta \circ \nu)(xa) \vee \alpha) \wedge (\delta(x) \vee \alpha) \wedge (\beta \vee \alpha) = \\
= ((\delta \circ \nu)(xa) \vee \alpha) \wedge \delta(x) \wedge \beta = \Big(\Big(\bigvee_{(s,t)\in A_{xa}} \min\{\delta(s), \nu(t)\}\Big) \vee \alpha\Big) \wedge \delta(x) \wedge \beta \geqslant \\
\geqslant (\{\delta(x) \wedge \nu((ax)a)\} \vee \alpha) \wedge \delta(x) \wedge \beta = (\delta(x) \vee \alpha) \wedge (\nu((ax)a) \vee \alpha) \wedge \delta(x) \wedge \beta \geqslant \\
\geqslant \delta(x) \wedge (\nu(x) \wedge \beta) \wedge \delta(x) \wedge \beta = \delta(x) \wedge \nu(x) \wedge \beta = (\delta \wedge \nu)(x) \wedge \beta = \\
= \{(\delta \wedge \nu)(x) \wedge \beta\} \vee \alpha = (\delta \wedge_\alpha^\beta \nu)(x) \Rightarrow \delta \wedge_\alpha^\beta \nu \subseteq (\delta \circ_\alpha^\beta \nu) \circ_\alpha^\beta \delta.
\end{aligned}
$$

Therefore $\delta \wedge_\alpha^\beta \nu = (\delta \circ_\alpha^\beta \nu) \circ_\alpha^\beta \delta$, i.e., (1) $\Rightarrow$ (4). Since (4) $\Rightarrow$ (3) and (3) $\Rightarrow$ (2). Assume that (2) holds. Then $\mu \wedge_\alpha^\beta S = (\mu \circ_\alpha^\beta S) \circ_\alpha^\beta \mu$, where S itself is a fuzzy two-sided ideal with thresholds $(\alpha, \beta]$ of S, i.e., $\mu_\alpha^\beta = (\mu \circ_\alpha^\beta S) \circ \mu_\alpha^\beta$. Hence S is a regular by the Theorem 8, i.e., (2) $\Rightarrow$ (1). ■

Theorem 11. Let S be an ordered AG-groupoid with left identity e, such that $(xe)S = xS$ for all $x \in S$. Then the following conditions are equivalent:

(1) S is a regular;
(2) $\mu \wedge_\alpha^\beta \lambda \subseteq \lambda \circ_\alpha^\beta \mu$ for every fuzzy quasi-ideal μ with thresholds $(\alpha, \beta]$ and every fuzzy right ideal λ with thresholds $(\alpha, \beta]$ of S;
(3) $\gamma \wedge_\alpha^\beta \lambda \subseteq \lambda \circ_\alpha^\beta \gamma$ for every fuzzy bi-ideal γ with thresholds $(\alpha, \beta]$ and every fuzzy right ideal λ with thresholds $(\alpha, \beta]$ of S;

(4) $\delta \wedge_\alpha^\beta \lambda \subseteq \lambda \circ_\alpha^\beta \delta$ for every fuzzy generalized bi-ideal δ with thresholds $(\alpha, \beta]$ and every fuzzy right ideal λ with thresholds $(\alpha, \beta]$ of S.

Proof. (1) $\Rightarrow$ (4) is obvious. It is clear that (4) $\Rightarrow$ (3) and (3) $\Rightarrow$ (2). Assume that (2) holds, this means that $\lambda \wedge_\alpha^\beta \mu = \mu \wedge_\alpha^\beta \lambda \subseteq \lambda \circ_\alpha^\beta \mu$, where μ is a fuzzy left ideal with thresholds $(\alpha, \beta]$ of S. Since $\lambda \circ_\alpha^\beta \mu \subseteq \lambda \wedge_\alpha^\beta \mu$, so $\lambda \wedge_\alpha^\beta \mu = \lambda \circ_\alpha^\beta \mu$. Therefore S is a regular by the Theorem 8, i.e., (2) $\Rightarrow$ (1). ∎

Theorem 12. Let S be an ordered AG-groupoid with left identity e, such that $(xe)S = xS$ for all $x \in S$. Then the following conditions are equivalent:

(1) S is a regular;

(2) $\mu \wedge_\alpha^\beta \lambda \wedge_\alpha^\beta \psi \subseteq (\mu \circ_\alpha^\beta \lambda) \circ_\alpha^\beta \psi$ for every fuzzy quasi-ideal μ with thresholds $(\alpha, \beta]$, every fuzzy right ideal λ with thresholds $(\alpha, \beta]$ and every fuzzy left ideal ψ with thresholds $(\alpha, \beta]$ of S;

(3) $\gamma \wedge_\alpha^\beta \lambda \wedge_\alpha^\beta \psi \subseteq (\gamma \circ_\alpha^\beta \lambda) \circ_\alpha^\beta \psi$ for every fuzzy bi-ideal γ with thresholds $(\alpha, \beta]$, every fuzzy right ideal λ with thresholds $(\alpha, \beta]$ and every fuzzy left ideal ψ with thresholds $(\alpha, \beta]$ of S;

(4) $\delta \wedge_\alpha^\beta \lambda \wedge_\alpha^\beta \psi \subseteq (\delta \circ_\alpha^\beta \lambda) \circ_\alpha^\beta \psi$ for every fuzzy generalized bi-ideal δ with thresholds $(\alpha, \beta]$, every fuzzy right ideal λ with thresholds $(\alpha, \beta]$ and every fuzzy left ideal ψ with thresholds $(\alpha, \beta]$ of S.

Proof. Consider that (1) holds. Let δ be a fuzzy generalized bi-ideal with thresholds $(\alpha, \beta]$, ψ be a fuzzy left ideal with thresholds $(\alpha, \beta]$ and λ be a fuzzy right ideal with thresholds $(\alpha, \beta]$ of S. Let $x \in S$, then there exists an element $a \in S$ such that $x \leqslant (xa)x$. Now

$$\begin{gathered} x \leqslant (xa)x; \\ xa \leqslant ((xa)x)a = (ax)(xa) = x((ax)a); \\ (ax)a \leqslant (a((xa)x))a = ((xa)(ax))a = (a(ax))(xa) = x((a(ax))a) = x(((ea)(ax))a) = \\ = x(((xa)(ae))a) = x((((ae)a)x)a) = x((nx)a) = x((nx)(ea)) = x((ae)(xn)) = \\ = x(x((ae)n)) = x(xm) \Rightarrow xa = x((ax)a) = x(x(xm)) = (ex)(x(xm)) = ((xm)x)(xe). \end{gathered}$$

Thus

$$\begin{gathered} ((\delta \circ_\alpha^\beta \lambda) \circ_\alpha^\beta \psi)(x) = \{((\delta \circ \lambda) \circ \psi)(x) \wedge \beta\} \vee \alpha = \\ = \Big\{\Big(\bigvee_{(y,z) \in A_x} \min\{(\delta \circ \lambda)(y), \psi(z)\}\Big) \wedge \beta\Big\} \vee \alpha \geqslant \{(\delta \circ \lambda)(xa) \wedge \psi(x) \wedge \beta\} \vee \alpha = \\ = ((\delta \circ \lambda)(xa) \vee \alpha) \wedge (\psi(x) \vee \alpha) \wedge (\beta \vee \alpha) = ((\delta \circ \lambda)(xa) \vee \alpha) \wedge \psi(x) \wedge \beta = \\ = \Big(\Big(\bigvee_{(s,t) \in A_{xa}} \min\{\delta(s), \lambda(t)\}\Big) \vee \alpha\Big) \wedge \psi(x) \wedge \beta \geqslant (\{\delta((xm)x) \wedge \lambda(xe)\} \vee \alpha) \wedge \psi(x) \wedge \beta = \\ = (\delta((xm)x) \vee \alpha) \wedge (\lambda(xe) \vee \alpha) \wedge \psi(x) \wedge \beta \geqslant (\delta(x) \wedge \delta(x) \wedge \beta) \wedge (\lambda(x) \wedge \beta) \wedge \psi(x) \wedge \beta = \\ = \delta(x) \wedge \lambda(x) \wedge \psi(x) \wedge \beta = (\delta(x) \wedge \lambda(x) \wedge \psi(x) \wedge \beta) \vee \alpha = (\delta \wedge_\alpha^\beta \lambda \wedge_\alpha^\beta \psi)(x). \end{gathered}$$

Hence $\delta \wedge_\alpha^\beta \lambda \wedge_\alpha^\beta \psi \subseteq (\delta \circ_\alpha^\beta \lambda) \circ_\alpha^\beta \psi$, i.e., (1) $\Rightarrow$ (4). It is clear that (4) $\Rightarrow$ (3) and (3) $\Rightarrow$ (2). Assume that (2) holds. Then $\mu \wedge_\alpha^\beta S \wedge_\alpha^\beta \psi \subseteq (\mu \circ_\alpha^\beta S) \circ_\alpha^\beta \psi$, where μ is a fuzzy right ideal with thresholds $(\alpha, \beta]$ of S, i.e., $\mu \wedge_\alpha^\beta \psi \subseteq \mu \circ_\alpha^\beta \psi$. Since $\mu \circ_\alpha^\beta \psi \subseteq \mu \wedge_\alpha^\beta \psi$, thus $\mu \circ_\alpha^\beta \psi = \mu \wedge_\alpha^\beta \psi$. So S is a regular by the Theorem 8, i.e., (2) $\Rightarrow$ (1). ∎

3. Intra-regular ordered AG-groupoids

An ordered AG-groupoid S will be called an intra-regular ordered AG-groupoid if for every $x \in S$ there exist elements $a, b \in S$ such that $x \leqslant (ax^2)b$. Equivalent definitions are as follows:

(1) $A \subseteq ((SA^2)S]$ for every $A \subseteq S$;
(2) $x \in ((Sx^2)S]$ for every $x \in S$.

In this section, we characterize intra-regular ordered AG-groupoids in terms of fuzzy left (right, quasi-, bi-, generalized bi-) ideals with thresholds $(\alpha, \beta]$.

Lemma 20. Every fuzzy left (right) ideal with thresholds $(\alpha, \beta]$ of an intra-regular ordered AG-groupoid S is a fuzzy ideal with thresholds $(\alpha, \beta]$ of S.

Proof. Suppose that μ is a fuzzy left ideal with thresholds $(\alpha, \beta]$ of S. Let $x, y \in S$, this implies that there exist $a, b \in S$, such that $x \leqslant (ax^2)b$. Thus

$$\max\{\mu(xy), \alpha\} \geqslant \max\{\mu(((ax^2)b)y), \alpha\} = \max\{\mu((yb)(ax^2)), \alpha\} \geqslant$$
$$\geqslant \min\{\mu(a(xx)), \beta\} \geqslant \min\{\mu(xx), \beta\} \geqslant \min\{\mu(x), \beta\}.$$

Hence μ is a fuzzy ideal with thresholds $(\alpha, \beta]$ of S. ■

Lemma 21. Let S be an intra-regular ordered AG-groupoid with left identity e. Then every fuzzy ideal with thresholds $(\alpha, \beta]$ of S is a fuzzy idempotent with thresholds $(\alpha, \beta]$.

Proof. Assume that μ is a fuzzy ideal with thresholds $(\alpha, \beta]$ of S and $\mu \circ^\beta_\alpha \mu \subseteq \mu^\beta_\alpha$. Let $x \in S$, this means that there exist $a, b \in S$, such that $x \leqslant (ax^2)b$. Now

$$x \leqslant (ax^2)b = (a(xx))b = (x(ax))b = (x(ax))(eb) = (xe)((ax)b) = (ax)((xe)b).$$

Thus

$$(\mu \circ^\beta_\alpha \mu)(x) = \{(\mu \circ \mu)(x) \wedge \beta\} \vee \alpha = \left\{\Big(\bigvee_{(y,z)\in A_x} \min\{\mu(y), \mu(z)\}\Big) \wedge \beta\right\} \vee \alpha \geqslant$$
$$\geqslant \{\mu\,(ax) \wedge \mu\,((xe)b) \wedge \beta\} \vee \alpha = (\mu\,(ax) \vee \alpha) \wedge (\mu\,((xe)b) \vee \alpha) \wedge (\beta \vee \alpha) \geqslant$$
$$\geqslant (\mu\,(x) \wedge \beta) \wedge (\mu\,(x) \wedge \beta) \wedge \beta = \mu\,(x) \wedge \beta = (\mu\,(x) \wedge \beta) \vee \alpha = \mu^\beta_\alpha(x) \Rightarrow \mu^\beta_\alpha \subseteq \mu \circ^\beta_\alpha \mu.$$

Therefore $\mu^\beta_\alpha = \mu \circ^\beta_\alpha \mu$. ■

Proposition 9. Let μ be a fuzzy subset of an intra-regular ordered AG-groupoid S with left identity e. Then μ is a fuzzy ideal with thresholds $(\alpha, \beta]$ of S if and only if μ is a fuzzy interior ideal with thresholds $(\alpha, \beta]$ of S.

Proof. Consider that μ is a fuzzy interior ideal with thresholds $(\alpha, \beta]$ of S. Let $x, y \in S$, then there exist elements $a, b \in S$, such that $x \leqslant (ax^2)b$. Thus

$$\max\{\mu(xy), \alpha\} \geqslant \max\{\mu(((ax^2)b)y), \alpha\} = \max\{\mu((yb)(ax^2)), \alpha\} =$$
$$= \max\{\mu((yb)(a(xx))), \alpha\} = \max\{\mu((yb)(x(ax))), \alpha\} = \max\{\mu((yx)(b(ax))), \alpha\} \geqslant$$
$$\geqslant \min\{\mu(x), \beta\} \Rightarrow \max\{\mu(xy), \alpha\} \geqslant \min\{\mu(x), \beta\}.$$

Therefore μ is a fuzzy right ideal with thresholds $(\alpha, \beta]$ of S. So μ is a fuzzy ideal with thresholds $(\alpha, \beta]$ of S by the Lemma 20. Converse is true by the Lemma 10. ■

Remark 6. The concept of fuzzy (two-sided, interior) ideals with thresholds $(\alpha, \beta]$ coincides in intra-regular ordered AG-groupoids with left identity.

Lemma 22. Let S be an intra-regular ordered AG-groupoid with left identity e. Then $\gamma \wedge_{\alpha}^{\beta} \mu \subseteq \mu \circ_{\alpha}^{\beta} \gamma$ for every fuzzy left ideal μ with thresholds $(\alpha, \beta]$ and every fuzzy right ideal γ with thresholds $(\alpha, \beta]$ of S.

Proof. Suppose that μ is a fuzzy left ideal with thresholds $(\alpha, \beta]$ and γ is a fuzzy right ideal with thresholds $(\alpha, \beta]$ of S. Let $x \in S$, this implies that there exist $a, b \in S$ such that $x \leqslant (ax^2)b$. Now

$$x \leqslant (ax^2)b = (a(xx))b = (x(ax))b = (x(ax))(eb) = (xe)((ax)b) = (ax)((xe)b).$$

Thus

$$\begin{aligned}(\mu \circ_{\alpha}^{\beta} \gamma)(x) = \{(\mu \circ \gamma)(x) \wedge \beta\} \vee \alpha = \left\{\Big(\bigvee_{(y,z)\in A_x} \min\{\mu(y), \gamma(z)\}\Big) \wedge \beta\right\} \vee \alpha \geqslant \\ \geqslant \{\mu(ax) \wedge \gamma\left((xe)b\right) \wedge \beta\} \vee \alpha = (\mu\left(ax\right) \vee \alpha) \wedge (\gamma\left((xe)b\right) \vee \alpha) \wedge (\beta \vee \alpha) \geqslant \\ \geqslant (\mu\left(x\right) \wedge \beta) \wedge (\gamma\left(x\right) \wedge \beta) \wedge \beta = \mu\left(x\right) \wedge \gamma\left(x\right) \wedge \beta = \gamma\left(x\right) \wedge \mu\left(x\right) \wedge \beta = \\ = (\gamma \wedge \mu)\left(x\right) \wedge \beta = \{(\gamma \wedge \mu)\left(x\right) \wedge \beta\} \vee \alpha = (\gamma \wedge_{\alpha}^{\beta} \mu)(x).\end{aligned}$$

Hence $\gamma \wedge_{\alpha}^{\beta} \mu \subseteq \mu \circ_{\alpha}^{\beta} \gamma$. ∎

Theorem 13. Let S be an ordered AG-groupoid with left identity e, such that $(xe)S = xS$ for all $x \in S$. Then the following conditions are equivalent:

(1) S is an intra-regular;
(2) $\gamma \wedge_{\alpha}^{\beta} \mu \subseteq \mu \circ_{\alpha}^{\beta} \gamma$ for every fuzzy left ideal μ with thresholds $(\alpha, \beta]$ and every fuzzy right ideal γ with thresholds $(\alpha, \beta]$ of S.

Proof. (1) $\Rightarrow$ (2) is true by the Lemma 22. Assume that (2) holds and $a \in S$. Then Sa is a left ideal of S containing a by the Lemma 18 and $aS \cup Sa$ is a right ideal of S containing a by the Proposition 8. This means that χ_{Sa} is a fuzzy left ideal with thresholds $(\alpha, \beta]$ and $\chi_{aS\cup Sa}$ is a fuzzy right ideal with thresholds $(\alpha, \beta]$ of S by the Theorem 2. By our assumption $\chi_{aS\cup Sa} \wedge_{\alpha}^{\beta} \chi_{Sa} \subseteq \chi_{Sa} \circ_{\alpha}^{\beta} \chi_{aS\cup Sa}$, i.e., $(\chi_{(aS\cup Sa)\cap Sa})_{\alpha}^{\beta} \subseteq (\chi_{((Sa)(aS\cup Sa)]})_{\alpha}^{\beta}$ by the Theorem 1. Thus $(aS \cup Sa) \cap Sa \subseteq (Sa(aS \cup Sa)]$. Since $a \in (aS \cup Sa) \cap Sa$, i.e., $a \in (Sa(aS \cup Sa)] = ((Sa)(aS) \cup (Sa)(Sa)]$. Now

$$\begin{aligned}(Sa)(aS) = (Sa)((ea)(SS)) = (Sa)((SS)(ae)) = (Sa)(((ae)S)S) = (Sa)((aS)S) = \\ = (Sa)((SS)a) = (Sa)(Sa).\end{aligned}$$

This implies that

$$\begin{aligned}((Sa)(aS) \cup (Sa)(Sa)] = ((Sa)(Sa) \cup (Sa)(Sa)] = ((Sa)(Sa)] = ((Sa)a)S] = \\ = (((Sa)(ea))S] = (((Se)(aa))S] = ((Sa^2)S].\end{aligned}$$

Thus $a \in (Sa^2)S$, i.e., a is an intra-regular. Hence S is an intra-regular, i.e., (2) $\Rightarrow$ (1). ∎

Theorem 14. Let S be an ordered AG-groupoid with left identity e, such that $(xe)S = xS$ for all $x \in S$. Then the following conditions are equivalent:

(1) S is an intra-regular;
(2) $\mu \wedge_{\alpha}^{\beta} \nu = (\mu \circ_{\alpha}^{\beta} \nu) \circ_{\alpha}^{\beta} \mu$ for every fuzzy quasi-ideal μ with thresholds $(\alpha, \beta]$ and every fuzzy ideal ν with thresholds $(\alpha, \beta]$ of S;
(3) $\gamma \wedge_{\alpha}^{\beta} \nu = (\gamma \circ_{\alpha}^{\beta} \nu) \circ_{\alpha}^{\beta} \gamma$ for every fuzzy bi-ideal γ with thresholds $(\alpha, \beta]$ and every fuzzy ideal ν with thresholds $(\alpha, \beta]$ of S;

(4) $\delta \wedge_{\alpha}^{\beta} \nu = (\delta \circ_{\alpha}^{\beta} \nu) \circ_{\alpha}^{\beta} \delta$ for every fuzzy generalized bi-ideal δ with thresholds $(\alpha, \beta]$ and every fuzzy ideal ν with thresholds $(\alpha, \beta]$ of S.

Proof. Consider that (1) holds. Let δ be a fuzzy generalized bi-ideal with thresholds $(\alpha, \beta]$ and ν be a fuzzy ideal with thresholds $(\alpha, \beta]$ of S. Now $(\delta \circ_{\alpha}^{\beta} \nu) \circ_{\alpha}^{\beta} \delta \subseteq (S \circ_{\alpha}^{\beta} \nu) \circ_{\alpha}^{\beta} S \subseteq \subseteq \nu \circ_{\alpha}^{\beta} S \subseteq \nu_{\alpha}^{\beta}$ and $(\delta \circ_{\alpha}^{\beta} \nu) \circ_{\alpha}^{\beta} \delta \subseteq (\delta \circ_{\alpha}^{\beta} S) \circ_{\alpha}^{\beta} \delta \subseteq \delta_{\alpha}^{\beta}$, thus $(\delta \circ \nu) \circ_{\alpha}^{\beta} \delta \subseteq \delta_{\alpha}^{\beta} \wedge \nu_{\alpha}^{\beta} = \delta \wedge_{\alpha}^{\beta} \nu$. Let $x \in S$, then there exist elements $a, b \in S$ such that $x \leqslant (ax^2)b$. Now

$$x \leqslant (ax^2)b = (a(xx))b = (x(ax))b = (b(ax))x;$$
$$b(ax) \leqslant b(a((ax^2)b)) = b((ax^2)(ab)) = b((ax^2)c) = (ax^2)(bc) = (ax^2)d = (ax^2)(ed) =$$
$$= (de)(x^2a) = m(x^2a) = x^2(ma) = (xx)l = (lx)x = (lx)(ex) = (xe)(xl) = x((xe)l).$$

Thus

$$((\delta \circ_{\alpha}^{\beta} \nu) \circ_{\alpha}^{\beta} \delta)(x) = \{((\delta \circ \nu) \circ \delta)(x) \wedge \beta\} \vee \alpha =$$
$$= \Big\{\Big(\bigvee_{(y,z)\in A_x} \min\{(\delta \circ \nu)(y), \delta(z)\}\Big) \wedge \beta\Big\} \vee \alpha \geqslant \{(\delta \circ \nu)(b(ax)) \wedge \delta(x) \wedge \beta\} \vee \alpha =$$
$$= ((\delta \circ \nu)(b(ax)) \vee \alpha) \wedge (\delta(x) \vee \alpha) \wedge (\beta \vee \alpha) = ((\delta \circ \nu)(b(ax)) \vee \alpha) \wedge \delta(x) \wedge \beta =$$
$$= \Big(\Big(\bigvee_{(s,t)\in A_{b(ax)}} \min\{\delta(s), \nu(t)\}\Big) \vee \alpha\Big) \wedge \delta(x) \wedge \beta \geqslant (\{\delta(x) \wedge \nu((xe)l)\} \vee \alpha) \wedge \delta(x) \wedge \beta =$$
$$= (\delta(x) \vee \alpha) \wedge (\nu((xe)l) \vee \alpha) \wedge \delta(x) \wedge \beta \geqslant \delta(x) \wedge (\nu(x) \wedge \beta) \wedge \delta(x) \wedge \beta =$$
$$= \delta(x) \wedge \nu(x) \wedge \beta = (\delta \wedge \nu)(x) \wedge \beta = \{(\delta \wedge \nu)(x) \wedge \beta\} \vee \alpha = (\delta \wedge_{\alpha}^{\beta} \nu)(x) \Rightarrow$$
$$\Rightarrow \delta \wedge_{\alpha}^{\beta} \nu \subseteq (\delta \circ_{\alpha}^{\beta} \nu) \circ_{\alpha}^{\beta} \delta.$$

Hence $\delta \wedge_{\alpha}^{\beta} \nu = (\delta \circ_{\alpha}^{\beta} \nu) \circ_{\alpha}^{\beta} \delta$, i.e., (1) implies (4). It is clear that (4) $\Rightarrow$ (3) and (3) $\Rightarrow$ (2). Suppose that (2) holds. Let μ be a fuzzy right ideal with thresholds $(\alpha, \beta]$ and ν be a fuzzy two-sided ideal with thresholds $(\alpha, \beta]$ of S. Since every fuzzy right ideal with thresholds $(\alpha, \beta]$ of S is a fuzzy quasi-ideal with thresholds $(\alpha, \beta]$ of S by the Lemma 13, this implies that μ is a fuzzy quasi-ideal with thresholds $(\alpha, \beta]$ of S. By our supposition, $\mu \wedge_{\alpha}^{\beta} \nu = = (\mu \circ_{\alpha}^{\beta} \nu) \circ_{\alpha}^{\beta} \mu \subseteq (S \circ_{\alpha}^{\beta} \nu) \circ_{\alpha}^{\beta} \mu \subseteq \nu \circ_{\alpha}^{\beta} \mu$, i.e., $\mu \wedge_{\alpha}^{\beta} \nu \subseteq \nu \circ_{\alpha}^{\beta} \mu$. So S is an intra-regular by the Theorem 13, i.e., (2) $\Rightarrow$ (1). ■

Theorem 15. Let S be an ordered AG-groupoid with left identity e, such that $(xe)S = = xS$ for all $x \in S$. Then the following conditions are equivalent:

(1) S is an intra-regular;
(2) $\mu \wedge_{\alpha}^{\beta} \psi \subseteq \psi \circ_{\alpha}^{\beta} \mu$ for every fuzzy quasi-ideal μ with thresholds $(\alpha, \beta]$ and every fuzzy left ideal ψ with thresholds $(\alpha, \beta]$ of S;
(3) $\gamma \wedge_{\alpha}^{\beta} \psi \subseteq \psi \circ_{\alpha}^{\beta} \gamma$ for every fuzzy bi-ideal γ with thresholds $(\alpha, \beta]$ and every fuzzy left ideal ψ with thresholds $(\alpha, \beta]$ of S;
(4) $\delta \wedge_{\alpha}^{\beta} \psi \subseteq \psi \circ_{\alpha}^{\beta} \delta$ for every fuzzy generalized bi-ideal δ with thresholds $(\alpha, \beta]$ and every fuzzy left ideal ψ with thresholds $(\alpha, \beta]$ of S.

Proof. Suppose that (1) holds. Let δ be a fuzzy generalized bi-ideal with thresholds $(\alpha, \beta]$ and ψ be a fuzzy left ideal with thresholds $(\alpha, \beta]$ of S. Let $x \in S$, this implies that there exist $a, b \in S$ such that $x \leqslant (ax^2)b$. Now $x \leqslant (a(xx))b = (x(ax))b = (b(ax))x$. Thus

$$(\psi \circ_{\alpha}^{\beta} \delta)(x) = \{(\psi \circ \delta)(x) \wedge \beta\} \vee \alpha = \Big\{\Big(\bigvee_{(y,z)\in A_x} \min\{\psi(y), \delta(z)\}\Big) \wedge \beta\Big\} \vee \alpha \geqslant$$
$$\geqslant \{\{\psi(b(ax)) \wedge \delta(x)\} \wedge \beta\} \vee \alpha = (\psi(b(ax)) \vee \alpha) \wedge (\delta(x) \vee \alpha) \wedge (\beta \vee \alpha) \geqslant$$

$$\geqslant (\psi (x) \wedge \beta) \wedge \delta (x) \wedge \beta = \psi (x) \wedge \delta (x) \wedge \beta = \delta (x) \wedge \psi (x) \wedge \beta = (\delta \wedge \psi) (x) \wedge \beta =$$
$$= \{(\delta \wedge \psi) (x) \wedge \beta\} \vee \alpha = (\delta \wedge_\alpha^\beta \psi)(x) \Rightarrow \delta \wedge_\alpha^\beta \psi \subseteq \psi \circ_\alpha^\beta \delta.$$

Hence (1) $\Rightarrow$ (4). It is clear that (4) $\Rightarrow$ (3) and (3) $\Rightarrow$ (2). Assume that (2) holds. Let μ be a fuzzy right ideal with thresholds $(\alpha,\beta]$ and ψ be a fuzzy left ideal with thresholds $(\alpha,\beta]$ of S. Since every fuzzy right ideal with thresholds $(\alpha,\beta]$ of S is a fuzzy quasi-ideal with thresholds $(\alpha,\beta]$ of S, this means that μ is a fuzzy quasi-ideal with thresholds $(\alpha,\beta]$ of S. By our assumption, $\mu \wedge_\alpha^\beta \psi \subseteq \psi \circ_\alpha^\beta \mu$. Therefore S is an intra-regular by the Theorem 13, i.e., (2) $\Rightarrow$ (1). ∎

Theorem 16. Let S be an ordered AG-groupoid with left identity e, such that $(xe)S = xS$ for all $x \in S$. Then the following conditions are equivalent:

(1) S is an intra-regular;
(2) $\mu \wedge_\alpha^\beta \psi \wedge_\alpha^\beta \lambda \subseteq (\psi \circ_\alpha^\beta \mu) \circ_\alpha^\beta \lambda$ for every fuzzy quasi-ideal μ with thresholds $(\alpha,\beta]$, every fuzzy left ideal ψ with thresholds $(\alpha,\beta]$, and every fuzzy right ideal λ with thresholds $(\alpha,\beta]$ of S;
(3) $\gamma \wedge_\alpha^\beta \psi \wedge_\alpha^\beta \lambda \subseteq (\psi \circ_\alpha^\beta \gamma) \circ_\alpha^\beta \lambda$ for every fuzzy bi-ideal γ with thresholds $(\alpha,\beta]$, every fuzzy left ideal ψ with thresholds $(\alpha,\beta]$, and every fuzzy right ideal λ with thresholds $(\alpha,\beta]$ of S;
(4) $\delta \wedge_\alpha^\beta \psi \wedge_\alpha^\beta \lambda \subseteq (\psi \circ_\alpha^\beta \delta) \circ_\alpha^\beta \lambda$ for every fuzzy generalized bi-ideal δ with thresholds $(\alpha,\beta]$, every fuzzy left ideal ψ with thresholds $(\alpha,\beta]$, and every fuzzy right ideal λ with thresholds $(\alpha,\beta]$ of S.

Proof. Assume that (1) holds. Let δ be a fuzzy generalized bi-ideal with thresholds $(\alpha,\beta]$, ψ be a fuzzy left ideal with thresholds $(\alpha,\beta]$ and λ be a fuzzy right ideal with thresholds $(\alpha,\beta]$ of S. Let $x \in S$, this means that there exist $a, b \in S$ such that $x \leqslant (ax^2)b$. Now

$$x \leqslant (a(xx))b = (x(ax))b = (b(ax))x;$$
$$b(ax) \leqslant b(a((ax^2)b)) = b((ax^2)(ab)) = b((ax^2)c) = (ax^2)(bc) = (ax^2)d =$$
$$= (a(xx))d = (x(ax))d = (d(ax))x.$$

Thus

$$((\psi \circ_\alpha^\beta \delta) \circ_\alpha^\beta \lambda)(x) = \{((\psi \circ \delta) \circ \lambda)(x) \wedge \beta\} \vee \alpha =$$
$$= \Big\{\Big(\bigvee_{(y,z)\in A_x} \min\{(\psi \circ \delta)(y), \lambda(z)\}\Big) \wedge \beta\Big\} \vee \alpha \geqslant \{(\psi \circ \delta) (b(ax)) \wedge \lambda (x) \wedge \beta\} \vee \alpha =$$
$$= ((\psi \circ \delta) (b(ax)) \vee \alpha) \wedge (\lambda (x) \vee \alpha) \wedge (\beta \vee \alpha) \geqslant ((\psi \circ \delta) (b(ax)) \vee \alpha) \wedge \lambda(x) \wedge \beta =$$
$$= \Big(\Big(\bigvee_{(s,t)\in A_{b(ax)}} \min\{\psi(s), \delta(t)\}\Big) \vee \alpha\Big) \wedge \lambda(x) \wedge \beta \geqslant (\{\psi(d(ax)) \wedge \delta(t)\} \vee \alpha) \wedge \lambda(x) \wedge \beta =$$
$$= (\psi(d(ax)) \vee \alpha) \wedge (\delta(x) \vee \alpha) \wedge \lambda(x) \wedge \beta \geqslant (\psi(x) \wedge \beta) \wedge \delta(x) \wedge \lambda(x) \wedge \beta =$$
$$= \psi(x) \wedge \delta(x) \wedge \lambda(x) \wedge \beta = (\psi \wedge \delta \wedge \lambda)(x) \wedge \beta = \{(\delta \wedge \psi \wedge \lambda)(x) \wedge \beta\} \vee \alpha =$$
$$= (\delta \wedge_\alpha^\beta \psi \wedge_\alpha^\beta \lambda)(x) \Rightarrow \delta \wedge_\alpha^\beta \psi \wedge_\alpha^\beta \lambda \subseteq (\psi \circ_\alpha^\beta \delta) \circ_\alpha^\beta \lambda.$$

Therefore (1) $\Rightarrow$ (4). Since (4) $\Rightarrow$ (3) and (3) $\Rightarrow$ (2). Suppose that (2) holds. Then $\psi \wedge_\alpha^\beta S \wedge_\alpha^\beta \delta \subseteq (S \circ_\alpha^\beta \psi) \circ_\alpha^\beta \delta$, where ψ is a fuzzy left ideal with thresholds $(\alpha,\beta]$ of S, i.e., $\psi \wedge_\alpha^\beta \delta \subseteq \psi \circ_\alpha^\beta \delta$. Hence S is an intra-regular, i.e., (2) $\Rightarrow$ (1). ∎

4. Regular and Intra-regular Ordered AG-groupoids

In this section, we give the characterizations of both regular and intra-regular ordered AG-groupoid in terms of fuzzy left (right, quasi-, bi-, generalized bi-) ideals with thresholds $(\alpha, \beta]$.

Theorem 17. Let S be an ordered AG-groupoid with left identity e, such that $(xe)S = xS$ for all $x \in S$. Then the following conditions are equivalent:

(1) S is both a regular and an intra-regular;
(2) Every fuzzy quasi-ideal with thresholds $(\alpha, \beta]$ of S is a fuzzy idempotent with thresholds $(\alpha, \beta]$.

Proof. Suppose that S is both a regular and an intra-regular. Let μ be a fuzzy quasi-ideal with thresholds $(\alpha, \beta]$ of S. Then μ be a fuzzy bi-ideal with thresholds $(\alpha, \beta]$ of S and $\mu \circ_\alpha^\beta \mu \subseteq \mu_\alpha^\beta$. Let $x \in S$, this implies that there exists an element $a \in S$ such that $x \leqslant (xa)x$, and also there exist elements $a, b \in S$ such that $x \leqslant (ax^2)b$. Now

$$\begin{gathered} x \leqslant (xa)x; \\ xa \leqslant ((ax^2)b)a = (ab)(ax^2) = c(a(xx)) = c(x(ax)) = x(c(ax)) = x((ec)(ax)) = \\ = x((xa)(ce)) = x((xa)d) = x((da)x) = x(lx) = l(xx) = (el)(xx) = (xx)(le) = \\ = (xx)m = (mx)x; \\ mx \leqslant m((ax^2)b) = (ax^2)(mb) = (a(xx))n = (x(ax))n = (x(ax))(en) = (xe)((ax)n) = \\ = (xe)((ax)(en)) = (xe)((ae)(xn)) = (xe)(x((ae)n)) = (xe)(xu) = x((xe)u) = xw; \\ xa \leqslant (mx)x = (xw)x. \end{gathered}$$

Thus

$$\begin{gathered} (\mu \circ_\alpha^\beta \mu)(x) = \{(\mu \circ \mu)(x) \wedge \beta\} \vee \alpha = \left\{\Big(\bigvee_{(y,z)\in A_x} \min\{\mu(y), \mu(z)\}\Big) \wedge \beta\right\} \vee \alpha \geqslant \\ \geqslant \{\mu\left((xw)x\right) \wedge \mu\left(x\right) \wedge \beta\} \vee \alpha = (\mu\left((xw)x\right) \vee \alpha) \wedge (\mu\left(x\right) \vee \alpha) \wedge (\beta \vee \alpha) \geqslant \\ \geqslant (\mu\left(x\right) \wedge \mu\left(x\right) \wedge \beta) \wedge \mu\left(x\right) \wedge \beta = \mu\left(x\right) \wedge \beta = (\mu\left(x\right) \wedge \beta) \vee \alpha = \mu_\alpha^\beta(x) \Rightarrow \mu_\alpha^\beta \subseteq \mu \circ_\alpha^\beta \mu. \end{gathered}$$

Hence $\mu_\alpha^\beta = \mu \circ_\alpha^\beta \mu$. Conversely, assume that every fuzzy quasi-ideal with thresholds $(\alpha, \beta]$ of S is a fuzzy idempotent with thresholds $(\alpha, \beta]$ of S. Let $a \in S$, then Sa is a left ideal of S containing a by the Lemma 18. This means that Sa is a quasi-ideal of S, so χ_{Sa} is a fuzzy quasi-ideal with thresholds $(\alpha, \beta]$ of S by the Theorem 4. By our assumption, $(\chi_{Sa})_\alpha^\beta = \chi_{Sa} \circ_\alpha^\beta \chi_{Sa} = (\chi_{((Sa)(Sa)]})_\alpha^\beta$, i.e., $Sa = ((Sa)(Sa)]$. Since $a \in Sa$, i.e., $a \in ((Sa)(Sa)]$. Thus a is both a regular and an intra-regular by the Theorems 8 and 13, respectively. Therefore S is both a regular and an intra-regular, i.e., (2) $\Rightarrow$ (1). ■

Theorem 18. Let S be an ordered AG-groupoid with left identity e, such that $(xe)S = xS$ for all $x \in S$. Then the following conditions are equivalent:

(1) S is both a regular and an intra-regular;
(2) $\mu \wedge_\alpha^\beta \gamma \subseteq \mu \circ_\alpha^\beta \gamma$ for all fuzzy quasi-ideals μ and γ with thresholds $(\alpha, \beta]$ of S;
(3) $\mu \wedge_\alpha^\beta \gamma \subseteq \mu \circ_\alpha^\beta \gamma$ for every fuzzy quasi-ideal μ with thresholds $(\alpha, \beta]$ and every fuzzy bi-ideal γ with thresholds $(\alpha, \beta]$ of S;
(4) $\mu \wedge_\alpha^\beta \gamma \subseteq \mu \circ_\alpha^\beta \gamma$ for every fuzzy bi-ideal μ with thresholds $(\alpha, \beta]$ and every fuzzy quasi-ideal γ with thresholds $(\alpha, \beta]$ of S;
(5) $\mu \wedge_\alpha^\beta \gamma \subseteq \mu \circ_\alpha^\beta \gamma$ for all fuzzy bi-ideals μ and γ with thresholds $(\alpha, \beta]$ of S;
(6) $\mu \wedge_\alpha^\beta \gamma \subseteq \mu \circ_\alpha^\beta \gamma$ for every fuzzy bi-ideal μ with thresholds $(\alpha, \beta]$ and every fuzzy generalized bi-ideal γ with thresholds $(\alpha, \beta]$ of S;

(7) $\mu \wedge_\alpha^\beta \gamma \subseteq \mu \circ_\alpha^\beta \gamma$ for every fuzzy generalized bi-ideal μ with thresholds $(\alpha, \beta]$ and every fuzzy quasi-ideal γ with thresholds $(\alpha, \beta]$ of S;

(8) $\mu \wedge_\alpha^\beta \gamma \subseteq \mu \circ_\alpha^\beta \gamma$ for every fuzzy generalized bi-ideal μ with thresholds $(\alpha, \beta]$ and every fuzzy bi-ideal γ with thresholds $(\alpha, \beta]$ of S;

(9) $\mu \wedge_\alpha^\beta \mu \subseteq \mu \circ_\alpha^\beta \gamma$ for all fuzzy generalized bi-ideals μ and γ with thresholds $(\alpha, \beta]$ of S.

