МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

Научный журнал

2015 № 4(30)

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

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Адрес редакции: 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 22.12.2015.
Формат $60 \times 84\frac{1}{8}$. Усл. п. л. 12,8. Уч.-изд. л. 14,2. Тираж 300 экз. Заказ № 1523.

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

СОДЕРЖАНИЕ

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ

ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

ДИСКРЕТНЫЕ МОДЕЛИ РЕАЛЬНЫХ ПРОЦЕССОВ

CONTENTS

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 512.624

КУСОЧНО-АФФИННЫЕ ПОДСТАНОВКИ КОНЕЧНЫХ ПОЛЕЙ

А. Д. Бугров

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

Определяется множество d-разбиений конечного поля $\mathrm{GF}(q)$. При $d = 2$ и $d = (q-1)/2$ оно полностью описано; при $d < \sqrt{q-1}$ выводится гипотеза о его строении. Приводится критерий на d-разбиение. Определяются кусочно-аффинные подстановки конечных полей. Получены оценка линейной характеристики кусочно-аффинных подстановок конечных полей и точные её значения при $d = 2$. Описаны многочлены, представляющие кусочно-аффинные подстановки. Доказано, что при $d \geqslant \sqrt{q-1}$ класс кусочно-аффинных подстановок образует всю симметрическую группу подстановок конечного поля.

Ключевые слова: *конечные поля, кусочно-линейные подстановки, кусочно-аффинные подстановки, линейная характеристика.*

DOI 10.17223/20710410/30/1

PIECEWISE-AFFINE PERMUTATIONS OF FINITE FIELDS

A. D. Bugrov

Certification Research Center, Moscow, Russia

E-mail: Bugrovalexey1@yandex.ru

Piecewise-affine permutations (p.-a. p.) are defined on any field $\mathrm{GF}(q)$. They are a generalization of piecewise-linear permutations firstly introduced by A. B. Evans. Here some estimates for linear characteristics of p.-a. p. on $\mathrm{GF}(q)$ are given. In some cases, their exact values are pointed. Polynomials representing p.-a. p. are described. Under some conditions on $\sqrt{q-1}$, it is proved that piecewise-affine permutations form the full symmetric group of $\mathrm{GF}(q)$.

Keywords: *finite field, piecewise-linear permutations, piecewise-affine permutations, linear characteristic of permutations.*

Введение

В данной работе рассматривается класс кусочно-аффинных подстановок конечных полей. Он является обобщением класса кусочно-линейных подстановок, впервые предложенного А. Б. Эвансом в работе [1]. А. Е. Тришиным в [2] получены оценки и в некоторых случаях найдены точные значения линейной характеристики кусочно-линейных подстановок поля, имеющего характеристику два.

Основным результатом настоящей работы являются оценки линейной характеристики для кусочно-аффинных подстановок произвольного поля (не обязательно характеристики два). В некоторых случаях для линейной характеристики приводятся точные значения. Кроме того, указываются некоторые свойства семейства всех кусочно-аффинных подстановок, свидетельствующие о том, что этот класс существенно более широкий, чем класс кусочно-линейных подстановок.

Для того чтобы определить кусочно-аффинные подстановки, будем использовать следующие обозначения: $P = \mathrm{GF}(q)$ — конечное поле из q элементов; e — единица поля P; ξ — примитивный элемент поля P; P^* — мультипликативная группа поля P. Пусть d, l — натуральные такие, что $q - 1 = dl$. Тогда $\langle \xi^d \rangle = H < P^*$ — подгруппа порядка l мультипликативной группы. Обозначим через $AGL(1, P)$ группу аффинных преобразований поля P:

$$AGL(1, P) = \{f_{a,b} : P \to P \mid f_{a,b}(x) = ax + b, a \in P^*, b \in P\}.$$

Введём следующее обозначение:

$$H_{a,b} = Ha + b, \quad a, b \in P.$$

Пусть векторы $\mathbf{a} = (a_0, \ldots, a_{d-1}) \in (P^*)^d$ и $\mathbf{b} = (b_0, \ldots, b_d) \in P^{d+1}$ такие, что множества H_{a_i,b_i}, $i \in \{0, \ldots, d-1\}$, попарно не пересекаются. Рассмотрим объединение

$$W = \bigsqcup_{i=0}^{d-1} H_{a_i,b_i} \sqcup \{b_d\},$$

где символ $\sqcup$ обозначает операцию объединения непересекающихся множеств. Если $W = P$, то будем говорить, что упорядоченная пара векторов $(\mathbf{a}, \mathbf{b})$ задает d-разбиение (H-разбиение) поля P. Пусть $R_d(P)$ — множество всех упорядоченных пар, задающих d-разбиения (H-разбиения) поля P:

$$R_d(P) = \left\{ (\mathbf{a}, \mathbf{b}) = ((a_0, a_1, \ldots, a_{d-1}), (b_0, b_1, \ldots, b_d)) \in (P^*)^d \times P^{d+1} : P = \bigsqcup_{i=0}^{d-1} H_{a_i,b_i} \sqcup \{b_d\} \right\}.$$

Заметим, что множество $R_d(P)$ не пусто для всех возможных d и q, так как мультипликативная группа поля P^* либо сама является подгруппой H (в случае $d = 1$) и $(e, (0, 0)) \in R_1(P)$, либо разбивается на смежные классы по подгруппе H:

$$P = P^* \sqcup \{0\} = \bigsqcup_{i=0}^{d-1} H_{\xi^i,0} \sqcup \{0\}, \quad ((e, \xi, \xi^2, \ldots, \xi^{d-1}), (0, 0, \ldots, 0)) \in R_d(P).$$

Разбиение, соответствующее паре $(\mathbf{a}, \mathbf{b}) \in R_d(P)$, будем называть тривиальным, если $b_0 = b_1 = \ldots = b_d$. Пусть $Rl_d(P)$ — множество всех упорядоченных пар векторов, задающих тривиальные d-разбиения:

$$Rl_d(P) = \{(\mathbf{a}, \mathbf{b}) \in R_d(P) : b_0 = b_1 = \ldots = b_d\}.$$

Заметим, что для любой пары $(\mathbf{a}, \mathbf{b}) \in Rl_d(P)$ выполняется следующее свойство: множества $\{H, H\xi, \ldots, H\xi^{d-1}\}$ и $\{Ha_0, Ha_1, \ldots, Ha_{d-1}\}$ совпадают. Таким образом, $Rl_d(P) = \{(\mathbf{a}, \mathbf{b}) \in (P^*)^d \times (P^{d+1}) : b_0 = b_1 = \ldots = b_d \in P, a_{s(i)} = \xi^i, s \in S_d\}$, где S_d — симметрическая группа подстановок множества $\{0, 1, \ldots, d-1\}$.

Кусочно-аффинной подстановкой поля P, соответствующей парам $(\mathbf{a},\mathbf{b}),(\mathbf{c},\mathbf{e}) \in$ $\in R_d(P)$, будем называть отображение

$$\Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{c},\mathbf{e}}(x) = \begin{cases} hc_i + e_i, & \text{если } x = ha_i + b_i \in H_{a_i,b_i},\ i \in \{0,\dots,d-1\}, \\ e_d, & \text{если } x = b_d. \end{cases}$$

В случае, когда $\mathbf{b} = \mathbf{e} = (0,0,\dots,0)$, кусочно-аффинные подстановки будем называть кусочно-линейными.

Введённое определение кусочно-аффинной подстановки корректно (заданное отображение действительно является подстановкой), так как

$$\Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{c},\mathbf{e}}(P) = \Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{c},\mathbf{e}}(\bigsqcup_{i=0}^{d-1} H_{a_i,b_i} \sqcup \{b_d\}) =$$
$$= \bigcup_{i=0}^{d-1} \Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{c},\mathbf{e}}(H_{a_i,b_i}) \cup \Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{c},\mathbf{e}}(b_d) = \bigcup_{i=0}^{d-1} H_{c_i,e_i} \cup \{e_d\} = \bigsqcup_{i=0}^{d-1} H_{c_i,e_i} \sqcup \{e_d\} = P.$$

Для обозначения подстановки $\Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{c},\mathbf{e}}$ будем также использовать запись

$$\Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{c},\mathbf{e}} = \begin{pmatrix} b_d & H_{a_0,b_0} & H_{a_1,b_1} & \dots & H_{a_{d-1},b_{d-1}} \\ e_d & H_{c_0,e_0} & H_{c_1,e_1} & \dots & H_{c_{d-1},e_{d-1}} \end{pmatrix},$$

где ограничение $\Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{c},\mathbf{e}}$ на $H_{a_i,b_i}, i \in \{0,\dots,d-1\}$ выглядит следующим образом:

$$\begin{pmatrix} H_{a_i,b_i} \\ H_{c_i,e_i} \end{pmatrix} = \begin{pmatrix} a_i\xi^0 + b_i & a_i\xi^d + b_i & \dots & a_i\xi^{d(l-1)} + b_i \\ c_i\xi^0 + e_i & c_i\xi^d + e_i & \dots & c_i\xi^{d(l-1)} + e_i \end{pmatrix}.$$

Заметим, что отображение $\omega : ((\mathbf{a},\mathbf{b}),(\mathbf{c},\mathbf{e})) \mapsto \Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{c},\mathbf{e}}$ неинъективно. Например, тождественная подстановка представляется как $\Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{a},\mathbf{b}} = \Delta^{\mathbf{c},\mathbf{e}}_{\mathbf{c},\mathbf{e}}$ для любых $(\mathbf{a},\mathbf{b}),(\mathbf{c},\mathbf{e}) \in$ $\in R_d(P)$.

Множество кусочно-аффинных подстановок, образованных d-разбиениями поля P, будем обозначать $A_d(P)$. Справедливо равенство

$$A_d(P) = \{\Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{c},\mathbf{e}} : (\mathbf{a},\mathbf{b}),(\mathbf{c},\mathbf{e}) \in R_d(P)\}.$$

Множество кусочно-линейных подстановок, образованных d-разбиениями поля P, будем обозначать $L_d(P)$. Таким образом,

$$L_d(P) = \{\Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{c},\mathbf{e}} : (\mathbf{a},\mathbf{b}),(\mathbf{c},\mathbf{e}) \in Rl_d(P), \mathbf{b} = \mathbf{e} = (0,0,\dots,0)\}.$$

1. Некоторые свойства класса кусочно-аффинных подстановок

Утверждение 1.

1) Для любых пар $(\mathbf{a},\mathbf{b}),(\mathbf{c},\mathbf{e}),(\mathbf{f},\mathbf{g})$ из $R_d(P)$ верно равенство

$$\Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{c},\mathbf{e}}\Delta^{\mathbf{c},\mathbf{e}}_{\mathbf{f},\mathbf{g}} = \Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{f},\mathbf{g}}.$$

2) Группа $AGL(1,P)$ аффинных подстановок поля P вложена в множество $A_d(P)$ так, что для любой подстановки $g \in AGL(1,P)$ и любой пары $(\mathbf{a},\mathbf{b}) \in R_d(P)$ найдутся пары $(\mathbf{c},\mathbf{e}),(\mathbf{k},\mathbf{t}) \in R_d(P)$, такие, что $g = \Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{c},\mathbf{e}} = \Delta^{\mathbf{k},\mathbf{t}}_{\mathbf{a},\mathbf{b}}$.

3) Для любой кусочно-аффинной подстановки $\Delta^{\mathbf{a,b}}_{\mathbf{c,e}} \in A_d(P)$ и для любых аффинных преобразований $k, g \in AGL(1,P)$, где $k(x) = \alpha x + \beta$, $g(x) = \gamma x + \lambda$, верно равенство $k\Delta^{\mathbf{a,b}}_{\mathbf{c,e}} g = \Delta^{\mathbf{u,v}}_{\mathbf{f,g}}$, где

$$(\mathbf{u},\mathbf{v})=((\alpha^{-1}a_0,\alpha^{-1}a_1,\dots,\alpha^{-1}a_{d-1}),(\alpha^{-1}b_0-\alpha^{-1}\beta,\alpha^{-1}b_1-\alpha^{-1}\beta,\dots,\alpha^{-1}b_d-\alpha^{-1}\beta)),$$
$$(\mathbf{f},\mathbf{g}) = ((\gamma c_0,\gamma c_1,\dots,\gamma c_{d-1}),(\gamma e_0+\lambda,\gamma e_1+\lambda,\dots,\gamma e_d+\lambda)).$$

4) Если $d_1|d_2$ и $d_2|(q-1)$, то $A_{d_1}(P) \subset A_{d_2}(P)$.

5) Если $\dfrac{q-1}{d} = l \leqslant 2$, то для любого произвольного разбиения $P = \bigsqcup\limits_{i=0}^{d-1} R_i \sqcup \{r\}$, где $|R_i| = l$, $i \in \{0,\dots,d-1\}$, существует пара $(\mathbf{a},\mathbf{b}) \in R_d(P)$, такая, что $H_{a_i,b_i} = R_i$, $b_d = r$ для любого $i \in \{0,\dots,d-1\}$.

6) Если $\dfrac{q-1}{d} = l \leqslant 2$, то $A_d(P) = S(P)$, где $S(P)$ — симметрическая группа подстановок поля P.

7) Если $R_d(P) = Rl_d(P)$, то $A_d(P) = V^+(P)L_d(P)V^+(P)$, где $V^+(P)$ — группа сдвигов поля P.

Доказательство.

1) Пусть $x \in H_{a_i,b_i}$, тогда существует $h \in H$, что $x = ha_i + b_i$. По определению $\Delta^{\mathbf{a,b}}_{\mathbf{c,e}}(x) = hc_i + e_i \in H_{c_i,e_i}$, следовательно, $\Delta^{\mathbf{c,e}}_{\mathbf{f,g}}(hc_i+e_i) = hf_i + g_i$. Если $x = b_d$, то

$$\Delta^{\mathbf{a,b}}_{\mathbf{c,e}}\Delta^{\mathbf{c,e}}_{\mathbf{f,g}}(x) = \Delta^{\mathbf{c,e}}_{\mathbf{f,g}}(e_d) = g_d.$$

2) Если $g(x) = \alpha x + \beta$, где $\alpha \in P^*$, $\beta \in P$, то при $(\mathbf{c},\mathbf{e}) = ((\alpha a_0,\dots,\alpha a_{d-1}),(\alpha b_0 + {}+\beta,\dots,\alpha b_{d-1}+\beta,\alpha b_d+\beta))$ для любых $i \in \{0,\dots,d-1\}$, $h \in H$ имеем

$$\Delta^{\mathbf{a,b}}_{\mathbf{c,e}}(ha_i+b_i) = ha_i\alpha + \alpha b_i + \beta = \alpha(ha_i+b_i)+\beta, \quad \Delta^{\mathbf{a,b}}_{\mathbf{c,e}}(b_d) = \alpha b_d + \beta,$$

то есть $\Delta^{\mathbf{a,b}}_{\mathbf{c,e}}$ действует на P, как и g.

Аналогично при

$$(\mathbf{c},\mathbf{e}) = ((\alpha^{-1}a_0,\dots,\alpha^{-1}a_{d-1}),(\alpha^{-1}b_0-\alpha^{-1}\beta,\dots,\alpha^{-1}b_{d-1}-\alpha^{-1}\beta,\alpha^{-1}b_d-\alpha^{-1}\beta))$$

для любых $i \in \{0,\dots,d-1\}$, $h \in H$ имеем

$$\Delta^{\mathbf{c,e}}_{\mathbf{a,b}}(hc_i+e_i) = ha_i + b_i = \alpha(hc_i+e_i)+\beta, \quad \Delta^{\mathbf{c,e}}_{\mathbf{a,b}}(e_d) = b_d = \alpha e_d + \beta.$$

3) Пусть $F = \Delta^{\mathbf{a,b}}_{\mathbf{c,e}}$, тогда по п. 2 существуют пары $(\mathbf{f},\mathbf{g}),(\mathbf{u},\mathbf{v}) \in R_d(P)$, такие, что $k = \Delta^{\mathbf{u,v}}_{\mathbf{a,b}}, g = \Delta^{\mathbf{c,e}}_{\mathbf{f,g}}$. Из п. 1 следует, что $kFg = \Delta^{\mathbf{u,v}}_{\mathbf{f,g}}$. Заметим, что для любых $i \in \{0,\dots,d-1\}$, $h \in H$

$$kFg(k^{-1}(a_ih+b_i)) = g(c_ih+e_i), \quad kFg(k^{-1}(b_d)) = g(e_d),$$

следовательно,

$$\Delta^{\mathbf{u,v}}_{\mathbf{f,g}}(\alpha^{-1}a_ih+\alpha^{-1}b_0-\alpha^{-1}\beta) = \gamma c_ih+\gamma e_i+\lambda, \quad \Delta^{\mathbf{u,v}}_{\mathbf{f,g}}(\alpha^{-1}b_d-\alpha^{-1}\beta) = \gamma e_d+\lambda.$$

4) Пусть H, G — подгруппы P^*, такие, что $|H| = l_1 = (q-1)/d_1$, $|G| = l_2 = (q-1)/d_2$. Тогда $l_2|l_1$ и $G < H$. Группу H разобьём на смежные классы по подгруппе G:

$$H = \bigsqcup_{j=0}^{d_2/d_1-1} G\xi^{d_1 j}.$$

Зададим отображение $\tau : R_{d_1}(P) \to (P^*)^{d_2} \times P^{d_2+1}$ таким образом, что $\tau(\mathbf{a}, \mathbf{b}) = (\mathbf{c}, \mathbf{e})$, где

$$(\mathbf{a}, \mathbf{b}) = ((a_0, \ldots, a_{d_1-1}), (b_0, \ldots, d_{d_1})),$$
$$(\mathbf{c}, \mathbf{e}) = ((\underbrace{a_0, \xi^{d_1} a_0, \ldots, \xi^{d_2-d_1} a_0}_{d_2/d_1}, \ldots, \underbrace{a_{d_1-1}, \xi^{d_1} a_{d_1-1}, \ldots, \xi^{d_2-d_1} a_{d_1-1}}_{d_2/d_1}),$$
$$(\underbrace{b_0, b_0, \ldots, b_0}_{d_2/d_1}, \ldots, \underbrace{b_{d_1-1}, b_{d_1-1}, \ldots, b_{d_1-1}}_{d_2/d_1}, b_{d_1})).$$

В силу равенств

$$P = \bigsqcup_{i=0}^{d_1-1} H_{a_i,b_i} \sqcup \{b_{d_1}\} = \bigsqcup_{i=0}^{d_1-1} \left(\left(\bigsqcup_{j=0}^{d_2/d_1-1} G\xi^{d_1 j} \right) a_i + b_i \right) \sqcup \{b_{d_1}\} =$$
$$= \bigsqcup_{i=0}^{d_1-1} \left(\bigsqcup_{j=0}^{d_2/d_1-1} G\xi^{jd_1} a_i + b_i \right) \sqcup \{b_{d_1}\} = \bigsqcup_{i=0}^{d_1-1} \left(G_{a_i,b_i} \sqcup G_{\xi^{d_1} a_i,b_i} \sqcup \ldots \sqcup G_{\xi^{d_2-d_1} a_i,b_i} \right) \sqcup \{b_{d_1}\}$$

имеем $(\mathbf{c}, \mathbf{e}) \in R_{d_2}(P)$.

Теперь покажем, что $\Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{u},\mathbf{v}} = \Delta^{\tau(\mathbf{a},\mathbf{b})}_{\tau(\mathbf{u},\mathbf{v})} \in A_{d_2}(P)$ для любой кусочно-аффинной подстановки $\Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{u},\mathbf{v}} \in A_{d_1}(P)$. Выберем любой элемент x поля P. Если он равен b_{d_1}, то

$$\Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{u},\mathbf{v}}(x) = \Delta^{\tau(\mathbf{a},\mathbf{b})}_{\tau(\mathbf{u},\mathbf{v})}(x).$$

Если $x = ha_i + b_i \in H_{a_i,b_i}$, где $h \in H$, $i \in \{0, \ldots, d_1 - 1\}$, то найдутся $g \in G$, $j \in \{0, \ldots, d_2/d_1 - 1\}$, такие, что $h = g\xi^{jd_1}$. Следовательно, $ha_i + b_i = g\xi^{jd_1} a_i + b_i$. Пусть $\tau(\mathbf{a}, \mathbf{b}) = (\mathbf{c}, \mathbf{e})$, $\tau(\mathbf{u}, \mathbf{v}) = (\mathbf{f}, \mathbf{t})$. Заметим, что

$$c_{id_2/d_1+j} = \xi^{jd_1} a_i, f_{id_2/d_1+j} = \xi^{jd_1} u_i,$$

$$e_{id_2/d_1+j} = b_i, t_{id_2/d_1+j} = v_i$$

при всех $i \in \{0, \ldots, d_1 - 1\}$, $j \in \{0, \ldots, d_2/d_1 - 1\}$. Тогда

$$\Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{u},\mathbf{v}}(ha_i + b_i) = hu_i + v_i = g\xi^{jd_1} u_i + v_i =$$
$$= gf_{id_2/d_1+j} + t_{id_2/d_1+j} = \Delta^{\mathbf{c},\mathbf{e}}_{\mathbf{f},\mathbf{t}}(gc_{id_2/d_1+j} + e_{id_2/d_1+j}) = \Delta^{\mathbf{c},\mathbf{e}}_{\mathbf{f},\mathbf{t}}(g\xi^{jd_1} a_i + b_i) = \Delta^{\mathbf{c},\mathbf{e}}_{\mathbf{f},\mathbf{t}}(ha_i + b_i).$$

5) Группа $AGL(1, P)$ 2-транзитивна, значит, для любого множества $R \subset P$ из не более чем двух элементов существуют $a \in P^*$, $b \in P$, такие, что $H_{a,b} = R$.

6) При $l = 1$ доказательство очевидно. Пусть $l = 2$. Выберем любую подстановку $s \in S(P)$, такую, что

$$s = \begin{pmatrix} u_0 & u_1 & \ldots & u_{q-1} \\ v_0 & v_1 & \ldots & v_{q-1} \end{pmatrix}.$$

Тогда из п. 5 следует, что существуют пары $(\mathbf{a}, \mathbf{b}), (\mathbf{c}, \mathbf{e}) \in R_2(P)$, такие, что $H_{a_i,b_i} = \{u_{2i}, u_{2i+1}\}$, $H_{c_i,e_i} = \{v_{2i}, v_{2i+1}\}$, $b_d = u_{q-1}$, $e_d = v_{q-1}$, то есть $s = \Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{c},\mathbf{e}}$.

7) Включение $V^+(P)L_d(P)V^+(P) \subset A_d(P)$ следует из п. 3. Для любых $\Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{c},\mathbf{e}} \in A_d(P)$, $(\mathbf{a}, \mathbf{b}), (\mathbf{c}, \mathbf{e}) \in Rl_d(P)$, $\mathbf{b} = (b, b, \ldots, b), \mathbf{e} = (e, e, \ldots, e)$ из п. 3 и $R_d(P) = Rl_d(P)$ следует равенство

$$\Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{c},\mathbf{e}} = k\Delta^{\mathbf{a},\theta}_{\mathbf{c},\theta} g,$$

где $\theta = (0, 0, \ldots, 0)$; $\Delta^{\mathbf{a},\theta}_{\mathbf{c},\theta} \in L_d(P)$; $k(x) = x - b$; $g(x) = x + e$. ■

Замечание 1. Из условия $d = 2$ следует, что $\mathrm{char}\ P \neq 2$, так как $d|(q-1)$.

Лемма 1. Пусть $d = 2$, $H = \langle \xi^2 \rangle$, $q > 5$. Тогда для любого $b \in P^*$ существуют $a_1, a_2 \in H$ и $a_3, a_4 \in H\xi$, такие, что $a_1 - a_2 = a_3 - a_4 = b$.

Доказательство. Пусть $f : P^n \to P$ — произвольное отображение и

$$N^*(f(x_1, \ldots, x_n) = b) = |\{(a_1, \ldots, a_n) : a_1, \ldots, a_n \in P^*, f(a_1, \ldots, a_n) = b\}|.$$

Если η — квадратичный характер поля P, то получим равенства

$$N^*(x_1^2 - x_2^2 = b) = \sum_{c_1+c_2=b; c_1,c_2 \in P^*} N^*(x_1^2 = c_1) N^*(-x_2^2 = c_2) =$$

$$= \sum_{c_1+c_2=b; c_1,c_2 \in P^*} (1 + \eta(c_1))(1 + \eta(-c_2)) = \sum_{c_1+c_2=b; c_1,c_2 \in P^*} [1 + \eta(-c_2) + \eta(c_1) + \eta(-c_1c_2)] =$$

$$= q - 2 + \sum_{c \notin \{0,b\}} \eta(-c) + \sum_{c \notin \{0,b\}} \eta(c) + \eta(-1) \sum_{c_1+c_2=b; c_1,c_2 \in P^*} \eta(c_1c_2) =$$

$$= q - 2 + \sum_{c \notin \{0,b\}} \eta(-c) + \sum_{c \notin \{0,b\}} \eta(c) + \eta(-1) \sum_{c \notin \{0,b\}} \eta(cb - c^2).$$

Используя равенства $\eta(0) = 0$, $\sum\limits_{c \in P^*} \eta(c) = 0$ (свойство мультипликативных характеров) и $\sum\limits_{c \in P} \eta(cb - c^2) = -\eta(-1)$ [3, теорема 5.48], имеем

$$N^*(x_1^2 - x_2^2 = b) = q - 2 - \eta(-b) - \eta(b) - \eta(-1)\eta(-1) = q - 3 - \eta(-b) - \eta(b).$$

Легко заметить, что при $q > 5$ выполнено $N^*(x_1^2 - x_2^2 = b) > 0$, следовательно, существуют $a_1, a_2 \in H$, такие, что $a_1 - a_2 = b$, для любого $b \in P^*$. Из существования решения уравнения

$$x_1 - x_2 = b, \quad \text{где} \quad x_1, x_2 \in H, \ b \in P^*,$$

следует существование решения уравнения

$$x_1 - x_2 = b, \quad \text{где} \quad x_1, x_2 \in H\xi, \ b \in P^*,$$

и существование $a_1, a_2 \in H\xi$, таких, что $a_1 - a_2 = b$, $b \in P^*$. ■

Лемма 2. Пусть $d = 2$, $q > 5$. Тогда для любого $b \in P^*$ существуют $a_1 \in H$, $a_2 \in H\xi$, такие, что $a_1 - a_2 = b$.