Proof. Assume that (1) holds. Let μ and γ be two fuzzy generalized bi-ideals with thresholds $(\alpha, \beta]$ of S. Let $x \in S$, then means that there exists an element $a \in S$ such that $x = (xa)x$, and also there exist elements $a, b \in S$ such that $x \leqslant (ax^2)b$. Since $x = (xa)x = ((xw)x)x$ by the Theorem 17. Thus

$$(\mu \circ_\alpha^\beta \gamma)(x) = \{(\mu_A \circ \gamma)(x) \wedge \beta\} \vee \alpha = \left\{\Big(\bigvee_{(y,z)\in A_x} \min\{\mu(y), \gamma(z)\}\Big) \wedge \beta\right\} \vee \alpha \geqslant$$
$$\geqslant \{\mu\left((xw)x\right) \wedge \gamma\left(x\right) \wedge \beta\} \vee \alpha = \left(\mu\left((xw)x\right) \vee \alpha\right) \wedge \left(\gamma\left(x\right) \vee \alpha\right) \wedge \left(\beta \vee \alpha\right) \geqslant$$
$$\geqslant \left(\mu\left(x\right) \wedge \mu\left(x\right) \wedge \beta\right) \wedge \gamma\left(x\right) \wedge \beta = \mu\left(x\right) \wedge \gamma\left(x\right) \wedge \beta = \left(\mu \wedge \gamma\right)\left(x\right) \wedge \beta =$$
$$= \{\left(\mu \wedge \gamma\right)\left(x\right) \wedge \beta\} \vee \alpha = (\mu \wedge_\alpha^\beta \gamma)(x) \Rightarrow \mu \wedge_\alpha^\beta \gamma \subseteq \mu \circ_\alpha^\beta \gamma.$$

Hence (1) $\Rightarrow$ (9). It is clear that (9) $\Rightarrow$ (8) $\Rightarrow$ (7) $\Rightarrow$ (4) $\Rightarrow$ (2) and (9) $\Rightarrow$ (6) $\Rightarrow$ (5) $\Rightarrow$ (3). Suppose that (2) holds. Let μ be a fuzzy right ideal with thresholds $(\alpha, \beta]$ and γ be a fuzzy left ideal with thresholds $(\alpha, \beta]$ of S. Since every fuzzy right ideal with thresholds $(\alpha, \beta]$ and every fuzzy left ideal with thresholds $(\alpha, \beta]$ of S is a fuzzy quasi-ideal with thresholds $(\alpha, \beta]$ of S by the Lemma 13. By our supposition, $\mu \wedge_\alpha^\beta \gamma \subseteq \mu \circ_\alpha^\beta \gamma$. Since $\mu \circ_\alpha^\beta \gamma \subseteq \mu \wedge_\alpha^\beta \gamma$, so $\mu \wedge_\alpha^\beta \gamma = \mu \circ_\alpha^\beta \gamma$, i.e., S is a regular. Again by our supposition, $\mu \wedge_\alpha^\beta \gamma = \gamma \wedge_\alpha^\beta \mu \subseteq \gamma \circ_\alpha^\beta \mu$, i.e., S is an intra-regular. Therefore S is both a regular and an intra-regular, i.e., (2) $\Rightarrow$ (1). In similar way, we can prove that (3) $\Rightarrow$ (1). ■

Theorem 19. Let S be an ordered AG-groupoid with left identity e, such that $(xe)S = xS$ for all $x \in S$. Then the following conditions are equivalent:

(1) S is both a regular and an intra-regular;

(2) $\mu \wedge_\alpha^\beta \gamma \subseteq (\mu \circ_\alpha^\beta \gamma) \wedge (\gamma \circ_\alpha^\beta \mu)$ for every fuzzy right ideal μ with thresholds $(\alpha, \beta]$ and every fuzzy left ideal γ with thresholds $(\alpha, \beta]$ of S;

(3) $\mu \wedge_\alpha^\beta \gamma \subseteq (\mu \circ_\alpha^\beta \gamma) \wedge (\gamma \circ_\alpha^\beta \mu)$ for every fuzzy right ideal μ with thresholds $(\alpha, \beta]$ and every fuzzy quasi-ideal γ with thresholds $(\alpha, \beta]$ of S;

(4) $\mu \wedge_\alpha^\beta \gamma \subseteq (\mu \circ_\alpha^\beta \gamma) \wedge (\gamma \circ_\alpha^\beta \mu)$ for every fuzzy right ideal μ with thresholds $(\alpha, \beta]$ and every fuzzy bi-ideal γ with thresholds $(\alpha, \beta]$ of S;

(5) $\mu \wedge_\alpha^\beta \gamma \subseteq (\mu \circ_\alpha^\beta \gamma) \wedge (\gamma \circ_\alpha^\beta \mu)$ for every fuzzy right ideal μ with thresholds $(\alpha, \beta]$ and every fuzzy generalized bi-ideal γ with thresholds $(\alpha, \beta]$ of S;

(6) $\mu \wedge_\alpha^\beta \gamma \subseteq (\mu \circ_\alpha^\beta \gamma) \wedge (\gamma \circ \mu)$ for every fuzzy left ideal μ with thresholds $(\alpha, \beta]$ and every fuzzy quasi-ideal γ with thresholds $(\alpha, \beta]$ of S;

(7) $\mu \wedge_\alpha^\beta \gamma \subseteq (\mu \circ_\alpha^\beta \gamma) \wedge (\gamma \circ_\alpha^\beta \mu)$ for every fuzzy left ideal μ with thresholds $(\alpha, \beta]$ and every fuzzy bi-ideal γ with thresholds $(\alpha, \beta]$ of S;

(8) $\mu \wedge_\alpha^\beta \gamma \subseteq (\mu \circ_\alpha^\beta \gamma) \wedge (\gamma \circ_\alpha^\beta \mu)$ for every fuzzy left ideal μ with thresholds $(\alpha, \beta]$ and every fuzzy generalized bi-ideal γ with thresholds $(\alpha, \beta]$ of S;

(9) $\mu \wedge_\alpha^\beta \gamma \subseteq (\mu \circ_\alpha^\beta \gamma) \wedge (\gamma \circ_\alpha^\beta \mu)$ for all fuzzy quasi-ideals μ and γ with thresholds $(\alpha, \beta]$ of S;

(10) $\mu \wedge_\alpha^\beta \gamma \subseteq (\mu \circ_\alpha^\beta \gamma) \wedge (\gamma \circ_\alpha^\beta \mu)$ for every fuzzy quasi-ideal μ with thresholds $(\alpha, \beta]$ and every fuzzy bi-ideal γ with thresholds $(\alpha, \beta]$ of S;

(11) $\mu \wedge_\alpha^\beta \gamma \subseteq (\mu \circ_\alpha^\beta \gamma) \wedge (\mu \circ_\alpha^\beta \gamma)$ for every fuzzy quasi-ideal μ with thresholds $(\alpha, \beta]$ and every fuzzy generalized bi-ideal γ with thresholds $(\alpha, \beta]$ of S;

(12) $\mu \wedge_\alpha^\beta \gamma \subseteq (\mu \circ_\alpha^\beta \gamma) \wedge (\gamma \circ_\alpha^\beta \mu)$ for all fuzzy bi-ideals μ and γ with thresholds $(\alpha, \beta]$ of S;

(13) $\mu \wedge_\alpha^\beta \gamma \subseteq (\mu \circ_\alpha^\beta \gamma) \wedge (\gamma \circ_\alpha^\beta \mu)$ for every fuzzy bi-ideal μ with thresholds $(\alpha, \beta]$ and every fuzzy generalized bi-ideal γ with thresholds $(\alpha, \beta]$ of S;

(14) $\mu \wedge_\alpha^\beta \gamma \subseteq (\mu \circ_\alpha^\beta \gamma) \wedge (\gamma \circ_\alpha^\beta \mu)$ for all fuzzy generalized bi-ideals μ and γ with thresholds $(\alpha, \beta]$ of S.

Proof. Consider that (1) holds. Since $\mu \wedge_\alpha^\beta \gamma \subseteq \mu \circ_\alpha^\beta \gamma$ and $\mu \wedge_\alpha^\beta \gamma \subseteq \gamma \circ_\alpha^\beta \mu$ for all fuzzy generalized bi-ideals μ and γ with thresholds $(\alpha, \beta]$ of S by the Theorem 18. Hence $\mu \wedge_\alpha^\beta \gamma \subseteq$ $\subseteq (\mu \circ_\alpha^\beta \gamma) \wedge (\gamma \circ_\alpha^\beta \mu)$, i.e., (1) $\Rightarrow$ (14). It is clear that (14) $\Rightarrow$ (13) $\Rightarrow$ (12) $\Rightarrow$ (9) $\Rightarrow$ (6) $\Rightarrow$ (2), (14) $\Rightarrow$ (11) $\Rightarrow$ (10) $\Rightarrow$ (9), (14) $\Rightarrow$ (8) $\Rightarrow$ (7) $\Rightarrow$ (6) and (14) $\Rightarrow$ (5) $\Rightarrow$ (4) $\Rightarrow$ (3) $\Rightarrow$ (2). Suppose that (2) holds. Let μ be a fuzzy right ideal with thresholds $(\alpha, \beta]$ and γ be a fuzzy left ideal with thresholds $(\alpha, \beta]$ of S. By our supposition, $\mu \wedge_\alpha^\beta \gamma \subseteq (\mu \circ_\alpha^\beta \gamma) \wedge (\gamma \circ_\alpha^\beta \mu) \subseteq \gamma \circ_\alpha^\beta \mu$, i.e., S is an intra-regular. Again $\mu \wedge_\alpha^\beta \gamma \subseteq (\mu \circ_\alpha^\beta \gamma) \wedge (\gamma \circ_\alpha^\beta \mu) \subseteq \mu \circ_\alpha^\beta \gamma$. Since $\mu \circ_\alpha^\beta \gamma \subseteq \mu \wedge_\alpha^\beta \gamma$, so $\mu \wedge_\alpha^\beta \gamma = \mu \circ_\alpha^\beta \gamma$, i.e., S is a regular. Hence S is both a regular and an intra-regular, i.e., (2) $\Rightarrow$ (1). ∎

REFERENCES

1. *Kazim M. A. and Naseeruddin M.* On almost semigroups. Alig. Bull. Math., 1972, no. 2, pp. 1–7.
2. *Protic P. V. and Stevanovic N.* AG-test and some general properties of Abel-Grassmann's groupoids. Pure Math. Appl., 1995, no. 6, pp. 371–383.
3. *Mushtaq Q. and Yusuf S. M.* On LA-semigroups. Alig. Bull. Math., 1978, no. 8, pp. 65–70.
4. *Jezek J. and Kepka T.* Medial Groupoids. Rozpravy CSAV Rada Mat. a Prir. Ved., 1983, no. 93/2, 93 pp.
5. *Cho J. R., Jezek J., and Kepka T.* Paramedial groupoids., Czechoslovak Math. J., 1999, no. 49, pp. 277–290.
6. *Kehayopulu N.* On left regular ordered semigroups. Math Japon., 1990, no. 35, pp. 1057–1060.
7. *Kehayopulu N.* On completely regular ordered semigroups. Sci. Math., 1998, no. 1, pp. 27–32.
8. *Kehayopulu N.* On intra-regular ordered semigroups. Semigroup Forum, 1993, no. 46, pp. 271–278.
9. *Zadeh L. A.* Fuzzy sets. Inform. and Control, 1965, no. 8, pp. 338–353.
10. *Rosenfeld A.* Fuzzy groups. J. Math. Anal. Appl., 1971, no. 35, pp. 512–517.
11. *Kuroki N.* Fuzzy bi-ideals in semigroups. Comment. Math. Univ. St. Pauli, 1979, no. 28, pp. 17–21.
12. *Kuroki N.* On fuzzy semigroups. Inform. Sci., 1991, no. 53, pp. 203–236.
13. *Mordeson J. N., Malik D. S., and Kuroki N.* Fuzzy Semigroups. Berlin, Springer, 2003.
14. *Kehayopulu N. and Tsingelis M.* Fuzzy sets in ordered groupoids. Semigroup Forum, 2002, no. 65, pp. 128–132.
15. *Kehayopulu N. and Tsingelis M.* Fuzzy bi-ideals in ordered semigroups. Inform. Sci., 2005, no. 171, pp. 13–28.

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 519.1+519.719.2+519.712

КРИПТОСИСТЕМА ШИФРОВАНИЯ С АУТЕНТИФИКАЦИЕЙ НА ОСНОВЕ КОДА АУТЕНТИФИКАЦИИ С СЕКРЕТНОСТЬЮ

А. Ю. Зубов

ООО «Центр сертификационных исследований», г. Москва, Россия

Предлагается идея построения криптосистемы шифрования с аутентификацией, представляющей собой модификацию кода аутентификации с секретностью на основе кода Рида — Соломона. Модификация состоит в использовании неповторяющегося вектора инициализации и производного ключа для шифрования каждого сообщения. Получены оценки стойкости криптосистемы как кода аутентификации с секретностью: стойкость шифрования оценивается близостью к совершенному шифрованию, а стойкость аутентификации — вероятностями успеха имитации и подмены. Приводятся соображения по выбору параметров и оценке стойкости криптосистемы.

Ключевые слова: *код аутентификации с секретностью, криптосистема шифрования с аутентификацией.*

DOI 10.17223/20710410/43/4

AUTHENTICATION ENCRYPTION BASED ON AUTHENTICATION CODE WITH SECRECY

A. Yu. Zubov

Center for Certification Research, Moscow, Russia

E-mail: zubovanatoly@yandex.ru

The idea of authentication encryption cryptosystem is proposed. This cryptosystem is a modification of an authentication code with secrecy considered in previous papers of the author and based on Reed — Solomon error-correcting code. The essence of the modification is to use a non-repeating initialization vector and derivative key for encryption of each message. Estimations of cryptosystem security as an authentication code with secrecy at a one-time usage of the key are received: the encryption security is estimated by proximity to perfect encryption, and the authentication security — by probabilities of imitation and substitution success. Considerations for selection of parameters and estimation of cryptosystem security to chosen plaintext attacks at multiple usage of the key as well as distinction attacks are provided.

Keywords: *authentication code with secrecy, authentication encryption.*

Введение

В [1 – 4] изучались коды аутентификации на основе кодов Рида — Соломона. В данной работе предлагается идея конструкции криптосистемы шифрования с аутентификацией, представляющей собой модификацию кода аутентификации с секретностью — $\mathbb{AC}$, введённого в [2, 4].

Код аутентификации $\mathbb{AC}$ (далее А-код) строится следующим образом. Он определяется множествами

$$\mathcal{S} = (\mathbb{F}_q)^r, \ \ \mathcal{K} = (\mathbb{F}_q)^2, \ \ \mathcal{M} = (\mathbb{F}_q)^{r+1},$$

где $\mathbb{F}_q = \mathbb{GF}(q)$ — поле из $q = 2^n$ элементов; $r \geqslant 2$; $\mathcal{S}$ — множество состояний источника (открытых текстов); $\mathcal{K}$ — множество номеров правил кодирования (ключей); $\mathcal{M}$ — множество сообщений (шифртекстов), и правилом кодирования (функцией зашифрования) строки $s = (s_1, \ldots s_r) \in \mathcal{S}$ на ключе $k = (a, b) \in \mathcal{K}$ по формуле

$$e_k(s) = (m_1, \ldots, m_r, a \oplus m_1 \cdot b^r \oplus \ldots \oplus m_r \cdot b^1),$$

где $\oplus, \cdot$ — операции поля $\mathbb{F}_q$; $m_i = s_i \oplus c_i \cdot a \oplus d_i \cdot b$, $i = 1, \ldots, r$; $c_1, \ldots, c_r$, $d_1, \ldots, d_r$ — ненулевые константы из $\mathbb{F}_q$, такие, что

$$c_i \cdot d_j \neq c_j \cdot d_i \tag{1}$$

при $j \neq i$. Фактически строка $(m_1, \ldots, m_r)$ является результатом зашифрования, а

$$m_{r+1} = a \oplus m_1 \cdot b^r \oplus \ldots \oplus m_r \cdot b^1$$

— имитовставкой. Предполагается, что ключи и состояния источника выбираются случайно в соответствии с распределениями вероятностей $\mathcal{P}_K = (p_K(k),\ k \in \mathcal{K})$, $\mathcal{P}_S = (p_S(s), s \in \mathcal{S})$ и независимо друг от друга.

Интерес к А-коду $\mathbb{AC}$ вызван тем, что он допускает эффективную реализацию, обеспечивает ε-совершенное шифрование и высокий уровень имитозащиты при однократном использовании ключа. Понятие ε-совершенного шифрования введено в [2, 3]. Оно обобщает понятие совершенного шифрования, введённого К. Шенноном, и определяется следующим образом.

$\mathcal{P}_S$ и $\mathcal{P}_K$ индуцируют распределение вероятностей $\mathcal{P}_M = (p_M(m), m \in \mathcal{M})$ на множестве сообщений А-кода по формуле

$$p_M(m) = \sum_{k \in \mathcal{K}(m)} p_K(k) p_S\left(e_k^{-1}(m)\right),$$

где

$$\mathcal{K}(m) = \left\{k \in \mathcal{K} : \exists s \in \mathcal{S}\, (e_k(s) = m)\right\},$$

а для $k \in \mathcal{K}(m)$ по определению $e_k^{-1}(m) = s$, если $e_k(s) = m$. Пусть $\mathcal{P}_{S,M}, \mathcal{P}_{S|M}, \mathcal{P}_{M|S}$ — совместное и условные распределения вероятностей, определяемые формулами

$$p_{S,M}(s, m) = p_S(s) \sum_{k \in \mathcal{K}(s,m)} p_K(k),$$

$$\mathcal{K}(s, m) = \left\{k \in \mathcal{K} : e_k(s) = m\right\},$$

$$p_{M|S}(m|s) = \sum_{k \in \mathcal{K}(s,m)} p_K(k),$$

$$p_{S|M}(s|m) = \frac{p_{M|S}(m|s) p_S(s)}{p_M(m)}.$$

Тогда говорят, что А-код реализует *совершенное шифрование*, если равенство

$$p_{S|M}(s|m) = p_S(s)$$

выполняется для любых $s \in \mathcal{S}$ и $m \in \mathcal{M}$. Используя обозначение

$$\Delta(s,m) = \left| p_{S|M}(s|m) - p_S(s) \right|,$$

это определение можно записать в виде равенства

$$\max_{s,m} \Delta(s,m) = 0.$$

В свою очередь, А-код с данными распределениями $\mathcal{P}_S$ и $\mathcal{P}_K$ реализует ε-*совершенное шифрование*, если

$$\max_{s,m} \Delta(s,m) \leqslant \varepsilon,$$

где $0 \leqslant \varepsilon < 1$.

Теорема 1 [3]. Пусть для А-кода $\mathbb{AC}$ распределение $\mathcal{P}_K$ равномерное, а $\mathcal{P}_S$ — любое такое распределение, что для действительных чисел α, β, σ, удовлетворяющих неравенствам $0 < \alpha, \beta < 1 \leqslant \sigma$, выполняются условия $\alpha \leqslant p_S(s) \leqslant \beta$, $\beta/\alpha \leqslant \sigma$ для каждого $s \in \mathcal{S}$. Тогда $\mathbb{AC}$ реализует ε-совершенное шифрование для $\varepsilon < \sigma q^{-1}$ и обеспечивает следующие значения вероятностей успеха имитации и подмены: $p_0 = q^{-1}$, $p_1 \leqslant r\sigma q^{-1}$.

1. Криптосистема $\mathbb{CS}$

Заметим, что А-код $\mathbb{AC}$ обеспечивает указанный в теореме 1 уровень стойкости лишь при однократном использовании ключа и при условии, что открытый текст неизвестен. При частично известном открытом тексте $\mathbb{AC}$ не обеспечивает стойкости. В самом деле, если известны две пары (s_i, m_i), (s_j, m_j), то ключ (a, b) можно определить из системы уравнений

$$\begin{cases} m_i \oplus s_i = c_i \cdot a \oplus d_i \cdot b, \\ m_j \oplus s_j = c_j \cdot a \oplus d_j \cdot b. \end{cases} \tag{2}$$

Константы c_i, d_i не являются секретными, кроме того, из условий (1) следует, что система (2) совместна, возможно, лишь за исключением случая, когда $a = b = 0$. Таким образом, $\mathbb{AC}$ нестоек к атаке на основе подобранного открытого текста.

Алгоритм шифрования, реализуемый $\mathbb{AC}$, можно трактовать как «одноразовый» алгоритм шифрования с аутентификацией. Он использует шифрсистему гаммирования и систему аутентификации полиномиального типа, известную под названием GMAC.

Модифицируем этот алгоритм таким образом, чтобы стало допустимо многократное использование ключа. Для этого введём зависимость констант c_i, d_i от основного ключа и будем использовать зависящие от вектора инициализации производные ключи для зашифрования каждого сообщения.

Введём обозначения $a, \overline{a}, \mathbf{a}$ соответственно для элемента поля $a \in \mathbb{F}_{2^n}$, строки $\overline{a} \in \{0,1\}^n$ коэффициентов многочлена, представляющего a как элемент фактор-кольца $\mathbb{F}_2[x]/(h(x)) \cong \mathbb{F}_{2^n}$, и числа $\mathbf{a} \in \mathbb{Z}_{2^n}$, двоичная запись которого совпадает с $\overline{a}$.

Определим криптосистему шифрования с аутентификацией $\mathbb{CS}$, которая использует основной ключ $k = (a, b) \in (\mathbb{F}_{2^n})^2$, наборы констант

$$\mathcal{A} = \{w_i \in \mathbb{F}_{2^n} : \mathbf{w}_i = p(i)\}, \ \mathcal{A}(k) = \{w_i(k) : w_i \in \mathcal{A}\},$$
$$c_i(k) = w_i(k), \ d_i(k) = \varphi(w_i(k)), \ i = 1, 2, \ldots, 2^n - 1,$$

и вектор инициализации
$$iv^{(\tau)} = \left(\gamma^{(\tau)}, \delta^{(\tau)}\right) \in (\mathbb{F}_{2^n})^2$$
для зашифрования текстов $s^{(\tau)}$, $\tau = 1, 2, \ldots, L$, $L \in \mathbb{N}$. Здесь p — биективное отображение $\mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$; $w_i(k) = f_k(w_i)$ определяется с помощью отображения $f_x : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $x \in (\mathbb{F}_{2^n})^2$, а φ — отображение $\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. Вектор инициализации $iv^{(\tau)}$ должен содержать счётчик, который делает вектор неповторяющимся, метку времени и необходимые атрибуты передаваемого сообщения.

Текст $s^{(\tau)}$, представленный в виде последовательности $s^{(\tau)} = (s_1^{(\tau)}, \ldots, s_{r_\tau}^{(\tau)})$ элементов из $\mathbb{F}_{2^n}$, шифруется на производном ключе $k^{(\tau)} = (a^{(\tau)}, b^{(\tau)}) = g\left(k, iv^{(\tau)}\right)$, где g — отображение $(\mathbb{F}_{2^n})^4 \to (\mathbb{F}_{2^n})^2$. Результатом зашифрования $s^{(\tau)}$ служит $m^{(\tau)} = (m_1^{(\tau)}, \ldots, m_{r_\tau}^{(\tau)}, m_{r_\tau+1}^{(\tau)})$ — последовательность элементов из $\mathbb{F}_{2^n}$, где
$$m_i^{(\tau)} = s_i^{(\tau)} \oplus c_i(k)a^{(\tau)} \oplus d_i(k)b^{(\tau)}, \ i = 1, \ldots, r_\tau,$$
$$m_{r_\tau+1}^{(\tau)} = a^{(\tau)} \oplus m_1^{(\tau)} \left(b^{(\tau)}\right)^{r_\tau} \oplus \ldots \oplus m_{r_\tau}^{(\tau)} \left(b^{(\tau)}\right)^1.$$

Отправитель посылает сообщение $(iv^{(\tau)}, m^{(\tau)})$. Получатель сообщения (iv, m), где $iv = (\gamma, \delta)$, $m = (m_1, \ldots, m_r, m_{r+1})$, вычисляет производный ключ $(a', b') = g(k, iv^{(\tau)})$. Критерий аутентичности сообщения — равенство
$$m_{r+1} = a' \oplus m_1 \cdot b'^r \oplus \ldots \oplus m_r \cdot b'^1.$$
Если оно выполнено, то получатель вычисляет константы $w_i' = f_k(w_i)$ и открытый текст $s = (s_1, \ldots, s_r)$, где
$$s_i = m_i \oplus w_i' \cdot a' \oplus \varphi(w_i')b', \ i = 1, 2, \ldots, r.$$

Уточним выбор отображений p, f_x, g и φ. Этот выбор должен обеспечить достаточный уровень стойкости, в частности достижимость оценок теоремы 1, а также возможность эффективной реализации криптосистемы. Далее мы остановимся на некоторых вариантах выбора указанных отображений. Подчеркнём, что предлагаемые варианты являются лишь примерами и не дают окончательного решения задачи синтеза криптосистемы. Заинтересованный читатель может предложить и свои варианты, возможно, более разумные и обоснованные.

Выбор отображения φ свяжем с необходимостью выполнения условия (1). Такими отображениями являются, например, $\varphi(c) = c^2$ или $\varphi(c) = c \oplus \alpha$, где α — любой фиксированный ненулевой элемент из $\mathbb{F}_{2^n}$. В самом деле, если, скажем, $\varphi(c) = c^2 = d$ и для ненулевых элементов поля c', c выполняется равенство $c \cdot d' = c' \cdot d$, то $c \cdot c'^2 = c' \cdot c^2$ и $c' = c$.

Набор констант $w_i \in \mathcal{A}$ играет роль «счётчика». Набор констант $w_i(k) = f_k(w_i) \in \mathcal{A}(k)$ делает «счётчик» зависимым от ключа. Естественно потребовать, чтобы отображение f_k было инъективным и, кроме того, делало зависимость констант $w_i(k)$ от ключа нелинейной. Это необходимо для того, чтобы нелинейной стала функция зашифрования. Один из вариантов такого f_k связан с использованием подходящих квазигрупповых операций $*$ на $\mathbb{F}_{2^n}$ (перемешивающие преобразования) и обратимых преобразований множества $\{0, 1\}^n$ (рассеивающие преобразования).

Такое отображение можно определить, например, формулой
$$f_k(w) = L(w * a) *' b, \tag{3}$$

где $*, *'$ — квазигрупповые операции (возможно, одинаковые), а L — обратимое преобразование множества $\{0,1\}^n$, обладающее хорошими рассеивающими свойствами. Подходящие квазигрупповые операции предложены, например, в [6, 7]. Так, в [6] операция $x * y = z$ на $\mathbb{F}_{2^t}$ задаётся формулой

$$\mathbf{z} = P(\mathbf{x}, \mathbf{y}) = \sum_{i,j} a_{i,j}\mathbf{x}^i\mathbf{y}^j \bmod 2^t \tag{4}$$

при условии, что $P(u,0), P(0,v), P(u,1)$ и $P(1,v)$ определяют биекции. Критерий биективности отображения $\mathbb{Z}_{2^t} \to \mathbb{Z}_{2^t}$, задаваемого многочленом $a_0 + a_1x + \ldots + a_mx^m$, определяется следующими уловиями: a_1 — нечётное число, а числа $(a_2 + a_4 + a_6 + \ldots)$ и $(a_3 + a_5 + a_7 + \ldots)$ — чётные. В [7] операция $x * y = z$ на $\mathbb{F}_{2^t}$ задаётся формулой

$$\mathbf{z} = \theta\mathbf{x} + \vartheta\mathbf{y} + \pi\mathbf{x}^\lambda\mathbf{y}^\mu \bmod 2^t, \tag{5}$$

где θ, ϑ — нечётные числа; π — чётное число; $\lambda, \mu \in \mathbb{N}$.

В качестве L в (3) можно предложить, например, следующее отображение. Представим вектор $\overline{x} \in \{0,1\}^n$ в виде последовательности байтов $\overline{x} = \overline{x}_1||\ldots||\overline{x}_{n/8}$. Пусть $\widehat{L}$ — максимально рассеивающая матрица размеров $n/8 \times n/8$. Тогда $L(x) = y$, где $\overline{y} = \overline{y}_1||\ldots||\overline{y}_{n/8}$, а $(\mathbf{y}_1, \ldots, \mathbf{y}_{n/8}) = (\mathbf{x}_1, \ldots, \mathbf{x}_{n/8})\,\widehat{L}$. Умножение выполняется в поле $\mathbb{F}_{256}$. Такое преобразование делает зависимым каждый байт вектора $\overline{y}$ от каждого байта вектора $\overline{x}$. Например, при $n = 128$ это преобразование, используемое в шифрсистеме «Кузнечик».

Отображение p, определяющее «счётчик», можно, например, задать перестановочным многочленом $p(x)$ над кольцом $\mathbb{Z}_{2^n}$. Критерий биективности такого многочлена сформулирован выше.

При выборе отображения g будем исходить из того, чтобы при случайном равновероятном выборе ключа $k = (a,b)$ ключ $k^{(\tau)} = (a^{(\tau)}, b^{(\tau)})$ также выбирался случайно равновероятно, разным значениям τ отвечали разные ключи $k^{(\tau)}$ и чтобы задача нахождения ключа k при известных $k^{(\tau)}$, $iv^{(\tau)}$ была вычислительно сложной. Один из вариантов такого отображения даёт использование введённых квазигрупповых операций

$$g\left(a, b, \gamma^{(\tau)}, \delta^{(\tau)}\right) = \left(L\left(a * \gamma^{(\tau)}\right) *' a, L\left(b * \delta^{(\tau)}\right) *' b\right), \tag{6}$$

где компоненты правой части равенства получены аналогично формуле (3).

2. Анализ криптосистемы $\mathbb{CS}$

Приведём некоторые общие соображения, которые качественно характеризуют стойкость криптосистемы $\mathbb{CS}$.

Заметим, что предложенный выбор отображений φ, f_k, p, g позволяет утверждать, что $w_i(k) \neq w_j(k)$ при $i \neq j$ и при неповторяющемся векторе инициализации $iv^{(\tau)}$ каждый производный ключ $k^{(\tau)}$ используется однократно, причём если k выбирается случайно равновероятно, то и $k^{(\tau)}$ выбирается случайно равновероятно. Эти замечания приводят к следующему утверждению.

Теорема 2. Пусть ключ k криптосистемы $\mathbb{CS}$ выбирается случайно равновероятно, а распределение $\mathcal{P}_S$ таково, что для действительных чисел α, β, σ, удовлетворяющих неравенствам $0 < \alpha, \beta < 1 \leqslant \sigma$, выполняются условия $\alpha \leqslant p_S(s) \leqslant \beta$, $\beta/\alpha \leqslant \sigma$ для каждого $s \in \mathcal{S}$. Тогда $\mathbb{CS}$ реализует ε-совершенное шифрование текста $s^{(\tau)}$, состоящего из $r^{(\tau)} > 1$ блоков, для $\varepsilon < \sigma 2^{-n}$. При этом для $\mathbb{CS}$ как А-кода с секретностью имеют место следующие оценки вероятностей успеха имитации и подмены: $p_0 = 2^{-n}$, $p_1 \leqslant r^{(\tau)}\sigma 2^{-n}$.

Доказательство. Заметим, что роль констант c_i, d_i для криптосистемы $\mathbb{CS}$ выполняют $f_k(w_i)$ и $\varphi(f_k(w_i))$. В нашем случае не исключается ситуация, когда $f_k(w_i) = L(w_i * a) *' b = 0$. В условиях теоремы 1 константы c_i, d_i ненулевые и удовлетворяют соотношению (1). Такой выбор констант позволял получить оценку величины ε. Для этого использовалась формула

$$\varepsilon = \max_{s,m} \left| \frac{|\mathcal{K}(s,m)|}{|\mathcal{K}(m)|} - \frac{1}{|\mathcal{S}|} \right|, \tag{7}$$

в которой величина $|\mathcal{K}(m)|$ равна q, а величина $|\mathcal{K}(s,m)|$ ограничена сверху единицей.

В условиях теоремы 2 величина $|\mathcal{K}(m)|$ не меняется, поскольку меняется лишь производный ключ $k^{(\tau)} = (a^{(\tau)}, b^{(\tau)})$, т. е., по сути дела, лишь вектор инициализации $iv^{(\tau)}$. Выясним, остается ли в силе ограничение для $|\mathcal{K}(s,m)|$.

Пусть для различных производных ключей $k' = (a', b')$ и $k'' = (a'', b'')$ выполняются равенства

$$m_i = s_i \oplus \widetilde{w}_i \cdot a' \oplus \widetilde{w}_i^2 \cdot b' = s_i \oplus \widetilde{w}_i \cdot a'' \oplus \widetilde{w}_i^2 \cdot b''.$$

Если $\widetilde{w}_i \neq 0$, то, как и в теореме 1, это невозможно. А если $\widetilde{w}_i = 0$, то это возможно лишь для одного значения i. Но по условию $r > 1$, поэтому либо $\widetilde{w}_{i-1} \neq 0$, либо $\widetilde{w}_{i+1} \neq 0$, и мы попадаем в условия предыдущего случая. Тем самым для различных k' и k'' при $r > 1$ невозможно равенство $E_{k'}(s) = E_{k''}(s)$. Следовательно, оценка величины ε по формуле (7) остаётся в силе, т. е. $\varepsilon < \sigma 2^{-n}$ в условиях теоремы 2. Вероятности успеха имитации и подмены оцениваются так же, как и в теореме 1. ■

Приведём числовой пример, характеризующий результаты теоремы 2. При $n = 128$, $\sigma = 2^{32}$, $r = 2^{32}$ криптосистема $\mathbb{CS}$ реализует ε-совершенное шифрование текста $s^{(\tau)}$ длины, не превосходящей 2^{32} блоков, для $\varepsilon < 2^{-96}$ и его аутентификацию, обеспечивая значения $p_0 = 2^{-128}$, $p_1 < 2^{-64}$.

Сделаем ряд замечаний по выбору параметров криптосистемы:

1) Выбор квазигрупповых операций в формулах (4) или (5) может быть достаточно произвольным. Он должен обеспечивать нелинейность преобразований в (3) и (6).
2) Задача определения ключа по открытому и шифрованному текстам для криптосистемы $\mathbb{CS}$ сводится к решению системы уравнений

$$\begin{cases} w_i(k)a^{(\tau)} \oplus w_i(k)^2 b^{(\tau)} = u_i^{(\tau)}, \\ a^{(\tau)} \oplus m_1^{(\tau)} (b^{(\tau)})^{r_\tau} \oplus \ldots \oplus m_{r_\tau}^{(\tau)} (b^{(\tau)})^1 = m_{r_\tau+1}^{(\tau)}, \\ i = 1, 2, \ldots, r_\tau,\ \tau = 1, 2, \ldots, L, \end{cases}$$

относительно ключа $k = (a, b)$, где $u_i^{(\tau)} = s_i^{(\tau)} \oplus m_i^{(\tau)}$. В этой системе можно считать известными лишь элементы $u_i^{(\tau)}$ и $m_j^{(\tau)}$, $j = 1, \ldots, r_{\tau+1}$. Для выбранных в (3) и (6) отображений f_k и g уравнения системы из первой строки приводят к нелинейным уравнениям относительно a, b, в записи которых используются как операции поля $\mathbb{F}_{2^n}$, так и операции кольца $\mathbb{Z}_{2^n}$.

Исключение $a^{(\tau)}$ из второй строки системы не даёт возможности исключить $a^{(\tau)}$ и из первой строки, поскольку $w_i(k)$ неизвестны. Остаётся возможность того, что при некотором τ шифртекст будет состоять из большого числа нулевых элементов поля, в результате чего получится уравнение невысокой степени в поле $\mathbb{F}_{2^n}$ относительно $a^{(\tau)}, b^{(\tau)}$. В худшем случае, когда $m_1^{(\tau)} = \ldots = m_{r_\tau}^{(\tau)} = 0$, получается равенство $a^{(\tau)} = m^{(\tau)}_{r_\tau+1}$. Однако вероятность такого события сравнима с величиной 2^{-nr_τ}. При этом найти $b^{(\tau)}$ не представляется возможным. Можно попытаться для нахождения производного ключа опробовать все варианты $b^{(\tau)}$ и вычислять из соотношения второй строки $a^{(\tau)}$. Но при этом для 2^n получившихся допустимых вариантов производного ключа необходимо проверить соотношение из первой строки. Для этого потребуется решить уравнения $a^{(\tau)} = L\left(a * \gamma^{(\tau)}\right) *' a$ и $b^{(\tau)} = L\left(b * \delta^{(\tau)}\right) *' b$ относительно неизвестных a и b. Ясно, что такая задача является вычислительно сложной. Это делает практически невозможной попытку нахождения производного ключа путём опробования. Тем самым задача определения ключа в атаке с подобранными открытыми текстами объективно сложна.

3) Выбор в определении (3) преобразования L с хорошими рассеивающими свойствами делает маловероятной возможность того, чтобы близким векторам $\overline{w}_i$ и $\overline{w}_j$ соответствовали близкие векторы $\overline{w}_i(k)$ и $\overline{w}_j(k)$. Поэтому даже для тривиального счётчика p, такого, что $p(x) = x$, маловероятна близость векторов $\overline{w}_i(k)$ и $\overline{w}_{i+1}(k)$, которую можно использовать для построения метода определения производного ключа. Использование нетривиального счётчика p, предложенного выше, ещё в большей степени защищает от указанной потенциальной слабости преобразования (3).
4) Оценка $\mathbb{CS}$ с позиций атак различения возможна по той же схеме, которая была использована при оценке стойкости криптосистемы GCM [5, 8]. В самом деле, $\mathbb{CS}$ отличается от GCM лишь тем, что использует в качестве базовой системы шифрования не систему подстановок $E = \{E_k : \{0,1\}^n \to \{0,1\}^n,\ k \in \mathcal{K}\}$, а систему функций $\Phi = \{\Phi_{k,iv} : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n} |\ k, iv \in (\mathbb{F}_{2^n})^2\}$, где
$$\Phi_{k,iv}(w) = f_k(w)a^{(\tau)} \oplus (f_k(w))^2 b^{(\tau)}, \tag{8}$$
и тем, что её система аутентификации основана на полиномах со свободным членом, тогда как GCM использует для аутентификации полиномы без свободного члена. Последнее, очевидно, не влияет на стойкость аутентификации. Значения функции $\Phi_{k,iv}$ — это блоки гаммы, используемые для шифрования блоков открытого текста. Так как при шифровании текста $a^{(\tau)}$ и $b^{(\tau)}$ не изменяются, мы имеем дело с семейством функций вида $\alpha w' \oplus \beta w'^2$ для некоторых $\alpha, \beta \in \mathbb{F}_{2^n}$, где $w' = L(w * a) *' b$. Поскольку многочлен $\alpha x \oplus \beta x^2$ может иметь более одного корня в $\mathbb{F}_{2^n}$, функции $\Phi_{k,iv}$ могут не быть биективными. В то же время, так как для любого $\rho \in \mathbb{F}_{2^n}$ и любых α, β, одновременно не равных нулю, уравнение $\alpha x \oplus \beta x^2 = \rho$ имеет не более двух решений, число образов $\Phi_{k,iv}$ (блоков гаммы) достаточно велико: $|\{\Phi_{k,iv}(w) | w \in \mathcal{A}\}| \geqslant 2^n/2 > 2^{n-1}$.
5) Биективная связь w' с w, зависящая от ключа, и зависимость от ключа $a^{(\tau)}$ и $b^{(\tau)}$ делают недоступными для атакующего ни w', ни α, β. Поэтому в атаке различения семейства функций Φ, получая от оракула значения $\Phi_{k,iv}(w)$, $i = 1, 2, \ldots$, различитель не может воспользоваться тем, что $\Phi_{k,iv}$ как функция от w'_i является многочленом. Если бы зависимость $w' = f(w)$ была известной, различитель воспользовался бы интерполяционной формулой Лагранжа и построил эффективную атаку, использующую всего лишь четыре запроса к оракулу.
6) Можно использовать криптосистему $\mathbb{CS}$ в режиме AEAD (режим шифрования с аутентификацией, использующий ассоциированные данные), добавив на этапе аутентификации блоки ассоциированных данных подобно тому, как это сделано в GCM.

7) При случайном выборе ключа не исключается случай, когда $k^{(\tau)} = (0,0)$. Этот случай нежелателен, поскольку все блоки гаммы становятся равными 0^n. Избавиться от этого можно следующим образом. При вычислении производного ключа $k^{(\tau)}$ можно ввести дополнительный шаг — проверку равенства $k^{(\tau)} = (0,0)$. Если оно выполняется, то нужно сменить $iv^{(\tau)}$. Для этого можно в $\overline{iv}^{(\tau)}$ выделить один бит, например старший, и в случае, когда $k^{(\tau)} = (0,0)$, инвертировать этот бит.
8) Схема алгоритма криптосистемы $\mathbb{CS}$ представлена на рис. 1.

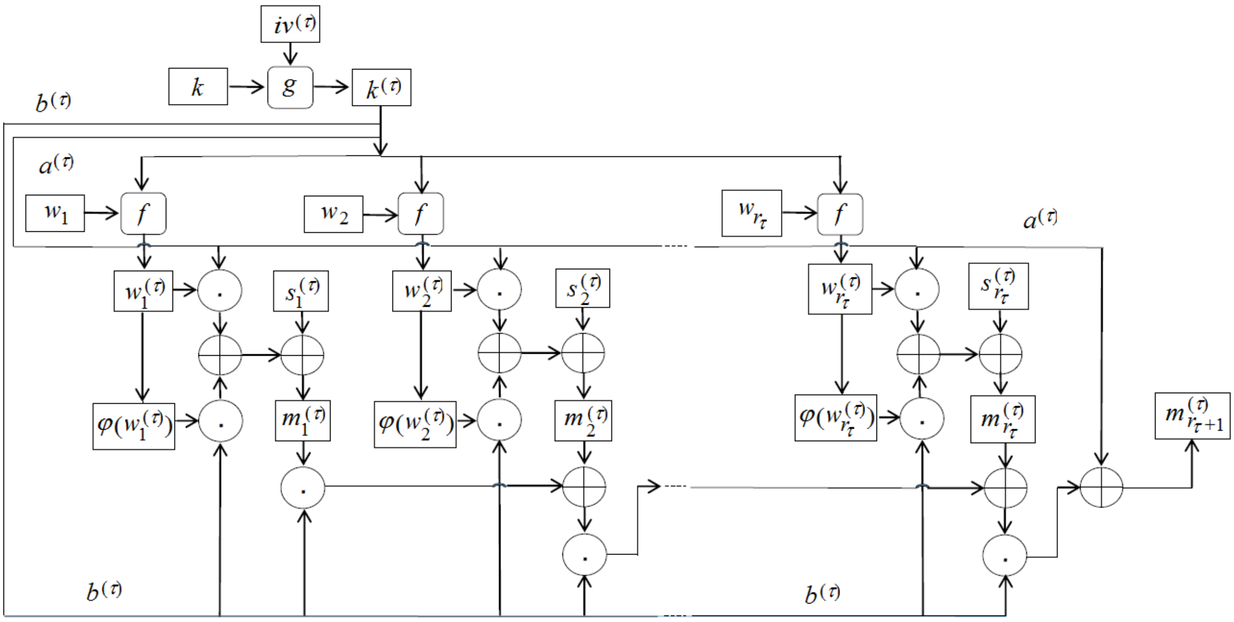

Рис. 1. Криптосистема $\mathbb{CS}$ (без дополнения последнего неполного блока)

Все шаги алгоритма эффективно реализуемы, об этом свидетельствует, например, то, что операции алгоритма реализуются стандартными средствами пакета «Математика». Наиболее трудоёмкими являются квазигрупповые операции $*$ и операции умножения элементов поля $\mathbb{F}_{2^n}$. Были бы интересны и другие варианты выбора квазигрупповых операций на множестве $\{0,1\}^n$, обладающие указанными выше свойствами и допускающие более эффективные реализации.

9) Заметим, что при использовании предложенного варианта отображения $\varphi(c) = c \oplus \alpha$, где α — любой фиксированный ненулевой элемент из $\mathbb{F}_{2^n}$, можно выиграть в трудоёмкости. Получим алгоритм, который при шифровании каждого блока использует не три, а лишь две операции умножения в поле. В таком варианте схемы вместо функций (8) используются функции вида $\Phi_{k,iv}(w) = f_k(w)a^{(\tau)} \oplus (f_k(w) \oplus \alpha)\, b^{(\tau)}$. Следует, однако, отметить недостаток такой схемы. В случае, если $a^{(\tau)} = b^{(\tau)}$, $\mathbb{CS}$ реализует шифр простой замены. Такой случай нежелателен. Он устраним таким же образом, как и в п. 7.
10) Выбор констант, используемых в алгоритме, позволяет параллельно вычислять блоки шифртекста и допускает возможность зашифрования текста вплоть до длины, сравнимой с числом элементов поля. Заметим, что предложенный алгоритм допускает этап предвычислений, который может дать существенный выигрыш в трудоёмкости при шифровании многих сообщений с помощью основного ключа k. В самом деле, при шифровании текстов $s^{(\tau)}$ используется один и тот

же набор констант $w_i(k)$, $i = 1, 2, \ldots$ Если в некотором приложении тексты $s^{(\tau)}$ имеют не слишом большие длины, то можно выделить память для записи этих констант и использовать их далее при шифровании многих текстов.

11) Схему дополнения последнего неполного блока для $\mathbb{CS}$ можно выбрать той же, что и в GCM.

Заключение

Представленная идея криптосистемы шифрования с аутентификацией допускает эффективную реализацию при широком спектре изменяемых параметров, прежде всего отображений φ, f_k, p, g, L. Конструкция криптосистемы позволяет в теореме 2 дать оценку её стойкости как кода аутентификации с секретностью и показать, что она реализует ε-совершенное шифрование сообщений с незначительными ограничениями на их частотные характеристики и обеспечивает стойкую аутентификацию. Подобная оценка для криптосистемы шифрования с аутентификацией получена впервые.

Приводятся соображения, указывающие на объективную сложность задачи определения ключа варианта криптосистемы в атаке с подобранными открытыми текстами. Выделяются некоторые «слабые» ключи и предлагаются пути обхождения этих слабостей. Вместе с тем задача определения ключа требует более детального анализа, как и задача оценки псевдослучайности семейства функций (8), определяющей оценку стойкости криптосистемы в атаках различения.

Некоторые детали алгоритма, реализуемого криптосистемой, такие, как выбор вектора инициализации, дополнение последнего неполного блока, способы реализации операций поля $\mathbb{F}_{2^n}$ и кольца $\mathbb{Z}_{2^n}$, организация и объём необходимой памяти, возможность использования ассоциированных данных, также требуют более тщательной проработки.

ЛИТЕРАТУРА

1. *Kabatianskii G. A., Johansson G., and Smeets B.* On the cardinality of systematic A-codes via error correcting codes // IEEE Trans. Inform. Theory. 1996. V. IT-42. No. 2. P. 566–578.
2. *Зубов А. Ю.* Почти совершенные шифры и коды аутентификации // Прикладная дискретная математика. 2011. № 4(14). С. 28–33.
3. *Зубов А. Ю.* О понятии ε-совершенного шифра // Прикладная дискретная математика. 2016. № 3(33). С. 45–52.
4. *Зубов А. Ю.* Коды аутентификации с секретностью // Математические вопросы криптографии. 2017. Т. 8. № 3. С. 5–40.
5. *Зубов А. Ю.* Об оценке стойкости AEAD-крипосистемы типа GCM // Прикладная дискретная математика. 2016. № 2(32). С. 49–62.
6. *Rivest R. R.* Permutation polynomials modulo 2^w // Finite Fields Their Appl. 2001. V. 7. No. 2. P. 287–292.
7. *Заец М. В.* Построение подстановок с использованием вариационно-координатно полиномиальных функций над примарным кольцом вычетов // Математические вопросы криптографии. 2015. Т. 6. № 1. С. 5–32.
8. *McGrew D. A. and Viega J.* The security and performance of Galois/Counter mode of operation // LNCS. 2004. V. 3348. P. 343–355.

REFERENCES

1. *Kabatianskii G. A., Johansson G., and Smeets B.* On the cardinality of systematic A-codes via error correcting codes. IEEE Trans. Inform. Theory, 1996, vol. IT-42, no. 2, pp. 566–578.

2. *Zubov A. Yu.* Pochti sovershennye shifry i kody authentifikatsii [Almost perfect ciphers and authentication codes]. Prikladnaya Diskretnaya Matematika, 2011, no. 4(14), pp. 28–33. (in Russian)
3. *Zubov A. Yu.* O ponyatii ε-sovershennogo shifra [About the concept of ε-perfect cipher]. Prikladnaya Diskretnaya Matematika, 2016, no. 3(33), pp. 45–52. (in Russian)
4. *Zubov A. Yu.* Kody authentifikatsii s sekretnostiu [Authentication codes with secrecy]. Matematicheskie Voprosy Kriptografii, 2017, vol. 8, no. 3, pp. 5–40. (in Russian)
5. *Zubov A. Yu.* Ob otcenke stoykosti AEAD-kriptosystemy tipa GCM [On the estimation of secrecy of the type GCM AEAD-cryptosystem]. Prikladnaya Diskretnaya Matematika, 2016, no. 2(32), pp. 49–62. (in Russian)
6. *Rivest R. R.* Permutation polynomials modulo 2^w. Finite Fields Their Appl., 2001, vol. 7, no. 2, pp. 287–292.
7. *Zaec M. V.* Postroenie podstanovok s ispolzovaniem variatcionno-koordinatno polinomialnykh funktciy nad primarnym koltcom vychetov [Build of permutations using variation-coordinate polynomiality functions over primary deduction ring]. Matematicheskie Voprosy Kriptografii, 2015, vol. 6, no. 1, pp. 5–32. (in Russian)
8. *McGrew D. A. and Viega J.* The security and performance of Galois/Counter mode of operation. LNCS, 2004, vol. 3348, pp. 343–355.

МАТЕМАТИЧЕСКИЕ ОСНОВЫ НАДЁЖНОСТИ ВЫЧИСЛИТЕЛЬНЫХ И УПРАВЛЯЮЩИХ СИСТЕМ

УДК 519.718

О СКОЛЬ УГОДНО НАДЁЖНОЙ РЕАЛИЗАЦИИ БУЛЕВЫХ ФУНКЦИЙ НЕВЕТВЯЩИМИСЯ ПРОГРАММАМИ С ОПЕРАТОРОМ УСЛОВНОЙ ОСТАНОВКИ В БАЗИСАХ С ОБОБЩЁННОЙ КОНЪЮНКЦИЕЙ[1]

С. М. Грабовская*, М. А. Алехина**

*Пензенский государственный университет, г. Пенза, Россия

**Пензенский государственный технологический университет, г. Пенза, Россия

Рассматривается реализация булевых функций неветвящимися программами с оператором условной остановки в полном конечном базисе, содержащем обобщённую конъюнкцию. Предполагается, что вычислительные операторы программы независимо друг от друга подвержены неисправностям произвольного типа, в свою очередь, операторы условной остановки также ненадёжны. Доказано, что произвольную булеву функцию можно реализовать сколь угодно надёжной неветвящейся программой.

Ключевые слова: *булева функция, неветвящаяся программа, оператор условной остановки, синтез, надёжность.*

DOI 10.17223/20710410/43/5

ON THE ARBITRARILY RELIABLE IMPLEMENTATION OF BOOLEAN FUNCTIONS BY NON-BRANCHING PROGRAMS WITH A CONDITIONAL STOP OPERATOR IN BASES WITH GENERALIZED CONJUNCTION

S. M. Grabovskaya*, M. A. Alekhina**

*Penza State University, Penza, Russia

**Penza State Technological University, Penza, Russia

E-mail: swetazin@mail.ru

The implementation of Boolean functions by non-branching programs with a conditional stop operator is considered in a complete finite basis containing a generalized conjunction, i.e. a function of the form $x_1^{\alpha_1} \& x_2^{\alpha_2}$ $(\alpha_1, \alpha_2 \in \{0, 1\})$. The computational operators are assumed to go into faulty states of an arbitrary type independently of each other with a probability not exceeding the value $N(B)$, i.e. unreliability of the most unreliable ("bad") of the basic elements. In addition, conditional stop operators are also unreliable and independently of each other are prone to two types of faults: the first and second kind. The fault of the first kind is characterized by the fact

[1]Работа поддержана грантом РФФИ № 17-01-00451-а

that on admission to the stop-operator input unit this operator does not work with a probability $\delta \in (0, 1/2)$ and, therefore, the program work continues. The fault of the second kind is that on admission to the stop-operator input zero this operator works with probability $\eta \in (0, 1/2)$, and, hence, the program work stops. Denote $\mu = \max\{\delta, \eta\}$. To increase the reliability of source programs, we use the function $g(x_1, x_2, x_3, x_4)$ of the form $(x_1^{\sigma_1} x_2^{\sigma_2} \vee x_3^{\sigma_3} x_4^{\sigma_4})^{\sigma_5}$ $(\sigma_i \in \{0,1\}, i \in \{1,2,3,4,5\})$ and the method of multiple duplication of circuits and programs. We prove that if the complete finite basis B contains a function of the form $x_1^{\alpha_1} \& x_2^{\alpha_2}$ $(\alpha_1, \alpha_2 \in \{0,1\})$, then any Boolean function f can be implemented by a non-branching program with unreliability no more than $[0{,}84]^t \cdot 5{,}17 \cdot N(B)$ for any natural t with $N(B) \in (0, 1/960]$ and $\mu \in (0, 1/10]$. So, it is proved that an arbitrary Boolean function can be implemented with an arbitrarily reliable non-branching program.

Keywords: *Boolean function, non-branching program, conditional stop operator, synthesis, reliability.*

Введение

Работа относится к одному из важнейших разделов математической кибернетики — теории синтеза, сложности и надёжности управляющих систем. Актуальность исследований в этой области обусловлена важностью многочисленных приложений, возникающих в различных разделах науки и техники.

Одной из важнейших задач математической кибернетики является задача синтеза надёжных неветвящихся программ (с оператором условной остановки или без него), содержащих ненадёжные операторы.

Неветвящиеся программы, реализующие булевы функции, относятся к числу основных модельных объектов математической теории синтеза, сложности и надёжности управляющих систем. Неветвящиеся программы с оператором условной остановки [1] отличаются от неветвящихся программ наличием управляющей команды — команды условной остановки, дающей возможность досрочного прекращения работы программы при выполнении определённого условия, а именно при поступлении единицы на вход оператора условной остановки (который ещё называют стоп-оператором).

Разработка специальных методов синтеза схем из ненадёжных функциональных элементов, реализующих булевы функции, связана главным образом с выбранной математической моделью неисправностей. К основным моделям неисправностей на выходах (входах) функциональных элементов относятся, например, инверсные неисправности, однотипные константные неисправности типа 0 или 1 [2–5]. В классе схем из функциональных элементов для почти любой булевой функции построение схемы сколь угодно высокой надёжности невозможно [6, 7].

Принципиально другой оказалась ситуация в случае синтеза надёжных неветвящихся программ с оператором условной остановки. В отличие от схем из ненадёжных функциональных элементов, в этой работе найдены методы синтеза неветвящихся программ, пригодные для использования при любых неисправностях вычислительных операторов и двух типах неисправностей стоп-операторов, которые позволяют строить для любой булевой функции не просто надёжные или асимптотически оптимальные по надёжности программы, а программы сколь угодно высокой надёжности.

Рассматривается реализация булевых функций неветвящимися программами с оператором условной остановки в полном конечном базисе, содержащем обобщённую двухместную конъюнкцию $x_1^{\alpha_1} \& x_2^{\alpha_2}$ $(\alpha_1, \alpha_2 \in \{0,1\})$. Все операторы (и вычислительные, и остановки) предполагаются ненадёжными, причём неисправности вычислительных операторов произвольные [8]. Таким образом, решаемая задача имеет самую общую формулировку (по сравнению с ранее опубликованными работами, например [9]) с одним лишь ограничением — полный базис не является произвольным, он содержит обобщённую двухместную конъюнкцию.

Прежде чем перейти к изложению результатов этой работы, сформулируем необходимые понятия, определения [1, 9] и ранее известные результаты.

1. Основные понятия, определения, ранее известные результаты

Пусть $X = \{x_1, \ldots, x_n\}$ — множество независимых булевых переменных, $\mathbf{x} = (x_1, \ldots, x_n)$ — набор независимых переменных, $n \in \mathbb{N}$. Введём множество переменных $Y = \{y_1, \ldots, y_l\}$, которое назовём множеством внутренних переменных, $l \in \mathbb{N}$. Кроме того, обозначим через z выходную переменную.

Пусть далее $a \in Y \cup \{z\}$, $b_1, \ldots, b_d \in X \cup Y \cup \{z\}$ $(d \in \{1, \ldots, n\})$, h — булева функция из базиса B, зависящая не более чем от d переменных. Вычислительной командой (или вычислительным оператором) p назовём выражение $p : a = h(b_1, \ldots, b_d)$. Переменную a назовём выходом вычислительного оператора, переменные $b_1, \ldots, b_d$ — его входами.

Пусть теперь $a \in X \cup Y \cup \{z\}$. Командой остановки (стоп-оператором) p назовём выражение $p : stop(a)$. Переменную a назовём входом оператора остановки p.

Последовательность $Pr = p_1 \ldots p_j \ldots p_L$, состоящая из вычислительных операторов и операторов условной остановки, называется неветвящейся программой с условной остановкой, если при любом $j \in \{1, \ldots, L\}$ каждый вход команды p_j есть либо независимая переменная, либо выход некоторого вычислительного оператора.

Неветвящаяся программа работает в дискретные моменты времени $t = 0, 1, 2, \ldots$, не изменяет значения независимых переменных и изменяет значения внутренних переменных y_i $(i \in \{1, \ldots, l\})$ и значение выходной переменной z.

Результат действия программы Pr на наборе $\mathbf{x}$ обозначим через $Pr(\mathbf{x})$. Значение $Pr(\mathbf{x})$ равно значению выходной переменной z в момент остановки программы. Программа Pr вычисляет n-местную булеву функцию $f(\mathbf{x})$, если при отсутствии неисправностей в программе для любого $\mathbf{x} \in \{0, 1\}^n$ справедливо равенство $Pr(\mathbf{x}) = f(\mathbf{x})$.

Пусть P_2 — множество всех булевых функций, т. е. функций вида $f(x_1, \ldots, x_n) : \{0, 1\}^n \to \{0, 1\}$, $n \in \mathbb{N}$. Рассмотрим реализацию булевых функций неветвящимися программами с оператором условной остановки в полном конечном базисе $B = \{e_1, \ldots, e_q\} \subseteq P_2$ $(q \in \mathbb{N})$, содержащем функцию вида $x_1^{\alpha_1} \& x_2^{\alpha_2}$ $(\alpha_1, \alpha_2 \in \{0, 1\})$. Обозначим через E_i базисный элемент с функцией e_i $(i \in \{1, \ldots, q\})$. Пусть $e_1 = x_1^{\alpha_1} \& x_2^{\alpha_2}$, обозначим данную базисную функцию через $e_\&$, а соответствующий ей базисный элемент — через $E_\&$.

Будем считать, что неисправности вычислительных операторов программы произвольные [8, с. 480] и статистически независимые, т. е. вычислительные операторы переходят в неисправные состояния независимо друг от друга.

Предполагается, что операторы условной остановки также ненадёжны и независимо друг от друга подвержены неисправностям двух типов: первого и второго рода. Неисправность первого рода характеризуется тем, что при поступлении единицы на вход стоп-оператора он с вероятностью $\delta \in (0, 1/2)$ не срабатывает и, следовательно, работа программы продолжается. Неисправность второго рода такова, что при поступлении нуля на вход стоп-оператора он с вероятностью $\eta \in (0, 1/2)$ срабатывает и, следовательно, работа программы прекращается. Обозначим $\mu = \max\{\delta, \eta\}$.

Говорят, что программа с ненадёжными операторами реализует булеву функцию $f(\mathbf{x})$, если при отсутствии неисправностей во всех её операторах на каждом входном наборе $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ значение выходной переменной z равно $f(\mathbf{a})$.

Замечание 1. Схему из функциональных элементов можно считать частным случаем неветвящихся программ, а именно неветвящейся программой, в которой нет стоп-операторов.

Ненадёжностью $N(Pr)$ программы Pr назовем максимальную вероятность ошибки на выходе программы Pr при всевозможных входных наборах. Надёжность программы Pr равна $1 - N(Pr)$.

Обозначим $N(B) = \max\{N(E_1), \ldots, N(E_q)\}$, т.е. $N(B)$ — ненадёжность самого ненадёжного («плохого») из базисных элементов.

Для схем из ненадёжных функциональных элементов, подверженных произвольным неисправностям, известен следующий результат.

Теорема 1 [4]. Пусть B — произвольный полный конечный базис. Тогда любую булеву функцию f можно реализовать схемой S в базисе B, ненадёжность которой $N(S) \leqslant 5{,}17 \cdot N(B)$ при $N(B) \in (0, 1/960]$.

Для повышения надёжности исходных схем (программ) будем использовать функцию $g(x_1, x_2, x_3, x_4)$ вида $(x_1^{\sigma_1} x_2^{\sigma_2} \vee x_3^{\sigma_3} x_4^{\sigma_4})^{\sigma_5}$ $(\sigma_i \in \{0,1\},\ i \in \{1,2,3,4,5\})$. Справедлива

Теорема 2 [10]. Пусть B — полный конечный базис и существует такое N, что любую булеву функцию f можно реализовать неветвящейся программой R_f с ненадёжностью $N(R_f) \leqslant N$. Пусть $g(x_1, x_2, x_3, x_4)$ — функция вида $(x_1^{\sigma_1} x_2^{\sigma_2} \vee x_3^{\sigma_3} x_4^{\sigma_4})^{\sigma_5}$ $(\sigma_i \in \{0,1\}, i \in \{1,2,3,4,5\})$, Pr_g — программа, реализующая функцию $g(x_1, x_2, x_3, x_4)$, а $N(Pr_g)$ — ненадёжность программы Pr_g. Тогда любую булеву функцию f в этом базисе можно реализовать такой программой Pr_f, что справедливо неравенство

$$N(Pr_f) \leqslant \max\{\nu^1, \nu^0\} + 4N \cdot N(Pr_g) + 4N^2,$$

где ν^1 и ν^0 — вероятности ошибок программы Pr_g на наборах $(\bar{\sigma}_1, \bar{\sigma}_2, \bar{\sigma}_3, \bar{\sigma}_4)$ и $(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ соответственно.

2. Основные результаты

Для функции вида $x_1^{\alpha_1} \& x_2^{\alpha_2}$ $(\alpha_1, \alpha_2 \in \{0,1\})$ с точностью до переименования переменных возможны три случая: $x_1 \& x_2$; $\bar{x}_1 \& x_2$; $\bar{x}_1 \& \bar{x}_2$.

Теорема 3. Если полный конечный базис B содержит функцию вида $x_1^{\alpha_1} \& x_2^{\alpha_2}$ $(\alpha_1, \alpha_2 \in \{0,1\})$, то для любой булевой функции f при любом $t \in \mathbb{N}$ можно построить такую неветвящуюся программу Pr_f с оператором условной остановки, реализующую f, что $N(Pr_f) \leqslant (0{,}84)^t \cdot 5{,}17 \cdot N(B)$ при $N(B) \in (0, 1/960]$ и $\mu \in (0, 1/10]$.

Для доказательства теоремы 3 сформулируем и докажем леммы 1–3.

Лемма 1. Если полный конечный базис содержит функцию $x_1 \& x_2$, то в этом базисе функцию $g(x_1, x_2, x_3, x_4) = x_1 x_2 \vee x_3 x_4$ можно реализовать такой неветвящейся программой Pr_g, что $\max\{\nu^0, \nu^1\} = 0$ и $N(Pr_g) \leqslant N(B) + 2\mu$, где ν^0, ν^1 — вероятности ошибок программы Pr_g на наборах $(1,1,1,1)$ и $(0,0,0,0)$ соответственно; $\mu = \max\{\delta, \eta\}$.

Доказательство. Пусть полный конечный базис содержит функцию $e_\&(x_1, x_2) = x_1 \& x_2$. Построим в этом базисе неветвящуюся программу Pr_g, реализующую функцию $g(x_1, x_2, x_3, x_4) = x_1 x_2 \vee x_3 x_4$:

$z = x_1$
$y = x_1 \& x_2$

$stop(y)$
$z = x_3$
$stop(x_4)$
$z = x_4$

Найдём вероятности ν^0 и ν^1 ошибок программы Pr_g на наборах $(1,1,1,1)$ и $(0,0,0,0)$ соответственно. Пусть $\mathbf{b} = (1,1,1,1)$, тогда $g(\mathbf{b}) = 1$. При возникновении неисправности вычислительного оператора либо стоп-оператора на выходе программы непременно появится значение одной из свободных переменных x_1, x_3 или x_4 равное 1. Поэтому для программы, в которой каждой выходной переменной z приписана свободная переменная, ошибки операторов не влияют на результат работы. Следовательно, $\nu^0 = 0$. Пусть теперь $\mathbf{b} = (0,0,0,0)$, тогда $g(\mathbf{b}) = 0$. Рассуждая аналогично предыдущему случаю, получим $\nu^1 = 0$. Таким образом, $\max\{\nu^0, \nu^1\} = 0$.

Поскольку программа Pr_g содержит один вычислительный оператор (ненадёжность его равна $N(E_\&)$) и два стоп-оператора (ненадёжность каждого из них не превосходит μ), её ненадёжность удовлетворяет неравенству $N(Pr_g) \leqslant N(E_\&)+2\mu$. Очевидно, что $N(E_\&) \leqslant N(B)$. Таким образом, $N(Pr_g) \leqslant N(B) + 2\mu$. ■

Лемма 2. Если полный конечный базис содержит функцию $\bar{x}_1\&x_2$, то в этом базисе функцию $g(x_1, x_2, x_3, x_4) = \bar{x}_1x_2 \vee x_3x_4$ можно реализовать такой неветвящейся программой Pr_g, что $\max\{\nu^0, \nu^1\} = 0$ и $N(Pr_g) \leqslant N(B) + 2\mu$, где ν^0, ν^1 — вероятности ошибок программы Pr_g на наборах $(0,1,1,1)$ и $(1,0,0,0)$ соответственно; $\mu = \max\{\delta, \eta\}$.

Доказательство. Пусть полный конечный базис B содержит функцию $e_\&(x_1, x_2) = \bar{x}_1\&x_2$. Построим в этом базисе неветвящуюся программу Pr_g, реализующую функцию $g(x_1, x_2, x_3, x_4) = \bar{x}_1x_2 \vee x_3x_4$:

$z = x_2$
$y = \bar{x}_1\&x_2$
$stop(y)$
$z = x_3$
$stop(x_4)$
$z = x_4$

Найдём вероятности ν^0 и ν^1 ошибок программы Pr_g на наборах $(0,1,1,1)$ и $(1,0,0,0)$ соответственно. Пусть $\mathbf{b} = (0,1,1,1)$, тогда $g(\mathbf{b}) = 1$. При возникновении неисправности вычислительного оператора или стоп-оператора на выходе программы непременно появится значение одной из свободных переменных x_2, x_3 или x_4 равное 1. Следовательно, $\nu^0 = 0$. Пусть теперь $\mathbf{b} = (1,0,0,0)$, тогда $g(\mathbf{b}) = 0$. Рассуждая аналогично, получим $\nu^1 = 0$. Таким образом, $\max\{\nu^0, \nu^1\} = 0$.

Поскольку программа Pr_g содержит один вычислительный оператор (ненадёжность его равна $N(E_\&)$) и два стоп-оператора (ненадёжность каждого из них не превосходит μ), её ненадёжность удовлетворяет неравенству $N(Pr_g) \leqslant N(E_\&)+2\mu$. Очевидно, что $N(E_\&) \leqslant N(B)$. Таким образом, $N(Pr_g) \leqslant N(B) + 2\mu$. ■

Лемма 3. Если полный конечный базис содержит функцию $\bar{x}_1\&\bar{x}_2$, то в этом базисе функцию $g(x_1, x_2, x_3, x_4) = (x_1 \vee x_2)(x_3 \vee x_4)$ можно реализовать такой неветвящейся программой Pr_g, что $\max\{\nu^0, \nu^1\} = 0$ и $N(Pr_g) \leqslant N(B) + 2\mu$, где ν^0, ν^1 — вероятности ошибок программы Pr_g на наборах $(1,1,1,1)$ и $(0,0,0,0)$ соответственно; $\mu = \max\{\delta, \eta\}$.

Доказательство. Пусть полный конечный базис B содержит функцию $e_{\&}(x_1,\, x_2) = \bar{x}_1 \& \bar{x}_2$. Построим в этом базисе неветвящуюся программу Pr_g, реализующую функцию $g(x_1, x_2, x_3, x_4) = (x_1 \vee x_2)(x_3 \vee x_4)$:

$z = x_1$
$y = \bar{x}_1 \& \bar{x}_2$
$stop(y)$
$z = x_3$
$stop(x_3)$
$z = x_4$

Найдём вероятности ν^0 и ν^1 ошибок программы Pr_g на наборах $(1,1,1,1)$ и $(0,0,0,0)$ соответственно. Пусть $\mathbf{b} = (1,1,1,1)$, тогда $g(\mathbf{b}) = 1$. При возникновении неисправности вычислительного оператора либо стоп-оператора на выходе программы непременно появится значение одной из свободных переменных x_1, x_3 или x_4 равное 1. Следовательно, $\nu^0 = 0$. Пусть теперь $\mathbf{b} = (0,0,0,0)$, тогда $g(\mathbf{b}) = 0$. Аналогично рассуждая, получим $\nu^1 = 0$. Таким образом, $\max\{\nu^0, \nu^1\} = 0$.

Поскольку программа Pr_g содержит один вычислительный оператор (ненадёжность его равна $N(E_{\&})$) и два стоп-оператора (ненадёжность каждого из них не превосходит μ), её ненадёжность удовлетворяет неравенству $N(Pr_g) \leqslant N(E_{\&}) + 2\mu$. Очевидно, что $N(E_{\&}) \leqslant N(B)$. Таким образом, $N(Pr_g) \leqslant N(B) + 2\mu$. ■

Доказательство теоремы 3.

Пусть B — полный конечный базис, содержащий хотя бы одну из функций $x_1 \& x_2$, $\bar{x}_1 \& x_2$ или $\bar{x}_1 \& \bar{x}_2$; операторы условной остановки и вычислительные операторы некоторой неветвящейся программы ненадёжны; $N(B) \in (0,\, 1/960]$ и $\mu \in (0,\, 1/10]$; f — любая булева функция. Реализуем её схемой S, ненадёжность которой $N(S) \leqslant 5{,}17 \cdot N(B)$ при $N(B) \in (0, 1/960]$ (см. теорему 1).

В зависимости от того, какая из функций $x_1 \& x_2$, $\bar{x}_1 \& x_2$ или $\bar{x}_1 \& \bar{x}_2$ содержится в базисе B, по одной из лемм 1–3 можно построить такую программу Pr_g, что $\max\{\nu^1, \nu^0\} = 0$ и $N(Pr_g) \leqslant N(B) + 2\mu$. Чтобы построить программу $Pr_f^{(1)}$, реализующую функцию f, воспользуемся теоремой 2, взяв в качестве программы R_f схему S (см. замечание 1) и полагая $N = 5{,}17 \cdot N(B)$. Тогда ненадёжность программы $Pr_f^{(1)}$ удовлетворяет неравенству

$$N(Pr_f^{(1)}) \leqslant 4N(N(Pr_g) + N) \leqslant 4N(2\mu + N(B) + 5{,}17 \cdot N(B)) \leqslant \\ \leqslant 4N(0{,}2 + 6{,}17/960) \leqslant 0{,}826 \cdot N,$$

т. е. $N(Pr_f^{(1)}) \leqslant 0{,}826 \cdot N$. Тогда верно неравенство

$$N(Pr_f^{(1)}) \leqslant 0{,}826 \cdot N \leqslant 0{,}826 \cdot 5{,}17 \cdot N(B).$$

Выполним ещё один шаг, т. е. построим программу $Pr_f^{(2)}$, реализующую функцию f, но заменим N на $0{,}826 \cdot N$ и в качестве R_f возьмём построенную программу $Pr_f^{(1)}$. Тогда справедливо неравенство

$$N(Pr_f^{(2)}) \leqslant 4 \cdot 0{,}826 \cdot N(2\mu + N(B) + 0{,}826 \cdot N) \leqslant \\ \leqslant 4 \cdot 0{,}826 \cdot N(0{,}2 + 1/960 + 0{,}826 \cdot 5{,}17/960) \leqslant (0{,}826)^2 N.$$

Далее методом индукции по числу итераций $t\,(t \geqslant 2)$ нетрудно доказать, что функцию f можно реализовать программой $Pr_f^{(t)}$, ненадёжность которой $N(Pr_f^{(t)}) \leqslant \leqslant (0{,}826)^t N$. Выполним индуктивный переход. Пусть функцию f можно реализовать программой $Pr_f^{(t-1)}$, ненадёжность которой $N(Pr_f^{(t-1)}) \leqslant (0{,}826)^{t-1}N$. Проделаем ещё одну итерацию, т. е. построим программу $Pr_f^{(t)}$ и оценим её ненадёжность с помощью теоремы 2:

$$N(Pr_f^{(t)}) \leqslant 4(0{,}826)^{t-1}N(2\mu + N(B) + (0{,}826)^{t-1}N) \leqslant$$
$$\leqslant 4(0{,}826)^{t-1}N(0{,}2 + 1/960 + (0{,}826)^{t-1}N) \leqslant$$
$$\leqslant 4(0{,}826)^{t-1}N(0{,}2 + 1/960 + 0{,}826 \cdot 5{,}17 \cdot N(B)) \leqslant$$
$$\leqslant 4(0{,}826)^{t-1}N(0{,}2 + 1/960 + 0{,}826 \cdot 5{,}17/960) \leqslant (0{,}826)^{t-1}N \cdot 0{,}826 = (0{,}826)^t N.$$

Поскольку $N = 5{,}17 \cdot N(B)$, функцию f можно реализовать программой $Pr_f^{(t)}$, ненадёжность которой $N(Pr_f^{(t)}) \leqslant (0{,}826)^t \cdot 5{,}17 \cdot N(B)$. ∎

Следствие 1. Если полный конечный базис B содержит функцию вида $x_1^{\alpha_1} \& x_2^{\alpha_2}$ $(\alpha_1, \alpha_2 \in \{0,1\})$, то любую булеву функцию f можно реализовать сколь угодно надёжной неветвящейся программой Pr_f с оператором условной остановки при $N(B) \in (0, 1/960]$ и $\mu \in (0, 1/10]$.

Доказательство. Пусть p — произвольное сколь угодно малое положительное число. Покажем, что, проделав достаточное число итераций, функцию f можно реализовать программой, ненадёжность которой не больше p.

По теореме 3 функцию f можно реализовать программой, ненадёжность которой $N(Pr_f^{(t)}) \leqslant (0{,}826)^t \cdot 5{,}17 \cdot N(B) \leqslant (0{,}826)^t \cdot 5{,}17/960$. Решим неравенство $(0{,}826)^t \cdot 5{,}17/960 \leqslant p$ относительно переменной t и получим $(0{,}826)^t \leqslant 960 \cdot p/5{,}17$, откуда $t \geqslant \log_{0{,}826}(960 \cdot p/5{,}17)$. Выберем наименьшее целое t, удовлетворяющее последнему неравенству (обозначим его t_0). Тогда программа $Pr_f^{(t_0)}$ функционирует с ненадёжностью $N(Pr_f^{(t_0)}) \leqslant p$. ∎

Заключение

Доказано, что если полный конечный базис B содержит функцию вида $x_1^{\alpha_1} \& x_2^{\alpha_2}$ $(\alpha_1, \alpha_2 \in \{0,1\})$, то любую булеву функцию можно реализовать сколь угодно надёжной неветвящейся программой, операторы которой ненадёжны, причём неисправности вычислительных операторов произвольные, при $N(B) \in (0, 1/960]$ и $\mu \in (0, 1/10]$.

ЛИТЕРАТУРА

1. *Чашкин А. В.* О среднем времени вычисления значений булевых функций // Дискретный анализ и исследование операций. Сер. 1. 1997. Т. 4. № 1. С. 60–78.
2. *Alekhina M. A.* Synthesis and complexity of asymptotically optimal circuits with unreliable gates // Fundamenta Informaticae. 2010. No. 104 (3). P. 219–225.
3. *Алехина М. А., Васин А. В.* О базисах с коэффициентом ненадежности 2 // Матем. заметки. 2014. Т. 95. № 2. С. 170–201.
4. *Алехина М. А., Гусынина Ю. С., Шорникова Т. А.* Верхняя оценка ненадежности схем в полном конечном базисе (в P_2) при произвольных неисправностях элементов // Изв. вузов. Математика. 2017. № 12. С. 70–75.
5. *Алехина М. А.* О синтезе надежных схем из функциональных элементов x/y при однотипных константных неисправностях на выходах элементов // Вест. Моск. ун-та. Матем. Механ. 1991. № 5. С. 80–83.

6. *Алехина М. А.* О надежности схем в произвольном полном конечном базисе при однотипных константных неисправностях на выходах элементов // Дискретная математика. 2012. Т. 24. № 3. С. 17–24.
7. *Алехина М. А., Курышева В. В.* О надежности схем в базисе «антиконъюнкция» при константных неисправностях на входах элементов // Изв. вузов. Математика. 2016. № 7. С. 3–9.
8. *Яблонский С. В.* Избранные труды / под ред. В. Б. Алексеева, В. И. Дмитриева. М.: МАКС Пресс, 2004. 584 с.
9. *Алехина М. А., Грабовская С. М.* О надежности неветвящихся программ в произвольном полном конечном базисе // Изв. вузов. Математика. 2012. № 2. С. 13–22.
10. *Грабовская С. М.* О методах повышения надежности неветвящихся программ с оператором условной остановки // Междунар. науч.-технич. конф. «Проблемы автоматизации и управления в технических системах — 2015, посвященная 70-летию Победы в Великой Отечественной войне». Пенза: Изд-во ПГУ, 2015. С. 339–342.

REFERENCES

1. *Chashkin A. V.* O srednem vremeni vychisleniya znacheniy bulevykh funktsiy [On the average time for the computation of the values of Boolean functions]. Diskretn. Anal. Issled. Oper., Ser. 1, 1997, vol. 4, no. 1, pp. 60–78. (in Russian)
2. *Alekhina M. A.* Synthesis and complexity of asymptotically optimal circuits with unreliable gates. Fundamenta Informaticae, 2010, no. 104 (3), pp. 219–225.
3. *Alekhina M. A. and Vasin A. V.* On bases with unreliability coefficient 2. Math. Notes, 2014, vol. 95, no. 1–2, pp. 147–173.
4. *Alekhina M. A., Gusynina Yu. S., and Shornikova T. A.* Upper estimate of unreliability of schemes in full finite basis (in P_2) for arbitrary faults of gates. Russian Mathematics, 2017, vol. 61, no. 12, pp. 70–72.
5. *Alekhina M. A.* O sinteze nadezhnykh skhem iz funktsional'nykh elementov x/y pri odnotipnykh konstantnykh neispravnostyakh na vykhodakh elementov [On the synthesis of reliable circuits of x/y functional elements at the same type constant faults at the element outputs]. Vest. MSU. Matem. Mekhan., 1991, no. 5, pp. 80–83. (in Russian)
6. *Alekhina M. A.* On reliability of circuits over an arbitrary complete finite basis under single-type constant faults at outputs of elements. Discrete Math. Appl., 2012, vol. 22, no. 4, pp. 383–391.
7. *Alekhina M. A. and Kurysheva V. V.* On the circuits reliability in anticonjunction basis with constant faults at gate inputs. Russian Mathematics, 2016, vol. 60, no. 7, pp. 1–6.
8. *Yablonskiy S. V.* Izbrannye trudy [Selected works]. Eds. V. B. Alekseev and V. I. Dmitriev. Moscow, MAKS Press Publ., 2004. 584 p. (in Russian)
9. *Alekhina M. A. and Grabovskaya S. M.* Reliability of nonbranching programs in an arbitrary complete finite basis. Russian Mathematics., 2012, vol. 56, no. 2, pp. 10–18.
10. *Grabovskaya S. M.* O metodakh povysheniya nadezhnosti nevetvyashchikhsya programm s operatorom uslovnoy ostanovki [On methods of raise the reliability of non-branching programs with a conditional stop operator]. Problems of Automation and Control in Technical Systems. Proc. Int. Conf., dedicated to the 70th anniversary of the Victory in the Great Patriotic War, Penza, Russia, May 19–21, 2015). Penza, Penz. State Univ., 2015, pp. 339–342. (in Russian)

УДК 519.718.7

СИНТЕЗ ЛЕГКОТЕСТИРУЕМЫХ СХЕМ ПРИ ПРОИЗВОЛЬНЫХ КОНСТАНТНЫХ НЕИСПРАВНОСТЯХ НА ВХОДАХ И ВЫХОДАХ ЭЛЕМЕНТОВ[1]

К. А. Попков

Институт прикладной математики им. М. В. Келдыша РАН, г. Москва, Россия

Доказаны следующие утверждения: для любого натурального k существует базис из булевых функций от не более чем $2k+2$ переменных (от не более чем $4k+2$ переменных), в котором любую булеву функцию, кроме константы 1, можно реализовать схемой из функциональных элементов, неизбыточной и допускающей проверяющий тест длины не более 3 (соответственно, диагностический тест длины не более 4) относительно не более k произвольных константных неисправностей на входах и выходах элементов. Показано, что при рассмотрении только произвольных константных неисправностей на входах элементов указанные оценки длин тестов можно понизить до 2.