Доказательство. Заметим, что H состоит из всех элементов, являющихся квадратами элементов из P^*, а $H\xi$ состоит из всех ненулевых элементов, не являющихся квадратами. Справедливы следующие соотношения:

$$N^*(x_1^2 - \xi x_2^2 = b) = \sum_{c_1+c_2=b; c_1,c_2 \in P^*} N^*(x_1^2 = c_1) N^*(x_2^2 = -\xi^{-1}c_2) =$$

$$= \sum_{c_1+c_2=b; c_1,c_2 \in P^*} (1 + \eta(c_1))(1 + \eta(-\xi^{-1}c_2)) =$$

$$= \sum_{c_1+c_2=b; c_1,c_2 \in P^*} [1 + \eta(-\xi^{-1}c_2) + \eta(c_1) + \eta(-\xi^{-1}c_1c_2)] =$$

$$= q - 2 + \eta(-\xi^{-1}) \sum_{c \notin \{0,b\}} \eta(c) + \sum_{c \notin \{0,b\}} \eta(c) + \eta(-\xi^{-1}) \sum_{c_1+c_2=b; c_1,c_2 \in P^*} \eta(c_1c_2) =$$

$$= q - 2 + \eta(-\xi^{-1}) \sum_{c \notin \{0,b\}} \eta(c) + \sum_{c \notin \{0,b\}} \eta(c) + \eta(-\xi^{-1}) \sum_{c \notin \{0,b\}} \eta(cb - c^2).$$

Используя равенства $\eta(0) = 0$, $\sum\limits_{c \in P^*} \eta(c) = 0$ (свойство мультипликативных характеров) и $\sum\limits_{c \in P} \eta(cb - c^2) = -\eta(-1)$ [3, теорема 5.48], имеем

$$N^*(x_1^2 - \xi x_2^2 = b) = q - 2 - \eta(-\xi^{-1})\eta(b) - \eta(b) - \eta(-\xi^{-1})\eta(-1) = \\ = q - 2 - \eta(b)(1 + \eta(-\xi^{-1})) - \eta(\xi^{-1}).$$

Легко заметить, что при $q > 5$ выполнено $N^*(x_1^2 - \xi x_2^2 = b) > 0$. ■

Замечание 2. При $q = 3, 5$ леммы 1 и 2 неверны.

Теорема 1. Если $q > 5$, то $R_2(P) = Rl_2(P)$.

Доказательство. Пусть $(\mathbf{a}, \mathbf{b}) = ((a_0, a_1), (b_0, b_1, b_2)) \in R_2(P)$.

1) Если $Ha_0 = Ha_1$, то $b_0 \neq b_1$ (в силу определения $(\mathbf{a}, \mathbf{b})$), и для любых $x \in H_{a_0,b_0}$, $y \in H_{a_1,b_1}$ выполнено

$$x = a_0 h_x + b_0 \neq a_1 h_y + b_1 = y,$$

где $h_x, h_y \in H$. Следовательно, $a_0 h_x - a_1 h_y \neq b_1 - b_0$. Заметим, что $a_0 h_x - a_1 h_y$ пробегает P^* по лемме 1. Значит, $b_1 - b_0 = 0$, и получено противоречие с соотношением $b_0 \neq b_1$.

2) Если $Ha_0 \neq Ha_1$ и $b_0 \neq b_1$, то аналогично случаю 1 получаем противоречие с помощью леммы 2.

Таким образом, если $Ha_0 = Ha_1$, то $(\mathbf{a}, \mathbf{b}) \notin R_2(P)$; если $Ha_0 \neq Ha_1$, то $(\mathbf{a}, \mathbf{b})$ может быть разбиением только в случае $b_0 = b_1 = b_2$. ■

Следствие 1. Если $q > 5$, то выполняется равенство

$$A_2(P) = V^+(P) L_2(P) V^+(P).$$

Если $q = 3, 5$, то выполняется равенство

$$A_2(P) = S(P).$$

Доказательство. Следует из п. 7 утверждения 1. ■

Утверждение 2. Пусть $(\mathbf{a}, \mathbf{b}) \in R_d(P)$ и $x_1^d - x_2^d$ пробегает всю группу P^* при $(x_1, x_2) \in (P^*)^2$, то есть для любого $c \in P^*$ существуют $f, e \in P^*$, такие, что $f^d - e^d = c$. Тогда среди смежных классов $Ha_0, Ha_1, \ldots, Ha_{d-1}$ нет двух одинаковых.

Доказательство. От противного: пусть в наборе $(Ha_0, Ha_1, \ldots, Ha_{d-1})$ есть два одинаковых класса $Ha_i = Ha_k$, $i, k \in \{0, \ldots, d-1\}$, $i \neq k$. Тогда $b_i \neq b_k$ ввиду $(Ha_i + b_i) \cap (Ha_k + b_k) = \varnothing$, из чего получаем противоречие по аналогии с доказательством теоремы 1. ■

Гипотеза 1. Если $d < \sqrt{q-1}$, то есть количество классов в разбиении меньше, чем элементов в одном классе, то $R_d(P)$ состоит только из тривиальных разбиений и выполняется равенство

$$A_d(P) = V^+(P) L_d(P) V^+(P).$$

Замечание 3. Теоретически обоснован случай $q > 5$, $d = 2$. Экспериментально гипотеза подтверждена на малых значениях d и q (см. п. 9).

Следующая теорема даёт способ построения нетривиального d-разбиения.

Теорема 2. Пусть $(l+1)|q$, $h_1, h_2 \in H$, $(\mathbf{a}, \mathbf{b}) \in R_d(P)$, $b_i = b_d$, $i \in \{0, \ldots, d-1\}$. Тогда $((a_0, \ldots, a_{i-1}, a_i h_1, a_{i+1}, \ldots, a_{d-1}), (b_0, \ldots, b_{i-1}, a_i h_2 + b_d, b_{i+1}, \ldots, b_{d-1}, a_i h_2 + b_d))$ — нетривиальное d-разбиение.

Доказательство. Достаточно показать, что

$$H_{a_i,b_d} \sqcup \{b_d\} = H_{a_i h_1, a_i h_2 + b_d} \sqcup \{a_i h_2 + b_d\}.$$

Если $(l+1)|q = p^n$, то $l = p^k - 1$ для некоторого $1 \leqslant k \leqslant n$, а так как $p^k - 1 = l|(q-1) = p^n - 1$, то $k|n$ и $H \cup \{0\}$ — подполе поля P. В частности, $H \cup \{0\}$ замкнуто относительно умножения на h_1 и прибавления h_2. Значит,

$$\begin{gathered} H_{a_i,b_d} \sqcup \{b_d\} = \{H \sqcup \{0\}\}a_i + b_d = \{Hh_1 \sqcup \{0\}\}a_i + b_d = \{Hh_1 + h_2 \sqcup \{h_2\}\}a_i + b_d = \\ = \{H_{h_1,h_2} \sqcup \{h_2\}\}a_i + b_d = H_{a_i h_1, a_i h_2 + b_d} \sqcup \{a_i h_2 + b_d\}. \end{gathered}$$

Теорема доказана. ■

Замечание 4. Данная теорема применима в случае, когда $P = \mathrm{GF}(q)$, где $q = p^n$, имеет собственное подполе, то есть n имеет собственный делитель.

2. Критерий на d-разбиение

Теорема 3. Пусть $2 < q$, $1 < d < q - 1$. Пара векторов

$$(\mathbf{a}, \mathbf{b}) \in (P^*)^d \times P^{d+1}$$

образует d-разбиение тогда и только тогда, когда для любых $i, j \in \{0, \ldots, d-1\}$, $i \neq j$, выполняются следующие условия:

1) $(b_j = b_i) \Rightarrow (\dfrac{a_j}{a_i} \notin H)$;
2) $(b_j \neq b_i) \Rightarrow \left(\dfrac{a_i h - a_j}{b_j - b_i} \notin H \text{ для всех } h \in H\right)$;
3) $b_d = -l \sum\limits_{j=0}^{d-1} b_j$.

Доказательство. Пара векторов $(\mathbf{a}, \mathbf{b})$ задает d-разбиение тогда и только тогда, когда

$$P = \bigsqcup_{i=0}^{d-1} H_{a_i,b_i} \sqcup \{b_d\},$$

то есть для любых $i, j \in \{0, \ldots, d-1\}$, $i \neq j$,

а) $H_{a_i,b_i} \cap H_{a_j,b_j} = \varnothing$;
б) $b_d \notin H_{a_i,b_i}$.

Условие «а» равносильно тому, что для любых $h_1, h_2 \in H$, $i, j \in \{0, \ldots, d-1\}$, $i \neq j$, выполняется неравенство $a_i h_1 + b_i \neq a_j h_2 + b_j$. Пусть $h_1 = h_2 h$, $h \in H$, тогда

$$h_2(a_i h - a_j) \neq b_j - b_i.$$

В итоге «а» равносильно следующим условиям:

$$\left(h_2^{-1} \neq \frac{a_i h - a_j}{b_j - b_i}\right) \Leftrightarrow \left(\frac{a_i h - a_j}{b_j - b_i} \notin H\right) \text{ при } b_i \neq b_j;$$

$$(a_i h - a_j \neq 0) \Leftrightarrow \left(\frac{a_j}{a_i} \in H\right) \text{ при } b_i = b_j.$$

Пункт «б», при условии «а», равносилен тому, что

$$b_d + \sum_{j=0}^{d-1} \sum_{c \in H_{a_j, b_j}} c = 0,$$

так как сумма элементов конечного поля, имеющего мощность, не равную двум, равна нулю. Тогда, пользуясь тем, что сумма элементов любой неединичной подгруппы группы P^* равна нулю, получаем

$$b_d = -\sum_{j=0}^{d-1} \sum_{c \in H_{a_j, b_j}} c = -\sum_{j=0}^{d-1} \sum_{c \in H} (a_j c + b_j) = -\sum_{j=0}^{d-1} a_j \sum_{c \in H} c - \sum_{j=0}^{d-1} |H| b_j = -l \sum_{j=0}^{d-1} b_j,$$

из чего следует утверждение теоремы. ■

3. Близость между дискретными функциями

Определим удобное для наших вычислений понятие близости в случае произвольного поля и сравним его с другими понятиями близости [4, 5].

Пусть $P_0 = \mathrm{GF}(p)$ — простое подполе поля $P = \mathrm{GF}(q)$, $f, g : P_0^n \to P_0$, χ — канонический аддитивный характер поля P_0, задаваемый равенством $\chi(x) = e^{2\pi i \frac{x}{p}}$, $x \in P_0$. Множество всех характеров группы $(P_0, +)$ имеет вид $\{\chi_a : a \in P_0\}$, где $\chi_a(x) = \chi(ax)$, $x \in P_0$, для всех $a \in P_0$. Определим коэффициент кросс-корреляции между функциями f и g равенством

$$C_a(f, g) = \sum_{\mathbf{x} \in P_0^n} \chi_a(f(\mathbf{x}) - g(\mathbf{x})), \quad a \in P_0 \backslash \{0\}.$$

Обозначим

$$C(f, g) = \max_{a \in P_0 \backslash \{0\}} |C_a(f, g)|.$$

Покажем, что $C(f, g) = 0$ тогда и только тогда, когда в множестве $\{f(\mathbf{x}) - g(\mathbf{x}) : \mathbf{x} \in P_0^n\}$ любой элемент из P_0 появляется ровно $\dfrac{|P_0|^n}{|P_0|} = |P_0|^{n-1}$ раз. В обратную сторону утверждение верно в силу равенства $\sum\limits_{c \in P_0} \chi_a(c) = 0$, $a \neq 0$.

Докажем утверждение в прямую сторону. Пусть N — число решений уравнения $f(\mathbf{x}) - g(\mathbf{x}) = b$. Тогда из равенства для любых элементов $c, d \in P_0$

$$\sum_{\chi} \chi(c)\overline{\chi(d)} = \begin{cases} 0, & \text{если } c \neq d, \\ p, & \text{если } c = d, \end{cases}$$

где суммирование осуществляется по всем характерам χ группы $(P_0, +)$, следуют равенства

$$N = \frac{1}{p} \sum_{\mathbf{c} \in P_0^n} \sum_{\chi} \chi(f(\mathbf{c}) - g(\mathbf{c}))\overline{\chi(b)} = p^{n-1} + \frac{1}{p} \sum_{\chi \neq \chi_0} \overline{\chi(b)} \sum_{\mathbf{c} \in P_0^n} \chi(f(\mathbf{c}) - g(\mathbf{c})) = p^{n-1}.$$

В двоичном случае ($P_0 = \{0, 1\}$) имеем

$$C(f, g) = |C_e(f, g)| = \left| \sum_{\mathbf{x} \in \{0,1\}^n} \chi_1(f(\mathbf{x}) - g(\mathbf{x})) \right| = \left| \sum_{\mathbf{x} \in \{0,1\}^n} (-1)^{f(\mathbf{x}) \oplus g(\mathbf{x})} \right|,$$

так как $\chi_1(x) = (-1)^x$ — единственный нетривиальный характер поля GF(2). Чем меньше $C(f,g)$, тем более «различны» функции $f(\mathbf{x})$ и $g(\mathbf{x})$.

Пусть теперь g пробегает всё множество аффинных функций от n переменных над полем P_0, то есть $g(\mathbf{x}) = g(x_1,\ldots,x_n) = a_1x_1 + a_2x_2 + \ldots + a_nx_n + b$, где $a_1,\ldots,a_n,b$ — элементы из P_0. Рассмотрим величину

$$C(f) = \max_g C(f,g) = \max_g \max_{a\in P_0^*} |C_a(f,g)|, \tag{1}$$

которую назовём близостью f к классу всех аффинных функций от n переменных над полем P_0. Вместо функции $g(x) = a_1x_1 + a_2x_2 + \ldots + a_nx_n + b$ достаточно рассмотреть только функции вида $h(x) = a_1x_1 + a_2x_2 + \ldots + a_nx_n$, так как

$$C_a(f,g) = \overline{\chi}_a(b)C_a(f,h), \quad |C_a(f,g)| = |C_a(f,h)|.$$

В работе [4] близость между функциями $f,g : P_0^n \to P_0$ определяется как

$$\delta(f,g) = \frac{p}{p-1}\sum_{y\in P_0}(\mathbf{P}(f-g=y) - 1/p)^2,$$

где вероятность $\mathbf{P}$ определяется при условии, что аргументы функций f и g выбираются случайно и равновероятно. Выразим $\delta(f,g)$ через коэффициенты кросс-корреляции $C_a(f,g)$. Рассмотрим величину

$$N_y(f-g) = |\{\mathbf{x}\in P_0^n : f(\mathbf{x}) - g(\mathbf{x}) = y\}|.$$

Пусть χ_a — аддитивный характер поля P_0. Из равенства

$$\sum_{a\in P_0}\chi_a(x) = \begin{cases} 0, & \text{если } x\neq 0,\\ p, & \text{если } x = 0,\end{cases}$$

следует, что

$$N_y(f-g) = \frac{1}{p}\sum_{\mathbf{x}\in P_0^n}\sum_{a\in P_0}\chi_a(f(\mathbf{x}) - g(\mathbf{x}) - y) = \frac{1}{p}\sum_{a\in P_0}\overline{\chi}_a(y)\sum_{\mathbf{x}\in P_0^n}\chi_a(f(\mathbf{x}) - g(\mathbf{x})) =$$
$$= \frac{1}{p}\sum_{a\in P_0\setminus\{0\}}\overline{\chi}_a(y)C_a(f,g) + p^{n-1}.$$

Тогда

$$P(f-g=y) - 1/p = \frac{N_y(f-g)}{p^n} - \frac{1}{p} =$$
$$= \frac{\dfrac{1}{p}\displaystyle\sum_{a\in P_0^*}\overline{\chi}_a(y)C_a(f,g) + p^{n-1}}{p^n} - \frac{1}{p} = \frac{1}{p^{n+1}}\sum_{a\in P_0^*}\overline{\chi}_a(y)C_a(f,g).$$

С использованием предыдущих равенств получаем

$$\delta(f,g) = \frac{p}{(p-1)p^{2(n+1)}}\sum_{y\in P_0}\left(\sum_{a\in P_0^*}\overline{\chi}_a(y)C_a(f,g)\right)^2 =$$
$$= \frac{p}{(p-1)p^{2(n+1)}}\sum_{y\in P_0}\left(\sum_{a\in P_0^*}\overline{\chi}_a(y)C_a(f,g)\right)\left(\sum_{b\in P_0^*}\overline{\chi}_b(y)C_b(f,g)\right) =$$
$$= \frac{p}{(p-1)p^{2(n+1)}}\sum_{a,b\in P_0^*}C_a(f,g)C_b(f,g)\sum_{y\in P_0}\overline{\chi}_a(y)\overline{\chi}_b(y).$$

Из свойств аддитивных характеров следует, что

$$\sum_{y\in P_0}\overline{\chi}_a(y)\overline{\chi}_b(y)=\begin{cases}0, & \text{если } a+b=0,\\ p & \text{иначе.}\end{cases}$$

Значит,

$$\delta(f,g)=\frac{p^2}{(p-1)p^{2(n+1)}}\sum_{a\in P_0^*}C_a(f,g)C_{-a}(f,g)=\frac{1}{(p-1)p^{2n}}\sum_{a\in P_0^*}|C_a(f,g)|^2.$$

Таким образом, нахождение точных значений коэффициентов кросс-корреляции $C_a(f,g)$ или получение оценок сверху их модулей позволяет соответственно найти величину $\delta(f,g)$ или получить её оценку сверху.

4. Линейная характеристика преобразований конечного поля

Определим линейную характеристику подстановки. Рассмотрим $P=\mathrm{GF}(q)$ — расширение степени n поля $P_0=\mathrm{GF}(p)$, $q=p^n$. Пусть $F: P\to P$, $\alpha_1,\ldots,\alpha_n$ — базис линейного пространства P_{P_0}, $F_1,\ldots,F_n$ — координатные функции отображения F, то есть

$$F(x)=\alpha_1F_1(x)+\ldots+\alpha_nF_n(x)=\alpha_1f_1(x_1,\ldots,x_n)+\ldots+\alpha_nf_n(x_1,\ldots,x_n),$$

где $f_i: P_0^n\to P_0$; $x=\alpha_1x_1+\ldots+\alpha_nx_n$. Введём обозначение

$$C_a^F(\alpha,\beta)=\sum_{x\in P}\chi_a(\alpha x-\beta F(x)),$$

где $\alpha\in P$; $a\in P^*$; $\beta\in P^*$; $\mathrm{Tr}_p^q: P\to P_0$ — функция следа; $\chi_a(y)=e^{2\pi i\frac{\mathrm{Tr}_p^q(ay)}{p}}$ — аддитивный характер поля P. Величину

$$\delta(F)=\max_{\alpha\in P,\beta\in P^*,a\in P_0^*}\left|C_a^F(\alpha,\beta)\right|=\max_{\alpha\in P,\beta\in P^*,a\in P_0^*}\left|\sum_{x\in P}\chi_a(\alpha x-\beta F(x))\right|$$

будем называть линейной характеристикой преобразования F. Пусть $\beta_1,\ldots,\beta_n$ — базис, двойственный к базису $\alpha_1,\ldots,\alpha_n$, то есть такой, что выполнено условие

$$\mathrm{Tr}_p^q(\alpha_i\beta_j)=\begin{cases}0, & \text{если } i\neq j,\\ 1, & \text{если } i=j.\end{cases}$$

Такой базис существует [3]. Пусть элементы $a_1,\ldots,a_n,c_1,\ldots,c_n\in P_0$ такие, что

$$\alpha=\beta_1a_1+\ldots+\beta_na_n,\beta=\beta_1c_1+\ldots+\beta_nc_n,$$

тогда

$$\beta F(x)=\left(\sum_{i=1}^n\beta_ic_i\right)\left(\sum_{j=1}^n\alpha_jf_j(x_1,\ldots,x_n)\right)=\sum_{i,j\in\{1,\ldots,n\}}\alpha_j\beta_if_j(x_1,\ldots,x_n)c_i,$$

$$\alpha x=\left(\sum_{i=1}^n\beta_ia_i\right)\left(\sum_{j=1}^n\alpha_jx_j\right)=\sum_{i,j\in\{1,\ldots,n\}}\alpha_j\beta_ix_ja_i,$$

$$\chi_a(\alpha x-\beta F(x))=\exp\left\{2\pi i\frac{1}{p}\mathrm{Tr}_p^q\left(a(\sum_{i,j\in\{1,\dots,n\}}\alpha_j\beta_i x_j a_i-\sum_{i,j\in\{1,\dots,n\}}\alpha_j\beta_i f_j(x_1,\dots,x_n)c_i)\right)\right\}=$$

$$=\exp\left\{2\pi i\frac{a}{p}\left(\sum_{i,j\in\{1,\dots,n\}}\mathrm{Tr}_p^q(\alpha_j\beta_i x_j a_i)-\sum_{i,j\in\{1,\dots,n\}}\mathrm{Tr}_p^q(\alpha_j\beta_i f_j(x_1,\dots,x_n)c_i)\right)\right\}=$$

$$=\exp\left\{2\pi i\frac{a}{p}\left(\sum_{j\in\{1,\dots,n\}}x_j a_j-\sum_{j\in\{1,\dots,n\}}f_j(x_1,\dots,x_n)c_j\right)\right\}.$$

Отсюда, согласно обозначениям п. 3,

$$\left|C_a^F(\alpha,\beta)\right|=\left|\sum_{\mathbf{x}\in P_0^n}\chi_a\left(\sum_{j=1}^n a_jx_j-\sum_{j=1}^n f_j(x_1,\dots,x_n)c_j\right)\right|=\left|C_a\left(\sum_{j=1}^n a_jx_j,\sum_{j=1}^n f_j(x_1,\dots,x_n)c_j\right)\right|.$$

Значит,

$$\delta(F)=\max_{\alpha\in P,\beta\in P^*,a\in P_0^*}\left|C_a^F(\alpha,\beta)\right)|=$$

$$=\max_{\mathbf{c}\in P_0^n\setminus\{\mathbf{0}\}}\max_{\mathbf{a}\in P_0^n}\max_{a\in P_0^*}\left|C_a\left(\sum_{j\in\{1,\dots,n\}}x_ja_j,\sum_{j\in\{1,\dots,n\}}f_j(x_1,\dots,x_n)c_j\right)\right|.$$

Согласно формуле (1), $\delta(F)=\max\limits_{\mathbf{c}\in P_0^n\setminus\{\mathbf{0}\}}C\left(\sum\limits_j f_j(x_1,\dots,x_n)c_j\right)$. Таким образом, $\delta(F)$ — максимальная близость нетривиальных линейных комбинаций координатных функций преобразования F к классу всех аффинных функций от n переменных над полем P_0. Кроме того, заметим, что при фиксированном $a\in P_0^*$

$$\max_{\alpha\in P,\beta\in P^*}\left|C_a^F(\alpha,\beta)\right|=\max_{\mathbf{c}\in P_0^n\setminus\{\mathbf{0}\}}\max_{\mathbf{a}\in P_0^n}\left|C_a\left(\sum_{j=1}^n x_ja_j-\sum_{j=1}^n f_j(x_1,\dots,x_n)c_j\right)\right|=$$

$$=\max_{\mathbf{c}\in P_0^n\setminus\{\mathbf{0}\}}\max_{\mathbf{a}\in P_0^n}\left|C_e\left(\sum_j ax_ja_j-\sum_j af_j(x_1,\dots,x_n)c_j\right)\right|=$$

$$=\max_{\mathbf{c}\in P_0^n\setminus\{\mathbf{0}\}}\max_{\mathbf{a}\in P_0^n}\left|C_e\left(\sum_j x_ja_j-\sum_j f_j(x_1,\dots,x_n)c_j\right)\right|=\max_{\alpha\in P,\beta\in P^*}\left|C_e^F(\alpha,\beta)\right|.$$

В итоге

$$\delta(F)=\max_{\alpha\in P,\beta\in P^*}\left|C_e^F(\alpha,\beta)\right|.$$

Этой формулой будем пользоваться всюду в дальнейшем. В случае поля чётной характеристики такое определение линейной характеристики используется в работе [2]. В [5] определяется функция согласия, которая отличается от функции δ только нормирующим множителем.

Оценим снизу величину $\delta(F)$, где F — подстановка поля P. Для этого выведем аналог равенства Парсеваля для коэффициентов Уолша — Адамара булевой функции:

$$\sum_{\alpha\in P}\sum_{\beta\in P^*}\left|C_e^F(\alpha,\beta)\right|^2=\sum_{\alpha\in P}\sum_{\beta\in P^*}C_e^F(\alpha,\beta)\overline{C_e^F(\alpha,\beta)}=$$

$$=\sum_{\alpha\in P}\sum_{\beta\in P^*}\left(\sum_{x\in P}\chi(\alpha x+\beta F(x))\right)\left(\sum_{y\in P}\chi(-\alpha y-\beta F(y))\right)=$$

$$=\sum_{x\in P}\sum_{\beta\in P^*}\sum_{y\in P}\chi(\beta(F(x)-F(y)))\sum_{\alpha\in P}\chi(\alpha(x-y))=\sum_{x\in P}\sum_{\beta\in P^*}\sum_{y\in P}\chi(\beta(F(x)-F(y)))q\delta_{x,y},$$

где

$$\delta_{x,y} = \begin{cases} 0, & \text{если } x \neq y, \\ 1, & \text{если } x = y. \end{cases}$$

Значит,

$$\sum_{\alpha\in P}\sum_{\beta\in P^*}\left|C_e^F(\alpha,\beta)\right|^2 = \sum_{x\in P}\sum_{y\in P} q\delta_{x,y}\sum_{\beta\in P^*}\chi(\beta(F(x)-F(y))) =$$
$$= \sum_{x\in P}\sum_{y\in P} q\delta_{x,y}\left(q\delta_{x,y}-1\right) = q^2(q-1).$$

Следовательно,

$$\delta(F) = \max_{\alpha\in P,\beta\in P^*}\left|C_e^F(\alpha,\beta)\right| \geqslant \sqrt{q}.$$

5. Линейная характеристика кусочно-аффинных подстановок

Исследуем некоторые свойства линейной характеристики кусочно-аффинных подстановок. Пусть $P = \mathrm{GF}(q)$, χ — канонический аддитивный характер поля P, определяемый равенством

$$\chi(y) = e^{2\pi i\frac{\mathrm{Tr}(y)}{p}}, y \in P,$$

где $\mathrm{Tr}(y)$ — функция абсолютного следа поля P.

Теорема 4. Пусть $\Delta_{(\mathbf{c},\mathbf{e})}^{(\mathbf{a},\mathbf{b})} = F \in A_d(P)$ и элементы $a_0^{-1}c_0, \ldots, a_{d-1}^{-1}c_{d-1}$ попарно различные. Если для любых $\alpha \in P$, $\beta \in P^*$:

1) среди элементов $\alpha a_j - \beta c_j$, $j \in \{0,\ldots,d-1\}$, нет нулевого, то

$$\left|C_e^F(\alpha,\beta) - \delta_1\right| \leqslant (d-1)\sqrt{q},$$

где

$$\delta_1 = \chi(\alpha b_d - \beta e_d) - \frac{1}{d}\sum_{j=0}^{d-1}\chi(\alpha b_j - \beta e_j);$$

2) среди элементов $\alpha a_j - \beta c_j$, $\alpha \in P$, $\beta \in P^*$, $j \in \{0,\ldots,d-1\}$, есть нулевой $\alpha a_{j_0} + \beta c_{j_0} = 0$, то

$$\left|C_e^F(\alpha,\beta) - \delta_2\right| \leqslant \frac{(d-1)^2}{d}\sqrt{q},$$

где

$$\delta_2 = \chi(\alpha b_d - \beta e_d) - \frac{1}{d}\sum_{j=0}^{d-1}\chi(\alpha b_j - \beta e_j) + \left(l + \frac{1}{d}\right)\chi(\alpha b_{j_0} - \beta e_{j_0}).$$

Доказательство. Для произвольных $\alpha \in P$, $\beta \in P^*$ имеем равенство

$$C_e^F(\alpha,\beta) = \sum_{x\in P}\chi(\alpha x - \beta F(x)).$$

Получим далее

$$C_e^F(\alpha,\beta) = \chi(\alpha b_d - \beta e_d) + \sum_{j=0}^{d-1}\sum_{x\in H_{a_j,b_j}}\chi(\alpha x - \beta((x-b_j){a_j}^{-1}c_j + e_j)) =$$

$$= \chi(\alpha b_d - \beta e_d) + \sum_{j=0}^{d-1}\sum_{x\in H_{a_j,b_j}}\chi(\alpha x - \beta x{a_j}^{-1}c_j - \beta(-b_j{a_j}^{-1}c_j + e_j)) =$$

$$= \chi(\alpha b_d - \beta e_d) + \sum_{j=0}^{d-1}\sum_{x\in H}\chi(\alpha x a_j + \alpha b_j - \beta x c_j - \beta{a_j}^{-1}c_j b_j - \beta(-b_j{a_j}^{-1}c_j + e_j)).$$

Тогда

$$C_e^F(\alpha,\beta)=\chi(\alpha b_d-\beta e_d)+\sum_{j=0}^{d-1}\sum_{x\in H}\chi((\alpha a_j-\beta c_j)x)\chi(\alpha b_j-\beta e_j). \tag{2}$$

Введём обозначение $\gamma_j=\alpha-\beta a_j^{-1}c_j$. Заметим, что по условию теоремы числа $a_0^{-1}c_0$, $\ldots$, $a_{d-1}^{-1}c_{d-1}$ попарно различны. Поэтому при фиксированных элементах $\alpha\in P$, $\beta\in P^*$ элементы $\gamma_0,\ldots,\gamma_{d-1}$ попарно различны и возможен один из двух случаев:

а) $\gamma_j\neq 0$ для всех $j\in\{0,\ldots,d-1\}$ (среди них нет нуля);

б) существует $j_0\in\{0,\ldots,d-1\}$, такой, что $\gamma_{j_0}=0$, и $\gamma_j\neq 0$ для всех $j\in\{0,\ldots,d-1\}\backslash\{j_0\}$ (среди них есть один нуль).

Пусть имеет место случай «а». Воспользуемся разложением аддитивного характера χ по мультипликативным характерам поля P [3]:

$$\chi(y)=\frac{1}{q-1}\sum_{\psi}G(\overline{\psi},\chi)\psi(y),\ y\in P^*,$$

где сумма берётся по всем мультипликативным характерам ψ поля P; $\overline{\psi}$ — характер, сопряжённый для характера ψ; $G(\psi,\chi)$ — сумма Гаусса, определяемая равенством

$$G(\psi,\chi)=\sum_{c\in P^*}\psi(c)\chi(c).$$

Из (2) получим

$$C_e^F(\alpha,\beta)=\chi(\alpha b_d-\beta e_d)+\frac{1}{dl}\sum_{j=0}^{d-1}\chi(\alpha b_j-\beta e_j)\sum_{\psi}G(\overline{\psi},\chi)\psi(\alpha a_j-\beta c_j)\sum_{x\in H}\psi(x).$$

Учитывая равенство

$$\sum_{x\in H}\psi(x)=\begin{cases}|H|, & \text{если } \psi\in\operatorname{Ann}(H),\\ 0, & \text{если } \psi\notin\operatorname{Ann}(H),\end{cases}$$

где $\operatorname{Ann}(H)$ — аннулятор группы $H=\langle\xi^d\rangle$, состоящий из всех мультипликативных характеров ψ поля P, для которых $\psi(\xi^d)=1$, получим

$$C_e^F(\alpha,\beta)=\chi(\alpha b_d-\beta e_d)+\frac{1}{d}\sum_{j=0}^{d-1}\chi(\alpha b_j-\beta e_j)\sum_{\psi\in\operatorname{Ann}(H)}G(\overline{\psi},\chi)\psi(\alpha a_j-\beta c_j).$$

Пусть ψ_0 — тривиальный мультипликативный характер. Тогда, учитывая равенства $dl=q-1$ и $G(\overline{\psi_0},\chi)=-1$, получим

$$\begin{aligned}C_e^F(\alpha,\beta)=\chi(\alpha b_d-\beta e_d)-\frac{1}{d}\sum_{j=0}^{d-1}\chi(\alpha b_j-\beta e_j)+\\ +\frac{1}{d}\sum_{j=0}^{d-1}\chi(\alpha b_j-\beta e_j)\sum_{\psi\in\operatorname{Ann}(H)\backslash\{\psi_0\}}G(\overline{\psi},\chi)\psi(\alpha a_j-\beta c_j).\end{aligned} \tag{3}$$

Учитывая равенства $|\chi(x)|=1$, $|\psi(y)|=1$ для любых $y\in P^*$, $x\in P$; $|\operatorname{Ann}(H)|=d$; $|G(\psi,\chi)|=\sqrt{q}$ для всех $\psi\neq\psi_0$; $\delta_1=\chi(\alpha b_d-\beta e_d)-\frac{1}{d}\sum_{j=0}^{d-1}\chi(\alpha b_j-\beta e_j)$, получим оценку

$$|C_e^F(\alpha,\beta)-\delta_1|\leqslant\frac{1}{d}(d-1)\sqrt{q}d=(d-1)\sqrt{q}. \tag{4}$$

Пусть имеет место случай «б»: $\gamma_{j_0}=0$ для некоторого индекса $j_0\in\{0,\dots,d-1\}$ и $\gamma_j\neq 0$ для всех $j\neq j_0$. Учитывая, что $\chi(0)=1$, из равенства (2) получим

$$C_e^F(\alpha,\beta)=\chi(\alpha b_d-\beta e_d)+\sum_{x\in H}\chi(\alpha b_{j_0}-\beta e_{j_0})+\sum_{j\in\{0,\dots,d-1\}\setminus\{j_0\}}\sum_{x\in H}\chi((\alpha a_j-\beta c_j)x)\chi(\alpha b_j-\beta e_j)=$$
$$=\chi(\alpha b_d-\beta e_d)+\sum_{x\in H}\chi(\alpha b_{j_0}-\beta e_{j_0})+$$
$$+\frac{1}{dl}\sum_{\psi}G(\overline{\psi},\chi)\sum_{j\in\{0,\dots,d-1\}\setminus\{j_0\}}\psi(\alpha a_j-\beta c_j)\chi(\alpha b_j-\beta e_j)\sum_{x\in H}\psi(x)=\chi(\alpha b_d-\beta e_d)+$$
$$+l\chi(\alpha b_{j_0}-\beta e_{j_0})+\frac{1}{d}\sum_{\psi\in\mathrm{Ann}(H)}G(\overline{\psi},\chi)\sum_{j\in\{0,\dots,d-1\}\setminus\{j_0\}}\psi(\alpha a_j-\beta c_j)\chi(\alpha b_j-\beta e_j)=$$
$$=\chi(\alpha b_d-\beta e_d)-\frac{1}{d}\sum_{j\in\{0,\dots,d-1\}\setminus\{j_0\}}\chi(\alpha b_j-\beta e_j)+l\chi(\alpha b_{j_0}-\beta e_{j_0})+ \tag{5}$$
$$+\frac{1}{d}\sum_{\psi\in\mathrm{Ann}(H)\setminus\{\psi_0\}}G(\overline{\psi},\chi)\sum_{j\in\{0,\dots,d-1\}\setminus\{j_0\}}\psi(\alpha a_j-\beta c_j)\chi(\alpha b_j-\beta e_j)=$$
$$=\chi(\alpha b_d-\beta e_d)-\frac{1}{d}\sum_{j\in\{0,\dots,d-1\}}\chi(\alpha b_j-\beta e_j)+\left(l+\frac{1}{d}\right)\chi(\alpha b_{j_0}-\beta e_{j_0})+$$
$$+\frac{1}{d}\sum_{\psi\in\mathrm{Ann}(H)\setminus\{\psi_0\}}G(\overline{\psi},\chi)\sum_{j\in\{0,\dots,d-1\}\setminus\{j_0\}}\psi(\alpha a_j-\beta c_j)\chi(\alpha b_j-\beta e_j).$$

Получаем оценку

$$|C_e^F(\alpha,\beta)-\delta_2|\leqslant\frac{1}{d}(d-1)\sqrt{q}(d-1)=\frac{(d-1)^2}{d}\sqrt{q}. \tag{6}$$

Объединяя (4) и (6), получаем требуемый результат. ■

6. Частные случаи и примеры

Лемма 3. Пусть $F:P\to P$ — произвольное преобразование поля P, $g,h\in$ $\in AGL(1,P)$. Тогда $|C_a^F(\alpha a^{-1},\beta c)|=|C_a^{gFh}(\alpha,\beta)|$.

Доказательство. Пусть $g(x)=ax+b$, $h(x)=cx+e$. Тогда справедливы следующие равенства:

$$C_a^{gFh}(\alpha,\beta)=\sum_{x\in P}\chi_a\left(\alpha x-\beta h(F(g(x)))\right)=$$
$$=\sum_{x\in P}\chi_a\left(\alpha g^{-1}(x)-\beta h(F(x))\right)=\sum_{x\in P}\chi_a\left(\alpha xa^{-1}-\alpha a^{-1}b-\beta cF(x)-\beta e\right)=$$
$$=\sum_{x\in P}\chi_a\left(\alpha a^{-1}x-\beta cF(x)\right)\chi_a\left(-\alpha a^{-1}b-\beta e\right)==\chi_a\left(-\alpha a^{-1}b-\beta e\right)C_a^F(\alpha a^{-1},\beta c).$$

Остаётся заметить, что $|\chi_a(-\alpha a^{-1}b-\beta e)|=1$. ■

Следствие 2. В условиях леммы 3 $\delta(F)=\delta(gFh)$.

Утверждение 3. Пусть $q>9$, $F\in A_2(P)$. Тогда $\delta(F)\in\left\{\dfrac{q\pm\sqrt{q}}{2},\dfrac{\sqrt{q^2+q}}{2},q\right\}$.

Доказательство. Из лемм 1 и 2 следует, что $R_2(P)=Rl_2(P)$ при $q>5$. Из п. 7 утверждения 1 следует $A_2(P)=V^+(P)L_2(P)V^+(P)$. Используя лемму 3, получаем, что для любой подстановки $F=\Delta_{\mathbf{c},\mathbf{e}}^{\mathbf{a},\mathbf{b}}\in A_2(P)$ существует $W=\Delta_{\mathbf{c},\theta}^{\mathbf{a},\theta}$, такая, что

$\delta(F) = \delta(W)$. Пусть $\langle \xi^2 \rangle = H < P^*$ — подгруппа, образованная всеми ненулевыми элементами поля P, возведёнными в квадрат. Заметим, что векторы (Ha_0, Ha_1), (Hc_0, Hc_1), $(H, H\xi)$ совпадают при некоторой перестановке координат. Тогда если $c_0/a_0 = c_1/a_1$, то для любого $h \in Ha_0$ верно $W(h) = hc_0/a_0$, для $h \in Ha_1$ верно $W(h) = hc_1/a_1$ и $W(0) = 0$, то есть W действует так же, как $g(x) = x \cdot c_0/a_0$, следовательно, W — линейная подстановка и $\delta(W) = q$.

Пусть $c_0/a_0 \neq c_1/a_1$. Тогда дословно повторим рассуждения теоремы 4 о значении $\delta(W)$, а именно: если в теореме 4 имеет место случай «а», то воспользуемся равенством (3) и при подстановке известных значений получим

$$C_e^W(\alpha, \beta) = \frac{1}{2}\left(G(\eta, \chi)\eta(\alpha a_0 - \beta c_0) + G(\eta, \chi)\eta(\alpha a_1 - \beta c_1)\right) \in \{\pm G(\eta, \chi), 0\},$$

где η — квадратичный характер. Если имеет место случай «б», то, используя равенство (5), получим

$$C_e^W(\alpha, \beta) = \frac{q}{2} + \frac{1}{2}G(\eta, \chi)\eta(\alpha a_j - \beta c_j), \text{ где } j \in \{0, 1\}.$$

Известно [3], что

$$G(\eta, \chi) = \begin{cases} (-1)^{n-1}\sqrt{q}, & \text{если } p \equiv 1 \pmod 4, \\ (-1)^{n-1} i^n \sqrt{q}, & \text{если } p \equiv 3 \pmod 4. \end{cases}$$

Значит, если $p \equiv 1 \pmod 4$ или $p \equiv 3 \pmod 4$ и при этом $2|n$, то $|C_e^W(\alpha, \beta)| \in \in \left\{\frac{q - \sqrt{q}}{2}, \frac{q + \sqrt{q}}{2}\right\}$; если $p \equiv 3 \pmod 4$ и $2 \not| n$, то $|C_e^W(\alpha, \beta)| = \frac{\sqrt{q^2 + q}}{2}$. Таким образом,

$$|C_e^W(\alpha, \beta)| \in \left\{0, \frac{q - \sqrt{q}}{2}, \frac{q + \sqrt{q}}{2}, \frac{\sqrt{q^2 + q}}{2}, \sqrt{q}\right\}.$$

Заметим, что $\delta(F) \neq 0$, так как при вычислении $\delta(F)$ всегда существуют такие α, β, что имеет место только случай «б» теоремы 4. Если $q > 9$, то $\frac{q - \sqrt{q}}{2} > \sqrt{q}$, и тогда

$$\delta(F) = \begin{cases} \frac{q \pm \sqrt{q}}{2}, & \text{если } (p \equiv 1 \pmod 4) \vee (p \equiv 3 \pmod 4) \wedge 2 \mid n), \\ \frac{\sqrt{q^2 + q}}{2} & \text{иначе.} \end{cases}$$

Утверждение доказано. ■

Пример 1. Рассмотрим подстановку в поле GF(13):

$$(\mathbf{a}, \mathbf{0}) = ((1, 2, 4, 8), (0, 0, 0, 0, 0)) \in Rl_4(\mathrm{GF}(13)),$$

$$(\mathbf{c}, \mathbf{e}) = ((3, 4, 1, 9), (5, 0, 2, 6, 0)) \in R_4(\mathrm{GF}(13)),$$

$$\delta(\Delta_{\mathbf{c},\mathbf{e}}^{\mathbf{a},\mathbf{0}})/q = 6{,}5/13 = 1/2.$$

7. О многочленах, соответствующих кусочно-аффинным подстановкам

Введём обозначение

$$\mathrm{pol}(x) = \sum_{i=0}^{d-1} x^{il} = x^{dl} + x^{(d-1)l} + \ldots + x^{l}.$$

Данный многочлен интересен для кусочных относительно H функций своими значениями:

$$\mathrm{pol}(h) = \begin{cases} d, & \text{если } h \in H, \\ 0 & \text{иначе.} \end{cases}$$

Используя $\mathrm{pol}(x)$, можно составить аналог интерполяционного многочлена Лагранжа для кусочно-аффинных подстановок.

Утверждение 4. Пусть $\Delta_{\mathbf{c},\mathbf{e}}^{\mathbf{a},\mathbf{b}} \in A_d(P)$. Тогда

$$\Delta_{\mathbf{c},\mathbf{e}}^{\mathbf{a},\mathbf{b}}(x) = (1-(x-b_d)^{q-1})e_d + \sum_{i=0}^{d-1} \left((x-b_i)a_i^{-1}c_i + e_i\right) \mathrm{pol}\left((x-b_i)a_i^{-1}\right) d^{-1}.$$

Доказательство. Заметим, что d^{-1} существует, так как d и p — взаимно простые числа. Нетрудно заметить, что $\mathrm{pol}\left((x-b_i)a_i^{-1}\right) d^{-1}$ принимает значение 1 на $Ha_i + b_i$ и 0 на остальных элементах поля P. Корректное отображение b_d в e_d обеспечивает слагаемое $(1-(x-b_d)^{q-1})e_d$. ■

Следствие 3. Для любой подстановки вида $\Delta_{\mathbf{c},\theta}^{\mathbf{a},\theta} \in L_d(P)$ существуют $f_0, \ldots, f_{d-1} \in P$, такие, что

$$\Delta_{\mathbf{c},\theta}^{\mathbf{a},\theta}(x) = x \sum_{i=0}^{d-1} f_i x^{il}.$$

Для любой подстановки вида $\Delta_{\mathbf{c},\mathbf{e}}^{\mathbf{a},\theta} \in A_d(P)$ существуют $f_0, \ldots, f_{d-1}, h_0, \ldots, h_{d-1} \in P$, такие, что

$$\Delta_{\mathbf{c},\mathbf{e}}^{\mathbf{a},\theta}(x) = x \sum_{i=0}^{d-1} f_i x^{il} + \sum_{i=0}^{d-1} h_i x^{il} + (1-x^{q-1})e_d.$$

Утверждение 5. Подстановка, задаваемая многочленом x^s, является кусочно-линейной из $L_d(P)$ тогда и только тогда, когда $l|(s-1)$ и $(s, q-1) = 1$, где $dl = q-1$.

Доказательство. Сразу заметим, что условие $(s, q-1) = 1$ равносильно тому, что x^s задает подстановку в поле $\mathrm{GF}(q)$. Пусть x^s задает подстановку $\Delta_{\mathbf{c},\theta}^{\mathbf{a},\theta} \in L_d(P)$, тогда найдётся $i \in \{0, \ldots, d-1\}$, что $a_i \in H$. Так как $(H, \cdot)$ — группа, x^s отображает блок H в себя так, что $x^s(h) = ha_i^{-1}c_i \in H$ для любого $h \in H$. Значит, $a_i^{-1}c_i \in H$. Заметим, что $x^s(1) = 1$, тогда $a_i^{-1}c_i = 1$. Из равенств $x^s(\xi^d) = \xi^{ds} = \xi^d a_i^{-1}c_i = \xi^d$ следует, что $\xi^{d(s-1)} = 1$, $q-1|d(s-1)$, а значит, $l|(s-1)$.

Пусть $l|(s-1)$, следовательно, $\xi^{ds} = \xi^d$. Достаточно показать, что x^s является кусочно-линейной функцией, то есть $x^s(ha) = hc$ для любого $h \in H$ и некоторых $a, c \in P^*$. Действительно, $x^s(ha) = h^s a^s = ha^s = hc$. ■

8. Группа, образуемая кусочно-аффинными подстановками, и группа кусочно-линейных подстановок

Пусть $G_d(P)$ — группа, порождённая всеми кусочно-аффинными подстановками. Нетрудно заметить, что $L_d(P)$ — группа.

Утверждение 6.

1) $L_d(P)$ имеет две орбиты — P^* и $\{0\}$;
2) пусть $W = \{H, H\xi, \ldots, H\xi^{d-1}\}$, $R \in W$. Тогда $f(R) \in W$ для любой подстановки $f \in L_d(P)$, то есть сохраняется структура смежного класса по подгруппе H;
3) $G_d(P)$ 2-транзитивна;
4) $G_d(P)$ примитивна.

Доказательство. Пункты 1 и 2 очевидны; п. 3 следует из того, что $AGL(1, P)$ 2-транзитивна и лежит в $A_d(P)$; п. 4 непосредственно следует из п. 3. ■

Минимальной степенью группы $G < S(\Omega)$ будем называть число

$$\mu(G) = \min\{|\mathrm{supp}(g)| : g \in G\backslash\{e\}\},$$

где $\mathrm{supp}(g) = \{\alpha \in P : g(\alpha) \neq \alpha\}$.

Приведём формулировку теоремы из работы [6, с. 155].

Теорема 5. Пусть 2-транзитивная группа $G < S_n$ не содержит группу A_n — знакопеременную группу. Тогда имеют место следующие оценки:

1) $\mu(G) > \sqrt{n-1} + 1 \geqslant \sqrt{n}$ для всех n;
2) $\mu(G) \geqslant n/8$ для всех n;
3) $\mu(G) \geqslant n/4$ для всех $n > 216$.

Следствие 4. Пусть $1 < l \leqslant d$, где $l = |H|$. Тогда $G_d(P)$ содержит знакопеременную группу поля P.

Доказательство. Выберем произвольную пару $(\mathbf{a}, \mathbf{b}) \in R_d(P)$. Заметим, что

$$(\mathbf{c}, \mathbf{b}) = ((a_0\xi^d, a_1, \ldots, a_{d-1}), \mathbf{b}) \in R_d(P),$$

так как $H_{a_0,b_0} = H_{a_0\xi^d,b_0}$. Рассмотрим подстановку $g = \Delta^{(\mathbf{a},\mathbf{b})}_{(\mathbf{c},\mathbf{b})}$. Легко видеть, что при $l > 1$

$$\mathrm{supp}(g) = H_{a_0,b_0}.$$

Из того, что $l \leqslant d$, $ld = q - 1$, следует соотношение $l \leqslant \sqrt{q-1}$, то есть

$$\mu(G_d(P)) \leqslant |\mathrm{supp}(g)| = l \leqslant \sqrt{q-1}.$$

Остаётся воспользоваться теоремой 5 и утверждением 6. ■

Следствие 5. Если $1 < l \leqslant d$, то $G_d(P) = S(P)$.

Доказательство. Заметим, что подстановка $g = \Delta^{(\mathbf{a},\mathbf{b})}_{(\mathbf{c},\mathbf{b})}$, определённая в доказательстве следствия 4, является циклом длины l, а именно $g(\xi^{kd}a_0 + b_0) = \xi^{(k+1)d}a_0 + b_0$. Если l чётное, то $g \notin A(P)$, следовательно, $G_d(P) = S(P)$. Пусть l нечётное. Определим подстановку $f = \Delta^{(\mathbf{a},\mathbf{b})}_{(\mathbf{c},\mathbf{b})}$, где $(\mathbf{a}, \mathbf{b}) \in R_d(P)$, $(\mathbf{c}, \mathbf{b}) = ((a_1, a_0, a_2, \ldots, a_{d-1}), (b_1, b_0, b_2, \ldots, b_d)) \in R_d(P)$. Из определения $\Delta^{(\mathbf{a},\mathbf{b})}_{(\mathbf{c},\mathbf{b})}$ следует, что

$$f = (a_0 + b_0, a_1 + b_1)(\xi^d a_0 + b_0, \xi^d a_1 + b_1) \cdots (\xi^{d(l-1)}a_0 + b_0, \xi^{d(l-1)}a_1 + b_1),$$

то есть f — произведение нечётного числа транспозиций. Следовательно, $f \notin A(P)$ и $G_d(P) = S(P)$. ■

9. Результаты эксперимента

В ходе выполнения работы написана программа, выполняющая построение множества $R_d(P)$. При изучении этого множества для малых значений d и q получены следующие результаты:

1) Если $d < l$, то $R_d(P) = Rl_d(P)$. Это подтвердилось на следующих парах (d, q): (3,16), (3,64), (7,64), (3,256), (5,256), (7,512), (3,1024), (11,1024), (2,17), (4,81), (5,81), (8,81), (4,25), (6,37).
2) В случае $d = l$ справедливы два результата: $R_d(P) = Rl_d(P)$ или $R_d(P) = Rl_d(P) \sqcup C_d(P)$, где $C_d(P)$ состоит из пар вида $(\mathbf{a}, \mathbf{b}) = ((\alpha, \alpha, \ldots, \alpha), (b_0, b_1, \ldots, b_d))$. Первое равенство подтвердилось для следующих значений (d, q): (6, 37), (10, 101), (13,197). Второе равенство выполняется при $(d, q) = (4, 17)$.
3) Если $d > l$, то $R_d(P) \neq Rl_d(P)$. Это подтвердилось на следующих парах (d, q): (4,13), (5,16), (6,25), (8, 25), (9,64), (12, 37), (21, 64).

ЛИТЕРАТУРА

1. *Evans A. B.* Orthomorphism Graphs of Groups. Lecture Notes in Mathematics. Berlin: Springer Verlag, 1992. 114 p.
2. *Тришин А. Е.* О показателе нелинейности кусочно-линейных подстановок аддитивной группы поля F_{2^n} // Прикладная дискретная математика. 2015. № 4(30). С. 32–42
3. *Лидл Р., Нидеррайтер Г.* Конечные поля: в 2-х т.: пер. с. англ. М.: Мир, 1988. 822 с.
4. *Солодовников В. И.* О совпадении класса бент-функций с классом функций, минимально близких к линейным // Прикладная дискретная математика. 2012. № 3(17). С. 25–33.
5. *Кузьмин А. С., Марков В. Т., Нечаев А. А. и др.* Бент-функции и гипербент-функции над полем из 2^l элементов // Проблемы передачи информации. 2008. Т. 44. № 1. С. 15–37.
6. *Dixon J. and Mortimer B.* Permutation Groups. Berlin; N. Y.: Springer Verlag, 1996. 346 p.