Ключевые слова: *схема из функциональных элементов, произвольная константная неисправность, проверяющий тест, диагностический тест.*

DOI 10.17223/20710410/43/6

SYNTHESIS OF EASILY TESTABLE LOGIC NETWORKS UNDER ARBITRARY STUCK-AT FAULTS AT INPUTS AND OUTPUTS OF GATES

K. A. Popkov

Keldysh Institute of Applied Mathematics, Moscow, Russia

E-mail: kirill-formulist@mail.ru

Two binary vectors are called k-adjacent if they differ in at most k components, where $k \in \mathbb{N}$. For $\alpha \in \{0,1\}$ and $s \in \mathbb{N}$, let α^s be the Boolean vector $(\alpha,\ldots,\alpha)$ with s coordinates α. For each natural k, consider the bases $B(k) = \{\varphi(x_1,\ldots,x_{2k+2}), x_1\ldots x_{k+1} \vee \overline{x}_1\ldots\overline{x}_{k+1}, \overline{x}, 0\}$ and $B'(k) = \{\varphi(x_1,\ldots,x_{2k+2}), \xi(x_1,\ldots,x_{3k+2}), \eta(x_1,\ldots,x_{4k+2}), \overline{x}, 0\}$, where $\varphi(x_1,\ldots,x_{2k+2})$ is an arbitrary non-self-dual Boolean function taking the value α on the vector α^{2k+2} and the value $\overline{\alpha}$ on all other vectors k-adjacent to this vector; $\xi(x_1,\ldots,x_{3k+2})$ is an arbitrary Boolean function taking the value α on the vector α^{3k+2}, the value $\overline{\alpha}$ on all other vectors k-adjacent to this vector, and the value α on all vectors k-adjacent to the vector $(\alpha^{k+1}, \overline{\alpha}^{2k+1})$; $\eta(x_1,\ldots,x_{4k+2})$ is an arbitrary Boolean function taking the value 1 on the vector α^{4k+2}, the value 0 on all other vectors k-adjacent to this vector, and the value α on all vectors k-adjacent to the vector $(\alpha_{2k+1}, \overline{\alpha}^{2k+1})$. Let $D_{k\,(\mathrm{I})}(f)$ ($D_{k\,(\mathrm{IO})}(f)$, $D'_{k\,(\mathrm{I})}(f)$, $D'_{k\,(\mathrm{IO})}(f)$) be the least length of a fault detection test (fault detection test, diagnostic test, diagnostic test, respectively) for irredundant logic networks consisting of logic gates in the basis $B(k)$ (basis $B(k)$, basis $B'(k)$, basis $B'(k)$, respectively), implementing given Boolean function $f(x_1,\ldots,x_n)$, and having at most k arbitrary

[1]Работа выполнена при поддержке РФФИ, проект № 18-01-00337.

stuck-at faults on inputs of gates (on inputs and/or outputs of gates, on inputs of gates, on inputs and/or outputs of gates, respectively). Let a Boolean function $f(x_1, \ldots, x_n)$ be called palindromic if it takes the same value on any two opposite binary n-tuples. The following facts are obtained. The quantity $D_{k\,(\mathrm{I})}(f)$ equals 0 iff f is an identical function (i.e., $f \equiv x_i$ for some $i \in \{1, \ldots, n\}$) and equals 2 otherwise. The quantity $D_{k\,(\mathrm{IO})}(f)$ equals 0 iff f is an identical function, equals 1 iff $f \equiv 0$, equals 2 iff f is not an identical or palindromic function, equals 3 iff f is a palindromic function and $f \not\equiv 0, 1$, and is undefined iff $f \equiv 1$. The quantity $D'_{k\,(\mathrm{I})}(f)$ equals 0 iff f is an identical function and equals 2 otherwise. The quantity $D'_{1\,(\mathrm{IO})}(f)$ equals 0 iff f is an identical function, equals 1 iff $f \equiv 0$, equals 2 iff $f \equiv \overline{x}_i$ for some $i \in \{1, \ldots, n\}$, equals 3 iff f is not a self-dual function and $f \not\equiv 0, 1$, equals 4 iff f is a self-dual function and $f \notin \{x_1, \ldots, x_n, \overline{x}_1, \ldots, \overline{x}_n\}$, and is undefined iff $f \equiv 1$. For each $k \in \mathbb{N}$, the equality $D'_{k\,(\mathrm{IO})}(f) = 4$ holds true under $n \geqslant 3$, and in the case $k \geqslant 2$, the proportion of those Boolean functions f in n variables, for which $D'_{k\,(\mathrm{IO})}(f) = 4$, tends to 1 under $n \to \infty$.

Keywords: *logic network, arbitrary stuck-at fault, fault detection test, diagnostic test.*

Введение

В работе рассматривается задача синтеза легкотестируемых схем, реализующих заданные булевы функции. Логический подход к тестированию электрических схем предложен С. В. Яблонским и И. А. Чегис в [1]; этот подход применим также к тестированию схем из функциональных элементов [2 – 4]. Пусть имеется схема из функциональных элементов S с одним выходом, реализующая булеву функцию $f(\tilde{x}^n)$, где $\tilde{x}^n = (x_1, \ldots, x_n)$. Под воздействием некоторого источника неисправностей один или несколько элементов схемы S могут перейти в неисправное состояние. В результате схема S вместо исходной функции $f(\tilde{x}^n)$ будет реализовывать некоторую булеву функцию $g(\tilde{x}^n)$, вообще говоря, отличную от f. Все такие функции $g(\tilde{x}^n)$, получающиеся при всевозможных допустимых для рассматриваемой задачи неисправностях элементов схемы S, называются *функциями неисправности* данной схемы.

Введём следующие определения [2 – 4]. *Проверяющим тестом* для схемы S называется такое множество T наборов значений переменных $x_1, \ldots, x_n$, что для любой отличной от $f(\tilde{x}^n)$ функции неисправности $g(\tilde{x}^n)$ схемы S в T найдётся набор $\tilde{\sigma}$, на котором $f(\tilde{\sigma}) \neq g(\tilde{\sigma})$. *Диагностическим тестом* для схемы S называется такое множество T наборов значений переменных $x_1, \ldots, x_n$, что T является проверяющим тестом и, кроме того, для любых двух различных функций неисправности $g_1(\tilde{x}^n)$ и $g_2(\tilde{x}^n)$ схемы S в T найдётся набор $\tilde{\sigma}$, на котором $g_1(\tilde{\sigma}) \neq g_2(\tilde{\sigma})$. Число наборов в T называется *длиной* теста. В качестве тривиального диагностического (и проверяющего) теста длины 2^n для схемы S всегда можно взять множество, состоящее из всех двоичных наборов длины n. Тест называется *полным*, если в схеме могут быть неисправны сколько угодно элементов, и *единичным*, если в схеме может быть неисправен только один элемент. Единичные тесты обычно рассматривают для *неизбыточных схем* [4, с. 110–111], т. е. для таких схем, в которых любая допустимая неисправность любого одного элемента приводит к функции неисправности, отличной от исходной функции, реализуемой данной схемой (такие функции неисправности называют *нетривиальными*).

Назовём проверяющий (диагностический) тест k-*проверяющим* (k-*диагностическим*), если в схеме могут быть неисправны не более k элементов, где $k \in \mathbb{N}$. Будем рассматривать такие тесты только для k-*неизбыточных схем* [5, с. 68], в которых любая допустимая неисправность не менее одного и не более k элементов приводит к нетривиальной функции неисправности. Очевидно, что понятия 1-проверяющего теста, 1-диагностического теста и 1-неизбыточной схемы совпадают с понятиями единичного проверяющего теста, единичного диагностического теста и неизбыточной схемы соответственно.

Любое множество булевых функций будем называть *базисом*.

Пусть зафиксирован вид неисправностей элементов, B — произвольный функционально полный базис и T — единичный проверяющий тест для некоторой схемы из функциональных элементов S в базисе B. Введём следующие обозначения: пусть $D^B_{\text{ЕП}}(T)$ — длина теста T; $D^B_{\text{ЕП}}(S) = \min D^B_{\text{ЕП}}(T)$, где минимум берётся по всем единичным проверяющим тестам T для схемы S; $D^B_{\text{ЕП}}(f) = \min D^B_{\text{ЕП}}(S)$, где минимум берётся по всем неизбыточным схемам S в базисе B, реализующим функцию f; $D^B_{\text{ЕП}}(n) = \max D^B_{\text{ЕП}}(f)$, где максимум берётся по всем булевым функциям f от n переменных, для которых определено значение $D^B_{\text{ЕП}}(f)$. Функция $D^B_{\text{ЕП}}(n)$ называется *функцией Шеннона* длины единичного проверяющего теста. По аналогии с функциями $D^B_{\text{ЕП}}$ можно ввести функции $D^B_{\text{ПП}}$, $D^B_{k\text{-П}}$, $D^B_{\text{ЕД}}$, $D^B_{\text{ПД}}$ и $D^B_{k\text{-Д}}$ для соответственно полного проверяющего, k-проверяющего, единичного, полного диагностического и k-диагностического тестов, зависящие от T, S, f и n (в определениях функций $D^B_{\text{ПП}}(f)$ и $D^B_{\text{ПД}}(f)$ не предполагается неизбыточность схем, а в определениях функций $D^B_{k\text{-П}}(f)$ и $D^B_{k\text{-Д}}(f)$ предполагается k-неизбыточность схем). Так, например, $D^B_{k\text{-Д}}(n)$ — функция Шеннона длины k-диагностического теста.

Перечислим основные результаты, касающиеся тестирования схем из функциональных элементов. Класс допустимых неисправностей функциональных элементов ограничим константными неисправностями на входах и выходах элементов, а также только на входах элементов, при которых значение на неисправном входе (выходе) любого элемента становится равно некоторой булевой константе. Неисправности на входах и выходах элементов называются однотипными константными типа p, если эта константа одна и та же для каждого неисправного элемента и равна p, и произвольными константными, если эта константа может быть равна как 0, так и 1 для каждого неисправного элемента независимо от неисправностей других элементов. Для удобства над буквой D после символов, обозначающих базис, через точку с запятой будем ставить символы «$0, 1$» или «p» в случаях, когда в схемах допускаются соответственно произвольные константные неисправности или однотипные константные неисправности типа p, $p \in \{0, 1\}$, на входах/выходах элементов, а под буквой D после символов, обозначающих вид функции, — символы «(IO)» или «(I)» в случаях, когда в схемах допускаются неисправности соответственно на входах и выходах элементов или только на входах элементов. Вполне разумно предполагать, что если в базисе содержится булева константа α, то у элемента, её реализующего, нет входов и не может быть неисправности типа α на его выходе.

В [4, с. 116] для базиса Жегалкина $B_1 = \{\&, \oplus, 1, 0\}$ показано, что $D^{B_1;\,0,1}_{\text{ЕП (IO)}}(n) \leqslant n + 3$; при этом используется метод построения схем из работы [6]. К. К. Салуджа и С. М. Редди в [7] получили оценку $D^{*\,B_1;\,0,1}_{k\text{-П (IO)}}(n) \leqslant 4 + \sum\limits_{i=1}^{\lfloor \log_2 2k \rfloor} C^n_i$; наличие звёздочки над буквой D обусловлено тем, что в указанной работе рассматривались схемы, содержащие, помимо входных переменных $x_1, \ldots, x_n$, дополнительную входную переменную h_0, вместо которой при реализации функций подавалась булева константа, но которая принимала значения как 0, так и 1 на наборах из теста. Д. С. Романовым и Е. Ю. Романовой в [8] для базисов $B'_1 = \{\&, \oplus, 1\}$, $B''_1 = \{\&, \oplus, \sim\}$ установлены неравенства $D^{B_1'; 0,1}_{\text{ЕП (IO)}}(n) \leqslant 16$ и $D^{B_1''; 0,1}_{\text{ЕП (IO)}}(n) \leqslant 16$; в частности, при $n \geqslant 14$ улучшен упомянутый результат из [4] (любая схема в базисе B_1' является также схемой в базисе B_1). Н. П. Редькин в [9−11] для базиса $B_2 = \{\&, \vee, \neg\}$ получил оценки $D^{B_2; p}_{\text{ПП (I)}}(n) \lesssim 4\left(2^{\lfloor \frac{n}{2} \rfloor} + 2^{\lceil \frac{n}{2} \rceil - 1}\right)$, $D^{B_2; p}_{\text{ЕД (I)}}(n) \lesssim 4\left(2^{\lfloor \frac{n}{2} \rfloor} + 2^{\lceil \frac{n}{2} \rceil - 1}\right)$ и $D^{B_2; 0,1}_{\text{ПП (I)}}(n) \lesssim \dfrac{2^n}{\sqrt{\log_2 n}}$ соответственно, где $p = 0$ или 1. В работе [12] для любого натурального k и для любой булевой константы p доказано существование базиса $B_3(k,p)$, состоящего из булевой функции от $\max(k+1; 3)$ переменных и функции $\overline{x}$, для которого, в частности, $D^{B_3(k,p); p}_{k\text{-П (IO)}}(n) = 2$ при $n \geqslant 1$ и $D^{B_3(k,p); p}_{k\text{-П (I)}}(n) = 1$ при $n \geqslant 0$, а также существование базиса $B_4(k,p)$, состоящего из булевой функции от не более чем $2{,}5k + 2$ переменных и отрицания этой функции, для которого, в частности, $D^{B_4(k,p); p}_{k\text{-Д (IO)}}(n) = 2$ и $D^{B_4(k,p); p}_{k\text{-Д (I)}}(n) = 1$ при $n \geqslant 0$ (следствия 1–4 и двойственные им результаты).

В данной работе рассматриваются k-проверяющие и k-диагностические тесты при $k \in \mathbb{N}$, а в качестве неисправностей функциональных элементов — произвольные константные неисправности на входах и выходах элементов, а также только на входах элементов. Определены базисы $B_5(k)$ и $B_6(k)$, состоящие из булевых функций от не более чем $2k+2$ и $4k+2$ переменных соответственно, для которых доказаны равенства $D^{B_5(k); 0,1}_{k\text{-П (I)}}(n) = D^{B_6(k); 0,1}_{k\text{-Д (I)}}(n) = 2$ при $n \geqslant 0$, $D^{B_5(k); 0,1}_{k\text{-П (IO)}}(n) = 3$ при $n \geqslant 2$ и $D^{B_6(k); 0,1}_{k\text{-Д (IO)}}(n) = 4$ при $n \geqslant 3$ (следствия 1–4 и теорема 5).

В дальнейшем для краткости верхние индексы $0, 1$ у величин вида $D^{B_5(k); 0,1}_{\dots}$ и $D^{B_6(k); 0,1}_{\dots}$, зависящих от f или n, будем опускать.

Введём обозначения $\tilde{0}^r = \underbrace{0, \dots, 0}_{r}$, $\tilde{1}^r = \underbrace{1, \dots, 1}_{r}$, где $r \in \mathbb{N} \cup \{0\}$.

Два двоичных набора называются *противоположными*, если они различаются во всех компонентах. Будем называть два двоичных набора *k-соседними*, если они различаются не более чем в k компонентах.

1. Проверяющие тесты

Рассмотрим базис $B_5(k) = \{\varphi(\tilde{x}^{2k+2}), \psi(\tilde{x}^{k+1}), \overline{x}, 0\}$, где $\psi(\tilde{x}^{k+1}) = x_1 \dots x_{k+1} \vee \vee\, \overline{x}_1 \dots \overline{x}_{k+1}$, а $\varphi(\tilde{x}^{2k+2})$ — произвольная несамодвойственная булева функция (определение самодвойственной булевой функции можно найти, например, в [13, с. 16]), для которой выполнены следующие условия:

(i) $\varphi(\tilde{\alpha}^{2k+2}) = \alpha$ для $\alpha = 0, 1$;

(ii) $\varphi(\tilde{\sigma}) = \overline{\alpha}$, где $\alpha = 0, 1$, а $\tilde{\sigma}$ — любой двоичный набор длины $2k+2$, k-соседний с набором $(\tilde{\alpha}^{2k+2})$, кроме него самого.

Отметим, что условия (i), (ii) однозначно определяют значения функции $\varphi(\tilde{x}^{2k+2})$ на всех наборах, кроме наборов ровно с $k+1$ нулевой и $k+1$ единичной компонентами. Для выполнения условия несамодвойственности необходимо и достаточно, чтобы на каких-то двух противоположных наборах ровно с $k+1$ нулевой и $k+1$ единичной компонентами функция φ принимала одинаковые значения.

Легко видеть, что функция ψ обладает следующими свойствами:

(iii) $\psi(x, \underbrace{y, \dots, y}_{k}) = x \oplus y \oplus 1$;

(iv) $\psi(\tilde{\sigma}') = 0$, где $\tilde{\sigma}'$ — любой двоичный набор длины $k+1$, отличный от наборов $(\tilde{0}^{k+1})$ и $(\tilde{1}^{k+1})$.

Любой функциональный элемент, реализующий функцию вида $\varphi(\tilde{x}^{2k+2})$ (вида $\psi(\tilde{x}^{k+1})$, $\overline{x}$, 0), будем называть *φ-элементом* (соответственно, *ψ-элементом*, *инвертором*, *элементом «константа* 0*»*).

Назовём булеву функцию $f(\tilde{x}^n)$, где $n \geqslant 1$, *тождественной*, если $f \equiv x_i$ для некоторого $i \in \{1, \ldots, n\}$.

Лемма 1. Любую тождественную булеву функцию $f(\tilde{x}^n)$ можно реализовать k-неизбыточной схемой в базисе $B_5(k)$, допускающей k-проверяющий тест длины 0 относительно неисправностей на входах и выходах элементов.

Доказательство. Функцию f, очевидно, можно реализовать схемой, не содержащей функциональных элементов. У такой схемы нет ни одной функции неисправности, поэтому пустое множество является для неё k-проверяющим тестом. ■

Лемма 2. В случае $f \equiv 0$ справедливы равенства $D^{B_5(k)}_{k\text{-П (I)}}(f) = 0$, $D^{B_5(k)}_{k\text{-П (IO)}}(f) = 1$.

Доказательство. Функцию f можно реализовать схемой S, состоящей из одного элемента «константа 0» (обозначим этот элемент через E). Он не имеет входов, поэтому пустое множество является для данной схемы k-проверяющим тестом относительно неисправностей на входах элементов, откуда следует равенство $D^{B_5(k)}_{k\text{-П (I)}}(f) = 0$. При рассмотрении неисправностей на входах и выходах элементов единственной возможной неисправностью схемы S является неисправность типа 1 на выходе элемента E, при которой схема станет реализовывать константу 1. Указанная неисправность обнаруживается на любом двоичном наборе длины n, поэтому $D^{B_5(k)}_{k\text{-П (IO)}}(f) \leqslant 1$. С другой стороны, выход любой схемы в базисе $B_5(k)$, реализующей константу 0, очевидно, не может совпадать ни с одним из её входов, поэтому он является выходом некоторого функционального элемента. Тогда при неисправности типа 1 выхода этого элемента получающаяся схема станет реализовывать константу 1, которую надо отличить от функции f хотя бы на одном наборе, откуда следует, что $D^{B_5(k)}_{k\text{-П (IO)}}(f) \geqslant 1$. ■

Лемма 3. Для любой k-неизбыточной схемы в базисе $B_5(k)$, реализующей не тождественную и отличную от константы 0 булеву функцию $f(\tilde{x}^n)$, любой k-проверяющий тест относительно неисправностей на входах элементов содержит хотя бы два набора.

Доказательство. Выход любой k-неизбыточной схемы S, реализующей функцию f, не может совпадать ни с одним из её входов, поэтому он является выходом некоторого функционального элемента E, отличного от элемента «константа 0» и, как следствие, имеющего хотя бы один вход. Тогда при неисправности типа α, $\alpha \in \{0, 1\}$, любого фиксированного входа этого элемента получающаяся схема будет реализовывать нетривиальную функцию неисправности, которая может отличаться от функции $f(\tilde{x}^n)$ только на тех наборах, на которых в случае отсутствия неисправностей в схеме S на указанном входе элемента E возникает значение $\overline{\alpha}$. Данные два множества наборов при $\alpha = 0$ и $\alpha = 1$ не пересекаются, а в любой k-проверяющий тест для схемы S относительно неисправностей на входах элементов должно входить хотя бы по одному набору из каждого из этих множеств. ■

Назовём булеву функцию $f(\tilde{x}^n)$ *палиндромной*, если на любой паре противоположных наборов длины n она принимает одинаковые значения.

Будем говорить, что функциональный элемент E' расположен в схеме S *ниже* функционального элемента E, если в этой схеме существует ориентированный путь от E к E'.

Введём обозначение $\alpha^\beta = \alpha \oplus \beta \oplus 1$, где $\alpha, \beta \in \{0, 1\}$. Очевидно, что $\alpha^1 = \alpha$, $\alpha^0 = \overline{\alpha}$, $1^\beta = \beta$ и $0^\beta = \overline{\beta}$.

Лемма 4. Любую не палиндромную булеву функцию $f(\tilde{x}^n)$ можно реализовать k-неизбыточной схемой в базисе $B_5(k)$, состоящей только из φ-элементов и инверторов и допускающей k-проверяющий тест $\{\tilde{\sigma}_0, \tilde{\sigma}_1\}$ относительно неисправностей на входах и выходах элементов, где $\tilde{\sigma}_0$ и $\tilde{\sigma}_1$ — произвольные два противоположных двоичных набора длины n, такие, что $f(\tilde{\sigma}_0) = 0$ и $f(\tilde{\sigma}_1) = 1$.

Замечание 1. Существование таких наборов $\tilde{\sigma}_0$ и $\tilde{\sigma}_1$ следует из того, что функция f не является палиндромной.

Доказательство леммы 4. Пусть $A = [\{\varphi(\tilde{x}^{2k+2})\}]$ — замыкание множества $\{\varphi(\tilde{x}^{2k+2})\}$, тогда $A \subseteq T_{01}$ в силу условия (i) (определения замыкания и замкнутого класса T_{01} можно найти, например, в [13] на с. 14 и 34 соответственно). Докажем, что $A = T_{01}$. Как было отмечено выше, функция φ принимает одинаковые значения на каких-то двух противоположных наборах длины $2k+2$, содержащих $k+1$ нулевую и $k+1$ единичную компоненты. Без ограничения общности это наборы $(\tilde{0}^{k+1}, \tilde{1}^{k+1})$ и $(\tilde{1}^{k+1}, \tilde{0}^{k+1})$. Если $\varphi(\tilde{0}^{k+1}, \tilde{1}^{k+1}) = \varphi(\tilde{1}^{k+1}, \tilde{0}^{k+1}) = 0$, то из определения функции φ нетрудно получить, что $\varphi(\underbrace{x, \ldots, x}_{k+1}, \underbrace{y, \ldots, y}_{k+1}) = xy$, $\varphi(\underbrace{x, \ldots, x}_{k}, \underbrace{y, \ldots, y}_{k}, xy, xy) = x \vee y$ и

$$\varphi(\underbrace{x, \ldots, x}_{k}, \underbrace{x \vee y, \ldots, x \vee y}_{k}, x \vee yz, x \vee yz) = x \vee y\overline{z}; \tag{1}$$

если же $\varphi(\tilde{0}^{k+1}, \tilde{1}^{k+1}) = \varphi(\tilde{1}^{k+1}, \tilde{0}^{k+1}) = 1$, то из определения функции φ получим, что $\varphi(\underbrace{x, \ldots, x}_{k+1}, \underbrace{y, \ldots, y}_{k+1}) = x \vee y$, $\varphi(\underbrace{x, \ldots, x}_{k}, \underbrace{y, \ldots, y}_{k}, x \vee y, x \vee y) = xy$ и выполнено соотношение (1). Таким образом, $\{x \vee y\overline{z}, xy\} \subseteq A$, следовательно, $T_{01} = [\{x \vee y\overline{z}, xy\}] \subseteq A$ (равенство $T_{01} = [\{x \vee y\overline{z}, xy\}]$ установлено, например, в [13, с. 41]). Отсюда и из соотношения $A \subseteq T_{01}$ получаем, что $A = T_{01}$, т. е. любую булеву функцию $h(\tilde{x}^n)$ из класса T_{01} можно выразить формулой ϕ_h над множеством $\{\varphi(\tilde{x}^{2k+2})\}$. Тогда существует схема S_h в базисе $B_5(k)$, моделирующая формулу ϕ_h и состоящая только из входных переменных $x_1, \ldots, x_n$ и φ-элементов, выход каждого из которых, кроме выходного, соединён ровно с одним входом ровно одного элемента.

На наборе $(\tilde{\alpha}^n)$ на всех $2k+2$ входах и на выходе каждого элемента схемы S_h в силу условия (i) возникнет значение α, где $\alpha = 0, 1$. Предположим, что среди всех входов и выходов элементов схемы S_h есть не менее одного и не более k неисправных. Из всех элементов схемы, у которых хотя бы один вход и/или выход неисправны, выберем произвольный «нижний» элемент E, ниже которого в схеме S_h не существует элемента с указанным свойством (это можно сделать, так как схема S конечна и не содержит ориентированных циклов). Пусть значение на выходе элемента E, если он неисправен, либо значение на произвольном неисправном входе элемента E, если выход этого элемента исправен, равно $\overline{\delta}$, $\delta \in \{0, 1\}$.

Докажем, что значение на выходе этого элемента на наборе $(\tilde{\delta}^n)$ в схеме S_h равно $\overline{\delta}$. Если неисправен выход элемента E, то утверждение очевидно. Если этот выход исправен, то хотя бы один из входов элемента E неисправен и значение на нём равно $\overline{\delta}$. Тогда на наборе $(\tilde{\delta}^n)$ значения не менее чем на одном и не более чем на k входах этого элемента в схеме S_h отличны от «правильных», т. е. от δ, поскольку всего в этой схеме неисправны не более k входов/выходов элементов, а выходы элементов в ней не ветвятся. Тогда в силу условия (ii) значение на выходе элемента E на наборе $(\tilde{\delta}^n)$ в схеме S равно $\overline{\delta}$, что и требовалось доказать.

Далее изменение значения на выходе элемента E на наборе $(\tilde{\delta}^n)$ в схеме S_h с «правильного» значения δ на $\overline{\delta}$ пройдёт по цепочке до выхода схемы S_h (здесь снова используются тот факт, что всего в этой схеме неисправны не более k входов/выходов элементов, а выходы элементов в ней не ветвятся, и условие (ii)). Таким образом, неисправность схемы S_h будет обнаружена на наборе $(\tilde{\delta}^n)$. Отсюда следует, что данная схема k-неизбыточна и множество $\{(\tilde{0}^n, \tilde{1}^n)\}$ является для неё k-проверяющим тестом.

Пусть $\tilde{\sigma}_1 = (\sigma_1, \ldots, \sigma_n)$ и $f'(\tilde{x}^n) = f(x_1^{\sigma_1}, \ldots, x_n^{\sigma_n})$. Тогда $\tilde{\sigma}_0 = (\overline{\sigma}_1, \ldots, \overline{\sigma}_n)$,

$$f'(\tilde{0}^n) = f(0^{\sigma_1}, \ldots, 0^{\sigma_n}) = f(\overline{\sigma}_1, \ldots, \overline{\sigma}_n) = f(\tilde{\sigma}_0) = 0,$$
$$f'(\tilde{1}^n) = f(1^{\sigma_1}, \ldots, 1^{\sigma_n}) = f(\sigma_1, \ldots, \sigma_n) = f(\tilde{\sigma}_1) = 1,$$

поэтому $f'(\tilde{x}^n) \in T_{01}$. Значит, существует k-неизбыточная схема $S_{f'}$ в базисе $B_5(k)$, реализующая функцию f' и допускающая k-проверяющий тест из наборов $(\tilde{0}^n)$ и $(\tilde{1}^n)$. Для каждого $i \in \{1, \ldots, n\}$ в случае $\sigma_i = 1$ подадим на вход данной схемы, отвечающий переменной x_i, саму эту переменную, а в случае $\sigma_i = 0$ соединим каждый вход каждого элемента схемы $S_{f'}$, на который подавалась переменная x_i, с выходом (своего) инвертора, на вход которого подадим переменную x_i. Полученную схему (с тем же выходным элементом, что и у схемы $S_{f'}$) обозначим через S; легко видеть, что на её выходе реализуется функция $f'(x_1^{\sigma_1}, \ldots, x_n^{\sigma_n}) = f(\tilde{x}^n)$.

Заметим, что неисправность на входе и/или выходе каждого «добавленного» инвертора схемы S равносильна некоторой неисправности на входе элемента, соединённого с выходом этого инвертора. Поэтому можно считать, что неисправными в схеме S могут быть только входы/выходы элементов из её подсхемы $S_{f'}$. На наборе $\tilde{\sigma}_1$ на все входы подсхемы $S_{f'}$ по построению поступят единицы, а на наборе $\tilde{\sigma}_0$ — нули. Множество $\{(\tilde{0}^n), (\tilde{1}^n)\}$ позволяет обнаружить любую неисправность не более k входов/выходов элементов в этой подсхеме. Отсюда следует, что схема S является k-неизбыточной и допускает k-проверяющий тест из наборов $\tilde{\sigma}_0$ и $\tilde{\sigma}_1$. ■

Лемма 5. Любую палиндромную булеву функцию $f(\tilde{x}^n)$, отличную от константы 0, можно реализовать схемой в базисе $B_5(k)$, k-неизбыточной и допускающей k-проверяющий тест длины 2 относительно неисправностей на входах и выходах элементов, кроме неисправности типа 1 на выходе выходного элемента схемы.

Доказательство. Существуют такие два противоположных набора длины n, на каждом из которых функция f принимает значение 1, поскольку $f \not\equiv 0$. Обозначим тот из них, первая компонента которого равна единице, через $\tilde{\sigma}_1$, а другой — через $\tilde{\sigma}_0$. Пусть $\tilde{\sigma}_1 = (\sigma_1, \ldots, \sigma_n)$ и $\hat{f}(\tilde{x}^n) = f(\tilde{x}^n) \oplus x_1 \oplus 1$. Тогда $\sigma_1 = 1$, $\tilde{\sigma}_0 = (\overline{\sigma}_1, \ldots, \overline{\sigma}_n)$,

$$\hat{f}(\tilde{\sigma}_0) = f(\tilde{\sigma}_0) \oplus \overline{\sigma}_1 \oplus 1 = 1 \oplus 0 \oplus 1 = 0,$$
$$\hat{f}(\tilde{\sigma}_1) = f(\tilde{\sigma}_1) \oplus \sigma_1 \oplus 1 = 1 \oplus 1 \oplus 1 = 1,$$

поэтому $\hat{f}(\tilde{x}^n)$ — не палиндромная функция. Тогда в силу леммы 4 существует k-неизбыточная схема S' в базисе $B_5(k)$, реализующая функцию $\hat{f}$ и допускающая k-проверяющий тест из наборов $\tilde{\sigma}_0$ и $\tilde{\sigma}_1$ относительно неисправностей на входах и выходах элементов. Соединим выход данной схемы со входом ψ-элемента E, отвечающим переменной x_1, а на все остальные входы этого элемента подадим переменную x_1. Выход элемента E объявим выходом полученной схемы, которую обозначим через S. В силу свойства (iii) она реализует функцию

$$\psi(\hat{f}(\tilde{x}^n), \underbrace{x_1, \ldots, x_1}_{k}) = \hat{f}(\tilde{x}^n) \oplus x_1 \oplus 1 = f(\tilde{x}^n) \oplus x_1 \oplus 1 \oplus x_1 \oplus 1 = f(\tilde{x}^n).$$

При отсутствии неисправностей в схеме S в силу равенств $\hat{f}(\tilde{\sigma}_1) = 1$, $\sigma_1 = 1$ и $\hat{f}(\tilde{\sigma}_0) = 0$ на все входы элемента E на наборе $\tilde{\sigma}_1$ поступят единицы, а на наборе $\tilde{\sigma}_0$ — нули. Если выход элемента E исправен, а хотя бы один из его входов или из входов/выходов элементов подсхемы S' неисправен, то хотя бы на одном из этих наборов не менее чем на одном и не более чем на k входах элемента E возникнут «неправильные» значения, а тогда в силу свойства (iv) значение на выходе элемента E, т. е. на выходе схемы S, изменится, поэтому неисправность будет обнаружена на одном из наборов $\tilde{\sigma}_0, \tilde{\sigma}_1$. Наконец, неисправность типа 0 на выходе элемента E обнаруживается на любом из этих двух наборов, так как $f(\tilde{\sigma}_0) = f(\tilde{\sigma}_1) = 1$. Поэтому схема S является k-неизбыточной относительно неисправностей на входах и выходах элементов, кроме неисправности типа 1 на выходе её выходного элемента, и допускает k-проверяющий тест из наборов $\tilde{\sigma}_0$ и $\tilde{\sigma}_1$ относительно неисправностей указанного вида. ■

Теорема 1. Для любой булевой функции $f(\tilde{x}^n)$ справедливо равенство

$$D^{B_5(k)}_{k\text{-П (I)}}(f) = \begin{cases} 0, & \text{если } f \text{ — тождественная функция или } f \equiv 0, \\ 2 & \text{в остальных случаях.} \end{cases}$$

Доказательство. Вместо $D^{B_5(k)}_{k\text{-П (I)}}(f)$ для краткости будем писать $D(f)$. Равенство $D(f) = 0$ в случаях, когда f — тождественная функция и $f \equiv 0$, следует из лемм 1 и 2 соответственно. Если функция f не тождественная и отлична от константы 0, то неравенство $D(f) \geqslant 2$ вытекает из леммы 3, а неравенство $D(f) \leqslant 2$ — из лемм 4 и 5. ■

Следствие 1. Для любого $n \geqslant 0$ справедливо равенство $D^{B_5(k)}_{k\text{-П (I)}}(n) = 2$.

Лемма 6. Не существует схем в базисе $B_5(k)$, реализующих константу 1 и k-неизбыточных относительно неисправностей на входах и выходах элементов.

Доказательство. Выход любой схемы в базисе $B_5(k)$, реализующей константу 1, очевидно, не может совпадать ни с одним из её входов, поэтому он является выходом некоторого функционального элемента. Тогда при неисправности типа 1 на выходе этого элемента получающаяся схема по-прежнему будет реализовывать константу 1, т. е. исходная схема k-избыточна. ■

Очевидно, что никакая тождественная функция не является палиндромной, а константа 0 является палиндромной функцией.

Теорема 2. Для любой булевой функции $f(\tilde{x}^n)$, отличной от константы 1, справедливо равенство

$$D^{B_5(k)}_{k\text{-П (IO)}}(f) = \begin{cases} 0, & \text{если } f \text{ — тождественная функция,} \\ 1, & \text{если } f \equiv 0, \\ 2, & \text{если } f \text{ — не тождественная и не палиндромная функция,} \\ 3, & \text{если } f \text{ — палиндромная функция и } f \not\equiv 0. \end{cases}$$

Если $f \equiv 1$, то значение $D^{B_5(k)}_{k\text{-П (IO)}}(f)$ не определено.

Доказательство. Вместо $D^{B_5(k)}_{k\text{-П (IO)}}(f)$ для краткости будем писать $D(f)$. В случае $f \equiv 1$ значение $D(f)$ не определено в силу леммы 6. Равенства $D(f) = 0$, если функция f тождественная, и $D(f) = 1$, если $f \equiv 0$, следуют из лемм 1 и 2 соответственно. В случае, когда функция f не тождественная и не палиндромная, неравенство $D(f) \geqslant 2$ следует из леммы 3, а $D(f) \leqslant 2$ — из леммы 4.

Пусть f — палиндромная функция и $f \not\equiv 0, 1$. В силу леммы 5 функцию f можно реализовать схемой S в базисе $B_5(k)$, k-неизбыточной и допускающей k-проверяющий тест длины 2 относительно неисправностей на входах и выходах элементов, кроме неисправности типа 1 на выходе выходного элемента схемы. Добавим в этот тест любой двоичный набор длины n, на котором функция f принимает значение 0. На нём обнаруживается неисправность типа 1 на выходе выходного элемента схемы S (возможно, при наличии в ней других неисправных входов/выходов элементов). Поэтому данная схема k-неизбыточна относительно неисправностей на входах и выходах элементов и допускает k-проверяющий тест длины не более 3 относительно неисправностей указанного вида. Отсюда следует, что $D(f) \leqslant 3$.

Докажем неравенство $D(f) \geqslant 3$. Предположим, что это не так, т. е. $D(f) \leqslant 2$. В силу леммы 3 имеем $D(f) \geqslant 2$, поэтому $D(f) = 2$. Значит, существует k-неизбыточная схема S' в базисе $B_5(k)$, реализующая функцию f и допускающая k-проверяющий тест из каких-то двух наборов $\tilde{\pi}_1$ и $\tilde{\pi}_2$. Пусть $x_{i_1}, \ldots, x_{i_s}$ — все существенные переменные функции f. Предположим, что i_j-е (слева) компоненты наборов $\tilde{\pi}_1$ и $\tilde{\pi}_2$ совпадают для некоторого $j \in \{1, \ldots, s\}$ и равны α. Переменная x_{i_j} обязана подаваться хотя бы на один вход хотя бы одного элемента схемы S', поскольку $x_{i_j} \in \{x_{i_1}, \ldots, x_{i_s}\}$. Тогда неисправность типа α этого входа нельзя обнаружить ни на одном из наборов $\tilde{\pi}_1, \tilde{\pi}_2$; противоречие. Следовательно, наборы $\tilde{\pi}_1$ и $\tilde{\pi}_2$ различаются в каждой из i_1-й, …, i_s-й компонент.

Далее, пусть $\tilde{\pi}_1'$ — набор, противоположный набору $\tilde{\pi}_1$. Тогда $f(\tilde{\pi}_1) = f(\tilde{\pi}_1')$ в силу палиндромности функции f. Наборы $\tilde{\pi}_1'$ и $\tilde{\pi}_2$ совпадают в i_1-й, …, i_s-й компонентах, а функция $f(\tilde{x}^n)$ существенно зависит только от переменных $x_{i_1}, \ldots, x_{i_s}$, поэтому $f(\tilde{\pi}_1') = f(\tilde{\pi}_2)$. Таким образом, $f(\tilde{\pi}_1) = f(\tilde{\pi}_2)$. Отсюда следует, что неисправность типа $f(\tilde{\pi}_1)$ на выходе выходного элемента схемы S' нельзя обнаружить ни на одном из наборов $\tilde{\pi}_1, \tilde{\pi}_2$, т. е. множество $\{\tilde{\pi}_1, \tilde{\pi}_2\}$ не является k-проверяющим тестом для этой схемы. Полученное противоречие означает, что $D(f) \geqslant 3$. ∎

Следствие 2. Для любого $n \geqslant 2$ справедливо равенство $D^{B_5(k)}_{k\text{-П (IO)}}(n) = 3$.

Замечание 2. Среди всех схем, построенных при доказательстве верхних оценок величин $D^{B_5(k)}_{k\text{-П (I)}}(f)$ и $D^{B_5(k)}_{k\text{-П (IO)}}(f)$ в теоремах 1 и 2 соответственно, элемент «константа 0» использовался только в построении схем, реализующих тождественный нуль, а ψ-элемент — только в построении схем, реализующих отличные от нуля палиндромные функции (причём в единственном числе).

2. Диагностические тесты

Пусть $\xi(\tilde{x}^{3k+2})$, $\eta(\tilde{x}^{4k+2})$ — булевы функции, удовлетворяющие следующим условиям при $\alpha = 0, 1$:

(v) $\xi(\tilde{\alpha}^{3k+2}) = \alpha$;

(vi) на всех наборах, k-соседних с набором $(\tilde{\alpha}^{3k+2})$, кроме него самого, функция ξ принимает значение $\overline{\alpha}$;

(vii) на всех наборах, k-соседних с набором $\tilde{\rho}_\alpha = \left(\tilde{\alpha}^{k+1}, \tilde{\overline{\alpha}}^{2k+1}\right)$, функция ξ принимает значение α;

(viii) $\eta(\tilde{\alpha}^{4k+2}) = 1$;

(ix) на всех наборах, k-соседних с набором $(\tilde{\alpha}^{4k+2})$, кроме него самого, функция η принимает значение 0;

(x) на всех наборах, k-соседних с набором $\tilde{\nu}_\alpha = \left(\tilde{\alpha}^{2k+1}, \tilde{\overline{\alpha}}^{2k+1}\right)$, функция η принимает значение α.

На всех остальных двоичных наборах длины $3k+2$ (длины $4k+2$) функция ξ (соответственно η) может принимать произвольные значения.

Покажем, что каждая из функций $\xi(\tilde{x}^{3k+2})$, $\eta(\tilde{x}^{4k+2})$ определена корректно, т. е. множества наборов, на которых она принимает значения 0 и 1, не пересекаются. Заметим, что для любого $\alpha \in \{0,1\}$ набор $(\tilde{\alpha}^{3k+2})$ отличается от каждого из наборов $\left(\tilde{\overline{\alpha}}^{3k+2}\right)$, $\tilde{\rho}_\alpha$ по крайней мере в $(2k+1)$ компонентах, поэтому любой набор, k-соседний с набором $(\tilde{\alpha}^{3k+2})$, отличается от каждого из наборов $\left(\tilde{\overline{\alpha}}^{3k+2}\right)$, $\tilde{\rho}_\alpha$ по крайней мере в $(k+1)$ компонентах, т. е. не может быть k-соседним ни с одним из этих наборов. Набор $(\tilde{\alpha}^{3k+2})$ отличается от набора $\tilde{\rho}_{\overline{\alpha}}$ в $(k+1)$ компонентах, поэтому не является k-соседним с этим набором. Кроме того, наборы $\tilde{\rho}_0$ и $\tilde{\rho}_1$ различаются в $(3k+2)$ компонентах, поэтому никакой набор, k-соседний с набором $\tilde{\rho}_0$, не может быть k-соседним с набором $\tilde{\rho}_1$. Из приведённых рассуждений и условий (v)–(vii) следует, что множества наборов, на которых функция $\xi(\tilde{x}^{3k+2})$ принимает значения 0 и 1, не пересекаются, значит, она определена корректно.