REFERENCES

1. *Evans A. B.* Orthomorphism Graphs of Groups. Lecture Notes in Mathematics, Berlin, Springer Verlag, 1992. 114 p.
2. *Trishin A. E.* O pokazatele nelineynosti kusochno-lineynykh podstanovok additivnoy gruppy polya F_{2^n} [The nonlinearity index is a piecewise-linear substitution of the additive group of the field F_{2^n}]. Prikladnaya diskretnaya matematika, 2015, no. 4(30), pp. 32–42 (in Russian)
3. *Lidl R., Niderrayter G.* Konechnye polya [Finite Fields]. Moscow, Mir Publ., 1988, vol. 1, 2. 822 p. (in Russian)
4. *Solodovnikov V. I.* O sovpadenii klassa bent-funktsiy s klassom funktsiy, minimal'no blizkikh k lineynym [On the coincidence of the class of bent-functions with the class of functions which are minimally close to linear functions]. Prikladnaya diskretnaya matematika, 2012, no. 3(17), pp. 25–33. (in Russian)
5. *Kuz'min A. S., Markov V. T., Nechaev A. A., et al.* Bent and hyper-bent functions over a field of 2^l elements. Problems of Information Transmission, 2008, vol. 44, no. 1, pp. 12–33.
6. *Dixon J. and Mortimer B.* Permutation Groups. Berlin, N. Y., Springer Verlag, 1996. 346 p.

УДК 519.7

О СЛОЖНОСТИ СХЕМ В БАЗИСАХ, СОДЕРЖАЩИХ МОНОТОННЫЕ ЭЛЕМЕНТЫ С НУЛЕВЫМИ ВЕСАМИ[1]

В. В. Кочергин*, А. В. Михайлович**

*Московский государственный университет им. М. В. Ломоносова,
**Национальный исследовательский университет «Высшая школа экономики»,
г. Москва, Россия

Исследуется сложность реализации булевых функций и систем булевых функций схемами в базисе, состоящем из элементов двух сортов. Элементами первого сорта являются произвольные монотонные функции, таким элементам приписан нулевой вес. Конечное число немонотонных функций образует непустое множество элементов второго сорта, каждой такой функции приписан положительный вес. Для случая, когда отрицание является единственным элементом второго сорта, А. А. Марковым в 1957 г. показано, что минимальное число немонотонных элементов, достаточное для реализации функции f, равно $\lceil \log_2(d(f)+1) \rceil$, где $d(f)$ — максимальное число переключений значений функции f с 1 на 0 (максимум берётся по всем возрастающим цепям наборов значений переменных). В работе установлено, что в общем случае сложность реализации булевой функции f равна $\rho\lceil \log_2(d(f)+1) \rceil - \mathrm{O}(1)$, где ρ — минимальный вес немонотонных элементов базиса. Получено также аналогичное обобщение классического результата А. А. Маркова о сложности реализации систем булевых функций.

Ключевые слова: *булевы схемы, схемы из функциональных элементов, базисы с нулевыми весами, сложность булевых функций, схемная сложность, инверсионная сложность, теорема Маркова.*

DOI 10.17223/20710410/30/2

ON THE COMPLEXITY OF CIRCUITS IN BASES CONTAINING MONOTONE ELEMENTS WITH ZERO WEIGHTS

V. V. Kochergin*, A. V. Mikhailovich**

*Lomonosov Moscow State University,
**National Research University Higher School of Economics,
Moscow, Russia

E-mail: vvkoch@yandex.ru, anna@mikhaylovich.com

Complexity of Boolean functions and Boolean function systems realization in a base consisting of all monotone functions and a finite number of non-monotone functions is researched. The weight of any monotone function in the base is supposed to be 0, the weight of non-monotone function in it is positive. A. A. Markov studied special case of this base, where the non-monotone part consisted of the negation function. He showed that the minimum number of negation elements which are needed to realize

[1]Исследование (№ 14-01-0144) выполнено при поддержке Программы «Научный фонд НИУ ВШЭ» в 2014–2015 гг. Работа первого автора выполнена при частичной финансовой поддержке РФФИ, проект № 14-01-00598.

an arbitrary function f equals $\lceil \log_2(d(f)+1) \rceil$. Here $d(f)$ is the maximum number of value changes from 1 to 0 over all increasing chains of arguments tuples. The aim of this paper is to prove that the complexity of a Boolean function f realization equals $\rho\lceil \log_2(d(f)+1) \rceil - \mathrm{O}(1)$, where ρ is the minimum weight of non-monotone elements in the base. Similar generalization of the classical Markov's result concerning the realization of Boolean function systems is obtained too.

Keywords: *Boolean circuits, logic circuits, bases with zero weight elements, Boolean function complexity, circuit complexity, inversion complexity, Markov's theorem.*

Введение

При построении логических схем (схем из функциональных элементов) [1, 2], а также формул (называемых также суперпозициями или схемами без ветвления выходов элементов) над конечными и бесконечными системами базисные элементы могут иметь разные сложностные характеристики, определяющие преимущество одних элементов над другими, причём эта разница может быть столь большой, что можно считать веса некоторых элементов нулевыми. Такой подход даёт возможность выявить более выпукло роль элементов того или иного типа при реализации заданных функций или систем функций. Таким образом, возникает задача о синтезе схем в вырожденных базисах, а именно требуется найти минимальное число элементов (сумму весов) некоторых сортов (положительной части базиса), необходимое для реализации произвольной булевой функции или системы функций с использованием произвольного числа элементов других сортов (нулевой части базиса). Исторически наибольший интерес вызывала задача о сложности реализации функций схемами и формулами в базисе, нулевая часть которых порождает множество всех монотонных булевых функций, а положительная часть состоит из отрицания. Первые результаты относительно этой меры сложности, которую принято называть инверсионной сложностью, получил Э. Н. Гилберт [3]. Позднее А. А. Марков установил [4, 5] точные формулы для инверсионной сложности произвольной булевой функции и произвольной системы булевых функций при реализации схемами. Точное значение инверсионной сложности любой булевой функции при реализации формулами было найдено Э. И. Нечипоруком [6] (им же установлены экспоненциального вида асимптотики роста функций Шеннона [1] сложности схем и формул в некоторых других базисах, содержащих элементы с нулевыми весами [6 – 8]). В настоящей работе исследуется сложность реализации булевых функций и систем функций в базисах, нулевая часть которых состоит из всех монотонных функций (или, что то же самое, из какого-либо порождающего множества класса монотонных функций), а ненулевая часть — произвольное конечное множество немонотонных функций. Для произвольной системы булевых функций значение сложности её реализации в базисе такого типа установлено с точностью до аддитивной константы, зависящей только от базиса. Предварительный вариант настоящей работы можно найти в [9].

1. Определения, известные результаты и некоторые наблюдения

Чтобы дать точные формулировки упомянутых результатов, а также основного утверждения настоящей работы, введём необходимые понятия.

Обозначим множество $\{0, 1\}$ через E_2. Последовательность

$$\tilde{\alpha}_1 = (\alpha_{11}, \ldots, \alpha_{1n}),\ \tilde{\alpha}_2 = (\alpha_{21}, \ldots, \alpha_{2n}),\ \ldots,\ \tilde{\alpha}_r = (\alpha_{r1}, \ldots, \alpha_{rn})$$

наборов из множества E_2^n назовём *возрастающей цепью* или просто *цепью*, если все наборы $\tilde{\alpha}_1, \tilde{\alpha}_2, \ldots, \tilde{\alpha}_r$ различны и выполняются неравенства

$$\alpha_{ij} \leqslant \alpha_{i+1,j}, \quad i = 1, \ldots, r-1, \quad j = 1, \ldots, n.$$

Наборы $\tilde{\alpha}_1$ и $\tilde{\alpha}_r$ будем называть *началом* и *концом* этой цепи соответственно.

Пусть $f(x_1, \ldots, x_n)$ — булева функция. Упорядоченную пару наборов $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$ и $\tilde{\beta} = (\beta_1, \ldots, \beta_n)$, $\tilde{\alpha}, \tilde{\beta} \in E_2^n$, будем называть *обрывом для функции* f, если выполнены следующие условия:

1) $\alpha_j \leqslant \beta_j$, $j = 1, \ldots, n$;

2) $f(\tilde{\alpha}) > f(\tilde{\beta})$.

Обрывом для системы функций будем называть любую пару наборов, являющуюся обрывом хотя бы для одной функции системы.

Пусть $F = \{f_1, \ldots, f_m\}$, $m \geqslant 1$, — система булевых функций от переменных $x_1, \ldots x_n$, а C — цепь, имеющая вид

$$\tilde{\alpha}_1, \tilde{\alpha}_2, \ldots, \tilde{\alpha}_r.$$

Под *падением* $d_C(F)$ *системы* F *на цепи* C будем понимать число обрывов для системы F на парах вида $(\tilde{\alpha}_i, \tilde{\alpha}_{i+1})$.

Спад $d(F)$ системы F определим равенством $d(F) = \max d_C(F)$, где максимум берётся по всем цепям C.

Пусть P_2 — множество всех булевых функций, M — класс всех монотонных функций из P_2. Будем исследовать сложность реализации булевых функций и систем функций в базисах B следующего вида:

$$B = M \cup \{\omega_1, \ldots, \omega_p\}, \quad \omega_i \in P_2 \setminus M, \ i = 1, \ldots, p,$$

причём функциям из множества M приписан нулевой вес, а функциям $\omega_1, \ldots, \omega_p$ — положительные веса $\rho_1, \ldots, \rho_p$ соответственно. В дальнейшем, если не оговорено иное, будем под базисом понимать базис такого вида.

Для сложности над базисом B схемы S, функции f и системы функций F будем использовать обозначения $I_B(S)$, $I_B(f)$ и $I_B(F)$.

Исчерпывающее описание сложности булевых функций и систем функций в базисе $B_0 = M \cup \{\overline{x}\}$ (т. е. инверсионной сложности) было получено А. А. Марковым [4, 5]: для любой системы F булевых функций в предположении, что вес инвертора равен единице, установлено равенство

$$I_{B_0}(F) = \lceil \log_2(d(F) + 1) \rceil .$$

Для случая реализации в базисе B_0 булевых функций схемами без ветвления выходов элементов (формулами) окончательное решение получено Э. И. Нечипоруком [6]. Им показано, что минимальное число отрицаний, достаточное для вычисления формулами произвольной булевой функции f, равно $d(f)$ (стоит сказать, что этот результат спустя почти полвека был «переоткрыт» в [10]).

Отметим также работы [11–15], в которых рассматривались близкие задачи.

Переходя к изучению сложности реализации функций в произвольном базисе B описанного вида, заметим, что в силу того факта, что из любой немонотонной функции путём подстановки констант (являющихся монотонными функциями) можно получить

отрицание, теоремы Маркова дают такую верхнюю оценку сложности произвольной системы F булевых функций:

$$I_B(F) \leqslant \rho_B \lceil \log_2(d(F)+1) \rceil ,$$

где $\rho_B = \min\limits_i \rho_i$.

Если в базисе B для всех i, $1 \leqslant i \leqslant p$, выполняются равенства $d(\omega_i) = 1$, то для сложности в таком базисе справедлива точно такая же нижняя оценка:

$$I_B(F) \geqslant \rho_B \lceil \log_2(d(F)+1) \rceil .$$

Для её доказательства можно использовать с минимальными изменениями вариант из [16] доказательства нижней оценки теоремы Маркова.

Если же в базисе, в котором все немонотонные функции имеют единичный вес, есть хотя бы одна немонотонная функция ω_j, удовлетворяющая условию $d(\omega_j) > 1$, то такое равенство становится, вообще говоря, неверным. Действительно, с одной стороны, очевидно равенство $I_B(\omega_j) = 1$, а с другой стороны, выполняется соотношение $\lceil \log_2(d(\omega_j)+1) \rceil \geqslant 2$. Кроме того, в этом случае сложность системы булевых функций уже может определяться не только значением спада этой системы. В качестве примера достаточно взять в некотором смысле самый простой базис, содержащий немонотонную функцию, имеющую падение более единицы: $B_2 = M \cup \{x \oplus y \oplus z \oplus 1\}$. Тогда для систем $F_1 = \{x \oplus y \oplus z \oplus 1\}$ и $F_2 = \{\overline{x}, \overline{y}\}$ имеем

$$d(F_1) = d(F_2) = 2, \qquad I_{B_2}(F_1) = 1, \quad I_{B_2}(F_2) = 2.$$

Для доказательства последнего равенства достаточно учесть тот факт, что никакая функция от двух переменнных не может иметь падение более единицы.

Однако при переходе от базиса B_0 к произвольному базису B, несмотря на указанные изменения даже в простейших случаях и на кажущееся значительное увеличение «инверсионнной силы» базиса, качественных изменений роста инверсионной сложности (с ростом значения спада системы) не происходит. В установлении этого факта и заключается основной результат работы.

2. Формулировка основного результата и его доказательство

Теорема 1. Для любого базиса B, имеющего вид

$$B = M \cup \{\omega_1, \ldots, \omega_p\}, \quad \omega_i \in P_2 \setminus M, \ i = 1, \ldots, p,$$

где все монотонные функции имеют нулевой вес, а функции $\omega_1, \ldots, \omega_p$ — положительные веса $\rho_1, \ldots, \rho_p$ соответственно, найдётся такая константа $c(B)$, что для любой системы F булевых функций справедливы неравенства

$$\rho_B \lceil \log_2(d(F)+1) \rceil - c(B) \leqslant I_B(F) \leqslant \rho_B \lceil \log_2(d(F)+1) \rceil ,$$

где $\rho_B = \min\{\rho_1, \ldots, \rho_p\}$.

Верхняя оценка, как уже говорилось, следует из верхней оценки теоремы Маркова и того факта, что из любой немонотонной функции путём подстановки констант можно получить отрицание.

Переходя к доказательству нижней оценки, для произвольной схемы S в базисе B обозначим число немонотонных элементов в этой схеме через $I_B^1(S)$. Величина $I_B^1(S)$ численно равна сложности схемы S как схемы в базисе, отличающемся от базиса B только тем, что все немонотонные элементы имеют вес 1.

Положим $r(B) = \max\{d(\omega_1), \ldots, d(\omega_p)\}$.

Лемма 1. Для любой схемы S справедливо неравенство

$$d(F_S) \leqslant (2r(B)+1)\left(2^{I_B^1(S)}-1\right),$$

где F_S — реализуемая схемой S система булевых функций.

Доказательство. Проведём индукцию по $I_B^1(S)$.

Если $I_B^1(S)=0$, то все функции системы F_S монотонны. Следовательно, $d(F_S)=0$.

Пусть для любой схемы S', такой, что $I_B^1(S') \leqslant I_B^1(S)-1$, утверждение леммы выполняется.

В схеме S со входами $x_1,\ldots,x_n$ выделим первую (относительно некоторой правильной нумерации) вершину, которой приписана какая-либо функция из множества $\{\omega_1,\ldots,\omega_p\}$, и функциональный элемент, соответствующий этой вершине, обозначим через E. Пусть на выходе элемента E реализуется функция $h(x_1,\ldots,x_n)$. Преобразуем схему S, удалив из неё элемент E и создав вместо него ещё один вход схемы, на который подадим переменную y. Полученная таким перестроением схема S' реализует систему функций $G=\{g_1,\ldots,g_m\}$, причём выполняются следующие условия:

$$f_i(x_1,\ldots,x_n) = g_i\left(h(x_1,\ldots,x_n),x_1,\ldots,x_n\right), \quad i=1,\ldots,m.$$

Кроме того, справедливо равенство $I_B^1(S')=I_B^1(S)-1$.

Пусть цепь $C=(\tilde\alpha_1,\tilde\alpha_2,\ldots,\tilde\alpha_r)$ удовлетворяет условию $d_C(F)=d(F)$. Рассмотрим последовательность C' наборов длины $n+1$:

$$C'=(h(\tilde\alpha_1),\tilde\alpha_1),\ldots,(h(\tilde\alpha_r),\tilde\alpha_r).$$

Последовательность C', вообще говоря, не является цепью. В силу неравенства $d(h) \leqslant r(B)$ первые разряды в наборах последовательности C' меняют своё значение не более $2r(B)+1$ раз. Обозначим через C'_1 подпоследовательность последовательности C', включающую в себя все наборы из C', начинающиеся с нуля, а через C'_2 — подпоследовательность последовательности C', включающую в себя все наборы из C', начинающиеся с единицы. Каждая из последовательностей наборов C'_j, $j=1,2$, является цепью наборов длины $n+1$.

По предположению индукции для j, $j=1,2$, выполняются соотношения

$$d_{C'_j}(G) \leqslant d(G) \leqslant (2r(B)+1)\left(2^{I_B^1(S')}-1\right) = (2r(B)+1)\left(2^{I_B^1(S)-1}-1\right).$$

Теперь, учитывая, что справедливы равенства

$$f_i(x_1,\ldots,x_n) = g_i\left(h(x_1,\ldots,x_n),x_1,\ldots,x_n\right), \quad i=1,\ldots,m,$$

получаем

$$\begin{gathered} d(F)=d_C(F) \leqslant d_{C'_1}(G)+d_{C'_2}(G)+2r(B)+1 \leqslant \\ \leqslant (2r(B)+1)\left(2(2^{I_B^1(S')}-1)+1\right) = (2r(B)+1)\left(2^{I_B^1(S)}-1\right). \end{gathered}$$

Лемма 1 доказана. ■

Положим $c(B)=\rho_B\big(\log_2(2r(B)+1)+1\big)$.

Лемма 2. Для любой системы F булевых функций справедливо неравенство

$$I_B(F) \geqslant \rho_B\lceil\log_2(d(F)+1)\rceil - c(B).$$

Доказательство. Для любой схемы S, реализующей систему функций F, в силу леммы 1 справедлива оценка

$$2^{I_B^1(S)} - 1 \geqslant \frac{d(F)}{2r(B)+1}.$$

Следовательно,

$$I_B^1(S) \geqslant \log_2\left(\frac{d(F)}{2r(B)+1}+1\right) \geqslant \log_2 \frac{d(F)+1}{2r(B)+1} = \log_2(d(F)+1) - \log_2(2r(B)+1) \geqslant$$
$$\geqslant \lceil \log_2(d(F)+1)\rceil - (\log_2(2r(B)+1)+1)\,.$$

Таким образом, любая схема, реализующая систему F в базисе B, содержит не менее $\lceil \log_2(d(F)+1)\rceil - (\log_2(2r(B)+1)+1)$ немонотонных элементов. Учитывая, что вес любого немонотонного элемента не менее ρ_B, получаем

$$I_B(F) \geqslant \rho_B\big(\lceil \log_2(d(F)+1)\rceil - (\log_2(2r(B)+1)+1)\big) = \rho_B\lceil \log_2(d(F)+1)\rceil - c(B).$$

Лемма 2 доказана. ■

Лемма 2 завершает доказательство теоремы.

Замечание 1. Оценка из леммы 1 является достаточно грубой. Более аккуратные рассуждения дают возможность уменьшить значение величины $c(B)$ из теоремы 1.

Замечание 2. Можно подобрать базис B, все немонотонные функции которого имеют вес 1, и функцию f так, что величина $\lceil \log_2(d(f)+1)\rceil - I_B(f)$ будет больше любого наперёд заданного значения. Действительно, при $n \geqslant 2$ в базисе $B_{l_n} = M \cup \{x_1 \oplus \oplus \ldots \oplus x_n\}$, где все монотонные функции имеют нулевой вес, а функция $l_n = x_1 \oplus \ldots \oplus \oplus\, x_n$ — единичный, выполняются равенства

$$\lceil \log_2(d(l_n)+1)\rceil - I_{B_{l_n}}(l_n) = \left\lceil \log_2\left(\left\lfloor \frac{n}{2}\right\rfloor + 1\right)\right\rceil - 1 = \lfloor \log_2(n+1)\rfloor - 1.$$

Таким образом, константа $c(B)$ из теоремы 1 не может быть абсолютной, не зависящей от базиса, даже если вес всех немонотонных элементов базиса равен единице.

Замечание 3. Оценки из теоремы 1 не изменятся, если в нулевой части базиса множество всех монотонных функций заменить на какое-либо порождающее множество класса монотонных функций, например на множество $\{x\&y, x \vee y, 0, 1\}$.

Следующая теорема является следствием теоремы 1 и трёх простых фактов: 1) из функции, не сохраняющей 0, отождествлением переменных получается либо константа 1, либо отрицание; 2) из функции, не сохраняющей 1, отождествлением переменных получается либо константа 0, либо отрицание; 3) из немонотонной функции подстановкой констант можно получить отрицание.

Теорема 2. Для любого полного базиса B, имеющего вид

$$B = \{x\&y, x \vee y, \omega_1, \ldots, \omega_p\}, \quad \omega_i \in P_2 \setminus M,\ i = 1, \ldots, p,$$

где конъюнкция и дизъюнкция имеют нулевой вес, а функции $\omega_1, \ldots, \omega_p$ — единичный, найдётся такая константа $c(B)$, что для любой системы F булевых функций справедливы неравенства

$$\lceil \log_2(d(F)+1)\rceil - c(B) \leqslant I_B(F) \leqslant \lceil \log_2(d(F)+1)\rceil + 2.$$

Замечание 4. В силу того, что из функции, сохраняющей 1, но не сохраняющей 0, отождествлением переменных получается константа 1, а из немонотонной функции, сохраняющей 0, но не сохраняющей 1, подстановкой константы 1 и отождествлением переменных можно получить отрицание, следует, что в условиях теоремы 2 для любой системы функций F, отличной от системы $\{0, 1\}$ (состоящей из двух констант), верхнюю оценку можно усилить:

$$I_B(F) \leqslant \lceil \log_2(d(F) + 1) \rceil + 1.$$

В случае реализации системы $\{0, 1\}$ такое усиление не имеет места, например, для базиса, в котором к функциям $x\&y$ и $x \vee y$ нулевого веса добавлены функции $x \oplus y$ и $x \oplus y \oplus 1$ единичного веса.

ЛИТЕРАТУРА

1. *Лупанов О. Б.* Асимптотические оценки сложности управляющих систем. М.: Изд-во МГУ, 1984.
2. *Сэвидж Д. Е.* Сложность вычислений. М.: Факториал, 1998.
3. *Гилберт Э. Н.* Теоретико-структурные свойства замыкающих переключательных функций // Кибернетический сборник. Вып. 1. М.: ИЛ, 1960. С. 175–188.
4. *Марков А. А.* Об инверсионной сложности систем функций // Докл. АН СССР. 1957. Т. 116. № 6. С. 917–919.
5. *Марков А. А.* Об инверсионной сложности систем булевых функций // Докл. АН СССР. 1963. Т 150. № 3. С. 477–479.
6. *Нечипорук Э. И.* О сложности схем в некоторых базисах, содержащих нетривиальные элементы с нулевыми весами // Проблемы кибернетики. Вып. 8. М.: Физматгиз, 1962. С. 123–160.
7. *Нечипорук Э. И.* О сложности схем в некоторых базисах, содержащих нетривиальные элементы с нулевыми весами // Докл. АН СССР. 1961. Т. 139. № 6. С. 1302–1303.
8. *Нечипорук Э. И.* О сложности суперпозиций в базисах, содержащих нетривиальные линейные формулы с нулевыми весами // Докл. АН СССР. 1961. Т. 136. № 3. С. 560–563.
9. *Kochergin V. V. and Mikhailovich A. V.* Some extensions of the inversion complexity of Boolean functions. Cornell University Library, 2015. `http://arxiv.org/abs/1506.04485`.
10. *Morizumi H.* Limiting negations in formulas // LNCS. 2009. V. 5555. P. 701–712.
11. *Fischer M. J.* The complexity of negation-limited networks — a brief survey // LNCS. 1975. V. 33. P. 71–82.
12. *Tanaka K., Nishino T., and Beals R.* Negation-limited circuit complexity of symmetric functions // Inf. Proc. Lett. 1996. V. 59. No. 5. P. 273–279.
13. *Sung S. and Tanaka K.* Limiting negations in bounded-depth circuits: an extension of Markovs theorem // LNCS. 2003. V. 2906. P. 108–116.
14. *Morizumi H. and Suzuki G.* Negation-limited inverters of linear size // IEICE Trans. Inform. and Systems. 2011. V. E93-D. No. 2. P. 257–262.
15. *Guo S., Malkin T., Oliveira I. C., and Rosen A.* The power of negations in cryptography // LNCS. 2015. V. 9014. P. 36–65.
16. *Jukna S.* Boolean Function Complexity. Advances and Frontiers. Berlin; Heidelberg: Springer, 2012. 620 p.

REFERENCES

1. *Lupanov O. B.* Asimptoticheskie otsenki slozhnosti upravlyayushchikh sistem [Asymptotic Estimations of Complexity of Control Systems]. Moscow, MSU Publ., 1984. (in Russian)

2. *Savage J. E.* The Complexity of Computing. N. Y., Wiley, 1976.
3. *Gilbert E. N.* Lattice theoretic properties of frontal switching functions. J. Math. Phys., 1954, no. 33, pp. 56–67.
4. *Markov A. A.* On the inversion complexity of systems of functions. J. ACM, 1958, vol. 5, no. 4, pp. 331–334.
5. *Markov A. A.* On the inversion complexity of systems of Boolean functions. Soviet Math. Dokl., 1963, no. 4, pp. 694–696.
6. *Nechiporuk E. I.* O slozhnosti skhem v nekotorykh bazisakh, soderzhashchikh netrivial'nye elementy s nulevymi vesami [On the complexity of schemes in some bases containing nontrivial elements with zero weights]. Problemy Kibernetiki, vyp. 8. Moscow, Fizmatgiz Publ., 1962, pp. 123–160. (in Russian)
7. *Nechiporuk E. I.* Complexity of schemes in certain bases containing nontrivial elements with zero weights. Soviet Math. Dokl., 1961, no. 2, pp. 1087–1088.
8. *Nechiporuk E. I.* Complexity of superpositions in bases that contain nontrivial linear formulas with zero weights. Soviet Physics. Dokl., 1961, vol. 6, no. 1, pp. 6–9.
9. *Kochergin V. V. and Mikhailovich A. V.* Some extensions of the inversion complexity of Boolean functions. Cornell University Library, 2015. `http://arxiv.org/abs/1506.04485`.
10. *Morizumi H.* Limiting negations in formulas. LNCS, 2009, vol. 5555, pp. 701–712.
11. *Fischer M. J.* The complexity of negation-limited networks — a brief survey. LNCS, 1975, vol. 33, pp. 71–82.
12. *Tanaka K., Nishino T., and Beals R.* Negation-limited circuit complexity of symmetric functions. Inf. Proc. Lett., 1996, vol. 59, no. 5, pp. 273–279.
13. *Sung S. and Tanaka K.* Limiting negations in bounded-depth circuits: an extension of Markovs theorem. LNCS, 2003, vol. 2906, pp. 108–116.
14. *Morizumi H. and Suzuki G.* Negation-limited inverters of linear size. IEICE Trans. Inform. and Systems, 2011, vol. E93-D, no. 2, pp. 257–262.
15. *Guo S., Malkin T., Oliveira I. C., and Rosen A.* The power of negations in cryptography. LNCS, 2015, vol. 9014, pp. 36–65.
16. *Jukna S.* Boolean Function Complexity. Advances and Frontiers. Berlin, Heidelberg, Springer, 2012. 620 p.

УДК 512.624

О ПОКАЗАТЕЛЕ НЕЛИНЕЙНОСТИ КУСОЧНО-ЛИНЕЙНЫХ ПОДСТАНОВОК АДДИТИВНОЙ ГРУППЫ ПОЛЯ $\mathbb{F}_{2^n}$

А. Е. Тришин

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

Получена нижняя оценка показателя нелинейности подстановок поля $\mathbb{F}_{2^n}$, ограничения которых на смежные классы группы $\mathbb{F}_{2^n}^*$ по её подгруппе H, $|H| = l$, $l \cdot r = 2^n - 1$, являются отображениями вида $x \mapsto A_j x$, $A_j \in \mathbb{F}_{2^n}^*$, $j = 0, \ldots, r-1$. В случаях $r = 3, 5$ найден спектр значений показателя нелинейности подстановок данного вида.

Ключевые слова: *кусочно-линейная функция, подстановка конечного поля, показатель нелинейности.*

DOI 10.17223/20710410/30/3

THE NONLINEARITY INDEX FOR A PIECEWISE-LINEAR SUBSTITUTION OF THE ADDITIVE GROUP OF THE FIELD $\mathbb{F}_{2^n}$

A. E. Trishin

Certification Research Center, Moscow, Russia

E-mail: Trishin17@yandex.ru

In this paper, we give a lower bound on the nonlinearity of permutations on a field $\mathbb{F}_{2^n}$ with restrictions to cosets of H in $\mathbb{F}_{2^n}^*$, $H < \mathbb{F}_{2^n}^*$, $|H| = l$, $l \cdot r = 2^n - 1$, being the maps $x \mapsto A_j x$, $A_j \in \mathbb{F}_{2^n}^*$, $j = 0, \ldots, r-1$. Nonlinearity spectra of this permutations are found in the cases $r = 3, 5$.

Keywords: *piecewise-linear function, permutation of a finite field, nonlinearity.*

Введение

Для натурального числа n введём обозначения: $V_n = \mathbb{F}_2^n$; (x, y) — стандартное скалярное произведение векторов $x, y \in V_n$.

Напомним некоторые определения [1].

Преобразованием Уолша — Адамара булевой функции $f : V_n \to \mathbb{F}_2$ называется целочисленная функция $W_f : V_n \to \mathbb{R}$, определяемая равенством

$$W_f(a) = \sum_{x \in V_n} (-1)^{f(x)+(a,x)} \text{ для всех } a \in V_n.$$

Здесь суммирование производится в действительной области, при этом считается, что $(-1)^0 = 1$, $(-1)^1 = -1$. Для каждого $a \in V_n$ значение $W_f(a)$ называется коэффициентом Уолша — Адамара функции f. Иногда используется термин «коэффициент Уолша — Адамара второго рода».

Нелинейностью N_f булевой функции $f : V_n \to \mathbb{F}_2$ называется расстояние по Хэммингу между функцией f и множеством всех аффинных функций $\mathcal{A}_n = \{f :$

$V_n \to \mathrm{GF}(2) : \deg f \leqslant 1\}$. Здесь через $\deg f$ обозначена алгебраическая степень функции f, равная степени её многочлена Жегалкина. Известно выражение нелинейности N_f через коэффициенты Уолша — Адамара функции f:

$$N_f = 2^{n-1} - \frac{1}{2} \max_{a \in V_n} |W_f(a)| .$$

Напомним, что любое отображение $F : V_n \to V_m$ задаётся набором координатных функций $(f_1, \ldots, f_m)$, таких, что

$$F(x) = (f_1(x), \ldots, f_m(x)) \text{ для всех } x \in V_n.$$

В этом случае пишут $F = (f_1, \ldots, f_m)$.

Нелинейностью или показателем нелинейности [2] отображения F называется число N_F, определяемое равенством

$$N_F = \min_{\beta \in V_m \setminus \{0\}} N_{\beta F},$$

где $\beta F = \beta_1 f_1 + \ldots + \beta_m f_m$ для произвольного вектора $\beta \in V_m$ и $F = (f_1, \ldots, f_m)$. Выражение показателя нелинейности N_F через коэффициенты Уолша — Адамара координатных функций $f_1, \ldots, f_m$ имеет вид

$$N_F = 2^{n-1} - \frac{1}{2} \max_{\beta \in V_m \setminus \{0\}} \max_{a \in V_n} |W_{\beta F}(a)| .$$

Рассмотрим поле $\mathbb{F}_q$ из $q = 2^n$ элементов с нулём 0 и единицей 1, и пусть $F : \mathbb{F}_q \to \mathbb{F}_q$. Обозначим через ζ образующий элемент группы $\mathbb{F}_q^*$. Поле $\mathbb{F}_q$ является векторным пространством размерности n над полем $\mathbb{F}_2$, а каждый его элемент $x \in \mathbb{F}_q$ задаётся вектором $\mathbf{x} = (x_0, \ldots, x_{n-1}) \in V_n$, таким, что $x = \sum\limits_{i=0}^{n-1} x_i \zeta^i$.

Если $a \in V_n$ — фиксированный вектор и $\mathbf{x} \in V_n$, то $(a, \mathbf{x})$ — линейная функция на V_n. Значит, существует однозначно определённый элемент $\alpha \in \mathbb{F}_q$, такой, что $(a, \mathbf{x}) = \mathrm{Tr}(\alpha x)$, где $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_2$ — функция абсолютного следа элементов поля $\mathbb{F}_q$ [3, теорема 2.24]. Данное наблюдение и свойство линейности функции следа позволяют для показателя нелинейности отображения $F : \mathbb{F}_q \to \mathbb{F}_q$ получить формулу

$$N_F = 2^{n-1} - \Delta_F,$$

где

$$\Delta_F = \frac{1}{2} \max_{\alpha \in \mathbb{F}_q} \max_{\beta \in \mathbb{F}_q^*} \left| U^F_{\alpha,\beta} \right|, \quad U^F_{\alpha,\beta} = \sum_{x \in \mathbb{F}_q} (-1)^{\mathrm{Tr}(\alpha x + \beta F(x))}.$$

В данной работе исследуется параметр N_F подстановок из класса подстановок группы $(\mathbb{F}_q, +)$, взятого из [4], являющихся при выполнении одного условия ортоморфизмами. Дадим определение.

Пусть $(G, \cdot)$ — конечная группа с единицей e. Подстановка τ из симметрической группы $S(G)$ подстановок на множестве G называется *ортоморфизмом* группы G [4, 5], если отображение $\tau' : G \to G$, определяемое условием

$$\tau'(g) = g^{-1}\tau(g) \text{ для всех } g \in G,$$

является подстановкой из $S(G)$.

Известно, что ортоморфизмы существуют для любой группы нечётного порядка [4, theorem 1.22]. Ортоморфизмами групп $(\mathbb{Z}_3, +)$ и $(\mathbb{Z}_5, +)$ являются, например, следующие подстановки:

$$\begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 2 & 4 & 1 & 3 \end{pmatrix}.$$

Примером ортоморфизма группы $(G, \cdot)$, $|G| = m$, является отображение $\varphi : G \to G$, $\varphi(g) = g^k$ для всех $g \in G$, где $k \in \mathbb{N}$, $(k, m) = (k-1, m) = 1$.

Для ортоморфизмов могут находиться применения, например при построении систем ортогональных латинских квадратов [6].

1. Определение кусочно-линейного преобразования конечного поля

Пусть $H < \mathbb{F}_q^*$ — подгруппа порядка l мультипликативной группы поля $\mathbb{F}_q$, $0 < l \leqslant q-1$, $q-1 = l \cdot r$, где $r \in \mathbb{N}$. Группа $\mathbb{F}_q^*$ раскладывается в объединение смежных классов по подгруппе H:

$$\mathbb{F}_q^* = \bigcup_{j=0}^{r-1} H_j, \quad H_j = \zeta^j H, \quad j = 0, \ldots, r-1.$$

Рассмотрим кусочно-линейное отображение $F : \mathbb{F}_q \to \mathbb{F}_q$, $F(0) = 0$, ограничение которого на каждый смежный класс H_j имеет вид

$$x \mapsto A_j x \ \text{ для всех } \ x \in H_j,$$

где $A_j \in \mathbb{F}_q^*$, $j = 0, \ldots, r-1$ (отображения такого вида изучаются в [4, chapter 3]). Заметим, что существуют однозначно определённые числа $a_j \in \{0, \ldots, q-2\}$, $j = 0, \ldots, r-1$, при которых $A_j = \zeta^{a_j}$.

Отображение F переводит смежные классы по подгруппе H в смежные классы по подгруппе H. Значит, F биективно в том и только в том случае, когда F осуществляет перестановку указанных смежных классов. Это выполняется тогда и только тогда, когда набор чисел a_0, $a_1 + 1$, $\ldots$, $a_{r-1} + r - 1$ образует полную систему вычетов по модулю r, то есть тогда и только тогда, когда отображение $\pi : \mathbb{Z}_r \to \mathbb{Z}_r$,

$$\pi(j) = (a_j + j) \bmod r, \quad j = 0, \ldots, r-1, \tag{1}$$

является биективным.

Подстановка F указанного вида является ортоморфизмом группы $(\mathbb{F}_{2^n}, +)$ в том и только в том случае, если $A_j \neq 1$ для всех $j = 0, \ldots, r-1$ и отображение $\pi' : \mathbb{Z}_r \to \mathbb{Z}_r$,

$$\pi'(j) = (\log_\zeta(A_j + 1) + j) \bmod r, \quad j = 0, \ldots, r-1,$$

является биективным, где функция $\log_\zeta : \mathbb{F}_q^* \to \{0, \ldots, q-2\}$ определяется условием: для любых $\gamma \in \mathbb{F}_q^*$, $c \in \{0, \ldots, q-2\}$ равенство $\log_\zeta(\gamma) = c$ имеет место в том и только в том случае, когда $\zeta^c = \gamma$.

2. Оценка показателя нелинейности кусочно-линейного преобразования поля характеристики 2

Теорема 1. Пусть $n, r, l \in \mathbb{N}$, $q = 2^n$, $q - 1 = rl$, $3 \leqslant r \leqslant \sqrt{q} + 1$, ζ — примитивный элемент поля $\mathbb{F}_q$, $H = \langle \zeta^r \rangle$ — подгруппа группы $\mathbb{F}_q^*$ порядка l, числа $a_j \in \{0, \ldots, q-2\}$,

$j = 0, \ldots, r-1$, попарно различные и такие, что отображение (1) является биективным, и отображение $F : \mathbb{F}_q \to \mathbb{F}_q$ имеет вид

$$F(x) = \begin{cases} 0, & x = 0, \\ \zeta^{a_j} x, & x \in \zeta^j H,\ j = 0, \ldots, r-1. \end{cases}$$

Тогда выполнено неравенство

$$N_F \geqslant \frac{\sqrt{q}(r-1)(\sqrt{q} - r + 1)}{2r}.$$

Доказательство. Для произвольных $\alpha \in \mathbb{F}_q$, $\beta \in \mathbb{F}_q^*$ имеем равенство

$$U^F_{\alpha,\beta} = \sum_{x \in \mathbb{F}_q} \chi(\alpha x + \beta F(x)),$$

где функция χ — канонический аддитивный характер поля $\mathbb{F}_q$, определяемый равенством

$$\chi(y) = (-1)^{\mathrm{Tr}(y)} \text{ для всех } y \in \mathbb{F}_q.$$

Получим далее

$$U^F_{\alpha,\beta} = 1 + \sum_{j=0}^{r-1} \sum_{x \in H_j} \chi(\alpha x + \beta F(x)),$$

или

$$U^F_{\alpha,\beta} = 1 + \sum_{j=0}^{r-1} \sum_{x \in H} \chi(\gamma_j \zeta^j x), \tag{2}$$

где $\gamma_j = \alpha + \beta A_j = \alpha + \beta\zeta^{a_j}$, $j = 0, \ldots, r-1$.

Заметим, что по условию теоремы числа a_0, a_1, …, a_{r-1} попарно различны. Поэтому при фиксированных элементах $\alpha \in \mathbb{F}_q$, $\beta \in \mathbb{F}_q^*$ элементы γ_0, γ_1, …, γ_{r-1} попарно различны, и возможен один из двух случаев:

а) $\gamma_j \neq 0$ для всех $j \in \{0, \ldots, r-1\}$;

б) $\gamma_{j_0} = 0$ для некоторого $j_0 \in \{0, \ldots, r-1\}$ и $\gamma_j \neq 0$ для всех $j \in \{0, \ldots, r-1\} \backslash \{j_0\}$.

1. Пусть имеет место случай «а». Воспользуемся разложением аддитивного характера χ по мультипликативным характерам поля $\mathbb{F}_q$ [3]:

$$\chi(y) = \frac{1}{q-1} \sum_{\psi} G(\bar{\psi}, \chi)\psi(y) \text{ для всех } y \in \mathbb{F}_q^*,$$

где сумма берётся по всем мультипликативным характерам поля $\mathbb{F}_q$; $\bar{\psi}$ — характер, сопряжённый для характера ψ; $G(\psi, \chi)$ — сумма Гаусса, определяемая равенством

$$G(\psi, \chi) = \sum_{c \in \mathbb{F}_q^*} \psi(c)\chi(c).$$

Из (2) получим

$$U^F_{\alpha,\beta} = 1 + \sum_{j=0}^{r-1} \sum_{x \in H} \frac{1}{q-1} \sum_{\psi} G(\bar{\psi}, \chi)\psi(\gamma_j \zeta^j x) = 1 + \frac{1}{q-1} \sum_{\psi} G(\bar{\psi}, \chi) \sum_{j=0}^{r-1} \psi(\gamma_j \zeta^j) \sum_{x \in H} \psi(x).$$

Учитывая равенство

$$\sum_{x \in H} \psi(x) = \begin{cases} |H|, & \psi \in \mathrm{Ann}(H), \\ 0, & \psi \notin \mathrm{Ann}(H), \end{cases}$$

получим

$$U^F_{\alpha,\beta} = 1 + \frac{l}{q-1} \sum_{\psi \in \mathrm{Ann}(H)} G(\bar{\psi}, \chi) \sum_{j=0}^{r-1} \psi(\gamma_j \zeta^j).$$

Здесь $\mathrm{Ann}(H)$ — аннулятор группы $H = \langle \zeta^r \rangle$, состоящий из всех мультипликативных характеров ψ поля $\mathbb{F}_q$, для которых $\psi(\zeta^r) = 1$.

Пусть ψ_0 — тривиальный мультипликативный характер, тогда, учитывая равенство $lr = q - 1$, получим

$$U^F_{\alpha,\beta} = 1 + \frac{l}{q-1} \sum_{\psi \in \mathrm{Ann}(H) \setminus \{\psi_0\}} G(\bar{\psi}, \chi) \sum_{j=0}^{r-1} \psi(\gamma_j \zeta^j) + G(\psi_0, \chi).$$

Так как $G(\psi_0, \chi) = -1$, то

$$U^F_{\alpha,\beta} = \frac{l}{q-1} \sum_{\psi \in \mathrm{Ann}(H) \setminus \{\psi_0\}} G(\bar{\psi}, \chi) \sum_{j=0}^{r-1} \psi(\gamma_j \zeta^j).$$

Учитывая неравенство $\left| \sum\limits_{j=0}^{r-1} \psi(\gamma_j \zeta^j) \right| \leqslant r$ и равенство $|G(\psi, \chi)| = \sqrt{q}$, справедливое для всех $\psi \neq \psi_0$ и всех χ, получим

$$\left| U^F_{\alpha,\beta} \right| \leqslant \frac{l}{q-1} \sum_{\psi \in \mathrm{Ann}(H) \setminus \{\psi_0\}} \left| G(\bar{\psi}, \chi) \right| \cdot r = \left(|\mathrm{Ann}(H)| - 1 \right) \sqrt{q}.$$

Так как $|\mathrm{Ann}(H)| = r$ [3, теорема 5.6], получим неравенство

$$\left| U^F_{\alpha,\beta} \right| \leqslant (r-1)\sqrt{q}. \tag{3}$$

2. Пусть теперь имеет место случай «б», т. е. $\gamma_{j_0} = 0$ для некоторого индекса $j_0 \in \{0, \ldots, r-1\}$ и $\gamma_j \neq 0$ для всех $j \in \{0, \ldots, r-1\} \setminus \{j_0\}$. Учитывая равенство $\chi(0) = 1$, из (2) получим

$$U^F_{\alpha,\beta} = 1 + |H| + \sum_{j \in \{0,\ldots,r-1\} \setminus \{j_0\}} \sum_{x \in H} \chi(\gamma_j \zeta^j x).$$

Воспользовавшись разложением аддитивного характера χ по мультипликативным характерам поля $\mathbb{F}_q$ и осуществив преобразования, аналогичные сделанным в п. 1, найдём

$$\begin{aligned} U^F_{\alpha,\beta} &= 1 + |H| + \sum_{j \in \{0,\ldots,r-1\} \setminus \{j_0\}} \sum_{x \in H} \frac{1}{q-1} \sum_{\psi} G(\bar{\psi}, \chi) \psi(\gamma_j \zeta^j x) = \\ &= 1 + |H| + \frac{l}{q-1} \sum_{\psi \in \mathrm{Ann}(H)} G(\bar{\psi}, \chi) \sum_{j \in \{0,\ldots,r-1\} \setminus \{j_0\}} \psi(\gamma_j \zeta^j) = \\ &= 1 + |H| + \frac{l(r-1)}{q-1} G(\psi_0, \chi) + \frac{l}{q-1} \sum_{\psi \in \mathrm{Ann}(H) \setminus \{\psi_0\}} G(\bar{\psi}, \chi) \sum_{j \in \{0,\ldots,r-1\} \setminus \{j_0\}} \psi(\gamma_j \zeta^j). \end{aligned}$$

Так как $G(\psi_0, \chi) = -1$, $|H| = l$ и $lr = q - 1$, то

$$U^F_{\alpha,\beta} = \frac{q}{r} + \frac{1}{r} \sum_{\psi \in \mathrm{Ann}(H) \setminus \{\psi_0\}} G(\bar{\psi}, \chi) \sum_{j \in \{0,\ldots,r-1\} \setminus \{j_0\}} \psi(\gamma_j \zeta^j). \tag{4}$$

Учитывая неравенство $\left|\sum\limits_{j\in\{0,\dots,r-1\}\setminus\{j_0\}}\psi(\gamma_j\zeta^j)\right| \leqslant r-1$ и равенство $|G(\psi,\chi)| = \sqrt{q}$, справедливое для всех $\psi \neq \psi_0$ и всех χ, получим неравенство

$$\left|U^F_{\alpha,\beta} - \frac{q}{r}\right| \leqslant \frac{(r-1)}{r}\left(|\mathrm{Ann}(H)|-1\right)\sqrt{q},$$

которое равносильно

$$\left|U^F_{\alpha,\beta} - \frac{q}{r}\right| \leqslant \frac{(r-1)^2}{r}\sqrt{q}. \tag{5}$$

Объединяя оба случая, из (3) и (5) получим

$$\max_{\alpha\in\mathbb{F}_q,\beta\in\mathbb{F}_q^*}\left|U^F_{\alpha,\beta}\right| \leqslant \max\left\{(r-1)\sqrt{q},\quad \frac{q}{r}+\frac{(r-1)^2}{r}\sqrt{q}\right\}.$$

Заметим, что неравенство $(r-1)\sqrt{q} \leqslant \dfrac{q}{r}+\dfrac{(r-1)^2}{r}\sqrt{q}$ выполняется тогда и только тогда, когда $r \leqslant \sqrt{q}+1$. Последнее выполняется по условию, значит,

$$\max_{\alpha\in\mathbb{F}_q,\beta\in\mathbb{F}_q^*}\left|U^F_{\alpha,\beta}\right| \leqslant \frac{q}{r}+\frac{(r-1)^2}{r}\sqrt{q}.$$

Таким образом, имеем неравенство $N_F \geqslant \dfrac{\sqrt{q}(r-1)(\sqrt{q}-r-1)}{2r}$. ■

Замечание 1. Если в условии теоремы 1 неравенство $r < \sqrt{q}+1$ заменить на $r \geqslant \sqrt{q}+1$, то получится оценка $N_F \geqslant 0$, которая является тривиальной.

3. Спектр показателя нелинейности кусочно-линейного преобразования поля характеристики 2 в частных случаях

В некоторых случаях для отображения F можно находить точные значения показателя нелинейности.

Теорема 2. Пусть $n \in \mathbb{N}$ — чётное число, $q = 2^n$, ζ — примитивный элемент поля $\mathbb{F}_q$, $H = \langle\zeta^3\rangle$ — подгруппа группы $\mathbb{F}_q^*$ порядка $(q-1)/3$, числа $a_0, a_1, a_2 \in \{0,\dots,q-2\}$ попарно различные и такие, что отображение

$$\pi : \mathbb{Z}_3 \to \mathbb{Z}_3,\quad \pi(j) = (a_j + j) \bmod 3,\quad j = 0,1,2,$$

является подстановкой группы $\mathbb{Z}_3$, и отображение $F : \mathbb{F}_q \to \mathbb{F}_q$ имеет вид

$$F(x) = \begin{cases} 0, & x = 0,\\ \zeta^{a_j}x, & x \in \zeta^j H,\quad j = 0,1,2.\end{cases}$$

Тогда если $n \equiv 0 \pmod 4$, то

$$N_F = \sqrt{q}(\sqrt{q}-1)/3,$$

а если $n \equiv 2 \pmod 4$, то

$$N_F \in \left\{\sqrt{q}(2\sqrt{q}-1)/6,\ \sqrt{q}(\sqrt{q}-2)/3\right\}.$$

При этом в случае $n \equiv 2 \pmod 4$ равенство $N_F = \sqrt{q}(2\sqrt{q}-1)/6$ имеет место тогда и только тогда, когда

$$c_{(j+1) \bmod 3} \not\equiv c_j + 1 \pmod 3, \quad j = 0, 1, 2,$$

где

$$c_j = (\log_\zeta(\zeta^{a_{(j+1) \bmod 3} - a_j} + 1) + a_j) \bmod 3, \quad j = 0, 1, 2.$$

Доказательство. Так как при $r = 3$ и $n \geqslant 2$ справедливо равенство

$$\max\left\{(r-1)\sqrt{q},\ \frac{q + (r-1)^2\sqrt{q}}{r}\right\} = \frac{q + (r-1)^2\sqrt{q}}{r},$$

то (как следует из доказательства теоремы 1) для нахождения N_F достаточно рассмотреть случай «б»: элементы $\alpha \in \mathbb{F}_q$, $\beta \in \mathbb{F}_q^*$ — произвольные такие, что $\gamma_{j_0} = 0$ для некоторого индекса $j_0 \in \{0, 1, 2\}$ и $\gamma_j \neq 0$ для всех $j \in \{0, 1, 2\} \backslash \{j_0\}$.

Обозначим $\{0, 1, 2\} \backslash \{j_0\} = \{j_1, j_2\}$. Так как $\mathrm{Ann}(H) = \{\psi_0, \psi, \psi^2\}$, где ψ_0 — тривиальный мультипликативный характер; ψ — мультипликативный характер порядка 3 поля $\mathbb{F}_q$ и $G(\psi, \chi) = G(\psi^2, \chi)$, то из (4) получим

$$U^F_{\alpha,\beta} = \frac{q}{3} + \frac{1}{3}G(\psi, \chi)\left(\sigma(\gamma_{j_1}\zeta^{j_1}) + \sigma(\gamma_{j_2}\zeta^{j_2})\right),$$

где $\sigma : \mathbb{F}_q^* \to \mathbb{C}^*$, $\sigma(\zeta^u) = \psi(\zeta^u) + \psi^2(\zeta^u)$ для всех $u \in \{0, \ldots, q-2\}$.

Известно [7, 8], что если ψ — мультипликативный характер порядка 3 поля $\mathbb{F}_{2^n}$, χ — канонический аддитивный характер поля $\mathbb{F}_{2^n}$, то

$$G(\psi, \chi) = (-1)^{(n-2)/2} \cdot 2^{n/2}.$$

Поэтому

$$U^F_{\alpha,\beta} = \frac{q}{3} + \frac{1}{3}(-1)^{(n-2)/2}\sqrt{q}\left(\sigma(\gamma_{j_1}\zeta^{j_1}) + \sigma(\gamma_{j_2}\zeta^{j_2})\right) =$$
$$= \frac{q}{3} + \frac{1}{3}(-1)^{(n-2)/2}\sqrt{q}\left(\sigma\left((\alpha + \beta\zeta^{a_{j_1}})\zeta^{j_1}\right) + \sigma\left((\alpha + \beta\zeta^{a_{j_2}})\zeta^{j_2}\right)\right).$$

Так как в рассматриваемом случае $\alpha + \beta\zeta^{a_{j_0}} = 0$, то

$$U^F_{\alpha,\beta} = \frac{q}{3} + \frac{1}{3}(-1)^{(n-2)/2}\sqrt{q}\left(\sigma(\alpha\zeta^{u_1}) + \sigma(\alpha\zeta^{u_2})\right),$$

где $\zeta^{u_1} = (\zeta^{a_{j_1} - a_{j_0}} + 1)\zeta^{j_1}$; $\zeta^{u_2} = (\zeta^{a_{j_2} - a_{j_0}} + 1)\zeta^{j_2}$; $u_1, u_2 \in \{0, \ldots, q-2\}$.