Далее, для любого $\alpha \in \{0,1\}$ набор $(\tilde{\alpha}^{4k+2})$ отличается от набора $\tilde{\nu}_1$ в $(2k+1)$ компонентах, поэтому никакой набор, k-соседний с набором $(\tilde{\alpha}^{4k+2})$, не может быть k-соседним с набором $\tilde{\nu}_1$. Наборы $\tilde{\nu}_0$ и $\tilde{\nu}_1$ различаются в $(4k+2)$ компонентах, поэтому никакой набор, k-соседний с набором $\tilde{\nu}_0$, не может быть k-соседним с набором $\tilde{\nu}_1$. Кроме того, любые два из наборов $(\tilde{0}^{4k+2})$, $(\tilde{1}^{4k+2})$ и $\tilde{\nu}_0$ различаются по крайней мере в $(2k+1)$ компонентах, поэтому не являются k-соседними. Из приведённых рассуждений и условий (viii)–(x) следует, что множества наборов, на которых функция $\eta(\tilde{x}^{4k+2})$ принимает значения 0 и 1, не пересекаются, значит, она определена корректно.

Рассмотрим базис $B_6(k) = \{\varphi(\tilde{x}^{2k+2}), \xi(\tilde{x}^{3k+2}), \eta(\tilde{x}^{4k+2}), \overline{x}, 0\}$, где $\varphi(\tilde{x}^{2k+2})$ — булева функция из базиса $B_5(k)$. Любой функциональный элемент, реализующий функцию вида $\xi(\tilde{x}^{3k+2})$ ($\eta(\tilde{x}^{4k+2})$), будем называть *ξ-элементом* (соответственно *η-элементом*).

По аналогии с леммами соответственно 1, 2, 3 и 6 доказываются следующие утверждения.

Лемма 7. Любую тождественную булеву функцию $f(\tilde{x}^n)$ можно реализовать k-неизбыточной схемой в базисе $B_6(k)$, допускающей k-диагностический тест длины 0 относительно неисправностей на входах и выходах элементов.

Лемма 8. В случае $f \equiv 0$ справедливы равенства $D^{B_6(k)}_{k\text{-Д (I)}}(f) = 0$, $D^{B_6(k)}_{k\text{-Д (IO)}}(f) = 1$.

Лемма 9. Для любой k-неизбыточной схемы в базисе $B_6(k)$, реализующей не тождественную и отличную от константы 0 булеву функцию $f(\tilde{x}^n)$, любой k-диагностический тест относительно неисправностей на входах элементов содержит хотя бы два набора.

Лемма 10. Не существует схем в базисе $B_6(k)$, реализующих константу 1 и k-неизбыточных относительно неисправностей на входах и выходах элементов.

Через $I_{\tilde{\sigma}}(\tilde{x}^n)$ будем обозначать булеву функцию, принимающую значение 1 на наборе $\tilde{\sigma}$ и 0 на всех остальных наборах длины n.

Лемма 11. Любую не палиндромную булеву функцию $f(\tilde{x}^n)$, принимающую значения 0 и 1 на каких-то противоположных наборах $\tilde{\sigma}_0$ и $\tilde{\sigma}_1$ соответственно, можно реализовать схемой в базисе $B_6(k)$, k-неизбыточной и допускающей k-диагностический тест $\{\tilde{\sigma}_0, \tilde{\sigma}_1\}$ относительно неисправностей на входах и выходах элементов, при которых выход выходного элемента схемы исправен, причём все её функции неисправности принадлежат множеству $\{f \oplus I_{\tilde{\sigma}_0}, f \oplus I_{\tilde{\sigma}_1}, f \oplus I_{\tilde{\sigma}_0} \oplus I_{\tilde{\sigma}_1}\}$.

Доказательство. Пусть $f' = f \oplus I_{\tilde\sigma_0} \oplus I_{\tilde\sigma_1} \oplus 1$. Тогда справедливы соотношения

$$f'(\tilde\sigma_0) = f(\tilde\sigma_0) \oplus I_{\tilde\sigma_0}(\tilde\sigma_0) \oplus I_{\tilde\sigma_1}(\tilde\sigma_0) \oplus 1 = 0 \oplus 1 \oplus 0 \oplus 1 = 0, \tag{2}$$

$$f'(\tilde\sigma_1) = f(\tilde\sigma_1) \oplus I_{\tilde\sigma_0}(\tilde\sigma_1) \oplus I_{\tilde\sigma_1}(\tilde\sigma_1) \oplus 1 = 1 \oplus 0 \oplus 1 \oplus 1 = 1, \tag{3}$$

из которых следует, что функция $f'(\tilde x^n)$ не является палиндромной.

Построим схему S в базисе $B_6(k)$, реализующую функцию $f(\tilde x^n)$ (рис. 1). Схема S состоит из $(3k+2)$ подсхем $S_1, \ldots, S_{3k+2}$ и выходного ξ-элемента E, входы которого соединяются с выходами этих подсхем (1-й вход — с выходом подсхемы S_1, ..., $(3k+2)$-й вход — с выходом подсхемы S_{3k+2}). Каждая из подсхем $S_1, \ldots, S_{k+1}$ реализует функцию $f(\tilde x^n)$, а каждая из подсхем $S_{k+2}, \ldots, S_{3k+2}$ — функцию $f'(\tilde x^n)$, причём каждая из подсхем $S_1, \ldots, S_{3k+2}$ является k-неизбыточной схемой, состоящей только из φ-элементов и инверторов и допускающей k-проверяющий тест $\{\tilde\sigma_0, \tilde\sigma_1\}$ относительно неисправностей на входах и выходах элементов; существование таких схем следует из леммы 4. При этом используется тот факт, что функции f и f' не являются палиндромными, а также соотношения $f(\tilde\sigma_0) = 0$, $f(\tilde\sigma_1) = 1$, (2) и (3).

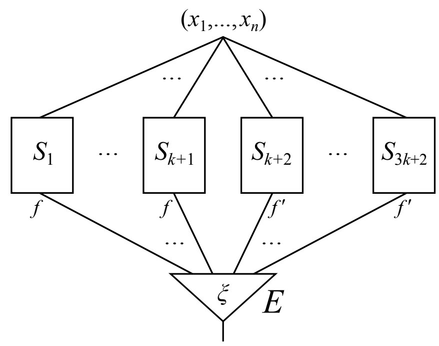

Рис. 1. Схема S

Докажем, что построенная схема S в случае отсутствия в ней неисправностей реализует функцию $f(\tilde x^n)$. Всюду ниже в доказательстве леммы 11 предполагаем, что α — произвольное число из множества $\{0,1\}$. На любом двоичном наборе $\tilde\tau_\alpha$ ($\tilde\tau_\alpha \neq \tilde\sigma_\alpha$), на котором функция f принимает значение α, на выходе каждой из подсхем $S_1, \ldots, S_{k+1}$ возникнет значение α, а на выходе каждой из подсхем $S_{k+2}, \ldots, S_{3k+2}$ — значение $f'(\tilde\tau_\alpha) = f(\tilde\tau_\alpha) \oplus I_{\tilde\sigma_0}(\tilde\tau_\alpha) \oplus I_{\tilde\sigma_1}(\tilde\tau_\alpha) \oplus 1 = \alpha \oplus 0 \oplus 0 \oplus 1 = \overline{\alpha}$, поскольку $\tilde\tau_\alpha \notin \{\tilde\sigma_0, \tilde\sigma_1\}$ (действительно, $\tilde\tau_\alpha \neq \tilde\sigma_\alpha$ по определению и $\tilde\tau_\alpha \neq \tilde\sigma_{\overline{\alpha}}$ в силу того, что $f(\tilde\tau_\alpha) = \alpha \neq f(\tilde\sigma_{\overline{\alpha}})$). Тогда на входы элемента E будет подан в точности набор $\tilde\rho_\alpha$, а на его выходе, т. е. на выходе схемы S, возникнет значение $\xi(\tilde\rho_\alpha) = \alpha = f(\tilde\tau_\alpha)$ в силу условия (vii). Далее, на наборе $\tilde\sigma_\alpha$ на выходе каждой из подсхем $S_1, \ldots, S_{k+1}$ возникнет значение $f(\tilde\sigma_\alpha) = \alpha$, а на выходе каждой из подсхем $S_{k+2}, \ldots, S_{3k+2}$ — значение

$$f'(\tilde\sigma_\alpha) = f(\tilde\sigma_\alpha) \oplus I_{\tilde\sigma_\alpha}(\tilde\sigma_\alpha) \oplus I_{\tilde\sigma_{\overline{\alpha}}}(\tilde\sigma_\alpha) \oplus 1 = \alpha \oplus 1 \oplus 0 \oplus 1 = \alpha.$$

Тогда на входы элемента E будет подан в точности набор $(\tilde\alpha^{3k+2})$, а на его выходе, т. е. на выходе схемы S, возникнет значение $\xi(\tilde\alpha^{3k+2}) = \alpha = f(\tilde\sigma_\alpha)$ в силу условия (v). Таким образом, на выходе схемы S реализуется функция $f(\tilde x^n)$.

Найдём все возможные функции неисправности схемы S относительно неисправностей на входах и выходах элементов, при которых выход выходного элемента E схемы исправен. Неисправность на i-м входе элемента E равносильна неисправности такого же типа на выходе выходного элемента подсхемы S_i, где i — произвольный индекс от 1 до $3k+2$. Поэтому можно считать, что неисправными в схеме S могут быть только входы/выходы элементов из её подсхем $S_1, \ldots, S_{3k+2}$. При произвольной неисправности не менее одного и не более k входов/выходов таких элементов на любом входном наборе схемы S могут измениться значения не более чем на k входах элемента E. Поэтому на любом наборе $\tilde{\tau}_\alpha$ ($\tilde{\tau}_\alpha \neq \tilde{\sigma}_\alpha$), на котором функция f принимает значение α, на входы элемента E поступит набор, k-соседний с набором $\tilde{\rho}_\alpha$, а на его выходе, т. е. на выходе схемы S, возникнет значение $\alpha = f(\tilde{\tau}_\alpha)$ в силу условия (vii).

На наборах $\tilde{\sigma}_0$ и $\tilde{\sigma}_1$ на входы элемента E поступят наборы $\tilde{\pi}_0$ и $\tilde{\pi}_1$ длины $3k+2$, k-соседние с наборами $(\tilde{0}^{3k+2})$ и $(\tilde{1}^{3k+2})$ соответственно. При этом выполнено хотя бы одно из соотношений $\tilde{\pi}_0 \neq (\tilde{0}^{3k+2})$, $\tilde{\pi}_1 \neq (\tilde{1}^{3k+2})$, поскольку множество $\{\tilde{\sigma}_0, \tilde{\sigma}_1\}$ является k-проверяющим тестом для каждой из k-неизбыточных схем $S_1, \ldots, S_{3k+2}$ (значение на выходе любой из этих схем, содержащей хотя бы один неисправный элемент, изменится хотя бы на одном из наборов $\tilde{\sigma}_0$, $\tilde{\sigma}_1$). Следовательно, значение на выходе элемента E, т. е. на выходе схемы S, изменится хотя бы на одном из наборов $\tilde{\sigma}_0$, $\tilde{\sigma}_1$ в силу условий (v), (vi). Таким образом, на выходе схемы S возникнет функция неисправности, отличающаяся от функции f по крайней мере на одном из этих двух наборов и совпадающая с функцией f на всех наборах длины n, отличных от указанных двух.

Тем самым показано, что все возможные функции неисправности схемы S принадлежат множеству $\{f \oplus I_{\tilde{\sigma}_0}, f \oplus I_{\tilde{\sigma}_1}, f \oplus I_{\tilde{\sigma}_0} \oplus I_{\tilde{\sigma}_1}\}$. Каждую из них можно отличить от любой другой и от функции f хотя бы на одном из наборов $\tilde{\sigma}_0$, $\tilde{\sigma}_1$, поэтому схема S является k-неизбыточной и допускает k-диагностический тест $\{\tilde{\sigma}_0, \tilde{\sigma}_1\}$ относительно неисправностей на входах и выходах элементов, при которых выход её выходного элемента исправен. ■

Лемма 12. Любую булеву функцию $f(\tilde{x}^n)$, для которой существуют такие два противоположных двоичных набора $\tilde{\sigma}_0$ и $\tilde{\sigma}_1$ длины n, что $f(\tilde{\sigma}_0) = f(\tilde{\sigma}_1) = 1$, можно реализовать схемой в базисе $B_6(k)$, k-неизбыточной и допускающей k-диагностический тест $\{\tilde{\sigma}_0, \tilde{\sigma}_1\}$ относительно неисправностей на входах и выходах элементов, при которых выход выходного элемента схемы исправен, причём все её функции неисправности принадлежат множеству $\{f \oplus I_{\tilde{\sigma}_0}, f \oplus I_{\tilde{\sigma}_1}, f \oplus I_{\tilde{\sigma}_0} \oplus I_{\tilde{\sigma}_1}\}$, а в случае $k = 1$ — множеству $\{f \oplus I_{\tilde{\sigma}_0}, f \oplus I_{\tilde{\sigma}_1}\}$.

Доказательство. Пусть $f' = f \oplus I_{\tilde{\sigma}_0}$, $f'' = f \oplus I_{\tilde{\sigma}_1} \oplus 1$. Тогда справедливы соотношения

$$f'(\tilde{\sigma}_0) = f(\tilde{\sigma}_0) \oplus I_{\tilde{\sigma}_0}(\tilde{\sigma}_0) = 1 \oplus 1 = 0, \tag{4}$$

$$f'(\tilde{\sigma}_1) = f(\tilde{\sigma}_1) \oplus I_{\tilde{\sigma}_0}(\tilde{\sigma}_1) = 1 \oplus 0 = 1, \tag{5}$$

$$f''(\tilde{\sigma}_0) = f(\tilde{\sigma}_0) \oplus I_{\tilde{\sigma}_1}(\tilde{\sigma}_0) \oplus 1 = 1 \oplus 0 \oplus 1 = 0, \tag{6}$$

$$f''(\tilde{\sigma}_1) = f(\tilde{\sigma}_1) \oplus I_{\tilde{\sigma}_1}(\tilde{\sigma}_1) \oplus 1 = 1 \oplus 1 \oplus 1 = 1, \tag{7}$$

из которых следует, что функции $f'(\tilde{x}^n)$ и $f''(\tilde{x}^n)$ не являются палиндромными.

Построим схему S в базисе $B_6(k)$, реализующую функцию $f(\tilde{x}^n)$ (рис. 2). Схема S состоит из $4k+2$ подсхем $S_1, \ldots, S_{4k+2}$ и выходного η-элемента E, входы которого соединяются с выходами этих подсхем (1-й вход — с выходом подсхемы S_1, ..., $(4k+2)$-й вход — с выходом подсхемы S_{4k+2}). Каждая из подсхем $S_1, \ldots, S_{2k+1}$ реализует функцию $f'(\tilde{x}^n)$, а каждая из подсхем $S_{2k+2}, \ldots, S_{4k+2}$ — функцию $f''(\tilde{x}^n)$, причём каждая из подсхем $S_1, \ldots, S_{4k+2}$ является k-неизбыточной схемой, состоящей только из φ-элементов и инверторов и допускающей k-проверяющий тест $\{\tilde{\sigma}_0, \tilde{\sigma}_1\}$ относительно неисправностей на входах и выходах элементов; существование таких схем следует из леммы 4, из того, что функции f' и f'' не являются палиндромными, и из соотношений (4)–(7).

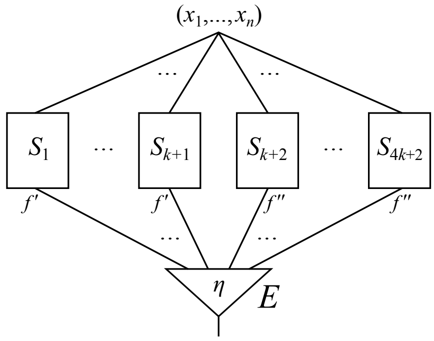

Рис. 2. Схема S

Докажем, что построенная схема S в случае отсутствия в ней неисправностей реализует функцию $f(\tilde{x}^n)$. Всюду ниже в доказательстве леммы предполагаем, что α — произвольное число из множества $\{0,1\}$. На любом двоичном наборе $\tilde{\tau}_\alpha$ длины n, на котором функция f принимает значение α, отличном от наборов $\tilde{\sigma}_0$ и $\tilde{\sigma}_1$, на выходе каждой из подсхем $S_1,\dots,S_{2k+1}$ возникнет значение

$$f'(\tilde{\tau}_\alpha) = f(\tilde{\tau}_\alpha) \oplus I_{\tilde{\sigma}_0}(\tilde{\tau}_\alpha) = \alpha \oplus 0 = \alpha,$$

а на выходе каждой из подсхем $S_{2k+2},\dots,S_{4k+2}$ — значение

$$f''(\tilde{\tau}_\alpha) = f(\tilde{\tau}_\alpha) \oplus I_{\tilde{\sigma}_1}(\tilde{\tau}_\alpha) \oplus 1 = \alpha \oplus 0 \oplus 1 = \overline{\alpha}.$$

Тогда на входы элемента E будет подан в точности набор $\tilde{\nu}_\alpha$, а на его выходе, т. е. на выходе схемы S, возникнет значение $\eta(\tilde{\nu}_\alpha) = \alpha = f(\tilde{\tau}_\alpha)$ в силу условия (x). Далее, на наборе $\tilde{\sigma}_\alpha$ на выходе каждой из подсхем $S_1,\dots,S_{4k+2}$ возникнет значение α в силу (4), (6) при $\alpha = 0$ и (5), (7) при $\alpha = 1$. Тогда на входы элемента E будет подан в точности набор $(\tilde{\alpha}^{4k+2})$, а на его выходе, т. е. на выходе схемы S, возникнет значение $\eta(\tilde{\alpha}^{4k+2}) = 1 = f(\tilde{\sigma}_\alpha)$ в силу условия (viii). Таким образом, на выходе схемы S реализуется в точности функция $f(\tilde{x}^n)$.

Найдём все возможные функции неисправности схемы S относительно неисправностей на входах и выходах элементов, при которых выход выходного элемента E схемы исправен. Неисправность на i-м входе элемента E равносильна неисправности такого же типа на выходе выходного элемента подсхемы S_i, где i — произвольный индекс от 1 до $4k+2$. Поэтому можно считать, что неисправными в схеме S могут быть только входы/выходы элементов из её подсхем $S_1,\dots,S_{4k+2}$. При произвольной неисправности не менее одного и не более k входов/выходов таких элементов на любом входном наборе схемы S могут измениться значения не более чем на k входах элемента E. Поэтому на любом наборе $\tilde{\tau}_\alpha$, на котором функция f принимает значение α, отличном от наборов $\tilde{\sigma}_0$ и $\tilde{\sigma}_1$, на входы элемента E поступит набор, k-соседний с набором $\tilde{\nu}_\alpha$, а на его выходе, т. е. на выходе схемы S, возникнет значение $\alpha = f(\tilde{\tau}_\alpha)$ в силу условия (x).

На наборах $\tilde{\sigma}_0$ и $\tilde{\sigma}_1$ на входы элемента E поступят наборы $\tilde{\pi}_0$ и $\tilde{\pi}_1$ длины $4k+2$, k-соседние с наборами $(\tilde{0}^{4k+2})$ и $(\tilde{1}^{4k+2})$ соответственно. При этом выполнено хотя бы одно из соотношений $\tilde{\pi}_0 \neq (\tilde{0}^{4k+2})$, $\tilde{\pi}_1 \neq (\tilde{1}^{4k+2})$, поскольку множество $\{\tilde{\sigma}_0, \tilde{\sigma}_1\}$ является k-проверяющим тестом для каждой из k-неизбыточных схем $S_1,\dots,S_{4k+2}$. Следовательно, значение на выходе элемента E, т. е. на выходе схемы S, изменится хотя бы на одном из наборов $\tilde\sigma_0$, $\tilde\sigma_1$ в силу условий (viii), (ix). Таким образом, на выходе схемы S возникнет функция неисправности, отличающаяся от функции f по крайней мере на одном из этих двух наборов и совпадающая с функцией f на всех наборах длины n, отличных от указанных двух.

Тем самым показано, что все возможные функции неисправности схемы S принадлежат множеству $\{f \oplus I_{\tilde\sigma_0}, f \oplus I_{\tilde\sigma_1}, f \oplus I_{\tilde\sigma_0} \oplus I_{\tilde\sigma_1}\}$. Каждую из них можно отличить от любой другой и от функции f хотя бы на одном из наборов $\tilde\sigma_0$, $\tilde\sigma_1$, поэтому схема S является k-неизбыточной и допускает k-диагностический тест $T = \{\tilde\sigma_0, \tilde\sigma_1\}$ относительно неисправностей на входах и выходах элементов, при которых выход её выходного элемента исправен.

Пусть $k = 1$. Если при отсутствии неисправностей в схеме S на некотором входе/выходе некоторого элемента этой схемы, кроме выхода элемента E, на двух наборах из множества T возникает одно и то же значение β, то неисправность типа β указанного входа/выхода нельзя обнаружить на наборах из данного множества, однако это противоречит последнему предложению предыдущего абзаца. Поэтому на любом входе/выходе любого элемента схемы S, за исключением выхода элемента E, на двух наборах из множества T возникают различные значения. Тогда неисправность типа γ, $\gamma \in \{0,1\}$, любого входа/выхода любого элемента этой схемы, кроме выхода элемента E, обнаруживается только на том наборе $\tilde\sigma'$ из множества T, на котором значение на указанном входе/выходе в отсутствие неисправностей равно $\overline{\gamma}$, и не обнаруживается на другом наборе $\tilde\sigma''$ из данного множества. Значит, при рассматриваемой неисправности на наборе $\tilde\sigma'$ схема S выдаст значение $\overline{f}(\tilde\sigma')$, а на наборе $\tilde\sigma''$ — «правильное» значение $f(\tilde\sigma'')$.

Приведённые рассуждения показывают, что любая функция неисправности схемы S отличается от функции $f(\tilde x^n)$ ровно на одном наборе из множества T и совпадает с ней на всех остальных наборах, т. е. принадлежит множеству $\{f \oplus I_{\tilde\sigma_0}, f \oplus I_{\tilde\sigma_1}\}$. ■

Теорема 3. Для любой булевой функции $f(\tilde x^n)$ справедливо равенство

$$D^{B_6(k)}_{k\text{-Д (I)}}(f) = \begin{cases} 0, & \text{если } f \text{ — тождественная функция или } f \equiv 0,\\ 2 & \text{в остальных случаях.} \end{cases}$$

Доказательство. Вместо $D^{B_6(k)}_{k\text{-Д (I)}}(f)$ для краткости будем писать $D(f)$. Равенство $D(f) = 0$ в случаях, когда f — тождественная функция и $f \equiv 0$, следует из лемм 7 и 8 соответственно. Если же функция f не тождественна и отлична от константы 0, то неравенство $D(f) \geqslant 2$ вытекает из леммы 9, а $D(f) \leqslant 2$ — из лемм 11 и 12. Стоит отметить, что если f — не палиндромная функция, то существуют такие два противоположных набора $\tilde\sigma_0$ и $\tilde\sigma_1$ длины n, для которых $f(\tilde\sigma_0) = 0$ и $f(\tilde\sigma_1) = 1$, а в случае, когда f — палиндромная функция и $f \not\equiv 0$, существуют такие два противоположных набора $\tilde\sigma_0$ и $\tilde\sigma_1$ длины n, что $f(\tilde\sigma_0) = f(\tilde\sigma_1) = 1$. ■

Следствие 3. Для любого $n \geqslant 0$ справедливо равенство $D^{B_6(k)}_{k\text{-Д (I)}}(n) = 2$.

Лемма 13. Любую не палиндромную булеву функцию $f(\tilde x^n)$ можно реализовать схемой в базисе $B_6(k)$, k-неизбыточной и допускающей k-диагностический тест длины не более 4 относительно неисправностей на входах и выходах элементов.

Доказательство. Существуют такие противоположные наборы $\tilde\sigma_0$ и $\tilde\sigma_1$ длины n, что $f(\tilde\sigma_0) = 0$ и $f(\tilde\sigma_1) = 1$. По лемме 11 функцию f можно реализовать схемой S

в базисе $B_6(k)$, k-неизбыточной и допускающей k-диагностический тест $\{\tilde{\sigma}_0, \tilde{\sigma}_1\}$ относительно неисправностей на входах и выходах элементов, при которых выход выходного элемента схемы исправен, причём все её функции неисправности принадлежат множеству $\{f \oplus I_{\tilde{\sigma}_0}, f \oplus I_{\tilde{\sigma}_1}, f \oplus I_{\tilde{\sigma}_0} \oplus I_{\tilde{\sigma}_1}\}$. Если указанный выход неисправен и выдаёт 0 (выдаёт 1), то на выходе схемы S возникнет функция неисправности, тождественно равная нулю (соответственно единице) и тем самым отличная от функции f, поскольку константы 0 и 1 являются палиндромными функциями. Таким образом, данная схема k-неизбыточна относительно неисправностей на входах и выходах элементов. Составим таблицу значений функции f и всех возможных функций неисправности схемы S на наборах $\tilde{\sigma}_0$ и $\tilde{\sigma}_1$ (табл. 1).

Таблица 1

Наборы	f	$f \oplus I_{\tilde{\sigma}_0}$	$f \oplus I_{\tilde{\sigma}_1}$	$f \oplus I_{\tilde{\sigma}_0} \oplus I_{\tilde{\sigma}_1}$	0	1
$\tilde{\sigma}_0$	0	1	0	1	0	1
$\tilde{\sigma}_1$	1	1	0	0	0	1

Видно, что указанные два набора не позволяют отличить только функцию $f \oplus I_{\tilde{\sigma}_0}$ от константы 1, если $f \oplus I_{\tilde{\sigma}_0} \not\equiv 1$, а также функцию $f \oplus I_{\tilde{\sigma}_1}$ от константы 0, если $f \oplus I_{\tilde{\sigma}_1} \not\equiv 0$. В случае $f \oplus I_{\tilde{\sigma}_0} \not\equiv 1$ добавим в множество $\{\tilde{\sigma}_0, \tilde{\sigma}_1\}$ произвольный набор длины n, на котором функция $f \oplus I_{\tilde{\sigma}_0}$ принимает значение 0, а в случае $f \oplus I_{\tilde{\sigma}_1} \not\equiv 0$ — произвольный набор длины n, на котором функция $f \oplus I_{\tilde{\sigma}_1}$ принимает значение 1. Итоговое множество будет являться k-диагностическим тестом длины не более 4 для схемы S относительно неисправностей на входах и выходах элементов. ■

Лемма 14. Пусть $x_{i_1}, \ldots, x_{i_s}$, где $s \geqslant 2$, — все существенные переменные булевой функции $f(\tilde{x}^n)$, а двоичные наборы $\tilde{\pi}_1$, $\tilde{\pi}_2$, $\tilde{\pi}_3$ длины n и элементы $\alpha, \gamma \in \{0,1\}$, $j \in \{1, \ldots, s\}$, таковы, что i_j-я (слева) компонента каждого из наборов $\tilde{\pi}_1$, $\tilde{\pi}_2$ равна γ, $f(\tilde{\pi}_1) = f(\tilde{\pi}_2) = \alpha$, а $f(\tilde{\pi}_3) = \overline{\alpha}$. Пусть схема S в базисе $B_6(k)$ является k-неизбыточной, реализует функцию $f(\tilde{x}^n)$ и множество $\{\tilde{\pi}_1, \tilde{\pi}_2, \tilde{\pi}_3\}$ является для неё k-диагностическим тестом относительно неисправностей на входах и выходах элементов. Тогда на любом наборе длины n, i_j-я компонента которого равна γ, функция f принимает значение α.

Доказательство. Переменная x_{i_j} обязана подаваться хотя бы на один вход v хотя бы одного элемента схемы S, поскольку $x_{i_j} \in \{x_{i_1}, \ldots, x_{i_s}\}$. Тогда неисправность типа γ этого входа нельзя обнаружить ни на одном из наборов $\tilde{\pi}_1$, $\tilde{\pi}_2$, значит, она должна обнаруживаться на наборе $\tilde{\pi}_3$. Отсюда вытекает, что для получающейся функции неисправности g схемы S справедливы равенства $g(\tilde{\pi}_1) = f(\tilde{\pi}_1) = \alpha$, $g(\tilde{\pi}_2) = f(\tilde{\pi}_2) = \alpha$ и $g(\tilde{\pi}_3) = \overline{f}(\tilde{\pi}_3) = \alpha$, т. е. функцию g нельзя отличить ни на одном из наборов $\tilde{\pi}_1$, $\tilde{\pi}_2$, $\tilde{\pi}_3$ от константы α, возникающей на выходе данной схемы при неисправности типа α на выходе её выходного элемента. С учётом того, что множество $\{\tilde{\pi}_1, \tilde{\pi}_2, \tilde{\pi}_3\}$ является k-диагностическим тестом для схемы S, это может быть только в том случае, когда $g \equiv \alpha$.

При подаче на входы схемы S произвольного двоичного набора длины n, i_j-я компонента которого равна γ, на вход v поступает значение γ, поэтому функция g, возникающая на выходе схемы при неисправности типа γ этого входа, на любом таком наборе принимает такое же значение, как и функция f. С учётом тождества $g \equiv \alpha$ получаем, что на любом наборе длины n, i_j-я компонента которого равна γ, функция f принимает значение α. ■

В следующей теореме рассмотрен случай неисправностей на входах и выходах элементов при $k = 1$, т. е. когда неисправным может быть только один вход/выход только одного элемента.

Теорема 4. Для любой булевой функции $f(\tilde{x}^n)$, отличной от константы 1, справедливо равенство

$$D^{B_6(1)}_{\text{ЕД (IO)}}(f) = \begin{cases} 0, & \text{если } f \text{ — тождественная функция,} \\ 1, & \text{если } f \equiv 0, \\ 2, & \text{если } f \equiv \overline{x}_i \text{ для некоторого } i \in \{1, \ldots, n\}, \\ 3, & \text{если } f \text{ — несамодвойственная функция и } f \not\equiv 0, \\ 4, & \text{если } f \text{ — самодвойственная функция} \\ & \text{и } f \notin \{x_1, \ldots, x_n, \overline{x}_1, \ldots, \overline{x}_n\}. \end{cases}$$

Если $f \equiv 1$, то значение $D^{B_6(1)}_{\text{ЕД (IO)}}(f)$ не определено.

Доказательство. Вместо $D^{B_6(1)}_{\text{ЕД (IO)}}(f)$ для краткости будем писать $D(f)$. В случае $f \equiv 1$ значение $D(f)$ не определено в силу леммы 10. Равенства $D(f) = 0$, если функция f тождественная, и $D(f) = 1$, если $f \equiv 0$, следуют из лемм 7 и 8 соответственно. Пусть $f \equiv \overline{x}_i$ для некоторого $i \in \{1, \ldots, n\}$. Тогда функцию f можно реализовать схемой в базисе $B_6(1)$, состоящей из одного инвертора, на вход которого подаётся переменная x_i. Очевидно, что у данной схемы есть только две функции неисправности — константы 0 и 1, которые можно отличить друг от друга и от функции f на множестве, состоящем из любых двух двоичных наборов длины n, i-я (слева) компонента одного из которых равна единице, а другого — нулю. Отсюда следует неравенство $D(f) \leqslant 2$. С другой стороны, $D(f) \geqslant 2$ в силу леммы 9, поэтому $D(f) = 2$.

Пусть $f(\tilde{x}^n)$ — произвольная булева функция, не принадлежащая множеству $\{0, 1, x_1, \ldots, x_n, \overline{x}_1, \ldots, \overline{x}_n\}$. Докажем неравенство $D(f) \geqslant 3$. Предположим, что это не так, т. е. $D(f) \leqslant 2$. В силу леммы 9 имеем $D(f) \geqslant 2$, поэтому $D(f) = 2$. Значит, существует неизбыточная схема S в базисе $B_6(1)$, реализующая функцию f и допускающая единичный диагностический тест из каких-то двух наборов $\tilde{\pi}_1$ и $\tilde{\pi}_2$ длины n. Заметим, что

$$f(\tilde{\pi}_1) \neq f(\tilde{\pi}_2), \tag{8}$$

поскольку в противном случае неисправность типа $f(\tilde{\pi}_1)$ на выходе выходного элемента схемы S нельзя было бы обнаружить ни на одном из этих двух наборов. Пусть x_i — произвольная существенная переменная функции f. Переменная x_i обязана подаваться хотя бы на один вход v хотя бы одного элемента схемы S. Если i-е (слева) компоненты наборов $\tilde{\pi}_1$ и $\tilde{\pi}_2$ совпадают и равны β, то неисправность типа β данного входа нельзя обнаружить на наборах $\tilde{\pi}_1$ и $\tilde{\pi}_2$; противоречие. Значит, i-е компоненты наборов $\tilde{\pi}_1$ и $\tilde{\pi}_2$ равны соответственно γ и $\overline{\gamma}$ для некоторого $\gamma \in \{0, 1\}$. Тогда неисправность типа γ входа v обнаруживается на наборе $\tilde{\pi}_2$ и не обнаруживается на наборе $\tilde{\pi}_1$, т. е. при рассматриваемой неисправности на наборе $\tilde{\pi}_1$ схема S выдаст значение $f(\tilde{\pi}_1)$, а на наборе $\tilde{\pi}_2$ — значение $\overline{f}(\tilde{\pi}_2)$, которое равно $f(\tilde{\pi}_1)$ в силу (8). Таким образом, полученную функцию неисправности g_1 схемы S нельзя отличить ни на одном из наборов $\tilde{\pi}_1$, $\tilde{\pi}_2$ от константы $f(\tilde{\pi}_1)$, возникающей на выходе данной схемы при неисправности типа $f(\tilde{\pi}_1)$ на выходе её выходного элемента. С учётом того, что $\{\tilde{\pi}_1, \tilde{\pi}_2\}$ — единичный диагностический тест для схемы S, это может быть только в том случае, когда

$g_1 \equiv f(\tilde{\pi}_1)$. Аналогично при неисправности типа $\overline{\gamma}$ входа v на выходе схемы S возникнет функция неисправности g_2, принимающая на наборах $\tilde{\pi}_1$ и $\tilde{\pi}_2$ значения $\overline{f}(\tilde{\pi}_1)$ и $f(\tilde{\pi}_2) = \overline{f}(\tilde{\pi}_1)$ соответственно. Её нельзя отличить ни на одном из этих наборов от константы $\overline{f}(\tilde{\pi}_1)$, возникающей на выходе данной схемы при неисправности типа $\overline{f}(\tilde{\pi}_1)$ на выходе её выходного элемента, поэтому $g_2 \equiv \overline{f}(\tilde{\pi}_1)$.

Далее заметим, что при подаче на входы схемы S произвольного двоичного набора длины n, i-я компонента которого равна γ, на вход v поступает значение γ, поэтому функция g_1, возникающая на выходе схемы при неисправности типа γ этого входа, на любом таком наборе принимает такое же значение, как и функция f. С учётом тождества $g_1 \equiv f(\tilde{\pi}_1)$ получаем, что на любом наборе длины n, i-я компонента которого равна γ, функция f принимает значение $f(\tilde{\pi}_1)$. Аналогично на любом наборе длины n, i-я компонента которого равна $\overline{\gamma}$, функция g_2 принимает такое же значение, как и функция f. С учётом тождества $g_2 \equiv \overline{f}(\tilde{\pi}_1)$ получаем, что на любом таком наборе функция f принимает значение $\overline{f}(\tilde{\pi}_1)$. Но тогда легко проверить, что на любом наборе длины n функция f принимает такое же значение, как и функция $x_i \oplus \gamma \oplus f(\tilde{\pi}_1)$, т. е. $f \equiv x_i \oplus \gamma \oplus f(\tilde{\pi}_1)$. Это означает, что либо $f \equiv x_i$, либо $f \equiv \overline{x}_i$, но в таком случае $f \in \{0, 1, x_1, \ldots, x_n, \overline{x}_1, \ldots, \overline{x}_n\}$; противоречие. Неравенство $D(f) \geqslant 3$ доказано.

Пусть f — несамодвойственная функция и $f \not\equiv 0, 1$. Докажем, что $D(f) \leqslant 3$; тогда с учётом неравенства $D(f) \geqslant 3$ будет установлено равенство $D(f) = 3$. Функция f принимает одно и то же значение на каких-то двух противоположных наборах $\tilde{\sigma}_0$ и $\tilde{\sigma}_1$ длины n. Рассмотрим два случая.

1. Пусть $f(\tilde{\sigma}_0) = f(\tilde{\sigma}_1) = 1$. Тогда по лемме 12 (при $k = 1$) функцию f можно реализовать схемой S' в базисе $B_6(1)$, неизбыточной и допускающей единичный диагностический тест $\{\tilde{\sigma}_0, \tilde{\sigma}_1\}$ относительно неисправностей на входах и выходах элементов, при которых выход выходного элемента схемы исправен, причём все её функции неисправности принадлежат множеству $\{f \oplus I_{\tilde{\sigma}_0}, f \oplus I_{\tilde{\sigma}_1}\}$. В случае, если указанный выход неисправен и выдаёт 0 (выдаёт 1), то на выходе схемы S' возникнет функция неисправности, тождественно равная нулю (соответственно единице). Таким образом, данная схема неизбыточна относительно неисправностей на входах и выходах элементов. Составим таблицу значений функции f и всех возможных функций неисправности схемы S' на наборах $\tilde{\sigma}_0$ и $\tilde{\sigma}_1$ (табл. 2).

Таблица 2

Наборы	f	$f \oplus I_{\tilde{\sigma}_0}$	$f \oplus I_{\tilde{\sigma}_1}$	0	1
$\tilde{\sigma}_0$	1	0	1	0	1
$\tilde{\sigma}_1$	1	1	0	0	1

Видно, что указанные два набора не позволяют отличить только функцию f от константы 1. Добавим к этим наборам ещё один произвольный набор длины n, на котором функция f принимает значение 0. Полученное множество будет являться единичным диагностическим тестом длины 3 для схемы S', откуда следует $D(f) \leqslant 3$. Случай 1 разобран.

2. Пусть $f(\tilde{\sigma}_0) = f(\tilde{\sigma}_1) = 0$. Функция $\overline{f}$ принимает значение 1 на каких-то противоположных наборах $\tilde{\sigma}_0$ и $\tilde{\sigma}_1$, поэтому по лемме 12 (при $k = 1$) её можно реализовать схемой $\hat{S}'$ в базисе $B_6(1)$, неизбыточной и допускающей единичный диагностический тест $\{\tilde{\sigma}_0, \tilde{\sigma}_1\}$ относительно неисправностей на входах и выходах элементов, при которых выход выходного элемента E схемы исправен, причём все функции неисправности схемы $\hat{S}'$ принадлежат множеству $\{f \oplus I_{\tilde{\sigma}_0}, f \oplus I_{\tilde{\sigma}_1}\}$. Соединим выход этой схемы со

входом инвертора I, выход которого объявим выходом полученной схемы; обозначим её через S'. Тогда при неисправности любого входа/выхода любого элемента подсхемы $\hat{S}'$, кроме выхода элемента E, на выходе схемы S' возникнет одна из функций неисправности

$$\overline{\overline{f} \oplus I_{\tilde{\sigma}_0}} = f \oplus 1 \oplus I_{\tilde{\sigma}_0} \oplus 1 = f \oplus I_{\tilde{\sigma}_0},$$
$$\overline{\overline{f} \oplus I_{\tilde{\sigma}_1}} = f \oplus 1 \oplus I_{\tilde{\sigma}_1} \oplus 1 = f \oplus I_{\tilde{\sigma}_1},$$

а при произвольной неисправности входа или выхода элемента I либо выхода выходного элемента подсхемы $\hat{S}'$ — одна из булевых констант 0 или 1. Таким образом, схема S' неизбыточна относительно неисправностей на входах и выходах элементов. Составим таблицу значений функции f и всех возможных функций неисправности данной схемы на наборах $\tilde{\sigma}_0$ и $\tilde{\sigma}_1$ (табл. 3).