Заметим, что если $\beta \neq 0$ и выполняется равенство $\alpha + \beta\zeta^{a_{j_0}} = 0$, то $\alpha \neq 0$. Заметим далее, что так как $\sigma(\zeta^u) = e^{2\pi i u/3} + e^{4\pi i u/3}$ для всех $u \in \{0, \ldots, q-2\}$, то

$$\sigma(\zeta^u) = \begin{cases} 2, & u \equiv 0 \pmod 3, \\ -1 & \text{иначе}, \end{cases} \qquad \text{т. е.} \quad \sigma(\zeta^u) = \begin{cases} 2, & \zeta^u \in H, \\ -1 & \text{иначе}. \end{cases}$$

Поэтому если $u_1 \equiv u_2 \pmod 3$, то найдётся элемент $\alpha \in \mathbb{F}_q^*$, для которого $\alpha\zeta^{u_1} \in H$, $\alpha\zeta^{u_2} \in H$, и найдётся элемент $\alpha' \in \mathbb{F}_q^*$, для которого $\alpha'\zeta^{u_1} \notin H$, $\alpha'\zeta^{u_2} \notin H$. Значит, если $u_1 \equiv u_2 \pmod 3$, то

$$\max_{\alpha \in \mathbb{F}_q^*}\left(\sigma\left(\alpha\zeta^{u_1}\right) + \sigma\left(\alpha\zeta^{u_2}\right)\right) = 4, \quad \min_{\alpha \in \mathbb{F}_q^*}\left(\sigma\left(\alpha\zeta^{u_1}\right) + \sigma\left(\alpha\zeta^{u_2}\right)\right) = -2.$$

Если же $u_1 \not\equiv u_2 \pmod 3$, то найдутся элементы $\alpha, \alpha' \in \mathbb{F}_q^*$, для которых $\alpha\zeta^{u_1} \in H$, $\alpha\zeta^{u_2} \notin H$ и $\alpha'\zeta^{u_1} \notin H$, $\alpha'\zeta^{u_2} \notin H$, но не найдётся элемента $\alpha'' \in \mathbb{F}_q^*$, для которого $\alpha''\zeta^{u_1} \in H$, $\alpha''\zeta^{u_2} \in H$. Значит, в этом случае

$$\max_{\alpha\in\mathbb{F}_q^*}\left(\sigma\left(\alpha\zeta^{u_1}\right)+\sigma\left(\alpha\zeta^{u_2}\right)\right)=1, \quad \min_{\alpha\in\mathbb{F}_q^*}\left(\sigma\left(\alpha\zeta^{u_1}\right)+\sigma\left(\alpha\zeta^{u_2}\right)\right)=-2.$$

Таким образом, если $n \equiv 0 \pmod 4$, то

$$\max_{\alpha\in\mathbb{F}_q,\beta\in\mathbb{F}_q^*}\left|U_{\alpha,\beta}^F\right| = (q+2\sqrt{q})/3,$$

а если $n \equiv 2 \pmod 4$, то

$$\max_{\alpha\in\mathbb{F}_q,\beta\in\mathbb{F}_q^*}\left|U_{\alpha,\beta}^F\right| \in \left\{(q+\sqrt{q})/3,\ (q+4\sqrt{q})/3\right\}.$$

При этом в случае $n \equiv 2 \pmod 4$ равенство $\max\limits_{\alpha\in\mathbb{F}_q,\beta\in\mathbb{F}_q^*}\left|U_{\alpha,\beta}^F\right| = (q+\sqrt{q})/3$ выполняется тогда и только тогда, когда для любого $j_0 \in \{0,1,2\}$ верно условие

$$u_1 \not\equiv u_2 \pmod 3. \tag{6}$$

Так как $\zeta^{u_1} = (\zeta^{a_{j_1}-a_{j_0}}+1)\zeta^{j_1}$, $\zeta^{u_2} = (\zeta^{a_{j_2}-a_{j_0}}+1)\zeta^{j_2}$, $u_1, u_2 \in \{0,\ldots,q-2\}$, то выполнение условия (6) для всех $j_0 \in \{0,1,2\}$ означает, что имеет место система

$$\begin{cases} \log_\zeta(\zeta^{a_1-a_0}+1) \not\equiv \log_\zeta(\zeta^{a_2-a_0}+1)+1 \pmod 3, \\ \log_\zeta(\zeta^{a_0-a_1}+1) \not\equiv \log_\zeta(\zeta^{a_2-a_1}+1)+2 \pmod 3, \\ \log_\zeta(\zeta^{a_0-a_2}+1) \not\equiv \log_\zeta(\zeta^{a_1-a_2}+1)+1 \pmod 3, \end{cases}$$

которая равносильна системе

$$c_{(j+1) \bmod 3} \not\equiv c_j + 1 \pmod 3, \quad j = 0,1,2,$$

где $c_j = (\log_\zeta(\zeta^{a_{(j+1) \bmod 3}-a_j}+1)+a_j) \bmod 3$, $j = 0,1,2$. ■

Следствие 1. В случае $n \equiv 2 \pmod 4$ при $r = 3$ оценка из теоремы 1 является достижимой.

Доказательство. В условиях теоремы 2 в случае $n \equiv 2 \pmod 4$ существует отображение F рассматриваемого вида, для которого имеет место равенство

$$\max_{\alpha\in\mathbb{F}_q,\beta\in\mathbb{F}_q^*}\left|U_{\alpha,\beta}^F\right| = (q+4\sqrt{q})/3.$$

Действительно, данное равенство выполнено, если, например,

$$\log_\zeta(\zeta^{a_2-a_1}+1)+a_1 \equiv \log_\zeta(\zeta^{a_1-a_0}+1)+a_0+1 \pmod 3.$$

Ясно, что для любого значения в правой части последнего сравнения найдётся такое $a_2 \in \{0,\ldots,q-2\}$, что сравнение будет справедливо. ■

Как и в случае мультипликативного характера порядка 3, сумма Гаусса для любого мультипликативного характера порядка 5 и канонического аддитивного характера поля $\mathbb{F}_q$ принимает одно и то же действительное значение.

Лемма 1. Пусть $n, m \in \mathbb{N}$, $n = 4m$, $q = 2^n$. Если ψ' — мультипликативный характер порядка 5 поля $\mathbb{F}_q$, χ' — канонический аддитивный характер этого поля, то

$$G(\psi', \chi') = (-1)^{m-1}\sqrt{q}.$$

Доказательство. Пусть ζ — примитивный элемент поля $\mathbb{F}_q$. Тогда $\eta = \zeta^{(q-1)/15}$ — примитивный элемент поля $\mathbb{F}_{16}$, и мультипликативный характер ψ поля $\mathbb{F}_{16}$, определяемый равенством

$$\psi(\eta) = \psi'(\zeta),$$

имеет порядок 5.

Пусть χ — канонический аддитивный характер поля $\mathbb{F}_{16}$. Для характера ψ поля $\mathbb{F}_{16} = \mathbb{F}_{4^2}$ выполняются условия теоремы Штикельбергера [3, теорема 5.16], и по этой теореме получим равенство $G(\psi, \chi) = 4$ (которое можно проверить и непосредственным вычислением). Так как χ' и ψ' — поднятия до поля $\mathbb{F}_q$ характеров χ и ψ поля $\mathbb{F}_{16}$ соответственно и $[\mathbb{F}_q : \mathbb{F}_{16}] = m$, то по теореме Дэвенпорта — Хассе [3, теорема 5.14] получим $G(\psi', \chi') = (-1)^{m-1}G(\psi, \chi)^m = (-1)^{m-1}\sqrt{q}$. ■

Теорема 3. Пусть $n, m \in \mathbb{N}$, $n = 4m$, $q = 2^n$, ζ — примитивный элемент поля $\mathbb{F}_q$, $H = \langle \zeta^5 \rangle$ — подгруппа группы $\mathbb{F}_q^*$ порядка $(q-1)/5$, числа $a_j \in \{0, \ldots, q-2\}$, $j = 0, \ldots, 4$, — попарно различные и такие, что отображение

$$\pi : \mathbb{Z}_5 \to \mathbb{Z}_5, \quad \pi(j) = (a_j + j) \bmod 5, \quad j = 0, \ldots, 4,$$

является биективным, и отображение $F : \mathbb{F}_q \to \mathbb{F}_q$ имеет вид

$$F(x) = \begin{cases} 0, & x = 0, \\ \zeta^{a_j} x, & x \in \zeta^j H,\ j = 0, \ldots, 4. \end{cases}$$

Тогда если $n \equiv 0 \pmod 8$, то

$$N_F = 2\sqrt{q}(\sqrt{q} - 1)/5,$$

а если $n \equiv 4 \pmod 8$, то

$$N_F \in \left\{ \sqrt{q}(4\sqrt{q} - t)/10 : t = 1, 6, 11, 16 \right\}.$$

Доказательство. Так как при $r = 5$ и $n \geqslant 4$ справедливо равенство

$$\max\left\{ (r-1)\sqrt{q},\ \frac{q + (r-1)^2\sqrt{q}}{r} \right\} = \frac{q + (r-1)^2\sqrt{q}}{r},$$

то (как следует из доказательства теоремы 1) для нахождения N_F достаточно рассмотреть случай «б»: элементы $\alpha \in \mathbb{F}_q$, $\beta \in \mathbb{F}_q^*$ — произвольные такие, что $\gamma_{j_0} = 0$ для некоторого индекса $j_0 \in \{0, \ldots, 4\}$ и $\gamma_j \neq 0$ для всех $j = \{0, \ldots, 4\} \backslash \{j_0\}$.

Обозначим $\{0, \ldots, 4\} \backslash \{j_0\} = \{j_1, j_2, j_3, j_4\}$ и пусть $l = (q-1)/5$. Если ψ — произвольный мультипликативный характер поля $\mathbb{F}_q$ порядка 5, χ — канонический аддитивный характер поля $\mathbb{F}_q$, то по лемме 1 имеем $G(\psi, \chi) = (-1)^{m-1}\sqrt{q}$. Тогда из (4) получим

$$U_{\alpha,\beta}^F = \frac{q}{5} + \frac{1}{5}(-1)^{m-1}\sqrt{q}\sum_{k=1}^{4} \sigma(\gamma_{j_k}\zeta^{j_k}),$$

где $\sigma : \mathbb{F}_q^* \to \mathbb{C}^*$, $\sigma(\zeta^u) = \sum\limits_{s=1}^{4} \psi^s(\zeta^u)$ для всех $u \in \{0, \dots, q-2\}$; $\gamma_{j_k} = \alpha + \beta\zeta^{a_{j_k}}$, $k = 1, \dots, 4$. Так как в рассматриваемом случае $\alpha + \beta\zeta^{a_{j_0}} = 0$, то

$$U_{\alpha,\beta}^F = \frac{q}{5} + \frac{1}{5}(-1)^{m-1}\sqrt{q}\sum_{k=1}^{4}\sigma(\alpha\zeta^{u_k}),$$

где $\zeta^{u_k} = (\zeta^{a_{j_k}-a_{j_0}} + 1)\zeta^{j_k}$, $u_k \in \{0, \dots, q-2\}$, $k = 1, \dots, 4$. Заметим, что если $\beta \neq 0$ и выполняется равенство $\alpha + \beta\zeta^{a_{j_0}} = 0$, то $\alpha \neq 0$. Заметим далее, что так как

$$\sigma(\zeta^u) = \sum_{s=1}^{4} e^{2\pi i s u/5},$$

то

$$\sigma(\zeta^u) = \begin{cases} 4, & u \equiv 0 \pmod 5, \\ -1 & \text{иначе}, \end{cases} \qquad \text{т. е.} \quad \sigma(\zeta^u) = \begin{cases} 4, & \zeta^u \in H, \\ -1 & \text{иначе}. \end{cases}$$

Какие бы ни были числа $u_k \in \{0, \dots, q-2\}$, $k = 1, \dots, 4$, найдётся элемент $\alpha \in \mathbb{F}_q^*$, для которого $\alpha\zeta^{u_k} \notin H$ для всех $k \in \{1, \dots, 4\}$. Следовательно,

$$\min_{\alpha\in\mathbb{F}_q^*}\left(\sum_{k=1}^{4}\sigma(\alpha\zeta^{u_k})\right) = -4,$$

и при $n \equiv 0 \pmod 8$ получим $\max\limits_{\alpha\in\mathbb{F}_q,\beta\in\mathbb{F}_q^*}\left|U_{\alpha,\beta}^F\right| = (q + 4\sqrt{q})/5$.

Пусть теперь $n \equiv 4 \pmod 8$.

С л у ч а й 1. Если $u_1 \equiv u_2 \equiv u_3 \equiv u_4 \pmod 5$, то найдётся элемент $\alpha \in \mathbb{F}_q^*$, для которого $\alpha\zeta^{u_k} \in H$ для всех $k \in \{1, \dots, 4\}$. Тогда $\max\limits_{\alpha\in\mathbb{F}_q^*}\left(\sum\limits_{k=1}^{4}\sigma(\alpha\zeta^{u_k})\right) = 16$, откуда получим

$$\max_{\alpha\in\mathbb{F}_q,\beta\in\mathbb{F}_q^*}\left|U_{\alpha,\beta}^F\right| = (q + 16\sqrt{q})/5.$$

С л у ч а й 2. Если $u_{k_1} \not\equiv u_{k_2} \equiv u_{k_3} \equiv u_{k_4} \pmod 5$, где $\{k_1, k_2, k_3, k_4\} = \{1, \dots, 4\}$, то возможны три подслучая:

2.1. $\exists\alpha \in \mathbb{F}_q^*$ $(\alpha\zeta^{u_{k_1}} \notin H, \alpha\zeta^{u_{k_2}}, \alpha\zeta^{u_{k_3}}, \alpha\zeta^{u_{k_4}} \in H)$;

2.2. $\exists\alpha' \in \mathbb{F}_q^*$ $(\alpha'\zeta^{u_{k_1}} \in H, \alpha'\zeta^{u_{k_2}}, \alpha'\zeta^{u_{k_3}}, \alpha'\zeta^{u_{k_4}} \notin H)$;

2.3. $\exists\alpha'' \in \mathbb{F}_q^*$ $(\alpha''\zeta^{u_{k_1}}, \alpha''\zeta^{u_{k_2}}, \alpha''\zeta^{u_{k_3}}, \alpha''\zeta^{u_{k_4}} \notin H)$.

Так как $\sum\limits_{k=1}^{4}\sigma(\alpha\zeta^{u_k}) = 11$, $\sum\limits_{k=1}^{4}\sigma(\alpha'\zeta^{u_k}) = 1$, $\sum\limits_{k=1}^{4}\sigma(\alpha''\zeta^{u_k}) = -4$, в случае 2 получим $\max\limits_{\alpha\in\mathbb{F}_q^*}\left(\sum\limits_{k=1}^{4}\sigma(\alpha\zeta^{u_k})\right) = 11$, следовательно, $\max\limits_{\alpha\in\mathbb{F}_q,\beta\in\mathbb{F}_q^*}\left|U_{\alpha,\beta}^F\right| = (q + 11\sqrt{q})/5$.

Аналогично получим следующее.

С л у ч а й 3. Если $u_{k_1} \not\equiv u_{k_2} \equiv u_{k_3} \not\equiv u_{k_4} \pmod 5$, $u_{k_1} \not\equiv u_{k_4} \pmod 5$, где $\{k_1, k_2, k_3, k_4\} = \{1, \dots, 4\}$, то $\max\limits_{\alpha\in\mathbb{F}_q^*}\left(\sum\limits_{k=1}^{4}\sigma(\alpha\zeta^{u_k})\right) = 6$, следовательно,

$$\max_{\alpha\in\mathbb{F}_q,\beta\in\mathbb{F}_q^*}\left|U_{\alpha,\beta}^F\right| = (q + 6\sqrt{q})/5.$$

С л у ч а й 4. Если $u_{k_1} \not\equiv u_{k_2} \pmod 5$ для всех $k_1, k_2 \in \{1, \ldots, 4\}$, $k_1 \neq k_2$, то $\max\limits_{\alpha \in \mathbb{F}_q^*} \left(\sum\limits_{k=1}^{4} \sigma(\alpha \zeta^{u_k}) \right) = 1$, следовательно, $\max\limits_{\alpha \in \mathbb{F}_q, \beta \in \mathbb{F}_q^*} \left| U_{\alpha,\beta}^F \right| = (q + \sqrt{q})/5$.

Теорема доказана. ■

Автор признателен О. В. Камловскому за полезные рекомендации и обсуждения в ходе выполнения работы.

ЛИТЕРАТУРА

1. *Логачёв О. А., Сальников А. А., Смышляев С. В., Ященко В. В.* Булевы функции в теории кодирования и криптологии. 2-е изд., доп. М.: МЦНМО, 2012. 584 с.
2. *Nyberg K.* On the construction of highly nonlinear permutations // EUROCRYPT'92. LNCS. 1993. V. 658. P. 92–98.
3. *Лидл Р., Нидеррайтер Г.* Конечные поля: в 2-х т.: пер. с. англ. М.: Мир, 1988. 822 с.
4. *Evans A. B.* Orthomorphisms Graphs and Groups. Berlin: Springer Verlag, 1992.
5. *Paige L. J.* Complete mappings of finite groups // Pacific J. Math. 1955. V. 1. P. 111–116.
6. *Глухов М. М.* О методах построения систем ортогональных квазигрупп с использованием групп // Математические вопросы криптографии. 2011. Т. 2. № 4. С. 5–24.
7. *Ding C.* Cyclotomic linear codes of order 3 // IEEE Trans. Inf. Theory. 2007. V. 53. No. 6. P. 2274–2277.
8. *McEliece R. J.* Irreducible cyclic codes and Gauss sums // Combinatorics / eds. M. Hall and J. H. van Lint. Amsterdam: Math. Centre, 1975. P. 185–202.

REFERENCES

1. *Logachev O. A., Sal'nikov A. A., Smyshlyaev S. V., Yashchenko V. V.* Bulevy funktsii v teorii kodirovaniya i kriptologii [Boolean Functions in Coding Theory and Cryptology]. Moscow, MCCME Publ., 2012. 584 p. (in Russian)
2. *Nyberg K.* On the construction of highly nonlinear permutations. EUROCRYPT'92, LNCS, 1993, vol. 658, pp. 92–98.
3. *Lidl R., Niderrayter G.* Konechnye polya [Finite Fields]. Moscow, Mir Publ., 1988, vol. 1, 2. 822 p. (in Russian)
4. *Evans A. B.* Orthomorphisms Graphs and Groups. Berlin, Springer Verlag, 1992.
5. *Paige L. J.* Complete mappings of finite groups. Pacific J. Math., 1955, vol. 1, pp. 111–116.
6. *Gluhov M. M.* O metodakh postroeniya sistem ortogonal'nykh kvazigrupp s ispol'zovaniem grupp [On a method of construction of orthogonal quasigroup systems by means of groups]. Mat. Vopr. Kriptogr., 2011, vol. 2, iss. 4, pp. 5–24. (in Russian)
7. *Ding C.* Cyclotomic linear codes of order 3. IEEE Trans. Inf. Theory, 2007, vol. 53, no. 6, pp. 2274–2277.
8. *McEliece R. J.* Irreducible cyclic codes and Gauss sums. Combinatorics (eds. M. Hall and J. H. van Lint). Amsterdam, Math. Centre, 1975, pp. 185–202.

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 512.64, 519.21, 519.72

ОПИСАНИЕ НЕЭНДОМОРФНЫХ МАКСИМАЛЬНЫХ СОВЕРШЕННЫХ ШИФРОВ С ДВУМЯ ШИФРВЕЛИЧИНАМИ

Н. В. Медведева, С. С. Титов

Уральский государственный университет путей сообщения, г. Екатеринбург, Россия

Исследуются неэндоморфные совершенные по Шеннону (абсолютно стойкие к атаке по шифртексту) шифры в случае, когда мощность множества шифрвеличин равна двум. В терминах линейной алгебры на основе теоремы Биркгофа о классификации дважды стохастических матриц описано множество (полиэдр) матриц вероятностей ключей неэндоморфных совершенных шифров с двумя шифрвеличинами. Построено множество возможных значений априорных вероятностей шифробозначений данных шифров.

Ключевые слова: *совершенные шифры, неэндоморфные шифры, максимальные шифры, дважды стохастические матрицы.*

DOI 10.17223/20710410/30/4

DESCRIPTION OF NON-ENDOMORPHIC MAXIMUM PERFECT CIPHERS WITH TWO-VALUED PLAINTEXT ALPHABET

N. V. Medvedeva, S. S. Titov

Ural State University of Railway Transport, Ekaterinburg, Russia

E-mail: medvedeva_n_v@mail.ru; stitov@usaaa.ru

This paper deals with non-endomorphic perfect (according to Shannon) ciphers, which are absolutely immune against the ciphertext-only attacks in the case when plaintext alphabet consists of two elements. Matrices of probabilities of cipher keys are described in terms of linear algebra on the basis of Birkhoff's theorem (about the classification of doubly stochastic matrices). The set of possible values of a priori probabilities for elements in ciphertext alphabet of a perfect cipher is constructed.

Keywords: *perfect ciphers, non-endomorphic ciphers, maximum ciphers, doubly stochastic matrices.*

Введение

К. Шеннон, разрабатывая теорию криптографической стойкости, ввел понятие совершенного шифра как шифра, абсолютно стойкого к атаке по шифртексту [1]. Такой шифр не даёт криптоаналитику никакой дополнительной информации об открытом тексте на основе изучения перехваченной криптограммы. Примерно в те же годы концепция совершенного шифра разрабатывалась в одной закрытой работе, выполненной

под руководством В. А. Котельникова [2, 3]. Впоследствии, в связи с изучением вопросов имитостойкости шифров, понятие совершенного шифра было обобщено для криптоатак на основе совокупностей шифртекстов, полученных на одном ключе, а также криптоатак на основе известного открытого текста [4 – 6].

В основе изучения совершенных шифров лежит математическая модель шифра. Впервые вероятностная модель шифра рассмотрена в фундаментальной работе К. Шеннона [1]. Имеются и другие подходы к построению таких моделей [7 – 10]. В [3] предлагается некоторая модификация модели, приведенной в [7]. Она использует понятия опорного шифра, ключевого потока; в ней введены два класса шифров — с ограниченным и неограниченным ключами.

Пусть X, Y — конечные множества соответственно шифрвеличин и шифробозначений, с которыми оперирует некоторый шифр замены; K — множество ключей; $|X| = \lambda$, $|Y| = \mu$, $|K| = \pi$, где $\lambda > 1$, $\mu \geqslant \lambda$. Это означает, что открытые и шифрованные тексты представляются словами в алфавитах X и Y соответственно. Согласно [3, 7], под *шифром* Σ_B будем понимать совокупность множеств правил зашифрования и расшифрования с заданными распределениями вероятностей на множествах открытых текстов и ключей. Шифры, для которых апостериорные вероятности открытых текстов совпадают с их априорными вероятностями, называются *совершенными*. В работе [1] полностью описаны *эндоморфные* ($|X| = |Y|$) совершенные шифры с минимально возможным числом ключей ($|K| = |Y|$). Согласно теореме К. Шеннона [1], эндоморфные совершеные шифры с минимально возможным числом ключей исчерпываются шифрами гаммирования со случайной равновероятной гаммой.

Изучение *неэндоморфных* ($|X| < |Y|$) шифров в общем виде предполагает знание распределения вероятностей на множестве открытых текстов. В качестве стандартного аппарата исследования распределения вероятностей на множестве открытых текстов используются дважды стохастические матрицы [11]. Шифры, содержащие все инъекции из X в Y, т. е. такие, что $|K| = \pi = \mu(\mu-1)\cdot\ldots\cdot(\mu-\lambda+1)$, называются *максимальными*. Для неэндоморфных максимальных совершенных шифров ключи могут быть неравновероятными [3, пример 2.2.10]. В [12] показано, что *неминимальный* ($|K| > |Y|$) совершенный шифр вкладывается в максимальный совершенный шифр.

Данная работа является продолжением [12, 13]. Здесь описано множество (полиэдр) матриц вероятностей ключей и множество вероятностей шифробозначений неэндоморфных совершенных шифров в случае, когда мощность множества шифрвеличин равна двум.

1. Постановка задачи

Рассмотрим неэндоморфный максимальный совершенный шифр в случае, когда мощность множества шифрвеличин равна двум. Пусть $X = \{x_1, x_2\}$ — множество шифрвеличин; $Y = \{y_1, y_2, \ldots, y_\mu\} = \{1, 2, \ldots, \mu\}$ — множество шифробозначений, с которыми оперирует некоторый шифр замены; $K = \{k_1, k_2, \ldots, k_\pi\}$ — множество ключей. Здесь $|X| = \lambda = 2$, $|Y| = \mu \geqslant 2$, $|K| = \pi = \mu(\mu - 1)$.

Зашифрование открытого текста $x = x_{i_1}x_{i_2}\ldots x_{i_\ell}$, где $x_{i_j} \in X$, т. е. $i_j \in \{1, 2\}$, заключается в замене каждой шифрвеличины x_{i_j} некоторым шифробозначением y_{i_j} в соответствии со случайно выбранным одним из

$$|K| = A_{|Y|}^{|X|} = A_\mu^2 = \frac{\mu!}{(\mu-2)!} = \mu(\mu-1) = \pi$$

всех инъективных отображений $e_k : X \to Y$, индексированных ключами $k \in K = \{k_1, k_2, \ldots, k_\pi\}$, занумерованными числами $1, 2, \ldots, \pi$. Инъективное отображение e_k, $k \in K$, при котором $e_k(x_1) = y_s = s$ и $e_k(x_2) = y_t = t$, будем также обозначать e_{st}, где $s, t = 1, \ldots, \mu$.

Пусть P_{st} — вероятность того, что при зашифровании шифрвеличины x_{i_j}, $i_j \in \{1, 2\}$, будет выбрано инъективное отображение e_{st}, т. е.

$$\mathsf{P}_{st} = \mathsf{P}\{e_{st}(x_1) = s \ \& \ e_{st}(x_2) = t\},$$

где $y_s \neq y_t$. Если $s = t$, то, в силу инъективности, $\mathsf{P}_{st} = 0$.

Отметим, что вероятности P_{st}, где $s, t = 1, \ldots, \mu$, задают распределение вероятностей ключей $P(K)$, которое не зависит от распределения $P(X)$ на множестве шифрвеличин [3].

Обозначим через $P = \| \mathsf{P}_{st} \|$ квадратную матрицу порядка μ, такую, что

$$\forall s \left(\sum_{t=1}^{\mu} \mathsf{P}_{st} = p_s \right), \ \forall t \left(\sum_{s=1}^{\mu} \mathsf{P}_{st} = p_t \right); \tag{1}$$

$$p_1 + \ldots + p_\mu = 1. \tag{2}$$

Заметим, что, как указано в [3], совершенный по Шеннону шифр является сильно совершенным, т. е. является совершенным при любом распределении на множестве шифрвеличин. Поэтому распределения вероятностей на множестве шифробозначений, индуцированные априорными распределениями вероятностей на множестве ключей, будем называть априорными.

Условие (1) задает равенство априорных $p_s = \mathsf{P}\{y = y_s\} = \mathsf{P}\{y = s\}$, $s = 1, \ldots, \mu$, и апостериорных (условных) $\mathsf{P}\{y = y_s |\ x = x_{i_j}\} = \mathsf{P}\{y = s |\ x = x_{i_j}\}$, $i_j \in \{1, 2\}$, вероятностей шифробозначений. Это, согласно [3, критерий (2.2.4)], означает, что условие (1) равносильно условию совершенности шифра.

Требуется описать множество возможных значений априорных вероятностей шифробозначений p_s, $s = 1, \ldots, \mu$, и найти общий вид матрицы P, удовлетворяющей условиям (1) и (2), в зависимости от значений вероятностей p_s. Согласно подходу [3, 7], для вероятностной модели Σ_B шифра это достаточно сделать при $\ell = 1$.

Для решения поставленной задачи будем использовать критерий совершенности шифра (2.2.4) из [3]. В частности, в примере 2.2.10 из [3] $X = \{x_1, x_2\}$, $Y = \{y_1, y_2, y_3\} = \{1, 2, 3\}$, $K = \{k_1, k_2, \ldots, k_6\}$, т. е. при $\lambda = 2$, $\mu = 3$, $\pi = 6$, таблица зашифрования имеет вид

$K \backslash X$	x_1	x_2	$\mathsf{P}_{st} = \mathsf{P}\{e_{st}(x_1) = s \ \& \ e_{st}(x_2) = t\}$
k_1	1	2	$\mathsf{P}_{12} = \mathsf{P}\{k = k_1\} = 19/80$
k_2	1	3	$\mathsf{P}_{13} = \mathsf{P}\{k = k_2\} = 3/20$
k_3	2	1	$\mathsf{P}_{21} = \mathsf{P}\{k = k_3\} = 21/80$
k_4	2	3	$\mathsf{P}_{23} = \mathsf{P}\{k = k_4\} = 1/10$
k_5	3	1	$\mathsf{P}_{31} = \mathsf{P}\{k = k_5\} = 1/8$
k_6	3	2	$\mathsf{P}_{32} = \mathsf{P}\{k = k_6\} = 1/8$

При этом для вероятностей $\mathsf{P}_{st} = \mathsf{P}\{e_{st}(x_1) = s \ \& \ e_{st}(x_2) = t\}$, где $s, t = 1, 2, 3$, выполняются равенства

$$p_1 = \mathsf{P}\{y = 1 \,|\, x = x_1\} = \mathsf{P}_{12} + \mathsf{P}_{13} = \frac{31}{80}; \quad p_1 = \mathsf{P}\{y = 1 \,|\, x = x_2\} = \mathsf{P}_{21} + \mathsf{P}_{31} = \frac{31}{80};$$

$$p_2 = \mathsf{P}\{y = 2 \,|\, x = x_1\} = \mathsf{P}_{21} + \mathsf{P}_{23} = \frac{29}{80}; \quad p_2 = \mathsf{P}\{y = 2 \,|\, x = x_2\} = \mathsf{P}_{12} + \mathsf{P}_{32} = \frac{29}{80};$$

$$p_3 = \mathsf{P}\{y = 3 \,|\, x = x_1\} = \mathsf{P}_{31} + \mathsf{P}_{32} = \frac{20}{80}; \quad p_3 = \mathsf{P}\{y = 3 \,|\, x = x_2\} = \mathsf{P}_{13} + \mathsf{P}_{23} = \frac{20}{80},$$

т. е. априорные и апостериорные (условные) вероятности шифробозначений y_i, $i = 1, 2, 3$, равны. Это, согласно критерию (2.2.4) из [3], означает, что матрица

$$P = ||\,\mathsf{P}_{st}\,|| = \begin{pmatrix} \mathsf{P}_{11} & \mathsf{P}_{12} & \mathsf{P}_{13} \\ \mathsf{P}_{21} & \mathsf{P}_{22} & \mathsf{P}_{23} \\ \mathsf{P}_{31} & \mathsf{P}_{32} & \mathsf{P}_{33} \end{pmatrix} = \begin{pmatrix} 0 & 19/80 & 3/20 \\ 21/80 & 0 & 1/10 \\ 1/8 & 1/8 & 0 \end{pmatrix}$$

удовлетворяет условию (1) совершенности шифра.

2. Основные понятия

Аналогично подходу [11], введём

Определение 1. Нормальным циклом длины $d \geqslant 1$ матрицы P будем называть последовательность $(i_1, i_2, \ldots, i_d)$ различных элементов множества $\{1, 2, \ldots, \mu\}$, такую, что

$$P_{i_1 i_2} > 0,\ P_{i_2 i_3} > 0,\ \ldots,\ P_{i_{d-1} i_d} > 0,\ P_{i_d i_1} > 0.$$

Будем считать, что нормальные циклы $(i_1, i_2, \ldots, i_d)$, отличающиеся друг от друга циклической перестановкой элементов, совпадают. Справедлива

Лемма 1. Пусть неотрицательная матрица P удовлетворяет условию (1) и не имеет нормальных циклов. Тогда P — нулевая матрица.

Доказательство. Предположим, что матрица P ненулевая, т. е. имеет ненулевой положительный элемент $\mathsf{P}_{ij} > 0$. Тогда $p_i \geqslant \mathsf{P}_{ij} > 0$ и $p_j \geqslant \mathsf{P}_{ij} > 0$.

Обозначим $i_1 = i$ и $i_2 = j$, где $i_1 \neq i_2$ (при $i_1 = i_2$ матрица P имеет нормальный цикл длины $d = 1$, что противоречит условию). Так как $p_j = p_{i_2} > 0$ является суммой элементов j-го столбца, а также суммой элементов i-й строки, в силу справедливости равенств (1) в матрице P существует k-й столбец, содержащий элемент $\mathsf{P}_{jk} > 0$. Обозначим $i_3 = k$. В силу отсутствия в матрице P нормальных циклов длины 1 имеем $i_2 \neq i_3$, а в силу отсутствия нормальных циклов длины 2 получаем, что $i_3 \neq i_1$, т. е. числа i_1, i_2, i_3 различны.

Продолжим нахождение ненулевых элементов матрицы P. Пусть последовательность $(i_1, i_2, \ldots, i_m)$, где $3 \leqslant m \leqslant \mu$, различных элементов такая, что выполняются неравенства

$$\mathsf{P}_{i_1 i_2} > 0,\ \mathsf{P}_{i_2 i_3} > 0,\ \ldots,\ \mathsf{P}_{i_{m-1} i_m} > 0.$$

Тогда $p_{i_1} > 0$, $p_{i_2} > 0$, $\ldots$, $p_{i_m} > 0$. Поскольку сумма элементов i_m-й строки равна p_{i_m}, в матрице P существует элемент $\mathsf{P}_{i_m i_{m+1}} > 0$. В силу отсутствия нормальных циклов длины 1 имеем $i_{m+1} \neq i_m$, а в силу отсутствия нормальных циклов длины 2 получаем, что $i_{m+1} \neq i_{m-1}$. В силу отсутствия нормальных циклов длины 3 имеем $i_{m+1} \neq i_{m-2}$ и т. д.; а именно из-за отсутствия нормальных циклов длины $4, 5, \ldots, m$ выполняются условия $i_{m+1} \neq i_{m-3}$, $i_{m+1} \neq i_{m-4}$, $\ldots$, $i_{m+1} \neq i_1$, т. е. все числа $i_1, i_2, \ldots, i_{m+1}$ различны.

Однако в силу конечности множества строк (столбцов) матрицы P множество $\{i_1, i_2, \ldots, i_m\}$ является подмножеством множества $\{1, 2, \ldots, \mu\}$ всех номеров строк матрицы P. Максимальное значение m равно μ, при котором $i_{m+1} = i_{\mu+1} \in \{i_1, i_2, \ldots, i_\mu\}$, т. е. $i_{\mu+1} = i_n$ для некоторого $n \in \{i_1, i_2, \ldots, i_\mu\}$. Получаем противоречие с тем, что все числа $i_1, i_2, \ldots, i_{\mu+1}$ различны. Следовательно, предположение, что P — ненулевая матрица, неверно. ■

Определение 1. Пусть Z — непустое подмножество множества $\{1, 2, \ldots, \mu\}$ номеров строк и столбцов матрицы $P = ||P_{ij}||$. Главной подматрицей, соответствующей множеству Z, назовём квадратную матрицу $Q_Z = ||Q_{ij}||$ порядка μ, такую, что при

всех $i, j \in Z$ выполняются неравенства $0 \leqslant Q_{ij} \leqslant P_{ij}$, а при $i \notin Z$ или $j \notin Z$ — равенство $Q_{ij} = 0$.

Определение 2 [11]. Квадратную матрицу $T = ||t_{ij}||$ будем называть дважды стохастической, если $t_{ij} \geqslant 0$ и

$$\sum_{j=1}^{n} t_{ij} = 1,\ 1 \leqslant i \leqslant n; \quad \sum_{i=1}^{n} t_{ij} = 1,\ 1 \leqslant j \leqslant n.$$

В случае, когда мощность алфавита шифрвеличин равна двум, множество возможных значений априорных вероятностей шифробозначений $p_s = \mathsf{P}\{y = y_s\} = \mathsf{P}\{y = s\}$, где $s = 1, \ldots, \mu$, допускает описание на основе теоремы Биркгофа о классификации дважды стохастических матриц [11]. В [14] такие матрицы называются двояко стохастическими.

Замечание 1. Пусть $\tau = \min\{p_1, \ldots, p_\mu\}$. Тогда, если $\tau = 0$, то среди $p_1, \ldots, p_\mu$ есть нуль, и в матрице P есть (для некоторого i) столбец и строка с номером i, все элементы которых — нули, так что в этом случае матрица P определяется некоторой своей подматрицей размерами $\mu_1 \times \mu_1$ с $\mu_1 < \mu$, в которой нет ни нулевых строк, ни нулевых столбцов. Если $\tau > 0$, то при $\tau = \max\{p_1, \ldots, p_\mu\}$ матрица $\dfrac{1}{\tau}P$ — дважды стохастическая.

Замечание 2. Каждой дважды стохастической матрице размера $\mu \times \mu$ соответствует матрица равновероятных распределений, которая получается из данной матрицы делением каждого её элемента на μ. Здесь имеется в виду не равновероятность ключей, а равенство всех априорных вероятностей шифробозначений, т. е. $p_1 = p_2 = \ldots = p_\mu$.

Замечание 3. Главная подматрица равновероятных распределений — это главная подматрица матрицы P, такая, что если вычеркнуть в ней нулевые строки и столбцы, то получится матрица равновероятных распределений.

Определение 3. Пусть $(i_1, i_2, \ldots, i_d)$ — нормальный цикл длины $d \geqslant 1$ матрицы P. Матрицей $C^{(i_1,i_2,\ldots,i_d)} = ||C_{ij}||$ нормального цикла $(i_1, i_2, \ldots, i_d)$ назовём квадратную матрицу порядка μ, в которой

$$C_{i_1 i_2}^{(i_1,i_2,\ldots,i_d)} = C_{i_2 i_3}^{(i_1,i_2,\ldots,i_d)} = \ldots = C_{i_d i_1}^{(i_1,i_2,\ldots,i_d)} = 1,$$

а остальные элементы равны нулю.

Матрица $C^{(i_1,i_2,\ldots,i_d)}$ — это в точности матрица перестановки подматрицы, полученная из матрицы P вычеркиванием строк и столбцов, номера которых не лежат в Z. Отметим, что сумма элементов i-й строки (или j-го столбца) матрицы $C^{(i_1,i_2,\ldots,i_d)}$ равна нулю, если $i \notin (i_1, i_2, \ldots, i_d)$ $(j \notin (i_1, i_2, \ldots, i_d))$, и равна 1, если $i \in (i_1, i_2, \ldots, i_d)$ $(j \in (i_1, i_2, \ldots, i_d))$.

Пример 1. Пусть $\mu = 3$ и матрица P имеет нулевую диагональ. Нормальные наборы при $|Z| = 3$, $Z = \{1, 2, 3\}$ задаются матрицами перестановок

$$C^{(1,2,3)} = C^{(2,3,1)} = C^{(3,1,2)} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad C^{(1,3,2)} = C^{(2,1,3)} = C^{(3,2,1)} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

которым соответствует произвольная дважды стохастическая матрица 3×3 с нулевой диагональю

$$T_Z = \tau_1 \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} + \tau_2 \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & \tau_1 & \tau_2 \\ \tau_2 & 0 & \tau_1 \\ \tau_1 & \tau_2 & 0 \end{pmatrix}, \quad \tau_1 \geqslant 0, \quad \tau_2 \geqslant 0, \quad \tau_1 + \tau_2 = 1,$$

и, тем самым, произвольная матрица P_Z равновероятного распределения (с равными априорными вероятностями)

$$P_{\{1,2,3\}} = \frac{1}{3} \begin{pmatrix} 0 & \tau_1 & \tau_2 \\ \tau_2 & 0 & \tau_1 \\ \tau_1 & \tau_2 & 0 \end{pmatrix}.$$

При $|Z| = 2$ нормальные циклы задаются матрицами

$$Z = \{1,2\} \Rightarrow C^{(1,2)} = C^{(2,1)} = T_Z = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

$$Z = \{1,3\} \Rightarrow C^{(1,3)} = C^{(3,1)} = T_Z = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

$$Z = \{2,3\} \Rightarrow C^{(2,3)} = C^{(3,2)} = T_Z = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

которым соответствуют единственные матрицы равновероятных распределений

$$P_{\{1,2\}} = \frac{1}{2} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \; P_{\{1,3\}} = \frac{1}{2} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \; P_{\{2,3\}} = \frac{1}{2} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Наконец, при $|Z| = 1$ нормальных циклов нет, так как диагональ матрицы P — нулевая.

3. Описание множества матриц вероятностей ключей

Пусть Z — непустое подмножество множества $\{1, 2, \ldots, \mu\}$ номеров строк и столбцов матрицы $P = ||\,\mathsf{P}_{ij}\,||$. Каждому множеству Z поставим в соответствие некоторое число $\rho_Z \geqslant 0$. Тогда можно составить матрицу

$$\sum_{\substack{Z \subset \{1,2,\ldots,\mu\}, \\ Z \neq \varnothing}} \rho_Z \cdot P_Z, \qquad \sum_{\substack{Z \subset \{1,2,\ldots,\mu\}, \\ Z \neq \varnothing}} \rho_Z = 1, \tag{3}$$

удовлетворяющую условиям (1) и (2). Справедлива

Теорема 1. Матрица P с неотрицательными элементами, удовлетворяющая условиям (1) и (2), лежит в выпуклой оболочке главных подматриц P_Z равновероятных распределений и определяется формулой (3), где суммирование проводится по всем непустым подмножествам Z множества номеров строк и $\rho_Z \geqslant 0$.

Доказательство. Согласно замечаниям 1–3, матрица, определяемая формулой (3), удовлетворяет условиям (1) и (2) совершенности шифра. Пусть неотрицательная матрица P удовлетворяет условиям (1) и (2), где $p_j \geqslant 0$, $\mathsf{P}_{st} \geqslant 0$ и $j, s, t = 1, \ldots, \mu$. Доказательство проведём в четыре этапа.

1. *Устранение нулевых априорных вероятностей.* Если $p_m = 0$, где $m \in \{1, \ldots, \mu\}$, то сумма элементов m-й строки (m-го столбца) матрицы P равна нулю. Поэтому, отбрасывая эти нулевые строку и столбец, придём к матрице P' порядка $\mu - 1$. Положим $P := P'$, $\mu := \mu - 1$. Продолжая исключать нулевые строки и столбцы, придём к матрице, для которой $p_i > 0$ для всех $i = 1, \ldots, \mu$ и в каждой строке и каждом столбце есть хотя бы один ненулевой элемент.

Пусть неотрицательная матрица P удовлетворяет условиям (1) и (2), где все $p_i > 0$, $i = 1, \ldots, \mu$, и в каждой строке и каждом столбце данной матрицы есть хотя бы один ненулевой элемент.

2. *Устранение нормальных циклов.* Обнулим некоторые элементы матрицы P с соответствующим уменьшением значений p_i и сохранением равенств (1), но без сохранения равенства (2).

Начнём с диагональных элементов. Если $\mathsf{P}_{ii} > 0$ для некоторого i, то построим новую матрицу P', в которой $\mathsf{P}'_{st} := \mathsf{P}_{st}$ для всех пар $\{s, t\}$, кроме случая $s = t = i$. Положим

$$Q_{(i)} := \mathsf{P}_{ii},\ \mathsf{P}'_{ii} := 0,\ p'_i := p_i - \mathsf{P}_{ii} = p_i - Q_{(i)}.$$

Поскольку $p_i = \mathsf{P}_{ii} + p'_i$, то $p_i \geqslant \mathsf{P}_{ii}$ и, следовательно, $p'_i \geqslant 0$. Переобозначая $\mathsf{P}_{st} := \mathsf{P}'_{st}$, $p_i := p'_i$, получим выполнение равенств (1). Перебирая таким образом все ненулевые диагональные элементы, придём к матрице P, которая удовлетворяет равенствам (1) и в которой все диагональные элементы равны нулю.

Далее будем обнулять элементы матрицы P, симметричные относительно главной диагонали, т. е. элементы P_{st} и P_{ts}, где $s \neq t$, $\mathsf{P}_{st} > 0$, $\mathsf{P}_{ts} > 0$. Положим

$$Q_{(s,t)} := \min\{\mathsf{P}_{st},\ \mathsf{P}_{ts}\},\ \mathsf{P}_{st} := \mathsf{P}_{st} - Q_{(s,t)},\ \mathsf{P}_{ts} := \mathsf{P}_{ts} - Q_{(s,t)},\ p_s := p_s - Q_{(s,t)},\ p_t := p_t - Q_{(s,t)}.$$

Перебирая таким образом все пары элементов P_{st} и P_{ts}, придём к матрице P, в которой нулевые не только диагональные элементы, но и для каждой пары $\{s, t\}$, где $s \neq t$, элемент $\mathsf{P}_{st} = 0$, или $\mathsf{P}_{ts} = 0$, или $\mathsf{P}_{st} = \mathsf{P}_{ts} = 0$.

Заметим, что, согласно определению 1, выше рассмотрены нормальные циклы длины $d = 1$ и $d = 2$ и из матрицы P вычитались главные подматрицы матрицы P, пропорциональные соответственно матрицам $C^{(i)}$ и $C^{(s,t)}$ нормальных циклов (i) и (s, t):

$$P := P - \sum_{(i)} \mathsf{P}_{ii} \cdot C^{(i)} = P - \sum_{(i)} Q_{(i)} \cdot C^{(i)}, \quad P := P - \sum_{(s,t)} Q_{(s,t)} \cdot C^{(s,t)}.$$

Отметим также, что при таком зануленении элементов матрицы P количество нулевых циклов возрастает, а количество нормальных циклов в матрице P убывает.

Аналогично будем действовать при $d \geqslant 3$. Пусть матрица P не имеет нормальных циклов длины $d = m - 1$, где $3 \leqslant m \leqslant \mu$. Будем устранять нормальные циклы $(i_1, i_2, \ldots, i_d)$ при $d = m$. Для этого положим

$$Q_{(i_1,i_2,\ldots,i_d)} := \min\{\mathsf{P}_{i_1i_2}, \mathsf{P}_{i_2i_3}, \ldots, \mathsf{P}_{i_{d-1}i_d}, \mathsf{P}_{i_di_1}\},$$
$$\mathsf{P}_{i_1i_2} := \mathsf{P}_{i_1i_2} - Q_{(i_1,i_2,\ldots,i_d)},\ \mathsf{P}_{i_2i_3} := \mathsf{P}_{i_2i_3} - Q_{(i_1,i_2,\ldots,i_d)}, \ldots, \mathsf{P}_{i_di_1} := \mathsf{P}_{i_di_1} - Q_{(i_1,i_2,\ldots,i_d)},$$
$$p_{i_1} := p_{i_1} - Q_{(i_1,i_2,\ldots,i_d)},\ p_{i_2} := p_{i_2} - Q_{(i_1,i_2,\ldots,i_d)}, \ldots, p_{i_d} := p_{i_d} - Q_{(i_1,i_2,\ldots,i_d)},$$

т. е. из матрицы P будем вычитать её главные подматрицы, пропорциональные матрицам $C^{(i_1,i_2,\ldots,i_d)}$ её нормальных циклов $(i_1,i_2,\ldots,i_d)$:

$$P' = P - \sum_{(i_1,i_2,\ldots,i_d)} Q_{(i_1,i_2,\ldots,i_d)} \cdot C^{(i_1,i_2,\ldots,i_d)}.$$

В силу конечности множества нормальных циклов за конечное число шагов придём к случаю, когда в матрице P отсутствуют нормальные циклы длины $d = m$.

Последовательно проводя данную процедуру, с увеличением длины d нормальных циклов на единицу придём к нормальным циклам длины $d = \mu$ и, после завершения процедуры, получим неотрицательную матрицу P, не имеющую нормальных циклов.

3. *Получение вида матрицы.* Согласно лемме 1, полученная неотрицательная матрица P — нулевая, а сумма всех отнятых матриц равна исходной матрице P. Следовательно, исходная матрица P удовлетворяет равенству

$$P = \sum_{d=1}^{\mu} \sum_{(i_1,i_2,\ldots,i_d)} Q_{(i_1,i_2,\ldots,i_d)} \cdot C^{(i_1,i_2,\ldots,i_d)}, \tag{4}$$

где $Q_{(i_1,i_2,\ldots,i_d)} \geqslant 0$. Матрица $Q^{(i_1,i_2,\ldots,i_d)} = Q_{(i_1,i_2,\ldots,i_d)} \cdot C^{(i_1,i_2,\ldots,i_d)}$ является главной подматрицей исходной матрицы P, согласно определению 2, со множеством $Z = \{i_1,i_2,\ldots,i_d\}$.

Для любой пары (i,j) имеем, в силу равенства (4), равенство $\mathsf{P}_{ij} = Q_{(i)}$ при $i = j$, а при $i \neq j$ и $d \geqslant 2$ имеем

$$\mathsf{P}_{ij} = \sum_{(i_1,i_2,\ldots,i_d)} Q_{(i_1,i_2,\ldots,i_d)},$$

где $i_1 = i$ и $i_2 = j$, так как нормальные циклы совпадают при циклической перестановке их элементов. Поскольку каждая такая пара (i,j) лежит в некотором цикле, а для элементов матрицы P имеем равенство $\sum\limits_{i=1}^{\mu}\sum\limits_{j=1}^{\mu} \mathsf{P}_{ij} = 1$, получаем, что

$$\sum_{(i_1,i_2,\ldots,i_d)} Q_{(i_1,i_2,\ldots,i_d)} = 1. \tag{5}$$

Следовательно, неотрицательная матрица P, удовлетворяющая условию (1), лежит в выпуклой оболочке матриц нормальных циклов — это аналог теоремы Биркгофа.

4. *Переход к равенству* (3). Далее для каждого $Z \subset \{1,2,\ldots,\mu\}$, где $d = |Z| \geqslant 2$, рассмотрим все нормальные циклы длины d, элементы которых берутся из Z. Это означает, что если $Z = \{j_1,j_2,\ldots,j_d\}$, то цикл $(i_1,i_2,\ldots,i_d)$ — это перестановка чисел $j_1,j_2,\ldots,j_d$. Положим

$$\tilde{P}_Z = \sum_{\{i_1,i_2,\ldots,i_d\}=Z} Q_{(i_1,i_2,\ldots,i_d)} \cdot C^{(i_1,i_2,\ldots,i_d)}, \quad \rho_Z = Q_Z = \sum_{\{i_1,i_2,\ldots,i_d\}=Z} Q_{(i_1,i_2,\ldots,i_d)},$$

где $\rho_Z = Q_Z \geqslant 0$ и, согласно (5), $\sum\limits_{\{i_1,i_2,\ldots,i_d\}=Z} \rho_Z = 1$. Тогда

$$\tilde{P}_Z = \left[\sum_{\{i_1,i_2,\ldots,i_d\}=Z} Q_{(i_1,i_2,\ldots,i_d)}\right] \cdot T_Z = \rho_Z \cdot T_Z,$$

где T_Z — дважды стохастическая матрица, номера строк и столбцов которой принадлежат множеству $\{i_1,i_2,\ldots,i_d\} = Z$.

Обозначим

$$P_Z = \frac{1}{d} \cdot T_Z$$

— главная подматрица равновероятных распределений, элементы которой $(\mathsf{P}_Z)_{ij} = 0$ при $i \notin Z$ или $j \notin Z$; $(\mathsf{P}_Z)_{ij} = (T_Z)_{ij}/d$ при $i, j \in Z$.