Таблица 3

Наборы	f	$f \oplus I_{\tilde{\sigma}_0}$	$f \oplus I_{\tilde{\sigma}_1}$	0	1
$\tilde{\sigma}_0$	0	1	0	0	1
$\tilde{\sigma}_1$	0	0	1	0	1

Видно, что указанные два набора не позволяют отличить только функцию f от константы 0. Добавим к этим наборам ещё один произвольный набор длины n, на котором функция f принимает значение 1. Полученное множество будет являться единичным диагностическим тестом длины 3 для схемы S', откуда следует $D(f) \leqslant 3$. Случай 2 разобран. Равенство $D(f) = 3$ доказано.

Пусть теперь $f(\tilde{x}^n)$ — самодвойственная функция и $f \notin \{x_1, \ldots, x_n, \overline{x}_1, \ldots, \overline{x}_n\}$. Неравенство $D(f) \leqslant 4$ следует из леммы 13 (при $k = 1$) и того, что функция f, очевидно, не является палиндромной. Докажем неравенство $D(f) \geqslant 4$. Предположим, что это не так, т. е. $D(f) \leqslant 3$. Выше установлено, что $D(f) \geqslant 3$, поэтому $D(f) = 3$. Значит, существует неизбыточная схема S'' в базисе $B_6(1)$, реализующая функцию f и допускающая единичный диагностический тест из каких-то трёх наборов длины n. Данная функция не может принимать одинаковое значение β на всех этих наборах, поскольку в противном случае её нельзя было бы отличить на них от константы β, возникающей при неисправности типа β на выходе выходного элемента схемы S''. Поэтому на каких-то двух наборах $\tilde{\pi}_1$ и $\tilde{\pi}_2$ из теста функция f принимает значение α, а на третьем наборе $\tilde{\pi}_3$ из теста — значение $\overline{\alpha}$, где $\alpha \in \{0, 1\}$.

Пусть $x_{i_1}, \ldots, x_{i_s}$ — все существенные переменные функции f. Предположим, что наборы $\tilde{\pi}_1$ и $\tilde{\pi}_2$ различаются в каждой из i_1-й, …, i_s-й (слева) компонент. Пусть $\tilde{\pi}_1'$ — набор, противоположный набору $\tilde{\pi}_1$. Тогда $f(\tilde{\pi}_1) \neq f(\tilde{\pi}_1')$ в силу самодвойственности функции f. Наборы $\tilde{\pi}_1'$ и $\tilde{\pi}_2$ совпадают в i_1-й, …, i_s-й компонентах, а функция $f(\tilde{x}^n)$ существенно зависит только от переменных $x_{i_1}, \ldots, x_{i_s}$, поэтому $f(\tilde{\pi}_1') = f(\tilde{\pi}_2)$. Таким образом, $f(\tilde{\pi}_1) \neq f(\tilde{\pi}_2)$, однако это противоречит тому, что $f(\tilde{\pi}_1) = f(\tilde{\pi}_2) = \alpha$. Следовательно, наборы $\tilde{\pi}_1$ и $\tilde{\pi}_2$ совпадают хотя бы в одной из i_1-й, …, i_s-й компонент; обозначим номер этой компоненты через i_j, а её значение в каждом из указанных наборов — через γ. Тогда выполнены все условия леммы 14 (при $S = S''$), из которой следует, что на любом наборе длины n, i_j-я компонента которого равна γ, функция f принимает значение α. В таком случае на любом наборе длины n, i_j-я компонента которого равна $\overline{\gamma}$, данная функция в силу её самодвойственности принимает значение $\overline{\alpha}$. Но тогда легко проверить, что на любом наборе длины n функция f принимает такое же значение, как и функция $x_i \oplus \gamma \oplus \alpha$, т. е. $f \equiv x_i \oplus \gamma \oplus \alpha$. Это означает, что либо $f \equiv x_i$, либо $f \equiv \overline{x}_i$, поэтому $f \in \{x_1, \ldots, x_n, \overline{x}_1, \ldots, \overline{x}_n\}$; противоречие. Неравенство $D(f) \geqslant 4$ доказано.

В итоге получаем, что $D(f) = 4$. ■

Следствие 4. Для любого $n \geqslant 3$ справедливо равенство $D^{B_6(1)}_{\text{ЕД (IO)}}(n) = 4$.

Для доказательства следствия 4 достаточно заметить, что функция $x_1 \oplus x_2 \oplus x_3$ является самодвойственной.

Теорема 5. Для любого $k \in \mathbb{N}$ справедливо равенство $D^{B_6(k)}_{k\text{-Д (IO)}}(n) = 4$ при $n \geqslant 3$, причём в случае $k \geqslant 2$ доля тех булевых функций f от n переменных, для которых $D^{B_6(k)}_{k\text{-Д (IO)}}(f) = 4$, стремится к 1 при $n \to \infty$.

Доказательство. Вместо $D^{B_6(k)}_{k\text{-Д (IO)}}(n)$, $D^{B_6(k)}_{k\text{-Д (IO)}}(f)$ для краткости будем писать соответственно $D(n)$, $D(f)$. Неравенство $D(n) \geqslant 4$ при $n \geqslant 3$ вытекает из следствия 4 (любой k-диагностический тест для любой k-неизбыточной схемы является единичным диагностическим тестом для той же схемы, которая при этом неизбыточна). Докажем неравенство $D(n) \leqslant 4$. Для этого достаточно доказать неравенство $D(f) \leqslant 4$ для любой булевой функции $f(\tilde{x}^n)$, для которой определено значение $D(f)$. При $f \equiv 1$ оно не определено в силу леммы 1; при $f \equiv 0$ указанное неравенство следует из леммы 8, а в случае, когда функция f не палиндромная, — из леммы 13.

Пусть f — палиндромная функция и $f \not\equiv 0, 1$. Тогда существуют такие два противоположных двоичных набора $\tilde{\sigma}_0$ и $\tilde{\sigma}_1$ длины n, что $f(\tilde{\sigma}_0) = f(\tilde{\sigma}_1) = 1$. По лемме 12 функцию f можно реализовать k-неизбыточной схемой S в базисе $B_6(k)$, допускающей k-диагностический тест $\{\tilde{\sigma}_0, \tilde{\sigma}_1\}$ относительно неисправностей на входах и выходах элементов, при которых выход выходного элемента схемы исправен, причём все её функции неисправности принадлежат множеству $\{f \oplus I_{\tilde{\sigma}_0}, f \oplus I_{\tilde{\sigma}_1}, f \oplus I_{\tilde{\sigma}_0} \oplus I_{\tilde{\sigma}_1}\}$. Если указанный выход неисправен и выдаёт 0 (выдаёт 1), то на выходе схемы S возникнет функция неисправности, тождественно равная нулю (соответственно единице). Таким образом, данная схема k-неизбыточна. Составим таблицу значений функции f и всех возможных функций неисправности схемы S на наборах $\tilde{\sigma}_0$ и $\tilde{\sigma}_1$ (табл. 4).

Таблица 4

Наборы	f	$f \oplus I_{\tilde{\sigma}_0}$	$f \oplus I_{\tilde{\sigma}_1}$	$f \oplus I_{\tilde{\sigma}_0} \oplus I_{\tilde{\sigma}_1}$	0	1
$\tilde{\sigma}_0$	1	0	1	0	0	1
$\tilde{\sigma}_1$	1	1	0	0	0	1

Видно, что указанные два набора не позволяют отличить только функцию $f \oplus I_{\tilde{\sigma}_0} \oplus I_{\tilde{\sigma}_1}$ от константы 0, если $f \oplus I_{\tilde{\sigma}_0} \oplus I_{\tilde{\sigma}_1} \not\equiv 0$, а также функцию f от константы 1. Добавим в множество $\{\tilde{\sigma}_0, \tilde{\sigma}_1\}$ произвольный набор длины n, на котором функция f принимает значение 0, а в случае $f \oplus I_{\tilde{\sigma}_0} \oplus I_{\tilde{\sigma}_1} \not\equiv 0$ добавим в полученное множество произвольный набор длины n, на котором функция $f \oplus I_{\tilde{\sigma}_0} \oplus I_{\tilde{\sigma}_1}$ принимает значение 1. Итоговое множество будет являться k-диагностическим тестом длины не более 4 для схемы S, откуда следует, что $D(f) \leqslant 4$. Неравенство $D(n) \leqslant 4$, а вместе с ним равенство $D(n) = 4$ при $n \geqslant 3$ доказаны.

Докажем второе утверждение теоремы. Пусть $k \geqslant 2$, $n \geqslant 2$ и f — произвольная булева функция от n переменных, не принадлежащая множеству $U = \{0, 1, x_1, \ldots, x_n, \overline{x}_1, \ldots, \overline{x}_n\}$, для которой $D(f) \leqslant 3$. Докажем, что $f \in F_n$, где F_n — множество булевых функций от n переменных, каждая из которых при подстановке вместо каких-то двух её переменных каких-то булевых констант становится равна некоторой булевой константе. Из теоремы 4 следует, что $D(f) \geqslant 3$, поэтому $D(f) = 3$. Значит, существует неизбыточная схема S' в базисе $B_6(k)$, реализующая функцию f и допускающая k-диагностический тест из каких-то трёх наборов длины n. Данная функция не может принимать одинаковое значение β на всех этих наборах, поскольку в противном случае её нельзя было бы отличить на них от константы β, возникающей при неисправности типа β на выходе выходного элемента схемы S'. Поэтому на каких-то двух наборах $\tilde{\pi}_1$ и $\tilde{\pi}_2$ из теста функция f принимает значение α, а на третьем наборе $\tilde{\pi}$ из теста — значение $\overline{\alpha}$, где $\alpha \in \{0, 1\}$.

Пусть $x_{i_1}, \ldots, x_{i_s}$ — все существенные переменные функции f. Ясно, что $s \geqslant 2$. Если i_j-е компоненты наборов $\tilde{\pi}_1$ и $\tilde{\pi}_2$ совпадают для некоторого $j \in \{1, \ldots, s\}$, то выполнены все условия леммы 14 (при $S = S'$, $\tilde{\pi}_3 = \tilde{\pi}$). Из неё следует, что на любом наборе длины n, i_j-я компонента которого равна γ, функция f принимает значение α. Но тогда при подстановке вместо переменной x_{i_j} константы γ, а вместо любой другой переменной из множества $x_1, \ldots, x_n$ произвольной булевой константы данная функция становится равна константе α, откуда вытекает, что $f \in F_n$, что и требовалось доказать.

Пусть теперь наборы $\tilde{\pi}_1$ и $\tilde{\pi}_2$ различаются в каждой из i_1-й, …, i_s-й компонент. Наборы $\tilde{\pi}$ и $\tilde{\pi}_1$ различаются хотя бы в одной из этих компонент, поскольку $f(\tilde{\pi}) \neq f(\tilde{\pi}_1)$. Пусть они различаются в i_q-й компоненте, $q \in \{1, \ldots, s\}$, причём i_q-е компоненты наборов $\tilde{\pi}$ и $\tilde{\pi}_1$ равны π_q и $\overline{\pi}_q$ соответственно. Тогда i_q-я компонента набора $\tilde{\pi}_2$ равна π_q. Аналогично наборы $\tilde{\pi}$ и $\tilde{\pi}_2$ различаются в какой-то i_t-й компоненте, $t \in \{1, \ldots, s\}$, и их i_t-е компоненты равны π_t и $\overline{\pi}_t$ соответственно, где $\pi_t \in \{0, 1\}$, а i_t-я компонента набора $\tilde{\pi}_1$ равна π_t. При этом $t \neq q$, так как в противном случае i_q-я компонента набора $\tilde{\pi}_2$ была бы равна одновременно π_q и $\overline{\pi}_q$. Составим для наглядности таблицу значений i_q-й и i_t-й компонент наборов $\tilde{\pi}_1$, $\tilde{\pi}_2$ и $\tilde{\pi}$ (табл. 5).

Таблица 5

Наборы	i_q	i_t
$\tilde{\pi}_1$	$\overline{\pi}_q$	π_t
$\tilde{\pi}_2$	π_q	$\overline{\pi}_t$
$\tilde{\pi}$	π_q	π_t

Каждая из переменных x_{i_q}, x_{i_t} обязана подаваться хотя бы на один вход хотя бы одного элемента схемы S', поскольку $x_{i_q}, x_{i_t} \in \{x_{i_1}, \ldots, x_{i_s}\}$; обозначим эти входы через v_q и v_t соответственно. Тогда неисправность типа π_q входа v_q нельзя обнаружить ни на одном из наборов $\tilde{\pi}_2$, $\tilde{\pi}$, так как их i_q-е компоненты равны π_q. Значит, данная неисправность должна обнаруживаться на наборе $\tilde{\pi}_1$. Отсюда вытекает, что для получающейся функции неисправности g_q схемы S' справедливы равенства $g_q(\tilde{\pi}_1) = \overline{f}(\tilde{\pi}_1) = \overline{\alpha}$. Если, помимо неисправности типа π_q входа v_q, в схеме S' также имеет место неисправность типа π_t входа v_t, то для получающейся функции неисправности g_{qt} данной схемы справедливы равенства $g_{qt}(\tilde{\pi}_1) = g_q(\tilde{\pi}_1) = \overline{\alpha}$, поскольку на наборе $\tilde{\pi}_1$ на вход v_t в случае исправности этого входа и неисправности типа π_q входа v_q подаётся i_t-я компонента набора $\tilde{\pi}_1$, которая равна π_t и, следовательно, неисправность типа π_t входа v_t никак не отразится на значении, выдаваемом схемой S' на этом наборе.

Далее, неисправность типа π_t входа v_t нельзя обнаружить ни на одном из наборов $\tilde{\pi}_1$, $\tilde{\pi}$, так как их i_t-е компоненты равны π_t. Значит, данная неисправность должна обнаруживаться на наборе $\tilde{\pi}_2$. Отсюда вытекает, что для получающейся функции неисправности g_t схемы S' справедливы равенства $g_t(\tilde{\pi}_2) = \overline{f}(\tilde{\pi}_2) = \overline{\alpha}$. Если, помимо неисправности типа π_t входа v_t, в схеме S' также имеет место неисправность типа π_q входа v_q, то для получающейся функции неисправности g_{qt} данной схемы справедливы равенства $g_{qt}(\tilde{\pi}_2) = g_t(\tilde{\pi}_2) = \overline{\alpha}$, поскольку на наборе $\tilde{\pi}_2$ на вход v_q в случае исправности этого входа и неисправности типа π_t входа v_t подаётся i_q-я компонента набора $\tilde{\pi}_2$, которая равна π_q и, следовательно, неисправность типа π_q входа v_q никак не отразится на значении, выдаваемом схемой S' на этом наборе.

В случае отсутствия неисправностей в схеме S' на наборе $\tilde{\pi}$ на входы v_q и v_t поступают значения π_q и π_t соответственно, поскольку i_q-я (i_t-я) компонента набора $\tilde{\pi}$ равна π_q (соответственно π_t). Поэтому одновременная неисправность входа v_q типа π_q и входа v_t типа π_t никак не отразится на значении, выдаваемом схемой S' на указанном наборе. Отсюда следуют равенства $g_{qt}(\tilde{\pi}) = f(\tilde{\pi}) = \overline{\alpha}$.

В итоге получаем, что функция неисправности g_{qt} схемы S' принимает значение $\overline{\alpha}$ на каждом из наборов $\tilde{\pi}_1$, $\tilde{\pi}_2$ и $\tilde{\pi}$, поэтому её нельзя отличить ни на одном из этих наборов от константы $\overline{\alpha}$, возникающей на выходе данной схемы при неисправности типа $\overline{\alpha}$ на выходе её выходного элемента. С учётом того, что множество $\{\tilde{\pi}_1, \tilde{\pi}_2, \tilde{\pi}\}$ является k-диагностическим тестом для схемы S', это может быть только в том случае, когда $g_{qt} \equiv \overline{\alpha}$.

Заметим, что при подаче на входы схемы S' произвольного двоичного набора длины n, i_q-я компонента которого равна π_q, а i_t-я компонента равна π_t, на вход v_q поступает значение π_q, а на вход v_t — значение π_t, поэтому функция g_{qt}, возникающая на выходе схемы при одновременной неисправности входа v_q типа π_q и входа v_t типа π_t, на любом таком наборе принимает такое же значение, как и функция f. С учётом тождества $g_{qt} \equiv \overline{\alpha}$ получаем, что на любом наборе длины n, i_q-я компонента которого равна π_q, а i_t-я компонента равна π_t, функция f принимает значение $\overline{\alpha}$. Следовательно, при подстановке вместо переменной x_{i_q} константы π_q, а вместо переменной x_{i_t} константы π_t данная функция становится равна константе $\overline{\alpha}$, т. е. $f \in F_n$, что и требовалось доказать.

Тем самым установлено, что в случае $n \geqslant 2$ произвольная булева функция f от n переменных, не принадлежащая множеству U, для которой $D(f) \leqslant 3$, принадлежит множеству F_n. Среди функций из множества U могут быть функции f от n переменных, для которых $D(f) \leqslant 3$ (и даже точно есть — см. леммы 7 и 8), но все они принадлежат F_n, поскольку $U \subseteq F_n$ в силу определений этих множеств. Значит, все булевы функции f от n переменных, где $n \geqslant 2$, для которых $D(f) \leqslant 3$, принадлежат множеству F_n.

Оценим величину $|F_n|$. Пусть $F_{n,i,j}^{\alpha,\beta,\gamma}$ — подмножество множества F_n, состоящее из всех булевых функций, каждая из которых при подстановке вместо переменной x_i константы α, а вместо переменной x_j константы β, где $1 \leqslant i < j \leqslant n$, становится равна константе γ. Любая функция из множества $F_{n,i,j}^{\alpha,\beta,\gamma}$ принимает значение γ на любом из 2^{n-2} двоичных наборов длины n, i-я (слева) компонента которых равна α и j-я равна β, а на остальных $2^n - 2^{n-2}$ наборах может принимать произвольные значения, поэтому $|F_{n,i,j}^{\alpha,\beta,\gamma}| = 2^{2^n - 2^{n-2}}$. Любая функция из множества F_n принадлежит множеству $F_{n,i,j}^{\alpha,\beta,\gamma}$ для некоторых i, j, α, β и γ, откуда следуют соотношения

$$F_n \subseteq \bigcup_{\substack{1 \leqslant i < j \leqslant n, \\ \alpha,\beta,\gamma \in \{0,1\}}} F_{n,i,j}^{\alpha,\beta,\gamma},$$

$$|F_n| \leqslant \sum_{\substack{1\leqslant i<j\leqslant n,\\ \alpha,\beta,\gamma\in\{0,1\}}} |F^{\alpha,\beta,\gamma}_{n,i,j}| = \sum_{\substack{1\leqslant i<j\leqslant n,\\ \alpha,\beta,\gamma\in\{0,1\}}} 2^{2^n-2^{n-2}} = C_n^2\cdot 2^3\cdot 2^{2^n-2^{n-2}} = 4n(n-1)2^{2^n-2^{n-2}},$$

$$\frac{|F_n|}{2^{2^n}} \leqslant \frac{4n(n-1)2^{2^n-2^{n-2}}}{2^{2^n}} = \frac{4n(n-1)}{2^{2^{n-2}}} \to 0 \ \ (n\to\infty),$$

т. е. отношение числа булевых функций из множества F_n к общему числу булевых функций от n переменных стремится к 0 при $n \to \infty$. В силу доказанного выше это означает, что доля тех булевых функций f от n переменных, для которых $D(f) \leqslant 3$, стремится к 0 при $n \to \infty$. Следовательно, доля тех булевых функций f от n переменных, для которых $D(f) \geqslant 4$, стремится к 1 при $n \to \infty$. Осталось заметить, что при $f \not\equiv 1$ из неравенства $D(f) \geqslant 4$ вытекает равенство $D(f) = 4$ в силу доказанного соотношения $D(f) \leqslant 4$ для любой булевой функции f от n переменных, кроме константы 1, а $1 \in F_n$. ∎

Замечание 3. Среди всех схем, построенных при доказательстве верхних оценок величин $D^{B_6(k)}_{k\text{-Д (I)}}(f)$, $D^{B_6(k)}_{k\text{-Д (IO)}}(f)$ и $D^{B_6(k)}_{k\text{-Д (IO)}}(n)$ в теоремах 3, 4 и 5 соответственно, элемент «константа 0» использовался только в построении схем, реализующих тождественный нуль, ξ-элемент — только в построении схем, реализующих не палиндромные функции (теоремы 3 и 5) либо самодвойственные функции (теорема 4), причём не более чем в единственном числе, а η-элемент — только в построении схем, реализующих палиндромные функции (теоремы 3 и 5) либо несамодвойственные функции (теорема 4), причём не более чем в единственном числе.

ЛИТЕРАТУРА

1. *Чегис И. А., Яблонский С. В.* Логические способы контроля работы электрических схем // Труды МИАН. 1958. Т. 51. С. 270–360.
2. *Яблонский С. В.* Надежность и контроль управляющих систем // Материалы Всес. семинара по дискретной математике и её приложениям (Москва, 31 января–2 февраля 1984 г.). М.: Изд-во МГУ, 1986. С. 7–12.
3. *Яблонский С. В.* Некоторые вопросы надежности и контроля управляющих систем // Математические вопросы кибернетики. Вып. 1. М.: Наука, 1988. С. 5–25.
4. *Редькин Н. П.* Надежность и диагностика схем. М.: Изд-во МГУ, 1992. 192 с.
5. *Коляда С. С.* Верхние оценки длины проверяющих тестов для схем из функциональных элементов: дис. ... канд. физ.-мат. наук. М., 2013. 77 с.
6. *Reddy S. M.* Easily testable realizations for logic functions // IEEE Trans. Comput. 1972. V. C-21. No. 11. P. 1183–1188.
7. *Saluja K. K. and Reddy S. M.* Fault detecting test sets for Reed-Muller canonic networks // IEEE Trans. Comput. 1975. V. C-24. No. 10. P. 995–998.
8. *Романов Д. С., Романова Е. Ю.* Метод синтеза неизбыточных схем, допускающих единичные проверяющие тесты константной длины // Дискретная математика. 2017. Т. 29. Вып. 4. С. 87–105.
9. *Редькин Н. П.* О проверяющих тестах для схем при однотипных константных неисправностях на входах элементов // Изв. вузов. Математика. 1988. № 7. С. 57–64.
10. *Редькин Н. П.* О схемах, допускающих короткие единичные диагностические тесты // Дискретная математика. 1989. Т. 1. Вып. 3. С. 71–76.
11. *Редькин Н. П.* О проверяющих тестах для схем при константных неисправностях на входах элементов // Вестник Московского университета. Сер. 1. Математика. Механика. 1997. № 1. С. 12–18.

12. *Попков К. А.* Синтез легкотестируемых схем при однотипных константных неисправностях на входах и выходах элементов // Препринты ИПМ им. М. В. Келдыша. 2018. № 87. 18 с.

13. *Угольников А. Б.* Классы Поста: учеб. пособие. М.: Изд-во ЦПИ при механико-математическом факультете МГУ, 2008. 64 с.

REFERENCES

1. *Chegis I. A. and Yablonskiy S. V.* Logicheskie sposoby kontrolya raboty elektricheskikh skhem [Logical methods of control of work of electric circuits]. Trudy Mat. Inst. Steklov, 1958, vol. 51, pp. 270–360. (in Russian)

2. *Yablonskiy S. V.* Nadezhnost' i kontrol' upravlyayushchikh sistem [Reliability and verification of control systems]. Materialy Vsesoyuznogo seminara po diskretnoy matematike i ee prilozheniyam (Moscow, 31 Jan.–2 Feb. 1984). Moscow, MSU Publ., 1986, pp. 7–12. (in Russian)

3. *Yablonskiy S. V.* Nekotorye voprosy nadezhnosti i kontrolya upravlyayushchikh sistem [Some questions of reliability and verification of control systems]. Matematicheskie Voprosy Kibernetiki, iss. 1, Moscow, Nauka Publ., 1988, pp. 5–25. (in Russian)

4. *Red'kin N. P.* Nadezhnost' i diagnostika skhem [Circuits Reliability and Diagnostics]. Moscow, MSU Publ., 1992. 192 p. (in Russian)

5. *Kolyada S. S.* Verkhnie otsenki dlin proveryayushchikh testov dlya skhem iz funktsional'nykh elementov [Upper bounds on the lengths of fault detection tests for logic networks]. Cand. Sci. Dissertation, MSU, Moscow, 2013. 77 p. (in Russian)

6. *Reddy S. M.* Easily testable realizations for logic functions. IEEE Trans. Comput., 1972, vol. C-21, no. 11, pp. 1183–1188.

7. *Saluja K. K. and Reddy S. M.* Fault detecting test sets for Reed-Muller canonic networks. IEEE Trans. Comput., 1975. vol. C-24, no. 10, pp. 995–998.

8. *Romanov D. S. and Romanova E. Yu.* Metod sinteza neizbytochnykh skhem, dopuskayushchikh edinichnye proveryayushchie testy konstantnoy dliny [Method of synthesis of irredundant circuits allowing single fault detection tests of constant length]. Diskretnaya Matematika, 2017, vol. 29, iss. 4, pp. 87–105. (in Russian)

9. *Red'kin N. P.* O proveryayushchikh testakh dlya skhem pri odnotipnykh konstantnykh neispravnostyakh na vkhodakh elementov [On fault detection tests for logic networks under one-type stuck-at faults at inputs of gates]. Izvestiya Vuzov, Matematika, 1988, no. 7, pp. 57–64. (in Russian)

10. *Red'kin N. P.* O skhemah, dopuskayushchikh korotkie edinichnye diagnosticheskie testy [On circuits allowing short single diagnostic tests]. Diskretnaya Matematika, 1989, vol. 1, iss. 3, pp. 71–76. (in Russian)

11. *Red'kin N. P.* O proveryayushchikh testakh dlya skhem pri konstantnykh neispravnostyakh na vkhodakh elementov [On fault detection tests for logic networks under stuck-at faults at inputs of gates]. Vestnik MSU, Ser. 1, 1997, no. 1, pp. 12–18. (in Russian)

12. *Popkov K. A.* Sintez legkotestiruemykh skhem pri odnotipnykh konstantnykh neispravnostyakh na vkhodakh i vykhodakh elementov [Synthesis of Easily Testable Logic Networks under One-Type Stuck-at Faults at Inputs and Outputs of Gates]. Preprinty IPM im. M. V. Keldysha, 2018, no. 87. 18 p. (in Russian)

13. *Ugol'nikov A. B.* Klassy Posta: uchebnoe posobie [Post Classes: Tutorial]. Moscow, MSU, TsPI Publ., 2008. 64 p. (in Russian)

ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

УДК 519.17

СВОЙСТВА ПРИМИТИВНЫХ МНОЖЕСТВ ОРИЕНТИРОВАННЫХ ГРАФОВ С ОБЩИМ МНОЖЕСТВОМ КОНТУРОВ

Я. Э. Авезова

Национальный исследовательский ядерный университет «МИФИ», г. Москва, Россия

Получены критерий примитивности и оценки экспонентов множеств орграфов с общим множеством простых контуров. Критерий примитивности позволил получить формулу для числа примитивных множеств n-вершинных орграфов с общим гамильтоновым контуром.

Ключевые слова: *гамильтонов орграф, примитивное множество орграфов, экспонент множества орграфов.*

DOI 10.17223/20710410/43/7

ON PROPERTIES OF PRIMITIVE SETS OF DIGRAPHS WITH COMMON CYCLES

Y. E. Avezova

National Research Nuclear University Moscow Engineering Physics Institute, Moscow, Russia

E-mail: avezovayana@gmail.com

Let $\hat{\Gamma} = \{\Gamma_1, \ldots, \Gamma_p\}$ be a set of digraphs with vertex set V, $p > 1$, and $U^{(p)}$ be the union of digraphs $\Gamma_1 \cup \ldots \cup \Gamma_p$ with no multiple arcs. The smallest number such that the union of μ digraphs of the set $\hat{\Gamma}$ contains all arcs of $U^{(p)}$ is denoted by μ. Suppose $\hat{C} = \{C_1, \ldots, C_m\}$ is a set of elementary cycles. This set is called common for $\hat{\Gamma}$ if every digraph of the set $\hat{\Gamma}$ contains all cycles of the set $\hat{C}$. Assume that $C_1^* \cup \ldots \cup C_m^* = V$ where C_i^* denotes the vertex set of C_i, $i = 1, \ldots, m$. For a given digraph Γ, the loop-character index in the semigroup $\langle \Gamma \rangle$ is the smallest integer h for which there is a loop on every vertex of Γ^h. In this paper, we study conditions for the set of digraphs with common cycles to be primitive. For $m \geqslant 1$, the set $\hat{\Gamma}$ with common cycles set $\hat{C}$ is primitive if and only if the digraph $U^{(p)}$ is primitive. If $\hat{\Gamma}$ is primitive, then $\exp \hat{\Gamma} \leqslant \big((\mu-1)h+1\big)\exp U^{(p)}$, where h is the loop-character index in the semigroup $\langle \Gamma(\hat{C}) \rangle$, $\Gamma(\hat{C}) = C_1 \cup \ldots \cup C_m$. For $m = 1$, we establish an improved bound on the exponent. Let all digraphs of the primitive set $\hat{\Gamma}$ have a common Hamiltonian cycle, then $\exp \hat{\Gamma} \leqslant (2n-1)\mu + \sum\limits_{\tau=1}^{\mu} \big(F(l_1^\tau, \ldots, l_{m(\tau)}^\tau) + d_\tau - l_1^\tau\big)$, where $l_1^\tau, \ldots, l_{m(\tau)}^\tau$ are all cycle lengths in Γ_τ, ordered so that $l_1^\tau < \ldots < l_{m(\tau)}^\tau = n$, $d_\tau = \gcd(l_1^\tau, \ldots, l_{m(\tau)}^\tau)$, $F(l_1^\tau, \ldots, l_{m(\tau)}^\tau) = d_\tau \Phi(l_1^\tau/d_\tau, \ldots, l_{m(\tau)}^\tau/d_\tau)$, $\Phi(l_1^\tau/d_\tau, \ldots, l_{m(\tau)}^\tau/d_\tau)$ denotes the Frobenius number, $\tau = 1, \ldots, \mu$. Finally, if $n = q^\alpha$, q is prime, $\alpha \in \mathbb{N}$, $m = n^2$, then the number of primitive sets of n-vertex digraphs with a common Hamiltonian cycle equals $2^\sigma - 2^\varepsilon$, where $\sigma = 2^{m-n}$, $\varepsilon = 2^{m/q-n}$.

Keywords: *Hamiltonian digraph, primitive set of digraps, exponent of digraphs set.*

Введение

Введем основные обозначения:

— $\mathbb{N}$ — множество натуральных чисел;
— $\mathbb{N}_p = \{1, \ldots, p\}$, $p \in \mathbb{N}$;
— $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$;
— $0,1$-матрица — матрица с элементами из множества $\{0, 1\}$;
— $M = (m_{i,j})$ — матрица смежности вершин орграфа;
— $M^t = (m_{i,j}^{(t)})$, $t \in \mathbb{N}$;
— $M > 0$ ($M \geqslant 0$) — все элементы матрицы M над полем действительных чисел неотрицательны (положительны);
— $\langle X \rangle$ — подполугруппа, порожденная подмножеством X мультипликативной полугруппы;
— $\|M\|$ — вес $0,1$-матрицы M, равный числу единичных элементов матрицы;
— M^{T} — транспонированная матрица M;
— НОД$(a_1, \ldots, a_n)$ — наибольший общий делитель натуральных чисел $a_1, \ldots, a_n$;
— (i, j) — дуга в орграфе Γ, инцидентная вершинам i и j;
— $[i, j]$ — путь в орграфе Γ из вершины i в вершину j;
— $\mathrm{len}[i, j]$ — длина пути $[i, j]$ в орграфе.

Важными характеристиками преобразования векторного пространства являются множества существенных переменных его координатных функций. Преобразование называется совершенным, если каждая координатная функция существенно зависит от всех переменных. Совершенность является одним из положительных свойств преобразований, применяемых в системах защиты информации. Часто совершенность преобразования обозначают как свойство полного перемешивания входных данных. В системах защиты информации полное перемешивание входных данных делает систему устойчивой к атакам типа последовательного опробования частей секретного параметра.

Существуют два равносильных подхода к оценке перемешивающих свойств преобразования: матричный и теоретико-графовый. Суть обоих подходов описана в [1, 2]. Полное перемешивание входных данных, как правило, осуществляется композицией несовершенных преобразований, допускающих несложную реализацию. Матрично-графовый подход позволяет оценить длину такой композиции. Основными задачами при этом являются распознавание примитивности неотрицательной матрицы и оценка её экспонента [3, 4]. Матрица M называется примитивной тогда и только тогда, когда существует $\gamma \in \mathbb{N}$, такое, что для любого $t \geqslant \gamma$ выполняется $M^t > 0$. Наименьшее $\gamma \in \mathbb{N}$, при котором $M^\gamma > 0$, называется экспонентом матрицы M, обозначается $\exp M$. Исследование примитивности для неотрицательных матриц и $0,1$-матриц равносильно. Умножение $0,1$-матриц определено как умножение матриц над множеством целых неотрицательных чисел с последующей заменой в произведении всех положительных элементов единицами. Сложение выполняется аналогично. Мультипликативный моноид всех $0,1$-матриц порядка n обозначим $M_n^{0,1}$.

Свойство примитивности исследуется с использованием следующей теоремы теории графов [5]: если M — матрица смежности вершин графа Γ и $M^t = (m_{i,j}^{(t)})$, то число путей длины t из i в j в графе Γ равно $m_{i,j}^{(t)}$, $i, j \in \{1, \ldots, n\}$. Известен критерий примитивности орграфа [6]: сильносвязный орграф примитивный, если и только если длины всех простых контуров орграфа взаимно простые.

Многообразие возникающих постановок задач в различных областях науки привели к обобщениям понятия примитивности неотрицательных матриц. В частности, введены определения примитивности множества матриц [1, 7−9]. В настоящей работе в соответствии с [1] множество матриц $\hat{M} \subseteq M_n^{0,1}$ называется примитивным, если порождённая множеством $\hat{M}$ мультипликативная полугруппа $\langle \hat{M} \rangle$ содержит положительную матрицу. Наименьшая длина слова из $\langle \hat{M} \rangle$, соответствующего положительной матрице, называется экспонентом множества $\hat{M}$ и обозначается $\exp \hat{M}$. Дадим равносильное определение примитивности множества на теоретико-графовом языке. Обозначим $\Gamma(n)$ множество всех орграфов с множеством вершин $V = \{0, \ldots, n-1\}$. Умножение орграфов из $\Gamma(n)$ определяется как умножение бинарных отношений. Множество $\hat{\Gamma} \subseteq \Gamma(n)$ называется примитивным, если порождённая множеством $\hat{\Gamma}$ мультипликативная полугруппа $\langle \hat{\Gamma} \rangle$ содержит полный орграф. Наименьшая длина слова из $\langle \hat{\Gamma} \rangle$, соответствующего полному орграфу, называется экспонентом множества $\hat{\Gamma}$ и обозначается $\exp \hat{\Gamma}$. Если положительной матрицы в алфавите $\hat{M}$ (полного орграфа в алфавите $\hat{\Gamma}$) не существует, то $\exp \hat{M} = \infty$ ($\exp \hat{\Gamma} = \infty$).

Универсальный критерий примитивности множества орграфов формулируется весьма сложно как на матричном, так и на теоретико-графовом языках, и распознавание его выполнимости предполагает проверку ряда условий для множества орграфов. В связи с этим актуальна задача поиска множеств орграфов, важных с прикладной точки зрения, для которых критерий примитивности существенно упрощается.

В множестве орграфов $\hat{\Gamma}$ простой контур назовем общим, если он имеется в любом орграфе этого множества. Множество орграфов $\hat{\Gamma}$ имеет общее множество контуров $\hat{C}$, если каждый орграф множества $\hat{\Gamma}$ содержит все контуры множества $\hat{C}$. Настоящая работа посвящена исследованию примитивности множеств орграфов с общим множеством контуров и логически продолжает работы [10−12], обобщая некоторые полученные в них результаты.

1. Комбинаторные свойства множества примитивных матриц (орграфов)

Если множество $\hat{M}$ содержит примитивную матрицу, то оно примитивное. В наиболее интересном для исследования примитивности случае множество $\hat{M}$ состоит из непримитивных матриц.

Известно необходимое условие примитивности множества матриц [2, теорема 11.8]: если множество $\hat{M} = \{M_1, \ldots, M_p\}$, $p > 1$, примитивное, то матрица $M = M_1 + \ldots + M_p$ примитивная и $\exp \hat{M} \geqslant \exp M$. Существуют непримитивные матрицы веса $n^2 - n + 1$, такие матрицы при $k = 1, \ldots, n$ образуют множество H_k, определяемое правилом: $M = (m_{i,j}) \in H_k \Leftrightarrow m_{k,j} = 0$ при всех $j \in \{1, \ldots, n\} \backslash \{k\}$, остальные элементы равны 1. Непримитивной является также матрица веса $n^2 - n + 1$, транспонированная к любой матрице из H_k, $k = 1, \ldots, n$. Любая матрица, вес которой превышает $n^2 - n + 1$, является примитивной [13].

На множестве $M_n^{0,1}$ введём частичный порядок: $M \leqslant M' \Leftrightarrow m_{i,j} \leqslant m'_{i,j}$ для всех $i, j = 1, \ldots, n$. Если M, M' — матрицы смежности орграфов Γ, Γ' соответственно и $M \leqslant M'$, то все дуги орграфа Γ являются дугами орграфа Γ', т. е. Γ — часть орграфа Γ' (обозначается $\Gamma \leqslant \Gamma'$).

Непримитивное множество матриц $\hat{M}$ назовем максимальным непримитивным, если при объединении с любой матрицей $B \in M_n^{0,1} \backslash \hat{M}$ множество $\hat{M} \cup \{B\}$ является примитивным. Актуальной является задача описания всех максимально непримитивных множеств и оценка их мощностей. Опишем одно из таких множеств.

Теорема 1. Пусть M — непримитивная $0,1$-матрица веса $n^2 - n + 1$, $\hat{M} = \{M_1, \ldots, M_p\}$ — множество матриц со свойством $M_\tau \leqslant M$, $\tau = 1, \ldots, p$, где $p = 2^{m-n+1}$, $m = n^2$. Тогда $\hat{M}$ — максимальное непримитивное множество.

Доказательство. Пусть $M = (m_{i,j})$, где, не ограничивая общности, положим, что $m_{1,j} = 0$ при $j = 2, \ldots, n$, остальные элементы матрицы положительны. Заметим, что $M = M_1 + \ldots + M_p$. В силу [2, теорема 11.8] из непримитивности матрицы M следует, что множество $\hat{M}$ также непримитивное. Покажем, что множество $\hat{M}$ максимальное непримитивное. Добавим к множеству $\hat{M}$ матрицу $B = (b_{i,j})$, $B \in M_n^{0,1} \backslash \hat{M}$, тогда $b_{1,k} > 0$ при некотором $k \in \{2, \ldots, n\}$. Следовательно, $\|M'\| > m - n + 1$, где $M' = M_1 + \ldots + M_p + B$, и матрица M' примитивная.

Покажем, что множество $\hat{M}' = \{M_1, \ldots, M_p, B\}$ примитивное, построив положительное слово в алфавите $\hat{M}'$. Обозначим: $C = M \cdot B$, $C' = C \cdot M$, $C = (c_{i,j})$, $C' = (c'_{i,j})$. В силу правила произведения матриц, $c_{i,j} = m_{i,1}b_{1,j} + \ldots + m_{i,n}b_{n,j}$, откуда следует, что $c_{i,k} > 0$ при $i = 1, \ldots, n$. Тогда $c'_{i,j} = c_{i,1}m_{1,j} + \ldots + c_{i,n}m_{n,j} > 0$ при всех $i, j = 1, \ldots, n$. Таким образом, произведение $C' = M \cdot B \cdot M$ является положительной матрицей в алфавите $\hat{M}'$. Следовательно, множество $\hat{M}'$ примитивное. Отсюда $\hat{M}$ — максимальное непримитивное множество. ■

Далее обозначим: $m = n^2$, $\sigma(n) = |M_n^{0,1}| = 2^m$ — число всех $0,1$-матриц порядка n; $\pi(n)$ — число примитивных $0,1$-матриц порядка n; $\beta(n)$ — число примитивных множеств, состоящих только из непримитивных $0,1$-матриц порядка n; $\eta(n)$ — число всех примитивных множеств $0,1$-матриц порядка n. Установим формулу для $\eta(n)$, которая далее используется при доказательстве одного из основных результатов.

Теорема 2. $\eta(n) = 2^{\sigma(n)} - 2^{\sigma(n)-\pi(n)} + \beta(n)$.

Доказательство. Множество матриц, содержащее хотя бы одну примитивную матрицу, примитивное. Число непустых множеств, состоящих только из примитивных матриц, равно $\eta_1(n) = 2^{\pi(n)} - 1$. Число непримитивных матриц равно $\sigma(n) - \pi(n)$, тогда число множеств непримитивных матриц равно $\eta_0(n) = 2^{\sigma(n)-\pi(n)}$. Объединяя каждое непустое множество примитивных матриц с каждым множеством непримитивных матриц, получим $\eta_1(n)\eta_0(n)$ примитивных множеств, в которых есть примитивные и, возможно, непримитивные матрицы. Тогда общее число примитивных множеств $\eta(n) = \eta_1(n)\eta_0(n) + \beta(n)$. После элементарных преобразований получаем необходимое равенство. ■

Критерий примитивности множества матриц $\hat{M}$ получен в [14]. Впервые универсальная оценка экспонента примитивного множества матриц порядка n дана в [15]:

$$\exp \hat{M} \leqslant \frac{n^3 + n^2}{2} - 2n + 1. \tag{1}$$

По замечанию автора оценки, она допускает уточнение, поскольку не зависит от мощности множества $\hat{M}$. Оценка (1) улучшена в [16]:

$$\exp \hat{M} \leqslant \frac{7n^3 + 6n^2 + 8n}{24} - 1. \tag{2}$$

Представляет также интерес критерий примитивности множества графов, полученный в [11]. Приведём этот критерий. Пусть в множестве орграфов $\hat{\Gamma} = \{\Gamma_1, \ldots, \Gamma_p\}$, $p > 1$, все дуги орграфа Γ_τ помечены числом τ, $\tau = 1, \ldots, p$. Тогда множеству $\hat{\Gamma}$ однозначно соответствует мультиграф $\Gamma^{(p)} = \Gamma_1 \cup \ldots \cup \Gamma_p$, в котором любой путь длины s

помечен непустым множеством слов длины s. Путь в мультиграфе $\Gamma^{(p)}$ имеет метку w^t, если он есть конкатенация t путей с метками w; путь с меткой w^0 положим пустым. В частности, путь длины t имеет метку w^t, если каждая дуга пути помечена числом $w \in N_p$. Если множество $\hat{\Gamma}$ примитивное, то мультиграф $\Gamma^{(p)}$ сильносвязный [1, 2]. Сильносвязный мультиграф $\Gamma^{(p)}$ называется w-сильносвязным, если для любых вершин i и j существует путь с меткой $w^{t_{ij}}$ из i в j при некотором $t_{ij} \in \mathbb{N}$. Из данного определения следует, что в w-сильносвязном мультиграфе $\Gamma^{(p)}$ есть контур с меткой w^{t_i} при некотором $t_i \in \mathbb{N}$ с началом обхода в вершине i, $i = 0, \ldots, n-1$. Критерий: орграф $\Gamma(w) = \Gamma_{w_1} \ldots \Gamma_{w_s}$, где $w = w_1 \ldots w_s$, примитивный, если и только если $\Gamma^{(p)}$ является w-сильносвязным и содержит контуры с метками $w^{t_1}, \ldots, w^{t_m}$, где НОД$(t_1, \ldots, t_m) = 1$.

Задача распознавания примитивности множества n-вершинных орграфов алгоритмически разрешима [11].

Критерий примитивности множества $\hat{\Gamma}$ существенно упрощается для некоторых частных классов, важных для приложений в области анализа систем защиты информации, в то же время уточняется оценка (2).

2. Примитивность множества орграфов с общим гамильтоновым контуром

Говорят, что «путь проходит через контур», если у пути и контура есть общая вершина. Путь проходит через множество контуров, если он проходит через каждый контур множества.

Обозначим: (θ, π) — тип орграфа Γ в мультипликативной циклической полугруппе $\langle \Gamma \rangle$, где θ и π — циклическая глубина и период орграфа Γ соответственно; $kC(i)$ — контур в Γ, соответствующий k-кратному проходу контура C из вершины i, где $k \in \mathbb{N}_0$; $0C(i)$ — пустой контур. Для подмножества натуральных чисел $\{a_1, \ldots, a_m\}$, таких, что НОД$(a_1, \ldots, a_m) = d = 1$, $m > 1$, числом Фробениуса $\Phi(a_1, \ldots, a_m)$ называется наибольшее целое число, не принадлежащее аддитивной полугруппе $\langle a_1, \ldots, a_m \rangle$. Обозначим $F(a_1, \ldots, a_m) = d\Phi(a_1/d, \ldots, a_m/d)$, $d \geqslant 1$ (если $d = 1$, то $F(a_1, \ldots, a_m) = \Phi(a_1, \ldots, a_m)$). Далее полагаем, что $1 \leqslant a_1 < \ldots < a_m$.

Установим соотношения между длинами простых контуров в гамильтоновом орграфе Γ и его типом (циклической глубиной и периодом) как элемента циклической полугруппы $\langle \Gamma \rangle$. Данные соотношения позволяют оценить экспонент примитивного множества орграфов с общим гамильтоновым контуром.

Обозначим: $L = \{l_1, \ldots, l_m\}$ — множество всех длин простых контуров в сильносвязном орграфе Γ, где $m > 1$, $l_1 < \ldots < l_m$; $\hat{C} = \{C_1, \ldots, C_m\}$ — множество простых контуров длин $l_1, \ldots, l_m$ соответственно; $l(i, \hat{C}, j)$ — длина кратчайшего пути из вершины i в вершину j, проходящего через множество контуров $\hat{C}$.

Лемма 1. Если НОД$(L) = d$ в n-вершинном сильносвязном орграфе Γ, то для любой пары вершин (i, j) длины всех путей из i в j сравнимы по модулю d.

Доказательство. Пусть для некоторых вершин i, j в Γ есть пути из i в j длин l и $l+c$. Обозначим l_{ji} длину любого простого пути из j в i в орграфе Γ. Простой путь из j в i существует, поскольку орграф Γ сильносвязный. Следовательно, в Γ есть контуры длин $l + l_{ji}$ и $l + c + l_{ji}$. Так как длина любого контура есть сумма длин нескольких простых контуров, то в условиях леммы $d \mid (l + l_{ji})$ и $d \mid (l + c + l_{ji})$. Следовательно, $d \mid c$. ■

Теорема 3. Гамильтонов n-вершинный орграф Γ, в котором НОД$(L) = d$, имеет полугрупповой тип (θ, π), где $\pi = d$ и $\theta \leqslant F(l_1, \ldots, l_m) + d + \max\limits_{0 \leqslant i,j \leqslant n-1} l(i, \hat{C}, j)$.

Доказательство. Так как НОД$(l_1/d, \ldots, l_m/d) = 1$, то в соответствии со свойствами чисел Фробениуса для любого $b \in \mathbb{N}$ при некоторых $k_1, \ldots, k_m \in \mathbb{N}_0$, зависящих от b, выполнено

$$k_1 l_1 + \ldots + k_m l_m = F(l_1, \ldots, l_m) + db.$$

Так как в Γ имеется путь из i в j длины $l(i, \hat{C}, j)$, проходящий через множество контуров $\hat{C}$, то для любого $b \in \mathbb{N}$ в Γ имеется путь из i в j длины $t_b(i, j)$, где

$$t_b(i, j) = l(i, \hat{C}, j) + F(l_1, \ldots, l_m) + db,$$

содержащий обход контуров $C_1, \ldots, C_m$ соответственно $k_1, \ldots, k_m$ раз. В силу леммы 1, $t_b(i, j) \equiv l(i, \hat{C}, j) \pmod d$. Следовательно, дуга (i, j) одновременно имеется или не имеется в орграфах Γ^t и Γ^{t+d}, $t \geqslant t_1(i, j)$. Данные рассуждения верны для любой пары вершин (i, j), значит, $\Gamma^t = \Gamma^{t+d}$, $t \geqslant \max\limits_{0 \leqslant i,j \leqslant n-1} t_1(i, j)$. Следовательно, $\pi \mid d$.

По определению, $\Gamma^t = \Gamma^{t+\pi}$, $t \geqslant \max\limits_{0 \leqslant i,j \leqslant n-1} t_1(i, j)$. Тогда в Γ имеются пути из i в j длины t и $t + \pi$ для некоторых вершин i и j, что при $\pi < d$ противоречит лемме 1. Отсюда $\pi = d$. ■

Следствие 1. Имеет место

$$\theta \leqslant 2n - l_1 + \begin{cases} F(l_1, \ldots, l_m) + d - 1, & d > 1, \\ \Phi(l_1, \ldots, l_m), & d = 1. \end{cases}$$

Доказательство. Обозначим: $w(i, j)$ — кратчайший путь из вершины i в вершину j, $w(i, i)$ — путь длины 0; $\lambda_k = n - l_k$, $k = 1, \ldots, m$.

Заметим, что путь $w(i, j)$ определен неоднозначно и $0 \leqslant \operatorname{len} w(i, j) \leqslant n - 1$ при любых i, j. Для вершин i, j построим путь $[i, j]$, проходящий через множество контуров $\hat{C}$, и оценим длину этого пути.

Если $\operatorname{len} w(i, j) \geqslant \lambda_k$, то $w(i, j)$ проходит через контур C_k, имеющий l_k вершин, $k = 1, \ldots, m$. Отсюда если $\operatorname{len} w(i, j) \geqslant \lambda_1$, то путь $w(i, j)$ проходит через множество контуров $\hat{C}$, так как $\lambda_1 > \lambda_2 > \ldots > \lambda_m$. В случае $\operatorname{len} w(i, j) \geqslant \lambda_1$ полагаем $[i, j] = w(i, j)$. В случае $\operatorname{len} w(i, j) < \lambda_1$ полагаем $[i, j] = w(i, j) \circ C_m(j)$, где путь $[i, j]$ проходит через множество контуров $\hat{C}$ в силу гамильтоновости контура C_m и $\operatorname{len}\, [i, j] = \operatorname{len} w(i, j) + n < \lambda_1 + n = 2n - l_1$. Следовательно, $l(i, \hat{C}, j) \leqslant \operatorname{len}\, [i, j] \leqslant 2n - l_1 - 1$ для любых вершин i, j. Отсюда и из теоремы 3 получаем нужную оценку θ. ■

Замечание 1. Данная оценка θ при $d = 1$ совпадает с оценкой экспонента примитивного гамильтонова орграфа Γ [17, следствие 2].

Пример 1. В табл. 1 приведены оценки и точные значения циклической глубины гамильтоновых орграфов при $n = 6$. Орграфы Γ_1 и Γ_2 непримитивные, орграф Γ_3 примитивный (граф Виландта). Как видно из табл. 1, для орграфов Γ_2 и Γ_3 достигается верхнее значение оценки величины $\max\limits_{0 \leqslant i,j \leqslant n-1} l(i, \hat{C}, j)$, для орграфа Γ_3 — верхняя оценка θ, приведённые в следствии 1.

Т а б л и ц а 1

Оценки и точные значения циклической глубины для орграфов Γ_1 и Γ_2

Γ	$\hat{C}$	d	$F(l_1,\ldots,l_m)$	$\max\limits_{0\leqslant i,j\leqslant n-1} l(i,\hat{C},j)$	$\max\limits_{0\leqslant i,j\leqslant n-1} t_1(i,j)$	θ
Γ_1	$C_1=(0,4,5)$, $C_2=(1,2,3)$, $C_3=(0,1,2,3,4,5)$	3	$3\Phi(1,2)=-3$	$l(1,\hat{C},0)=5$	$3-3+5=5$	3
Γ_2	$C_1=(0,4,5)$, $C_2=(0,1,2,3,4,5)$	3	$3\Phi(1,2)=-3$	$l(1,\hat{C},3)=8$	$3-3+8=8$	6
Γ_3	$C_1=(0,1,2,3,4)$, $C_2=(0,1,2,3,4,5)$	1	$\Phi(5,6)=19$	$l(5,\hat{C},5)=6$	$1+19+6=26$	26

Рассмотрим множество орграфов $\hat{\Gamma}=\{\Gamma_1,\ldots,\Gamma_p\}$, $p>1$. Обозначим $U^{(p)}$ орграф, полученный из мультиграфа $\Gamma^{(p)}=\Gamma_1\cup\ldots\cup\Gamma_p$ удалением всех меток и отождествлением кратных дуг. Наименьшее количество орграфов множества $\hat{\Gamma}$, объединение которых содержит все дуги орграфа $U^{(p)}$, обозначим μ. По определению $1\leqslant\mu\leqslant p$.

Множество орграфов называется сокращённым (понятие введено в [18]), если ни один из орграфов множества не является частью другого орграфа этого множества. Примитивность любого множества равносильна примитивности его сокращённого подмножества (следует из [18, утверждение 5]), и в случае примитивности их экспоненты равны. При $p>\mu=1$ множество $\hat{\Gamma}$ не сокращённое, поскольку все орграфы являются частью одного из орграфов множества $\hat{\Gamma}$. Этот случай выходит за рамки данной работы, так как исследование примитивности множества $\hat{\Gamma}$ сводится к проверке свойства примитивности орграфа с наибольшим числом дуг. Без ограничения общности далее полагаем, что $U^{(p)}=U^{(\mu)}$, где $1<\mu\leqslant p$.

Установим критерий примитивности множества орграфов с общим гамильтоновым контуром.

Теорема 4. Пусть $\hat{\Gamma}=\{\Gamma_1,\ldots,\Gamma_p\}$ — множество орграфов с общим гамильтоновым контуром $Z=(0,\ldots,n-1)$, $p>1$. Множество $\hat{\Gamma}$ примитивное, если и только если орграф $U^{(p)}$ примитивный. Для экспонента примитивного множества орграфов $\hat{\Gamma}$ верна оценка

$$\exp\hat{\Gamma}\leqslant(2n-1)\mu+\sum_{\tau=1}^{\mu}\left(F(l_1^\tau,\ldots,l_{m(\tau)}^\tau)+d_\tau-l_1^\tau\right),\qquad(3)$$

где $l_1^\tau,\ldots,l_{m(\tau)}^\tau$ — длины всех простых контуров орграфа Γ_τ, $l_1^\tau<\ldots<l_{m(\tau)}^\tau=n$; $d_\tau=\text{НОД}(l_1^\tau,\ldots,l_{m(\tau)}^\tau)$, $\tau=1,\ldots,\mu$.

Доказательство. *Необходимость.* Пусть множество $\hat{\Gamma}=\{\Gamma_1,\ldots,\Gamma_p\}$ примитивное и $M_1,\ldots,M_p$ — матрицы смежности орграфов $\Gamma_1,\ldots,\Gamma_p$ соответственно. Из примитивности множества $\hat{\Gamma}$ следует примитивность множества $\hat{M}=\{M_1,\ldots,M_p\}$. Тогда матрица $M=M_1+\ldots+M_p$ примитивная в силу [2, теорема 11.8]. Заметим, что матрица M является матрицей смежности вершин орграфа $U^{(p)}$. Следовательно, орграф $U^{(p)}$ примитивный.

Достаточность. Считаем, что все орграфы множества $\hat{\Gamma}$ непримитивные, иначе очевидно, что орграф $U^{(p)}$ примитивный и теорема верна.

Пусть примитивный орграф $U^{(p)}$ содержит множество простых контуров $\hat{C}=\{C_1,\ldots,C_m\}$ длин $l_1,\ldots,l_m$ соответственно, где $\text{НОД}(l_1,\ldots,l_m)=1$ и $m>1$, иначе один из орграфов множества $\hat{\Gamma}$ гамильтонов и имеет петлю, т. е. примитивный.

Поскольку $U^{(p)}=U^{(\mu)}$, то $U^{(\mu)}$ содержит все дуги контуров множества $\hat{C}$. Обозначим: (θ_τ,π_τ) — тип орграфа Γ_τ, $\tau=1,\ldots,\mu$; $\pi=\text{НОД}(\pi_1,\ldots,\pi_\mu)$. Из теоремы 3 следует, что $\pi_\tau = d_\tau = \text{НОД}(l_1^\tau, \ldots, l_{m(\tau)}^\tau)$, $\tau = 1, \ldots, \mu$, значит, π делит длину любого контура любого орграфа из множества $\{\Gamma_1, \ldots, \Gamma_\mu\}$. Докажем, что $\pi = 1$.

Пусть $C = (u_0, \ldots, u_{l-1})$ — любой контур. Конкатенация дуги $(u_k, u_{(k+1) \bmod l})$ и части контура Z образуют в некотором из орграфов $\Gamma_1, \ldots, \Gamma_\mu$ контур длины $\lambda_k = n - (u_{(k+1) \bmod l} - u_k) \bmod n + 1$, значит, $\pi \mid \lambda_k$, $k = 0, \ldots, l-1$, и $\pi \mid \sum\limits_{k=0}^{l-1}(n - \lambda_k)$, где

$$\sum_{k=0}^{l-1}(n - \lambda_k) = \sum_{k=0}^{l-1}\big((u_{(k+1) \bmod l} - u_k) \bmod n - 1\big) = n - l.$$

Тогда $\pi \mid (n-l)$ и π делит длину l любого контура из $\hat{C}$, что при $\pi > 1$ противоречит условию $\text{НОД}(l_1, \ldots, l_m) = 1$. Следовательно, $\pi = 1$.

Построим в мультиграфе $\Gamma^{(p)}$ для любых вершин i, j путь из i в j с меткой $1^{t_1} \ldots \mu^{t_\mu}$, где $t_1, \ldots, t_\mu \in \mathbb{N}$. Контур Z гамильтонов, следовательно, в Γ_1 есть пути из вершины i в вершину $(i + t_1) \bmod n$ длины t_1 и в вершину $(i + t_1 + \pi_1) \bmod n$ длины $t_1 + \pi_1$ при любом $t_1 \in \mathbb{N}$. Тогда $(i, (i + t_1) \bmod n)$ есть дуга орграфа $\Gamma_1^{t_1}$ и $(i, (i + t_1 + \pi_1) \bmod n)$ есть дуга орграфа $\Gamma_1^{t_1+\pi_1}$. В соответствии с теоремой 3, $\Gamma_1^{t_1} = \Gamma_1^{t_1+\pi_1}$ при $t_1 \geqslant \theta_1$, значит, при указанных t_1 в орграфе $\Gamma_1^{t_1}$ есть дуга $(i, (i+t_1+\pi_1) \bmod n)$, тогда в Γ_1 есть путь из вершины i в вершину $(i+t_1+\pi_1) \bmod n$ длины t_1. Поскольку π_1 — период орграфа Γ_1, то в орграфе Γ_1 есть пути из вершины i в вершину $(i + t_1 + k_1\pi_1) \bmod n$ длины t_1 для любых $t_1 \geqslant \theta_1$ и $k_1 \in \mathbb{N}_0$. Тогда в мультиграфе $\Gamma^{(p)}$ есть пути с меткой 1^{t_1} из вершины i в любую вершину множества $I_1 = \{(i + t_1 + k_1\pi_1) \bmod n \colon k_1 \in \mathbb{N}_0\}$.

Пусть $i_1 \in I_1$. Повторив на втором шаге рассуждения для вершины i_1, получаем, что в мультиграфе $\Gamma^{(p)}$ при $t_2 \geqslant \theta_2$ есть пути с меткой 2^{t_2} из вершины i_1 в любую вершину множества $I_2 = \{(i_1 + t_2 + k_2\pi_2) \bmod n \colon k_2 \in \mathbb{N}_0\}$. Объединяя утверждения двух шагов, получаем, что в $\Gamma^{(p)}$ есть пути с меткой $1^{t_1}2^{t_2}$ из вершины i в любую вершину множества $I_{12} = \{(i + t_1 + t_2 + k_1\pi_1 + k_2\pi_2) \bmod n \colon k_1, k_2 \in \mathbb{N}_0\}$ при $t_1 \geqslant \theta_1$ и $t_2 \geqslant \theta_2$.

Продолжая следующие шаги рассуждений, получаем, что в $\Gamma^{(p)}$ есть пути с меткой $1^{t_1} \ldots \mu^{t_\mu}$ из i в любую вершину множества $I_{1\mu} = \{(i + t + k_1\pi_1 + \ldots + k_\mu\pi_\mu) \bmod n \colon k_1, \ldots, k_\mu \in \mathbb{N}_0\}$, где $t = t_1 + \ldots + t_\mu$, $t_1 \geqslant \theta_1, \ldots, t_\mu \geqslant \theta_\mu$. В зависимости от чисел $k_1, \ldots, k_\mu$ величина $k_1\pi_1 + \ldots + k_\mu\pi_\mu$ принимает любые значения, превышающие число Фробениуса $\Phi(\pi_1, \ldots, \pi_\mu)$. Значит, множество $I_{1\mu}$ содержит полную систему вычетов по модулю n — множество $\{0, \ldots, n-1\}$. Таким образом, построены пути с меткой $1^{t_1} \ldots \mu^{t_\mu}$ из вершины i в любую вершину. Следовательно, орграф $\Gamma_1^{t_1} \ldots \Gamma_\mu^{t_\mu}$ полный и множество $\hat{\Gamma}$ примитивное. Критерий доказан.

Получим оценку $\exp\hat{\Gamma}$. Орграф $\Gamma_1^{t_1} \ldots \Gamma_\mu^{t_\mu}$ полный при любых $t_\tau \geqslant \theta_\tau$, $\tau = 1, \ldots, \mu$, следовательно, $\exp\hat{\Gamma} \leqslant \theta_1 + \ldots + \theta_\mu$. По следствию 1, $\theta_\tau \leqslant 2n - 1 - l_1^\tau + F(l_1^\tau, \ldots, l_{m(\tau)}^\tau) + d_\tau$. Тогда $\exp\hat{\Gamma} \leqslant (2n-1)\mu + \sum\limits_{\tau=1}^{\mu}\big(F(l_1^\tau, \ldots, l_{m(\tau)}^\tau) + d_\tau - l_1^\tau\big)$. ∎

Примитивный орграф называется минимальным, если после удаления любой дуги нарушается свойство его примитивности [19]. Обозначим: $G(n, Z)$ — множество n-вершинных орграфов, имеющих гамильтонов контур Z, $\sigma(n, Z) = |G(n, Z)| = 2^{m-n}$, где $m = n^2$; $G^P(n, Z)$ — множество примитивных n-вершинных орграфов, имеющих гамильтонов контур Z, $\pi(n, Z) = |G^P(n, Z)|$; $G^P_{\min}(n, Z)$ — множество минимальных примитивных орграфов, имеющих гамильтонов контур Z, $\omega(n, Z) = |G^P_{\min}(n, Z)|$; $G^P_{\min}(n, Z) \subset G^P(n, Z) \subset G(n, Z)$. Множество примитивных n-вершинных орграфов, имеющих гамильтонов контур, представляет особый интерес при исследовании перемешивающих свойств регистровых преобразований, в частности при $n = 2^\alpha$, $\alpha \in \mathbb{N}$. Следующая теорема устанавливает количество таких орграфов для примарного числа вершин n.

Теорема 5. Пусть $n = q^\alpha$, q — простое число, $\alpha \in \mathbb{N}$, $m = n^2$. Тогда

$$\pi(n, Z) = \frac{2^m - 2^{m/q}}{2^n}.$$

Доказательство. Любое число, не кратное q, взаимно просто с $n = q^\alpha$, $\alpha \in \mathbb{N}$. Тогда по условию минимальный примитивный орграф с гамильтоновым контуром Z имеет $n{+}1$ дугу, где дуги образуют простые контуры длин l и n, $1 \leqslant l < n$, НОД(l, n)=1. Следовательно, любой примитивный гамильтонов орграф с числом дуг больше $n + 1$ не минимальный.

Найдём $\omega(n, Z) = |G^P_{\min}(n, Z)|$. Обозначим $\Pi(n) = \{l_1, \ldots, l_r\}$ — множество чисел, взаимно простых с n, где $r = q^\alpha - q^{\alpha-1} = n - n/q$ — значение функции Эйлера при $n = q^\alpha$. Существует n изоморфных орграфов множества $G^P_{\min}(n, Z)$, имеющих простой контур длины l_i, $i = 1, \ldots, r$. Следовательно, $\omega(n, Z) = n(n - n/q)$.

Положим $G^P_{\min}(n, Z) = \{\Gamma_1, \ldots, \Gamma_\omega\}$, где $\omega = \omega(n, Z)$, и рассмотрим множества $U_i = \{\Gamma \colon \Gamma \geqslant \Gamma_i\}$, $i = 1, \ldots, \omega$. Тогда $G^P(n, Z) = U_1 \cup \ldots \cup U_\omega$. Заметим, что $|U_{i_1} \cap \ldots \cap U_{i_k}| = 2^{m-(n+k)}$ при любом $k = 1, \ldots, \omega$. Используя принцип включения-исключения, найдём $|G^P(n, Z)|$:

$$\begin{gathered}\pi(n, Z) = |G^P(n, Z)| = |U_1 \cup \ldots \cup U_\omega| = \\ = \sum_{k=1}^{\omega} (-1)^{k-1} C_\omega^k 2^{m-(n+k)} = 2^{m-n} \left(\sum_{k=1}^{\omega} (-1)^{k-1} C_\omega^k 2^{-k} \right).\end{gathered} \tag{4}$$

Применяя формулу бинома Ньютона, преобразуем (4) к виду $\pi(n, Z) = 2^{m-n}(1 - 2^{-\omega})$. Поскольку $\omega = n(n - n/q) = m - m/q$, $\pi(n, Z) = 2^{m-n}(1 - 2^{m/q-m}) = (2^m - 2^{m/q})/2^n$. ■

Пример 2. При $n = 4$ существует $2^{m-n} = 2^{12} = 4096$ орграфов с гамильтоновым контуром $Z = (0, 1, 2, 3)$. Из них, по теореме 5, 4080 орграфов — примитивные.

Обозначим $\beta(n, Z)$ число примитивных множеств n-вершинных орграфов с общим гамильтоновым контуром Z, в которых каждый орграф не примитивен.

Из критерия примитивности множества орграфов с общим гамильтоновым контуром и теорем 2 и 5 следует точное значение числа примитивных множеств орграфов с общим гамильтоновым контуром Z при $n = q^\alpha$, где q — простое число, $\alpha \in \mathbb{N}$.

Следствие 2. Пусть $n = q^\alpha$, q — простое число, $\alpha \in \mathbb{N}$, $m = n^2$. Тогда число примитивных множеств орграфов с общим гамильтоновым контуром Z равно

$$\eta(n, Z) = 2^\sigma - 2^\varepsilon,$$

где $\sigma = 2^{m-n}$; $\varepsilon = 2^{m/q-n}$.

Доказательство. Из теоремы 2 следует, что

$$\eta(n, Z) = 2^{\sigma(n,Z)} - 2^{\sigma(n,Z)-\pi(n,Z)} + \beta(n, Z).$$

Найдём $\beta(n, Z)$. При $n = q^\alpha$ если орграф Γ_i содержит гамильтонов контур Z и не примитивен, то длины всех простых контуров орграфа Γ_i кратны q, $i = 1, \ldots, p$. Следовательно, длины всех простых контуров орграфа $U^{(p)}$ также кратны q и $U^{(p)}$ непримитивный. Тогда $\beta(n, Z) = 0$ согласно критерию теоремы 4. Значит, $\eta(n, Z) = 2^{\sigma(n,Z)} - 2^{\sigma(n,Z)-\pi(n,Z)}$, где $\sigma(n, Z) = \sigma = 2^{m-n}$, $\pi(n, Z) = (2^m - 2^{m/q})/2^n$ (по теореме 5). Тогда $\sigma(n, Z) - \pi(n, Z) = \varepsilon = 2^{m/q-n}$. ■

3. Критерий примитивности множества орграфов с общим множеством контуров

Обозначим: C^* — множество вершин контура C; $\Gamma(\hat{C}) = C_1 \cup \ldots \cup C_m$ — часть орграфа Γ; $E(\hat{C})$ — множество дуг орграфа $\Gamma(\hat{C})$.

Воспользуемся терминами теории признаков в полугруппах [1, гл. 9]. Подмножество H полугруппы G, состоящее из всех элементов G, обладающих определённым свойством, называется признаком H (H-признаком) в полугруппе G. Если $H \leqslant G$ — подполугруппа, то H называется полугрупповым признаком в G. В полугруппе $\Gamma(n)$ полугрупповым признаком (обозначается P_{loop}) является, в частности, множество всех орграфов, имеющих петли в каждой вершине множества P, $\varnothing \neq P \subseteq V$. Показателем P_{loop}-признака в полугруппе $\langle\Gamma\rangle$ называется наименьшее натуральное h, при котором $\Gamma^h \in P_{\text{loop}}$ (обозначается $\text{pok}P_{\text{loop}}$ или кратко l_P). В [20] получены оценки и точное значение показателя P_{loop}-признака.

Следующая теорема устанавливает критерий примитивности и оценку экспонента множества орграфов с общим множеством простых контуров.

Теорема 6. Пусть $\hat{\Gamma} = \{\Gamma_1, \ldots, \Gamma_p\}$ — множество орграфов с общим множеством контуров $\hat{C} = \{C_1, \ldots, C_m\}$, $p, m > 1$, $C_1^* \cup \ldots \cup C_m^* = V$. Множество $\hat{\Gamma}$ примитивное, если и только если орграф $U^{(p)}$ примитивный. Для экспонента примитивного множества орграфов $\hat{\Gamma}$ верна оценка

$$\exp \hat{\Gamma} \leqslant \big((\mu - 1)h + 1\big) \exp U^{(p)}, \tag{5}$$

где h — показатель V_{loop}-признака в полугруппе $\langle\Gamma(\hat{C})\rangle$.

Доказательство. *Необходимость* критерия доказывается, как в теореме 4.

Достаточность. Рассмотрим неочевидный случай, когда все орграфы множества $\hat{\Gamma}$ непримитивные. Обозначим $G_{1,r} = \Gamma_1^h \ldots \Gamma_{r-1}^h \Gamma_r$. Докажем по индукции, что орграф $U^{(r)}$ является частью орграфа $G_{1,r}$, $1 < r \leqslant \mu$.

При $r = 2$ покажем, что $U^{(2)}$ — часть орграфа $G_{1,2} = \Gamma_1^h \Gamma_2$, т. е. $G_{1,2}$ содержит все дуги орграфов Γ_1 и Γ_2. Поскольку $h = \text{pok}V_{\text{loop}}$ в полугруппе $\langle\Gamma(\hat{C})\rangle$ и орграф Γ_1 содержит множество контуров $\hat{C}$, то орграф Γ_1^h имеет петли во всех вершинах. Отсюда орграф $G_{1,2}$ содержит все дуги орграфа Γ_2, в том числе множество общих контуров $\hat{C}$.

Пусть (i, j) — дуга орграфа Γ_1 и $(i, j) \notin E(\hat{C})$. Покажем, что орграф $G_{1,2}$ содержит дугу (i, j). Из условия $C_1^* \cup \ldots \cup C_m^* = V$ следует, что любая вершина орграфа Γ_1 принадлежит хотя бы одному из контуров множества $\hat{C}$. Тогда в Γ_1 есть дуга $(a, j) \in E(\hat{C})$, $a \neq i$, такая, что из j в a в Γ_1 есть путь длины $h - 1$ (следует из определения показателя V_{loop}-признака). Тогда в орграфе Γ_1^h есть дуга (i, a). Орграф Γ_2 имеет дугу (a, j), поскольку множество $\hat{C}$ есть множество общих контуров и $(a, j) \in E(\hat{C})$. Тогда, в силу правила умножения орграфов, орграф $G_{1,2}$ содержит дугу (i, j). Таким образом, $G_{1,2}$ содержит все дуги орграфов Γ_1 и Γ_2 и, следовательно, $U^{(2)}$ является частью орграфа $G_{1,2}$.

Пусть утверждение доказано для $r = 2, \ldots, q - 1$, где $2 < q \leqslant \mu$, докажем его для $r = q$. По условию $G_{1,q} = G_{1,q-1} \Gamma_{q-1}^{h-1} \Gamma_q$. По предположению индукции орграф $U^{(q-1)}$ является частью орграфа $G_{1,q-1}$, т. е. $G_{1,q-1}$ содержит общее множество контуров $\hat{C}$ и все дуги орграфов $\Gamma_1, \ldots, \Gamma_{q-1}$. Рассмотрим орграф $\Gamma = \Gamma_{q-1}^{h-1} \Gamma_q$. Поскольку $h = \text{pok}V_{\text{loop}}$ в полугруппе $\langle\Gamma(\hat{C})\rangle$ и орграф $\Gamma(\hat{C})$ является общей частью Γ_{q-1} и Γ_q, орграф Γ имеет петли во всех вершинах множества V. Отсюда $G_{1,q} = G_{1,q-1}\Gamma$ содержит все дуги орграфа $G_{1,q-1}$. Таким образом, $G_{1,q}$ содержит все дуги орграфов $\Gamma_1, \ldots, \Gamma_{q-1}$.

Покажем, что орграф $G_{1,q}$ содержит все дуги орграфа Γ_q. Рассмотрим орграф $\Gamma' = G_{1,q-1}\Gamma_{q-1}^{h-1} = \Gamma_1^h \ldots \Gamma_{q-1}^h$. Орграф $\Gamma(\hat{C})$ является общей частью орграфов $\Gamma_1, \ldots, \Gamma_{q-1}$, откуда следует, что Γ' имеет петли во всех вершинах. Тогда орграф $G_{1,q} = \Gamma'\Gamma_q$ содержит все дуги орграфа Γ_q.

Таким образом, $G_{1,q}$ содержит все дуги орграфов $\Gamma_1, \ldots, \Gamma_q$, т. е. орграф $U^{(q)}$ является частью орграфа $G_{1,q}$. Отсюда орграф $U^{(\mu)}$, а следовательно, и $U^{(p)}$ являются частями орграфа $G_{1,\mu} = \Gamma_1^h \ldots \Gamma_{\mu-1}^h \Gamma_\mu$. Из примитивности орграфа $U^{(p)}$ следует примитивность $G_{1,\mu}$ и $\exp G_{1,\mu} \leqslant \exp U^{(p)}$. Орграф $G_{1,\mu}$ является словом в алфавите $\hat{\Gamma}$, следовательно, множество $\hat{\Gamma}$ примитивное и $\exp \hat{\Gamma} \leqslant \big((\mu-1)h+1\big)\exp G_{1,\mu} \leqslant \big((\mu-1)h+1\big)\exp U^{(p)}$. ■

Пример 3. На рис. 1 изображены множества орграфов $\hat{\Gamma} = \{\Gamma_1, \Gamma_2\}$ с множеством вершин $\{0, \ldots, 5\}$. На рис. 1, *а* орграфы имеют общий гамильтонов контур $Z = (0, \ldots, 5)$, на рис. 1, *б* множество общих контуров есть $\hat{C} = \{(0,1,2,3), (0,1), (2,3), (4,5)\}$. Оценки экспонентов и их точные значения приведены в табл. 2.

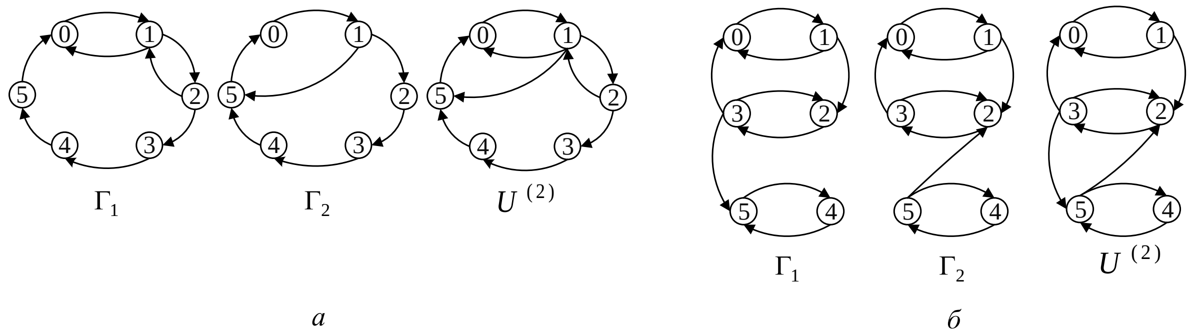

Рис. 1. Множества $\hat{\Gamma} = \{\Gamma_1, \Gamma_2\}$ и соответствующие орграфы $U^{(2)}$

Таблица 2

$\hat{\Gamma}$	Универсальная оценка (1)	Улучшенная оценка (2)	Оценка (3)	Оценка (5)	$\exp\hat{\Gamma}$
а	$\exp\hat{\Gamma} \leqslant 115$	$\exp\hat{\Gamma} \leqslant 73$	$\exp\hat{\Gamma} \leqslant 17$	$\exp\hat{\Gamma} \leqslant 63$	11
б			–	$\exp\hat{\Gamma} \leqslant 21$	8

Заключение

Исследованы условия примитивности и оценки экспонентов множества орграфов с множеством общих контуров, в частности с общим гамильтоновым контуром. Данные классы множеств содержат классы множеств перемешивающих орграфов регистров сдвига, широко используемых для построения систем защиты информации. Получен существенно более простой (по сравнению с общим случаем) критерий примитивности множества орграфов, имеющих семейство общих контуров, содержащих все n вершин, в частности имеющих общий гамильтонов контур.

Критерий примитивности множества орграфов с общим гамильтоновым контуром позволил получить точное значение числа примитивных множеств таких орграфов для примарного числа вершин. В случае когда n — степень числа 2, этот результат имеет прикладное значение для исследования регистровых преобразований.

На примере множеств из двух орграфов с общими контурами показана возможность получения более точных оценок (3) и (5) по сравнению с универсальными оценками (1) и (2). Если общее множество контуров содержит гамильтонов контур, оценка (3) существенно уточняет оценку (5).

ЛИТЕРАТУРА

1. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.
2. *Фомичев В. М., Мельников Д. А.* Криптографические методы защиты информации. Ч. 1. Математические аспекты. М.: Изд-во «ЮРАЙТ», 2016. 209 с.
3. *Frobenius G.* Uber Matrizen aus nicht negativen Elementen // Sitzungsber K. Preuss. Akad. Wiss., 1912. P. 456–477.
4. *Dulmage A. L. and Mendelsohn N. S.* The exponent of a primitive matrix // Canad. Math. Bull. 1962. No. 5. P. 241–244.
5. *Harary F.* Graph Theory. Addison-Wesley Publ., 1969. 275 p.
6. *Perkins P.* A theorem on regular graphs // Pacific J. Math. 1912. V. II. P. 1529–1533.
7. *Протасов Ю. В.* Полугруппы неотрицательных матриц // Успехи математических наук. 2010. Т. 65. Вып. 6(396). С. 191–192.
8. *Cohen J. E. and Sellers P. H.* Sets of nonnegative matrices with positive inhomogeneous products // Linear Algebra Appl. 1982. V. 47. P. 185–192.
9. *Olesky D. D., Shader B., and van den Driessche P.* Exponents of tuples of nonnegative matrices // Linear Algebra Appl. 2002. V. 356. No. 1–3. P. 123–134.
10. *Авезова Я. Э.* О примитивности некоторых множеств перемешивающих орграфов регистровых преобразований // Прикладная дискретная математика. Приложение. 2017. № 10. С. 60–62.
11. *Авезова Я. Э., Фомичев В. М.* Условия примитивности и оценки экспонентов множеств ориентированных графов // Прикладная дискретная математика. 2017. № 35. С. 89–101.
12. *Авезова Я. Э.* Критерий примитивности и оценки экспонентов множества орграфов с общим множеством контуров // Прикладная дискретная математика. Приложение. 2018. № 11. С. 102–104.
13. *Кяжин С. Н.* Весовые свойства примитивных матриц // Прикладная дискретная математика. Приложение. 2018. № 11. С. 10–12.
14. *Protasov V. Yu. and Voynov A. S.* Sets of nonnegative matrices without positive products // Linear Algebra Appl. 2012. V. 437. No. 3. P. 749–765.
15. *Voynov A. S.* Shortest positive products of nonnegative matrices // Linear Algebra Appl. 2013. V. 439. No. 6. P. 1627–1634.
16. *Blondel V. D., Jungers R. M., and Olshevsky A.* On primitivity of sets of matrices // Automatica. 2015. V. 61. P. 80–88.
17. *Фомичев В. М.* Новая универсальная оценка экспонентов графов // Прикладная дискретная математика. 2016. № 3(33). С. 78–84.
18. *Авезова Я. Э., Фомичев В. М.* Комбинаторные свойства систем разноразмерных 0, 1-матриц // Прикладная дискретная математика. 2014. № 2(24). С. 5–11.
19. *Фомичев В. М.* Свойства минимальных примитивных орграфов // Прикладная дискретная математика. 2015. № 2(28). С. 86–96.
20. *Авезова Я. Э., Фомичев В. М.* Об одном наследственном признаке в циклических полугруппах графов // Прикладная дискретная математика. Приложение. 2016. № 9. С. 105–109.

REFERENCES

1. *Fomichev V. M.* Metody diskretnoy matematiki v kriptologii [Methods of Discrete Mathematics in Cryptology]. Moscow, Dialog-MIFI Publ., 2010. 424 p. (in Russian)
2. *Fomichev V. M. and Mel'nikov D. A.* Kriptograficheskie metody zashchity informatsii. Ch. 1. Matematicheskie aspekty [Cryptographic Methods of Information Security. P. 1. Mathematical Aspects]. Moscow, YuRAYT Publ., 2016. 209 p. (in Russian)
3. *Frobenius G.* Uber Matrizen aus nicht negativen Elementen. Sitzungsber K. Preuss. Akad. Wiss., 1912, pp. 456–477.
4. *Dulmage A. L. and Mendelsohn N. S.* The exponent of a primitive matrix. Canad. Math. Bull., 1962, no. 5, pp. 241–244.
5. *Harary F.* Graph Theory. Addison-Wesley Publ., 1969. 275 p.
6. *Perkins P.* A theorem on regular graphs. Pacific J. Math., 1961, vol. II, pp. 1529–1533.
7. *Protasov Yu. V.* Semigroups of non-negative matrices. Russian Math. Surveys, 2010, vol. 65, no. 6, pp. 1186–1188.
8. *Cohen J. E. and Sellers P. H.* Sets of nonnegative matrices with positive inhomogeneous products. Linear Algebra Appl., 1982, vol. 47, pp. 185–192.
9. *Olesky D. D., Shader B., and van den Driessche P.* Exponents of tuples of nonnegative matrices. Linear Algebra Appl., 2002. vol. 356, no. 1–3, pp. 123–134.
10. *Avezova Y. E.* O primitivnosti nekotorykh mnozhestv peremeshivayushchikh orgrafov registrovykh preobrazovaniy [On primitivity of some shift registers mixing digraphs sets]. Prikladnaya Diskretnaya Matematika. Prilozheniye, 2017, no. 10, pp. 60–62. (in Russian)
11. *Avezova Y. E. and Fomichev V. M.* Usloviya primitivnosti i otsenki eksponentov mnozhestv oriyentirovannykh grafov [Conditions of primitivity and exponent bounds for sets of digraphs]. Prikladnaya Diskretnaya Matematika, 2017, no. 35, pp. 89–101. (in Russian)
12. *Avezova Y. E.* Kriteriy primitivnosti i otsenki eksponentov mnozhestva orgrafov s obshchim mnozhestvom konturov [The criterion of primitivity and exponent bounds for a set of digraphs with common cycles]. Prikladnaya Diskretnaya Matematika. Prilozheniye, 2018, no. 11, pp. 102–104. (in Russian)
13. *Kyazhin S. N.* Vesovye svoystva primitivnykh matrits [Weight properties of primitive matrices]. Prikladnaya Diskretnaya Matematika. Prilozheniye, 2018, no. 11, pp. 10–12. (in Russian)
14. *Protasov V. Yu. and Voynov A. S.* Sets of nonnegative matrices without positive products. Linear Algebra Appl., 2012, vol. 437, no. 3, pp. 749–765.
15. *Voynov A. S.* Shortest positive products of nonnegative matrices. Linear Algebra Appl., 2013, vol. 439, no. 6, pp. 1627–1634.
16. *Blondel V. D., Jungers R. M., and Olshevsky A.* On primitivity of sets of matrices. Automatica, 2015, vol. 61. pp. 80–88.
17. *Fomichev V. M.* Novaya universal'naya otsenka eksponentov grafov [The new universal estimation for exponents of graphs]. Prikladnaya Diskretnaya Matematika, 2016, no. 3(33), pp. 78–84. (in Russian)
18. *Avezova Y. E. and Fomichev V. M.* Kombinatornyye svoystva sistem raznorazmernykh 0, 1-matrits [Combinatorial properties of rectangular 0,1-matrix systems]. Prikladnaya Diskretnaya Matematika, 2014, no. 2(24), pp. 5–11. (in Russian)
19. *Fomichev V. M.* Svoystva minimal'nykh primitivnykh orgrafov [Properties of minimal primitive digraphs]. Prikladnaya Diskretnaya Matematika, 2015, no. 2(28), pp. 86–96. (in Russian)

20. *Avezova Y. E. and Fomichev V. M.* Ob odnom nasledstvennom priznake v tsiklicheskikh polugruppakh grafov [About one heritable character in cyclic semigroups of graphs]. Prikladnaya Diskretnaya Matematika. Prilozheniye, 2016, no. 9, pp. 105–109. (in Russian)

УДК 519.17

ОБ УЛУЧШЕННОЙ УНИВЕРСАЛЬНОЙ ОЦЕНКЕ ЭКСПОНЕНТОВ ОРГРАФОВ[1]

В. М. Фомичев

Финансовый университет при Правительстве Российской Федерации, г. Москва, Россия
Национальный исследовательский ядерный университет «МИФИ», г. Москва, Россия
Институт проблем информатики ФИЦ ИУ РАН, г. Москва, Россия

Способ универсальной оценки экспонента n-вершинного примитивного орграфа, предложенный А. Далмэджем и Н. Мендельсоном (1964), сохранял до настоящего времени статус наилучшего среди всех известных универсальных оценок. Этот способ использует множество контуров $\hat{C}$ орграфа, длины которых равны $l_1, \ldots, l_m$, где НОД$(l_1, \ldots, l_m) = 1$, и множество длин кратчайших путей $\{r_{i,j}(\hat{C}) : 1 \leqslant i, j \leqslant n\}$, проходящих из вершины i в вершину j через множество контуров $\hat{C}$. Улучшение этого способа использует множество контуров $\hat{C}$, где НОД$(l_1, \ldots, l_m) = d \geqslant 1$, и множество длин кратчайших путей $\{r_{i,j}^{s/d}(\hat{C}) : s = 0, \ldots, d-1; 1 \leqslant i, j \leqslant n\}$ из вершины i в вершину j, проходящих через множество контуров $\hat{C}$ и образующих полную систему вычетов по модулю d. Доказана оценка $\exp\Gamma \leqslant 1 + \hat{F}(L(\hat{C})) + R(\hat{C})$, где $\hat{F}(L) = d \cdot F(l_1/d, \ldots, l_m/d)$; $F(a_1, \ldots, a_m)$ — число Фробениуса; $R(\hat{C}) = \max\limits_{(i,j)} \max\limits_{s} \{r_{i,j}^{s/d}(\hat{C})\}$. Построен класс орграфов с множеством вершин $\{0, \ldots, 2k-1\}$, $k > 2$, для которых новая оценка принимает значение $2k$ при чётных k и $2k-1$ при нечётных k, в то время как оценка Далмэджа и Мендельсона принимает значение $3k-2$ при чётных k и $3k-3$ при нечётных k.

Ключевые слова: *число Фробениуса, примитивный граф, экспонент орграфа.*

DOI 10.17223/20710410/43/8

ON IMPROVED UNIVERSAL ESTIMATION OF EXPONENTS OF DIGRAPHS

V. M. Fomichev

Financial University under the Government of the Russian Federation, Moscow, Russia
National Research Nuclear University Moscow Engineering Physics Institute, Moscow, Russia
The Institute of Informatics Problems of the Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences, Moscow, Russia

E-mail: fomichev.2016@yandex.ru

An improved formula for universal estimation of exponent is obtained for n-vertex primitive digraphs. A previous formula by A. L. Dulmage and N. S. Mendelsohn (1964) is based on a system $\hat{C}$ of directed circuits $C_1, \ldots, C_m$, which are held in a graph and have lengths $l_1, \ldots, l_m$ with $\gcd(l_1, \ldots, l_m) = 1$. A new formula is based on a similar circuit system $\hat{C}$, where $\gcd(l_1, \ldots, l_m) = d \geqslant 1$. Also, the new formula uses $r_{i,j}^{s/d}(\hat{C})$, that is the length of the shortest path from i to j going through the circuit system $\hat{C}$ and having the length which is comparable to s modulo d, $s = 0, \ldots, d-1$. It is

[1]Работа поддержана грантом РФФИ № 16-01-00226.

shown, that $\exp\Gamma \leqslant 1 + \hat{F}(L(\hat{C})) + R(\hat{C})$, where $\hat{F}(L) = d\cdot F(l_1/d,\ldots,l_m/d)$ and $F(a_1,\ldots,a_m)$ is the Frobenius number, $R(\hat{C}) = \max\limits_{(i,j)}\max\limits_{s}\{r_{i,j}^{s/d}(\hat{C})\}$. For some class of $2k$-vertex primitive digraphs, it is proved, that the improved formula gives the value of estimation $2k$, and the previous formula gives the value of estimation $3k-2$.

Keywords: *the Frobenius number, primitive graph, exponent of graph.*

Введение

Введём основные обозначения:

- $\mathbb{N}$ — множество натуральных чисел, $n \in \mathbb{N}$, $\mathbb{N}_0 = \mathbb{N}\cup\{0\}$;
- НОД$(l_1,\ldots,l_m)$ — наибольший общий делитель натуральных чисел $l_1,\ldots,l_m$;
- $F(l_1,\ldots,l_m)$ — число Фробениуса, где НОД$(l_1,\ldots,l_m) = 1$;
- $M_n^{0,1}$ — множество $0,1$-матриц порядка n;
- $\exp\Gamma$ ($\exp M$) — экспонент орграфа Γ (матрицы M);
- (i,j) — дуга в орграфе, инцидентная вершинам i и j;
- $\operatorname{len} w$ ($\operatorname{len} C$) — длина пути w (контура C), равная числу дуг пути (контура);
- LW — множество длин всех путей из множества путей W;
- $w\cdot w'$ — конкатенация путей w и w', где совпадают последняя вершина пути w и первая вершина пути w'.

К активно разрабатываемым в комбинаторном анализе объектам относятся неотрицательные матрицы, то есть матрицы, все элементы которых суть неотрицательные действительные числа. Свойство неотрицательности матрицы M записывают так: $M \geqslant 0$. Матрицу M, все элементы которой положительные, называют положительной ($M > 0$).

В 1912 г. Ф. Фробениусом [1] был поставлен вопрос для квадратных неотрицательных матриц M: имеются ли положительные матрицы в циклической полугруппе $\langle M\rangle$? Если имеются, то матрицу называют примитивной, в противном случае — непримитивной. Наименьшее натуральное γ, при котором $M^\gamma > 0$, называется экспонентом матрицы M, обозначается $\exp M$. Если матрица M непримитивная, то положим $\exp M = \infty$. В случае примитивной матрицы $M^{\gamma+i} > 0$ при любом $i \in \mathbb{N}$.

Мультипликативная полугруппа всех неотрицательных матриц гомоморфно отображается на полугруппу всех $0,1$-матриц (все элементы суть целые числа 0 или 1) с помощью замены каждого положительного элемента единицей. Этот эпиморфизм согласован со свойством примитивности, то есть прообразом любой примитивной $0,1$-матрицы является класс, состоящий только из примитивных матриц, и прообразом любой непримитивной $0,1$-матрицы — класс, состоящий только из непримитивных матриц. Это свойство позволяет ограничиться исследованием мультипликативных моноидов $M_n^{0,1}$, $n \in \mathbb{N}$, где умножение в $M_n^{0,1}$ выполняется как обычное умножение целочисленных матриц с последующей заменой положительных элементов единицами.

Множество матриц смежности вершин n-вершинных ориентированных графов с петлями совпадает с $M_n^{0,1}$, это позволяет распространить на орграфы понятия примитивности и экспонента, где умножение орграфов определено как умножение бинарных отношений. Известно, что примитивный граф является сильносвязным.

Далее M — матрица смежности вершин орграфа Γ; $\{0,\ldots,n-1\}$ — множество вершин Γ. Связь между графами и неотрицательными матрицами устанавливает хорошо известная теорема теории графов (назовем её основной теоремой): число путей длины t из i в j в графе Γ равно $m_{ij}^{(t)}$, $i,j \in \{1,\ldots,n\}$, где $M^t = \bigl(m_{ij}^{(t)}\bigr)$. Таким образом, примитивность орграфа и величина экспонента определяется свойствами путей в графе, в частности $M > 0$, если и только если орграф Γ полный. Далее используется в основном язык теории графов.

Известные оценки экспонентов матриц и орграфов можно разделить на универсальные и специальные (для частных классов). В данной работе предложена новая формула универсальной оценки экспонента n-вершинного примитивного орграфа, улучшающая известную формулу А. Далмэджа и Н. Мендельсона [2].

1. Известные универсальные оценки экспонентов

Исторические этапы прогресса в развитии оценок экспонентов матриц и графов отражены в [3]. Приведём самые необходимые сведения для иллюстрации происходивших достижений в части улучшения универсальных оценок.

Критерий примитивности орграфа Γ, доказанный в 1961 г. П. Перкинсом [4], определяется множеством его контуров. Обозначим $\hat{C} = \{C_1, \ldots, C_m\}$ множество контуров в Γ длин $l_1, \ldots, l_m$ соответственно, то есть $L(\hat{C}) = \{l_1, \ldots, l_m\}$. Индексом множества контуров $\hat{C}$ назовём число $d = \text{НОД}(l_1, \ldots, l_m)$, обозначается $\operatorname{ind} \hat{C}$. Критерий примитивности орграфа можно сформулировать так: сильносвязный орграф Γ примитивный, если и только если он содержит множество контуров индекса 1.

Универсальная оценка (без доказательства) экспонента n-вершинного примитивного орграфа Γ дана Х. Виландтом [5] в 1950 г.:

$$\exp \Gamma \leqslant n^2 - 2n + 2. \tag{1}$$

Доказательство оценки (1) представлено в [4, 6]. При $n > 1$ описаны n-вершинные орграфы [7, 2] (названные в [7] в честь Виландта), на которых достигается оценка (1). Эти орграфы изоморфны, имеют $n + 1$ дугу и содержат ровно два простых контура длин n и $n - 1$.

В [2] уточнена оценка (1) при известной длине l контура в орграфе:

$$\exp \Gamma \leqslant n + l(n - 2).$$

Формула Далмэджа и Мендельсона для вычисления более точных оценок требует дополнительных определений. Приведём эту формулу и затем усилим её.

Говорят, что «путь проходит через контур», если у пути и контура есть общая вершина. Путь проходит через множество контуров, если он проходит через каждый контур множества.

В орграфе Γ обозначим: $\mathcal{C}$ — множество всех простых контуров орграфа Γ; $\mathcal{C}_d$ — класс всех подмножеств индекса d множества $\mathcal{C}$.

Множество $2^{\mathcal{C}}$ образует решётку относительно теоретико-множественного включения. Единицей решетки является множество $\mathcal{C}$, нулём — пустое множество. Если $\operatorname{ind} \mathcal{C} = d$, то класс $\mathcal{C}_d$ является верхней подполурешеткой решетки $2^{\mathcal{C}}$.

Пусть в орграфе Γ $r_{i,j}(\hat{C})$ — длина кратчайшего пути из i в j, проходящего через множество контуров $\hat{C}$ индекса 1, $r(\hat{C}) = \max\limits_{0 \leqslant i,j \leqslant n-1} r_{i,j}(\hat{C})$, тогда [2]

$$\exp \Gamma \leqslant 1 + F\big(L(\hat{C})\big) + r(\hat{C}), \tag{2}$$

где $F\big(L(\hat{C})\big)$ — число Фробениуса для аргументов $l_1, \ldots, l_m$ (наибольшее целое число, не принадлежащее аддитивной полугруппе $\langle l_1, \ldots, l_m \rangle$). Так как оценка (2) верна для любого множества контуров $\hat{C}$ индекса 1, то [3]

$$\exp \Gamma \leqslant 1 + \min_{\hat{C} \in \mathcal{C}_1} \big\{ F(L(\hat{C})) + r(\hat{C}) \big\}. \tag{3}$$

Технические трудности вычисления оценок (2) и (3) в общем случае состоят в определении числа Фробениуса $F\big(L(\hat{C})\big)$ и величины $r(\hat{C})$. При $m > 2$ для общего вида множества $L(\hat{C})$ не существует формулы числа Фробениуса, выраженной с помощью только арифметических операций над аргументами. Вместе с тем проблема вычисления $F(L(\hat{C}))$ в целом решена, различные алгоритмы и формулы, использующие теоретико-множественные операции, изложены в [8, 9]. Что касается величины $r(\hat{C})$, то получены несколько её оценок через n и числа $l_1, \ldots, l_m$. Например, с использованием (2) получена оценка [10, ч. 1, с. 185]

$$\exp \Gamma \leqslant n(m+1) + F(L(\hat{C})) - l_1 - \ldots - l_m. \tag{4}$$

С учётом структурных свойств множества $\hat{C}$ оценка (4) улучшена [11, с. 80]. Обозначим $\Gamma(\hat{C}) = C_1 \cup \ldots \cup C_m$ — часть орграфа Γ, где $l_1 \leqslant \ldots \leqslant l_m$. Если орграф $\Gamma(\hat{C})$ сильносвязный, то он содержит контур Z, проходящий через множество контуров $\hat{C}$ и проходящий через каждую дугу столько раз, сколько контуров множества $\hat{C}$ содержат эту дугу. Контур Z в общем случае определён неоднозначно и называется квазиэйлеровым $\hat{C}$-контуром, его длина определена однозначно: $\operatorname{len} Z = l_1 + \ldots + l_m$. Пусть орграф $\Gamma(\hat{C})$ имеет компоненты связности $\hat{C}_1, \ldots, \hat{C}_r$, $1 \leqslant r \leqslant m$, содержащие независимые квазиэйлеровы контуры $Z_1, \ldots, Z_r$ длин $\lambda_1, \ldots, \lambda_r$ соответственно. Полагая без ущерба для общности $\lambda_1 \geqslant \ldots \geqslant \lambda_r$, получаем оценку

$$\exp\Gamma \leqslant n(r+1) + F(L(\hat{C})) - \sum_{j=1}^{r}(l_j + (j-1)\lambda_j). \tag{5}$$

В частности, если орграф $\Gamma(\hat{C})$ связный, то

$$\exp \Gamma \leqslant 2n - l_1 + F(L(\hat{C})).$$

Таким образом, (5) следует из (2) и использует наилучшую на сегодняшний день универсальную оценку величины $r(\hat{C})$ для примитивных орграфов.

2. Улучшение универсальной оценки экспонента орграфа

Для улучшения оценки (3) использовано понятие локального экспонента орграфа. Орграф Γ называется (i,j)-примитивным, $0 \leqslant i,j \leqslant n-1$, если при некотором $\gamma \in \mathbb{N}$ для любого $t \geqslant \gamma$ в орграфе Γ имеется путь длины t из вершины i в вершину j. Наименьшее такое γ называется (i,j)-экспонентом орграфа Γ и обозначается (i,j)-$\exp \Gamma$. Примитивный орграф Γ является (i,j)-примитивным для любых $i,j \in \{0,\ldots,n-1\}$ и

$$\exp \Gamma = \max_{(i,j)} (i,j)\text{-}\exp \Gamma.$$

Оценим (i,j)-$\exp \Gamma$ примитивного орграфа Γ. Пусть $w = (i_0, i_1, \ldots, i_t)$ — путь в орграфе Γ, проходящий через множество контуров $\hat{C} = \{C_1, \ldots, C_m\}$. Путь $e(w)$ называется $\hat{C}$-расширением пути w:

$$e(w) = k_{0,1}C_1(i_0)\cdot\ldots\cdot k_{0,m}C_m(i_0)\cdot(i_0,i_1)\cdot k_{1,1}C_1(i_1)\cdot\ldots\cdot(i_{t-1},i_t)k_{t,1}C_1(i_t)\cdot\ldots\cdot k_{t,m}C_m(i_t). \tag{6}$$

Здесь $k_{u,v} = 0$, если вершина i_u не принадлежит контуру C_v, в противном случае $k_{u,v} \in \mathbb{N}_0$, $0 \leqslant u \leqslant t$, $1 \leqslant v \leqslant m$; $kC(j)$ есть k-кратно пройденный из вершины j контур C, если j лежит на контуре C, и есть пустой контур в противном случае. Все дуги пути w являются дугами пути $e(w)$ и порядок их следования в пути $e(w)$ сохраняется. Начальные (и конечные) вершины путей w и $e(w)$ совпадают в силу определения расширения пути.

Обозначим $S+S' = \{s+s' : s \in S, s' \in S'\}$, где $S, S' \subseteq \mathbb{N}$, в частности $r+S = \{r\}+S$ для $r \in \mathbb{N}$; $E(\hat{C}, w)$ — множество всех $\hat{C}$-расширений пути w; $W(i, \hat{C}, j)$ — множество путей из i в j, проходящих через множество контуров $\hat{C}$. Путь w является тривиальным расширением самого себя.

Лемма 1. Пусть $\operatorname{ind}\hat{C} = d \geqslant 1$ и $L(\hat{C}) = \{l_1, \ldots, l_m\}$, тогда:

а) $\operatorname{len} w \equiv \operatorname{len} e(w) \pmod d$ для любого $\hat{C}$-расширения $e(w)$ пути w;

б) $LE(\hat{C}, w) = \{\operatorname{len} w + \langle l_1, \ldots, l_m\rangle\}$, где $\langle l_1, \ldots, l_m\rangle$ — аддитивная полугруппа, порождённая множеством чисел $\{l_1, \ldots, l_m\}$.

Доказательство. Из равенства (6) следует, что

$$\operatorname{len} e(w) - \operatorname{len} w = \sum_{u=0}^{t}\sum_{v=1}^{m} k_{u,v} l_v,$$

где $k_{u,v}$ — кратность прохождения контура длины l_v. Все слагаемые суммы в правой части равенства и, значит, сумма в целом кратны d, то есть сравнение верно.

Если вершина i_u принадлежит контуру C_v, то, варьируя всевозможные целые неотрицательные значения $k_{u,v}$, получаем из последнего равенства выражение для множества $LE(\hat{C}, w)$. ■

Для множества натуральных чисел $L = \{l_1, \ldots, l_m\}$, где НОД$(L) = d$, обозначим $\hat{F}(L)$ число $d \cdot F(l_1/d, \ldots, l_m/d)$. Заметим, что $\hat{F}(L) = F(L)$ при $d = 1$.

Следствие 1. Множество $LE(\hat{C}, w)$ содержит все числа, сравнимые с $\operatorname{len} w$ по модулю d и превышающие $\operatorname{len} w + \hat{F}(L(\hat{C}))$, то есть числа вида $\operatorname{len} w + \hat{F}(L(\hat{C})) + kd$, $k \in \mathbb{N}$.

Доказательство. Следует из определения чисел Фробениуса и чисел $\hat{F}$. ■

Пусть $d \in \mathbb{N}$, $\varnothing \neq Y \subset \mathbb{Z}$. Множество Y, содержащее полную систему вычетов по модулю d, называется d-полным. Любое непустое множество целых чисел является 1-полным.

Лемма 2. Если орграф Γ примитивный, то множество $LW(i, \hat{C}, j)$ является d-полным при любых $i, j \in \mathbb{Z}_n$ и любом множестве контуров $\hat{C}$ индекса $d \geqslant 1$.

Доказательство. В силу примитивности в Γ имеются пути $w_l(i, u)$ из вершины i в вершину u длин $l = \gamma, \gamma+1, \ldots, \gamma+d-1$, где $\gamma = \exp\Gamma$. Так как Γ сильносвязный, то в Γ имеется путь w из u в j, проходящий через множество контуров $\hat{C}$ индекса d. Следовательно, $W = \{w_l(i, u) \cdot w : l = \gamma, \gamma+1, \ldots, \gamma+d-1\}$ есть множество путей из i в j, проходящих через множество контуров $\hat{C}$ индекса d, и множество LW является d-полным. ■

Обозначим $r_{i,j}^{s/d}(\hat{C})$ — длина кратчайшего пути w из i в j, проходящего через множество контуров $\hat{C}$, при условии, что $\operatorname{len} w \equiv s \pmod d$, $s = 0, \ldots, d-1$ (в силу леммы 2 такие пути в Γ имеются); $R_{i,j}(\hat{C}) = \max\{r_{i,j}^{0/d}(\hat{C}), \ldots, r_{i,j}^{d-1/d}(\hat{C})\}$; $R(\hat{C}) = \max\limits_{(i,j)} R_{i,j}(\hat{C})$. Заметим, что $r_{i,j}(\hat{C}) = \min\{r_{i,j}^{0/d}(\hat{C}), \ldots, r_{i,j}^{d-1/d}(\hat{C})\}$.

Теорема 1. Для любого непустого множества контуров $\hat C$ индекса более 1

$$(i,j)\text{-}\exp\Gamma \leqslant 1 + \hat F\big(L(\hat C)\big) + R_{i,j}(\hat C),$$
$$\exp\Gamma \leqslant 1 + \hat F\big(L(\hat C)\big) + R(\hat C).$$

Доказательство. Для множества путей $W(i,\hat C,j)$, где $\mathrm{ind}\hat C = d$, имеем разбиение

$$W(i,\hat C,j) = W_0(i,\hat C,j) \cup \ldots \cup W_{d-1}(i,\hat C,j), \tag{7}$$

где $W_s(i,\hat C,j)$ — множество всех путей из i в j, проходящих через множество контуров $\hat C$, длина которых сравнима с s по модулю d, $s = 0,\ldots,d-1$. По лемме 2 множество $LW(i,\hat C,j)$ является d-полным, значит, в $W_s(i,\hat C,j)$ есть путь w_s длины $r_{i,j}^{s/d}(\hat C)$, и в силу леммы 1 длина любого $\hat C$-расширения пути w_s сравнима с $r_{i,j}^{s/d}(\hat C)$ по модулю d. Наибольшее целое число, сравнимое с s по модулю d и не входящее в LW_s, в силу следствия 1 не превышает $r_{i,j}^{s/d}(\hat C) + \hat F(L(\hat C))$, $s = 0,\ldots,d-1$. Следовательно, в соответствии с разбиением (7) наибольшее натуральное число, не входящее в $LW(i,\hat C,j)$, не превышает $R_{i,j}(\hat C) + \hat F(L(\hat C))$. Отсюда получаем оценки для (i,j)-$\exp\Gamma$ и $\exp\Gamma$. ■

Следствие 2. Для любого примитивного орграфа Γ

$$\exp\Gamma \leqslant 1 + \min_{\varnothing\neq\hat C\subseteq\mathcal C}\big\{\hat F(L(\hat C)) + R(\hat C)\big\}. \tag{8}$$

Доказательство. Следует из (7) для любого непустого множества $\hat C \subseteq \mathcal C$. ■

Замечание 1. Оценка (8) уточняет оценку (3) на множестве примитивных орграфов: если $\mathrm{ind}\,\hat C = 1$ в орграфе Γ, то $F(L(\hat C)) = \hat F(L(\hat C))$, $r(\hat C) = R(\hat C)$, то есть оценки совпадают. Уточнение возможно, если $\mathrm{ind}\,\hat C > 1$.

Покажем, что существует бесконечный класс орграфов, для которого оценки (8) и (3) существенно отличаются.

Теорема 2. Пусть множество вершин орграфа Γ есть $\{0,1,\ldots,2k-1\}$, $k > 1$, множество дуг содержит дуги контуров $C_0 = (k-1, 2k-1)$, $C_1 = (0,\ldots,k-2,2k-1)$, $C_2 = (k-1,\ldots,2k-2)$ и ещё дуги $(k-2,k-1)$ и $(2k-2,2k-1)$ (рис. 1). Тогда для орграфа Γ:

— оценка (3) принимает значение $3k-2$ при чётных k и $3k-3$ при нёчетных k;
— оценка (8) принимает значение $2k$ при чётных k и $2k-1$ при нечётных k.

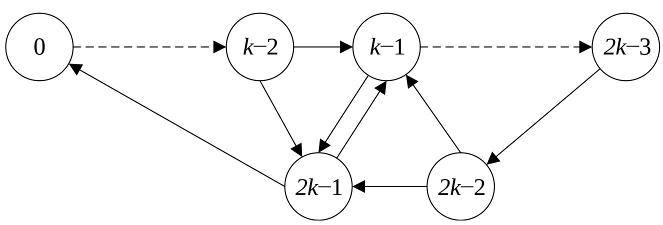

Рис. 1. Орграф Г

Доказательство. По условию множество простых контуров орграфа Γ есть $\mathcal C = \{C_0, C_1, C_2, C_3, C_4, C_5\}$, где $C_3 = (0,\ldots,k-2,k-1,2k-1)$, $C_4 = (k-1,\ldots,2k-2,2k-1)$ и C_5 есть гамильтонов контур $(0,1,\ldots,2k-1)$. Множество длин всех простых контуров есть $L(\mathcal C) = \{2,k,k+1,2k\}$, $\mathrm{ind}\,\mathcal C = 1$.

Пусть $\hat{C} \subseteq \mathcal{C}$. При нечётном k $\operatorname{ind}\hat{C} = 1$, если и только если $\{2,k\} \subseteq L(\hat{C})$ или $\{k,k+1\} \subseteq L(\hat{C})$. Отсюда класс $\mathcal{C}_1$ состоит из 42 множеств: $\{C_0,C_1\}$, $\{C_0,C_2\}$, $\{C_1,C_3\}$, $\{C_1,C_4\}$, $\{C_2,C_3\}$, $\{C_2,C_4\}$, $\{C_0,C_1,C_2\}$, $\{C_0,C_1,C_3\}$, $\{C_0,C_1,C_4\}$, $\{C_0,C_1,C_5\}$, $\{C_0,C_2,C_3\}$, $\{C_0,C_2,C_4\}$, $\{C_0,C_2,C_5\}$, $\{C_1,C_2,C_3\}$, $\{C_1,C_2,C_4\}$, $\{C_1,C_3,C_4\}$, $\{C_1,C_3,C_5\}$, $\{C_1,C_4,C_5\}$, $\{C_2,C_3,C_4\}$, $\{C_2,C_3,C_5\}$, $\{C_2,C_4,C_5\}$, $\{C_0,C_1,C_2,C_3\}$, $\{C_0,C_1,C_2,C_4\}$, $\{C_0,C_1,C_2,C_5\}$, $\{C_0,C_1,C_3,C_4\}$, $\{C_0,C_1,C_3,C_5\}$, $\{C_0,C_1,C_4,C_5\}$, $\{C_0,C_2,C_3,C_4\}$, $\{C_0,C_2,C_3,C_5\}$, $\{C_0,C_2,C_4,C_5\}$, $\{C_0,C_3,C_4,C_5\}$, $\{C_1,C_2,C_3,C_4\}$, $\{C_1,C_2,C_3,C_5\}$, $\{C_1,C_3,C_4,C_5\}$, $\{C_2,C_3,C_4,C_5\}$; $\mathcal{C}\backslash C_r$, $r = 0,\ldots,5$; $\mathcal{C}$.

При чётном k имеем: $\operatorname{ind}\hat{C} = 1$, если и только если $\{2,k+1\} \subseteq L(\hat{C})$ или $\{k,k+1\} \subseteq L(\hat{C})$. Класс $\mathcal{C}_1$ состоит из 42 множеств, полученных из предыдущего списка с помощью взаимной замены $C_1 \leftrightarrow C_3$ и $C_2 \leftrightarrow C_4$.

Покажем, что в орграфе Γ величина $F(L(\hat{C})) + R(\hat{C})$ принимает наименьшее значение при $\hat{C} = \mathcal{C}$. Обозначим через $\rho(i,j)$ длину кратчайшего пути из i в j. Заметим, что

$$\max_{0\leqslant i,j\leqslant 2k-1} \rho(i,j) = \rho(0,2k-2) = \rho(k,k-2) = 2k-2.$$

Кратчайшие пути $w = (0,\ldots,2k-2)$ и $w' = (k,\ldots,k-2)$ суть части гамильтонова контура и проходят через вершины $k-1$ и $2k-1$ соответственно. Значит, через любое множество контуров индекса 1 проходит либо w, либо w'. Отсюда $r(\hat{C}) = 2k-2$ для любого $\hat{C} \in \mathcal{C}_1$.

В силу определения числа Фробениуса $F(L) \leqslant F(L')$ при $\text{НОД}(L') = \text{НОД}(L) = 1$, если $L' \subseteq L$. Следовательно, $F(L(\hat{C})) \geqslant F(L(\mathcal{C})) = F(2,k,k+1,2k)$ для любого множества $\hat{C}$ индекса 1. Отсюда получаем значение оценки (3), так как $F(L(\mathcal{C})) = F(2,k) = k-2$ при нечётных k и $F(L(\mathcal{C})) = F(2,k+1) = k-1$ при чётных k.

Вычислим оценку экспонента (8) с использованием одноэлементного множества контуров $\hat{C}=\{C_0\}$ индекса 2. Оценим величину $R(C_0)=\max\limits_{0\leqslant i,j\leqslant 2k-1} \max\{r_{i,j}^{0/2}(C_0), r_{i,j}^{1/2}(C_0)\}$.

Множество длин путей из $2k-1$ в $2k-2$ является 2-полным. При нечётных k кратчайшие пути w и w', проходящие через контур C_0, длины которых соответственно нечётная и чётная, имеют вид $w = (2k-1,k-1,k,\ldots,2k-2)$, $w' = C_1(2k-1)\cdot w$, где $C_1(2k-1)$ — контур C_1, пройденный из вершины $2k-1$. Отсюда $R(C_0) = R_{2k-1,2k-2}(C_0) = \max\{\operatorname{len} w, \operatorname{len} w'\} = 2k$.

При чётных k кратчайшие пути w и w', проходящие через контур C_0, длины которых соответственно чётная и нечётная, имеют вид $w = (2k-1,k-1,k,\ldots,2k-2)$, $w' = C_3(2k-1)\cdot w$, где $C_3(2k-1)$ — контур C_3, пройденный из вершины $2k-1$. Значит, $R(C_0) = R_{2k-1,2k-2}(C_0) = \max\{\operatorname{len} w, \operatorname{len} w'\} = 2k+1$. Так как $\hat{F}(C_0) = \hat{F}(2) = -2$, то в обоих случаях имеем нужные значения оценки (8). ■

Пример 1. В таблице приведены экспоненты орграфов из теоремы 2 и значения их оценок (3) и (8) при $k = 2,3,4,5,6,7$.

Значения экспонентов и оценок для орграфов из теоремы 2

Число вершин орграфа $2k$	Оценка (3) $\exp\Gamma$	Оценка (8) $\exp\Gamma$ для контура C_0	$\exp\Gamma$
4	4	4	4
6	6	5	5
8	10	8	8
10	12	9	9
12	16	12	11
14	18	13	13

Нерешённая задача: описание множества примитивных n-вершинных орграфов, для которых оценка (3) допускает улучшение типа оценки (8) с использованием множества контуров индекса $d > 1$.

ЛИТЕРАТУРА

1. *Frobenius F. G.* Über Matrizen aus nicht negativen Elementen // Sitzungsber K. Preuss. Akad. Wiss. 1912. P. 456–477.
2. *Dulmage A. L. and Mendelsohn N. S.* Gaps in the exponent set of primitive matrices // Illinoise J. Math. 1964. No. 8. P. 642–656.
3. *Фомичев В. М., Авезова Я. Э., Коренева А. М., Кяжин С. Н.* Примитивность и локальная примитивность орграфов и неотрицательных матриц // Дискретный анализ и исследование операций. 2018. Т. 25. № 3. С. 95–125.
4. *Perkins P.* A theorem on regular graphs // Pacific J. Math. 1961. V. II. P. 1529–1533.
5. *Wielandt H.* Unzerlegbare nicht negative Matrizen // Math. Zeitschr. 1950. No. 52. P. 642–648.
6. *Holladay J. C. and Varga R. S.* On powers of non-negative matrices // Proc. Amer. Math. Soc. 1958. V. IX. P. 631.
7. *Фомичев В. М.* Оценки экспонентов примитивных графов // Прикладная дискретная математика. 2011. № 2(12). С. 101–112.
8. *Фомичев В. М.* О вычислительной сложности оригинальной и расширенной диофантовой проблемы Фробениуса // Дискретный анализ и исследование операций. 2017. Т. 24. № 3. С. 104–124.
9. *Alfonsin J. R.* The Diophantine Frobenius Problem. Oxford: Oxford University Press, 2005.
10. *Фомичев В. М., Мельников Д. А.* Криптографические методы защиты информации. Ч. 1. Математические аспекты. М.: Изд-во «ЮРАЙТ», 2016. 209 с.
11. *Фомичев В. М.* Новая универсальная оценка экспонентов графов // Прикладная дискретная математика. 2016. № 3(33). С. 78–84.

REFERENCES

1. *Frobenius F. G.* Über Matrizen aus nicht negativen Elementen. Sitzungsber K. Preuss. Akad. Wiss., 1912, pp. 456–477.
2. *Dulmage A. L. and Mendelsohn N. S.* Gaps in the exponent set of primitive matrices. Illinoise J. Math., 1964, no. 8, pp. 642–656.
3. *Fomichev V. M., Avezova Y. E., Koreneva A. M., and Kyazhin S. N.* Primitivnost' i lokal'naya primitivnost' orgrafov i neotritsatel'nykh matrits [Primitivity and local primitivity of digraphs and non-Negative matrices]. Diskretnyy Analiz i Issledovanie Operatsiy, 2018, vol. 25, no. 3, pp. 95–125. (in Russian)
4. *Perkins P.* A theorem on regular graphs. Pacific J. Math., 1961, vol. II, pp. 1529–1533.
5. *Wielandt H.* Unzerlegbare nicht negative Matrizen. Math. Zeitschr., 1950, no. 52, pp. 642–648.
6. *Holladay J. C. and Varga R. S.* On powers of non-negative matrices. Proc. Amer. Math. Soc., 1958, vol. IX, pp. 631.
7. *Fomichev V. M.* Otsenki eksponentov primitivnykh grafov [The estimates of exponents for primitive graphs]. Prikladnaya Diskretnaya Matematika, 2011, no. 2(12), pp. 101–112. (in Russian)
8. *Fomichev V. M.* O vychislitel'noy slozhnosti original'noy i rasshirennoy diofantovoy problemy Frobeniusa [Computational complexity of the original and extended Diophantine Frobenius problem]. Diskretnyy Analiz i Issledovanie Operatsiy, 2017, vol. 24, no. 3, pp. 104–124. (in Russian)
9. *Alfonsin J. R.* The Diophantine Frobenius Problem. Oxford, Oxford University Press, 2005.

10. *Fomichev V. M. and Mel'nikov D. A.* Kriptograficheskie metody zashchity informatsii. Ch. 1. Matematicheskie aspekty [Cryptographic Methods of Information Security. P. 1. Mathematical Aspects]. Moscow, YuRAYT Publ., 2016. 209 p. (in Russian)
11. *Fomichev V. M.* Novaya universal'naya otsenka eksponentov grafov [The new universal estimation for exponents of graphs]. Prikladnaya Diskretnaya Matematika, 2016, no. 3(33), pp. 78–84. (in Russian)

СВЕДЕНИЯ ОБ АВТОРАХ

АВЕЗОВА Яна Эдуардовна — ассистент Национального исследовательского ядерного университета «МИФИ», г. Москва. E-mail: **avezovayana@gmail.com**

АЛЕХИНА Марина Анатольевна — доктор физико-математических наук, профессор, заведующая кафедрой математики Пензенского государственного технологического университета, г. Пенза. E-mail: **alekhina@penzgtu.ru**

БЕЛОВ Сергей Алексеевич — аспирант Московского государственного университета имени М. В. Ломоносова, г. Москва. E-mail: **serbel.sci@gmail.com**

БЕСПАЛОВ Михаил Сергеевич — доктор физико-математических наук, доцент, профессор кафедры функционального анализа и его приложений Владимирского государственного университета имени Александра Григорьевича и Николая Григорьевича Столетовых, г. Владимир. E-mail: **bespalov@vlsu.ru**

ГРАБОВСКАЯ Светлана Михайловна — кандидат физико-математических наук, доцент кафедры компьютерных технологий Пензенского государственного университета, г. Пенза. E-mail: **swetazin@mail.ru**

ЗУБОВ Анатолий Юрьевич — кандидат физико-математических наук, доцент, ООО «Центр сертификационных исследований», г. Москва.
E-mail: **zubovanatoly@yandex.ru**

ПОПКОВ Кирилл Андреевич — кандидат физико-математических наук, научный сотрудник Института прикладной математики им. М. В. Келдыша РАН, г. Москва.
E-mail: **kirill-formulist@mail.ru**

ФОМИЧЕВ Владимир Михайлович — доктор физико-математических наук, профессор, профессор Финансового университета при Правительстве Российской Федерации, профессор НИЯУ МИФИ, ведущий научный сотрудник ФИЦ ИУ РАН, г. Москва.
E-mail: **fomichev.2016@yandex.ru**

NASREEN Kausar — Department of Mathematics, Quaid-i-Azam University Islamabad.
E-mail: **kausar.nasreen57@gmail.com**