Таким образом, для неотрицательной матрицы P, удовлетворяющей условиям (1) и (2), выполняется равенство

$$P = \sum_{\substack{Z \subset \{1,2,\ldots,\mu\}, \\ Z \neq \varnothing}} \rho_Z \cdot P_Z, \quad \text{где} \sum_{\substack{Z \subset \{1,2,\ldots,\mu\}, \\ Z \neq \varnothing}} \rho_Z = 1,$$

т. е. матрица P лежит в выпуклой оболочке главных подматриц P_Z равновероятных распределений. ■

В обзоре [15] представлены некоторые работы, примыкающие к проблематике теоремы Биркгофа. В [16, 17] приведены результаты об экстремальных точках для полиэдра конечных симметрических матриц с заданными суммами по строкам. Для специального класса дважды стохастических матриц, определяемого границами для элементов матрицы, в [18] строятся экстремальные точки. В доказанной аналогичным образом выше теореме 1 описан соответствующий полиэдр указанием его вершин (экстремальных точек), которые представляют собой нормальные циклы.

Рассмотрим примеры, иллюстрирующие теорему 1.

Пример 2. Пусть $\mu = 2$ и матрица P имеет нулевую диагональ. Тогда $p_{12} = p_{21} = p_1 = p_2 = 1/2$ и матрица P единственна:

$$P = \begin{pmatrix} 0 & 1/2 \\ 1/2 & 0 \end{pmatrix} = \frac{1}{2} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \frac{1}{2} \cdot T,$$

где T — дважды стохастическая матрица. Это частный случай теоремы Шеннона для эндоморфного минимального шифра.

Пример 3. Пусть $\mu = 3$, P имеет нулевую диагональ и

$$a = \tau_1 \cdot \rho_{\{1,2,3\}} \geqslant 0, \quad b = \tau_2 \cdot \rho_{\{1,2,3\}} \geqslant 0, \quad c = \rho_{\{1,2\}} \geqslant 0, \quad d = \rho_{\{1,3\}} \geqslant 0, \quad e = \rho_{\{2,3\}} \geqslant 0,$$

где произвольные параметры τ_1, τ_2, ρ_Z таковы, что $\tau_1 \geqslant 0$, $\tau_2 \geqslant 0$, $\tau_1 + \tau_2 = 1$, $\rho_Z \geqslant 0$,

$$\rho_{\{1,2,3\}} + \rho_{\{1,2\}} + \rho_{\{1,3\}} + \rho_{\{2,3\}} = a + b + c + d + e = 1.$$

Тогда при $\lambda = 2$ и $\mu = 3$ матрица P в общем случае определяется формулой

$$P = \frac{1}{3}a \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} + \frac{1}{3}b \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} + \frac{1}{2}c \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} +$$

$$+\frac{1}{2}d \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} + \frac{1}{2}e \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a/3 + c/2 & \frac{1}{3}b + \frac{1}{2}d \\ b/3 + c/2 & 0 & a/3 + e/2 \\ a/3 + d/2 & b/3 + e/2 & 0 \end{pmatrix},$$

где $a, b, c, d, e \geqslant 0$ — произвольные параметры, такие, что $a + b + c + d + e = 1$.

Отметим, что для любых $a \geqslant 0$, $e \geqslant 0$, где $2a + 3e = 3/5$, и однозначно по ним определённым параметрам $b = a + 3/40$, $c = e + 11/40$, $d = e + 1/20$ получаются числовые значения примера 2.2.10 из [3]. В частности, они получаются при крайних значениях параметров: $a = 0$, $e = 1/5$ и $a = 3/10$, $e = 0$.

4. Описание множества априорных вероятностей шифробозначений

Если для соблюдения условия инъективности операций зашифрования потребовать, чтобы диагональ в матрице P была нулевой, то не каждый набор априорных вероятностей элементов множества Y шифробозначений может быть реализован в совершенном по Шеннону шифре. Справедлива

Лемма 2. Точка $(p_1, \ldots, p_\mu)$ в $\mathbb{R}^\mu$ $(\mu \geqslant 2)$, координаты которой удовлетворяют условиям

$$p_1 + \ldots + p_\mu = 1, \quad 0 \leqslant p_i \leqslant \frac{1}{2}, \quad i = 1, \ldots, \mu, \tag{6}$$

лежит в выпуклой оболочке точек

$$V_{ij} = (0, \ldots, 0, v_i, 0, \ldots, 0, v_j, 0, \ldots, 0) = (0, \ldots, 0, \frac{1}{2}, 0, \ldots, 0, \frac{1}{2}, 0, \ldots, 0),$$

где $i, j = 1, \ldots, \mu,\ i \neq j$.

Доказательство. Пусть $p_1 + \ldots + p_\mu = 1$, $p_i \geqslant 0$ $(i = 1, \ldots, \mu)$. Эти условия определяют $(\mu - 1)$-мерный симплекс в μ-мерном пространстве $\mathbb{R}^\mu$. Полупространства $p_i \leqslant 1/2$, $i = 1, \ldots, \mu$, высекают в этом симплексе $(\mu-1)$-мерный выпуклый многогранник, на границе которого хотя бы одно из этих неравенств обращается в равенство. Найдём его вершины. На гиперпространстве $p_j = 1/2$, например, $p_1 = 1/2$ при $j = 1$, имеем наибольшее евклидово расстояние от начала координат

$$\sqrt{p_1^2 + p_2^2 + \ldots + p_\mu^2} = \sqrt{\frac{1}{4} + p_2^2 + \ldots + p_\mu^2} \leqslant \sqrt{\frac{1}{4} + (p_2 + \ldots + p_\mu)^2} = \sqrt{\frac{1}{4} + \left(\frac{1}{2}\right)^2} = \frac{\sqrt{2}}{2},$$

и оно достигается на вершинах в силу центральной симметричности этой гиперграни; однако неравенство обращается в равенство при $p_1^2 + p_2^2 + \ldots + p_\mu^2 = (p_1 + p_2 + \ldots + p_\mu)^2$, что может быть только если все p_i обращаются в нуль, кроме одного: $p_i = 0$ для $i = 2, \ldots, \mu$, $i \neq j$; $p_j = 1/2$. Итак, на этой грани имеется $\mu - 1$ вершин с двумя ненулевыми координатами $p_1 = 1/2$, $p_j = 1/2$, $j \in \{2, \ldots, \mu\}$. Ясно, что это верно для любой грани, поэтому описываемый многогранник имеет $\mu(\mu-1)/2$ вершин V_{ij} с двумя ненулевыми координатами $p_i = 1/2$, $p_j = 1/2$, $i, j \in \{1, 2, \ldots, \mu\}$, $i \neq j$. ■

В приложении к совершенным шифрам лемма 2 означает, что любой набор чисел p_i, $i = 1, \ldots, \mu$, с условиями (6) может быть набором априорных вероятностей шифробозначений совершенного шифра. Справедлива

Теорема 2. Набор чисел $p_1, \ldots, p_\mu$ при $\mu \geqslant 2$ является набором априорных вероятностей шифробозначений совершенного шифра в модели Σ_B с мощностью алфавита шифрвеличин, равной двум, тогда и только тогда, когда эти числа удовлетворяют условиям (6).

Доказательство. Необходимость. Пусть набор чисел $p_1, \ldots, p_\mu$ при $\mu \geqslant 2$ является набором априорных вероятностей шифробозначений совершенного шифра в модели Σ_B с мощностью алфавита шифрвеличин равной двум. Обозначим через $\sigma_Z^{(j)}$ сумму элементов j-й строки матрицы P_Z главной подматрицы со множеством строк Z. Так как $P_Z = T_Z/|Z|$, где T_Z соответствует дважды стохастической матрице, то

$$\sigma_Z^{(j)} = \begin{cases} 0, & j \notin Z, \\ 1, & j \in Z. \end{cases}$$

Имеем $\sigma_Z^{(j)} \leqslant 1/|Z| \leqslant 1/2$ при любом j, если диагональ нулевая и, стало быть, $|Z| \geqslant 2$. Суммируя все элементы j-й строки для определения p_j, из формулы (3) ввиду

$$P = \sum_{\substack{Z\subset\{1,2,\ldots,\mu\},\\ |Z|\geqslant 2}} \rho_Z P_Z$$

получаем формулу

$$p_j = \sum_{\substack{Z\subset\{1,2,\ldots,\mu\},\\ |Z|\geqslant 2}} \rho_Z \sigma_Z^{(j)} \leqslant \frac{1}{2}\sum_Z \rho_Z = \frac{1}{2},$$

поскольку из (2) сумма всех коэффициентов ρ_Z равна единице. Итак, априорные вероятности p_j $(j = 1, \ldots, \mu)$ совершенного шифра лежат в сегменте

$$0 \leqslant p_j \leqslant \frac{1}{2}.$$

Достаточность докажем путём построения симметричной матрицы. Пусть, в силу леммы 2, имеется разложение $P = \sum\limits_{i=1}^{\mu-1}\sum\limits_{j=i+1}^{\mu} r_{ij}V_{ij}$, в котором $\sum\limits_{i=1}^{\mu-1}\sum\limits_{j=i+1}^{\mu} r_{ij} = 1$, $r_{ij} \geqslant 0$, $1 \leqslant i < j \leqslant \mu$.

Сопоставляя каждой точке V_{ij} матрицу W_{ij}, у которой только два ненулевых элемента $w_{ij} = 1/2$ и $w_{ji} = 1/2$, построим симметричную матрицу P, лежащую в выпуклой оболочке этих матриц, как сумму $P = \sum\limits_{i=1}^{\mu-1}\sum\limits_{j=i+1}^{\mu} r_{ij}W_{ij}$. Для любого l, $1 \leqslant l \leqslant \mu$, выполняется равенство

$$p_l = \frac{1}{2}\sum\nolimits_{j=l+1}^{\mu} r_{ij} + \frac{1}{2}\sum_{i=1}^{l-1} r_{il},$$

и сумма элементов l-й строки (l-го столбца) матрицы P равна p_l, т. е. условия (1) и (2) выполнены. ■

Заключение

Таким образом, в работе описано множество (полиэдр) матриц вероятностей ключей и множество априорных вероятностей шифробозначений неэндоморфных максимальных совершенных шифров с двумя шифрвеличинами. Отметим, что в случае, когда мощность множества шифрвеличин строго больше двух, эта задача сильно усложняется по причине отсутствия аналога теоремы Биркгофа о дважды стохастических матрицах.

Получение обобщений теоремы Шеннона на неэндоморфные совершенные шифры с неравновероятными ключами и шифробозначениями оправдано изучением современных аналогов совершенных шифров [3], обладающих такими свойствами, как имитостойкость и помехоустойчивость, с более полным учётом свойств канала связи.

ЛИТЕРАТУРА

1. *Шеннон К.* Теория связи в секретных системах // Работы по теории информации и кибернетике. М.: Наука, 1963. С. 333–402.
2. *Андреев Н. Н., Петерсон А. П., Прянишников К. В., Старовойтов А. В.* Основоположник отечественной засекреченной телефонной связи // Радиотехника. 1998. № 8. С. 8–12.
3. *Зубов А. Ю.* Совершенные шифры. М.: Гелиос АРВ, 2003. 160 с.
4. *Stinson D. R.* A construction for authentication secrecy codes from certain combinatorial designs // Proc. Crypto'87. Advances in Cryptology. 1998. P. 355–366.

5. *De Soete M.* Some constructions for authentication-secrecy codes // Proc. Crypto'87. Advances in Cryptology. 1998. P. 57–75.
6. *Goldlewsky P. and Mitchell C.* Key-minimal cryptosystems for unconditional secrecy // J. Cryptology. 1990. No. 1. P. 1–25.
7. *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии. М.: Гелиос АРВ, 2001. 480 с.
8. *Бабаш А. В., Шанкин Г. П.* Криптография (аспекты защиты). М.: СОЛОН-Р, 2002. 512 с.
9. *Брассар Ж.* Современная криптология. М.: ПОЛИМЕД, 1999. 176 с.
10. *Stinson D. R.* Cryptography: Theory and Practice. N. Y.: CRC Press, 1995. 616 p.
11. *Birkhoff G. D* Tres observations sobre el algebra lineal // Revista Universidad Nacional Tucuman. 1946. Ser. A. V. 5. P. 147–151.
12. *Медведева Н. В., Титов С. С.* О неминимальных совершенных шифрах // Прикладная дискретная математика. Приложение. 2013. № 6. С. 42–44.
13. *Медведева Н. В., Титов С. С.* Неэндоморфные совершенные шифры с двумя шифрвеличинами // Прикладная дискретная математика. Приложение. 2015. № 8. С. 63–66.
14. *Гантмахер Ф. Р.* Теория матриц. М.: Наука, 1967. 576 с.
15. *Носов В. А., Сачков В. Н., Тараканов В. Е.* Комбинаторный анализ (неотрицательные матрицы, алгоритмические проблемы) // Итоги науки и техники. Сер. Теор. вероятн. Мат. стат. Теор. кибернет. Т. 21. М.: ВИНИТИ, 1983. С. 120–178.
16. *Converse G. and Katz M.* Symmetric matrices with given row sums // J. Combin. Theory. 1975. Ser. A. V. 18. No. 2. P. 171–176.
17. *Lewin M.* On the extreme points of the polytope of symmetric matrices with given row sums // J. Combin. Theory. 1977. Ser. A. V. 23. No. 2. P. 223–231.
18. *Koontz M.* Convex sets of some doubly stochastic matrices // J. Combin. Theory. 1978. Ser. A. V. 24. No. 1. P. 111–112.

REFERENCES

1. *Shennon K.* Teoriya svyazi v sekretnykh sistemakh [Communication theory of secrecy systems]. Raboty po Teorii Informatsii i ibernetike. Moscow, Nauka Publ., 1963, pp. 333–402. (in Russian)
2. *Andreev N. N., Peterson A. P., Pryanishnikov K. V., Starovoytov A. V.* Osnovopolozhnik otechestvennoy zasekrechennoy telefonnoy svyazi [The founder of the national classified telephone]. Radiotekhnika, 1998, no. 8, pp. 8–12. (in Russian)
3. *Zubov A. Yu.* Sovershennye shifry [Perfect Ciphers]. Moscow, Gelios ARV Publ., 2003. 160 p. (in Russian)
4. *Stinson D. R.* A construction for authentication secrecy codes from certain combinatorial designs. Proc. Crypto'87. Advances in Cryptology, 1998, pp. 355–366.
5. *De Soete M.* Some constructions for authentication-secrecy codes. Proc. Crypto'87. Advances in Cryptology, 1998, pp. 57–75.
6. *Goldlewsky P. and Mitchell C.* Key-minimal cryptosystems for unconditional secrecy. J. Cryptology, 1990, no. 1, pp. 1–25.
7. *Alferov A. P., Zubov A. Yu., Kuzmin A. S., Cheremushkin A. V.* Osnovy kriptografii [Basics of cryptography]. Moscow, Gelios ARV Publ., 2001. 480 p. (in Russian)
8. *Babash A. V., Shankin G. P.* Kriptografiya (aspekty zashchity) [Cryptography (protection aspects)]. Moscow, SOLON-R Publ., 2002. 512 p. (in Russian)
9. *Brassar Zh.* Sovremennaya kriptologiya [Modern Cryptology]. Moscow, POLIMED, 1999. 176 p. (in Russian)
10. *Stinson D. R.* Cryptography: Theory and Practice. N. Y., CRC Press, 1995. 616 p.

11. *Birkhoff G. D* Tres observations sobre el algebra lineal. Revista Universidad Nacional Tucuman, 1946, ser. A, vol. 5, pp. 147–151.
12. *Medvedeva N. V., Titov S. S.* O neminimal'nykh sovershennykh shifrakh [On non-minimal perfect ciphers]. Prikladnaya diskretnaya matematika. Prilozhenie, 2013, no. 6, pp. 42–44. (in Russian)
13. *Medvedeva N. V., Titov S. S.* Neendomorfnye sovershennye shifry s dvumya shifrvelichinami [Non-endomorphic perfect ciphers with two elements in plaintext alphabet]. Prikladnaya diskretnaya matematika. Prilozhenie, 2015, no. 8, pp. 63–66. (in Russian)
14. *Gantmacher F. R.* The Theory of Matrices. N. Y., Chelsea Publ. Company, 1959.
15. *Nosov V. A., Sachkov V. N., Tarakanov V. E.* Combinatorial analysis (nonnegative matrices, algorithmic problems). J. Soviet Math., 1985, vol. 29, no. 1, pp. 1051–1099.
16. *Converse G. and Katz M.* Symmetric matrices with given row sums. // J. Combin. Theory, 1975, ser. A, vol. 18, no. 2, pp. 171–176.
17. *Lewin M.* On the extreme points of the polytope of symmetric matrices with given row sums. J. Combin. Theory, 1977, ser. A, vol. 23, no. 2, pp. 223–231.
18. *Koontz M.* Convex sets of some doubly stochastic matrices. J. Combin. Theory, 1978, ser. A, vol. 24, no. 1, pp. 111–112.

УДК 519.719.2

ОБ ОДНОЙ СХЕМЕ ГИБРИДНОГО ШИФРОВАНИЯ

А. Ю. Нестеренко*, А. В. Пугачев**

**Национальный исследовательский университет «Высшая школа экономики»,*
***Московский государственный университет информационных технологий, радиотехники и электроники,*
г. Москва, Россия

Предлагается гибридная схема шифрования, которая базируется на схеме асимметричного шифрования Эль-Гамаля и использует предварительно распределённые секретные ключи для защиты от навязывания сообщений. Стойкость схемы основывается на высокой трудоёмкости решения задачи дискретного логарифмирования в группе точек эллиптической кривой. Основная особенность предлагаемой схемы заключается в том, что шифруемое сообщение не представляется в виде точки эллиптической кривой, что позволяет зашифровывать длинные сообщения. Приводится обоснование стойкости предложенной схемы, а также описание её возможных модификаций, направленных на выполнение дополнительных криптографических свойств, например аутентификации отправителя сообщения. Приводятся также результаты практической реализации схемы.

Ключевые слова: *асимметричное шифрование, схема Эль-Гамаля, эллиптические кривые, аутентификация отправителя сообщений.*

DOI 10.17223/20710410/30/5

A NEW HYBRID ENCRYPTION SCHEME

A. Yu. Nesterenko*, A. V. Pugachev**

**National Research University Higher School of Economics,*
***Moscow State University of Information Technologies, Radio Engineering and Electronics, Moscow, Russia*

E-mail: nesterenko_a_y@mail.ru, a_pugachev@mirea.ru

A new hybrid encryption scheme based on ElGamal asymmetric encryption scheme with distributed secret keys is presented. The keys are used for defence against unauthorised intrusion of encrypted messages. The security of the scheme is based on elliptic curve discrete logarithm problem. The main feature of the scheme is the fact that plain message is not represented as a point of elliptic curve, hence, we can encrypt a long messages. We validate the cryptographic properties of the scheme and give some examples of its practical evaluations.

Keywords: *asymmetric encryption, authentication, ElGamal scheme, elliptic curves.*

Введение

В настоящее время известно много схем асимметричного шифрования, позволяющих обеспечить процесс передачи зашифрованного сообщения от одного абонента

к другому. К таким схемам можно отнести схемы RSA, Эль-Гамаля, Рабина, Голдвассер — Микали и т. д. [1, гл. 8]. Стойкость каждой из перечисленных схем основывается на трудоёмкости решения некоторой теоретико-числовой задачи, например разложения больших чисел на множители или дискретного логарифмирования.

Основным недостатком асимметричных схем шифрования является тот факт, что они позволяют эффективно зашифровывать и расшифровывать только сообщения малой длины, например криптографические ключи. В связи с этим для шифрования длинных сообщений применяются так называемые «гибридные» схемы, в которых сообщение шифруется при помощи симметричного алгоритма шифрования, а ключ — при помощи асимметричной схемы [2].

В настоящей работе предлагается новый вариант схемы гибридного шифрования, основывающийся на схеме асимметричного шифрования Эль-Гамаля и использующий предварительно распределённые секретные ключи для защиты от навязывания сообщений. Кроме того, представлены несколько модификаций схемы, позволяющих её участникам:

— эффективно зашифровывать сообщения большой длины;
— использовать цифровую подпись для аутентификации отправителя сообщений.

В п. 1 приводится подробное описание предложенного нового варианта схемы асимметричного шифрования, определяется ключевая система, а также процедуры зашифрования и расшифрования сообщений. В п. 2 дан краткий анализ предложенной схемы: определены возможности нарушителя и перечень целей компрометации; рассмотрены основные атаки и показано, что при выполнении ряда предположений схема является стойкой.

В п. 3 приведены несколько модификаций предложенной схемы. Каждая модификация позволяет обеспечить дополнительные криптографические свойства, например обеспечить аутентификацию отправителя сообщений или увеличить длину шифруемого сообщения. В заключение приводятся результаты практической реализации схемы с конкретными значениями параметров и используемыми криптографическими примитивами.

1. Описание базовой схемы

1.1. Параметры схемы и её ключевая система

1) Пусть $p > 3$ — простое число. Рассмотрим эллиптическую кривую $\mathcal{E}$, заданную над конечным простым полем $\mathbb{F}_p$ сравнением

$$y^2 \equiv x^3 + ax + b \pmod{p}, \tag{1}$$

где $a, b \in \mathbb{F}_p$ удовлетворяют условию $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$.
2) Рассмотрим простое число $q > 2$, делящее порядок группы точек эллиптической кривой $\mathcal{E}$, и выберем точку $P = (x_P, y_P) \in \mathcal{E}$, которая порождает циклическую подгруппу $\langle P \rangle \subset \mathcal{E}$ порядка q.
3) Рассмотрим целое число m, такое, что $p < m < 2p^2$. Каждое сообщение s будем представлять в виде вычета по модулю m: $s \in \mathbb{Z}_m$.
4) Введём два простых отображения

$$f : \mathbb{F}_p \times \mathbb{F}_p \to \mathbb{Z}_m, \quad h : \mathbb{F}_p \times \mathbb{F}_p \times \mathbb{F}_p \to \mathbb{Z}_m,$$

которые будут использованы при зашифровании и расшифровании сообщений. В п. 1.3 мы дадим корректное определение этих отображений.

5) Пусть r — натуральное число. Будем использовать отображение

$$\mathrm{mac} : \mathbb{F}_q \times \mathbb{Z}_m \to \mathbb{Z}_r,$$

позволяющее вычислить код целостности или, другими словами, имитовставку сообщения $s \in \mathbb{Z}_m$, зависящую от некоторого секретного ключа из $\mathbb{F}_q$. В качестве такого отображения может выступать алгоритм HMAC [3] или отечественный алгоритм выработки имитовставки [4].

6) Для генерации ключа, используемого при выработке имитовставки, будем использовать функцию выработки ключа

$$\mathrm{kdf} : \mathbb{F}_p \times \mathcal{E} \to \mathbb{F}_q.$$

Примером функции выработки ключа может служить алгоритм, описанный в рекомендациях [5].

Далее будем считать, что все перечисленные параметры (целые числа p, a, b, q, m, r; точка эллиптической кривой $P = (x_P, y_P)$; отображения f, h, mac() и kdf()) известны как отправителю и получателю сообщения, так и нарушителю.

Теперь рассмотрим ключевую систему. Абонент Б, являющийся получателем сообщений, должен обладать следующими параметрами:

1) секретным ключом d — целым числом, удовлетворяющим неравенствам $0<d<q$;
2) открытым ключом Y — точкой эллиптической кривой $\mathcal{E}$, заданной парой координат (x_Y, y_Y) и определяемой равенством

$$Y = [d]P = \underbrace{P + \cdots + P}_{d \text{ раз}}.$$

Кроме того, будем считать, что абоненты А и Б обладают общим долговременным секретным ключом S — точкой эллиптической кривой $\mathcal{E}$, заданной парой своих координат (x_S, y_S) и удовлетворяющей сравнению (1). Дополнительно будем считать, что координата x_S выбрана таким образом, что величина $(ax_S + b)^2 + 4bx_S^3$ является квадратичным невычетом по модулю p.

1.2. Процедуры зашифрования и расшифрования

Для зашифрования сообщения $s \in \mathbb{Z}_m$ абонент А (отправитель сообщения) выполняет следующие шаги:

1) Вычисляет случайное целое число k, удовлетворяющее неравенствам $0 < k < q$.
2) Вычисляет точку $U = [k]Y$, $U = (x_U, y_U)$, эллиптической кривой $\mathcal{E}$ и определяет $\alpha, \beta \in \mathbb{F}_p$, где

$$\begin{cases} \alpha \equiv \dfrac{y_U - y_S}{x_U - x_S} \pmod p, \\ \beta \equiv \dfrac{y_S x_U - x_S y_U}{x_U - x_S} \pmod p. \end{cases} \tag{2}$$

3) Вычисляет точку $W = [k]P$, $W = (x_W, y_W)$, и определяет

$$t \equiv f(\alpha, y_U)s + h(\alpha, \beta, y_U) \pmod m. \tag{3}$$

4) Определяет ключ $d_U = \mathrm{kdf}(x_U, S)$. Затем вычисляет код целостности $\mathrm{mac}(d_U, s)$ и формирует сообщение

$$M = t||(x_W, y_W)||\,\mathrm{mac}(d_U, s). \tag{4}$$

Сообщение M является шифртекстом, который отправляется абоненту Б.

Легко видеть, что длина открытого текста s равна $\log_2 m$ бит, а длина соответствующего ему шифртекста M равна $\log_2 m + 2\log_2 p + \log_2 r$ бит.

В случае, когда преобразования f и h имеют вид

$$f(\alpha, y_U) \equiv \alpha \pmod m, \quad h(\alpha, \beta, y_U) \equiv \beta \pmod m,$$

предложенный способ зашифрования сообщения s имеет красивую геометрическую интерпретацию. Действительно, рассмотрим координаты точек S, U эллиптической кривой $\mathcal{E}$ как пары целых неотрицательных чисел. Расположим эти точки на действительной плоскости и проведём через них прямую линию. Рассмотрим открытый текст s как целое неотрицательное число, определяющее абсциссу некоторой точки T на данной прямой. Тогда шифртекст t есть ордината точки T, взятая по модулю m (рис. 1).

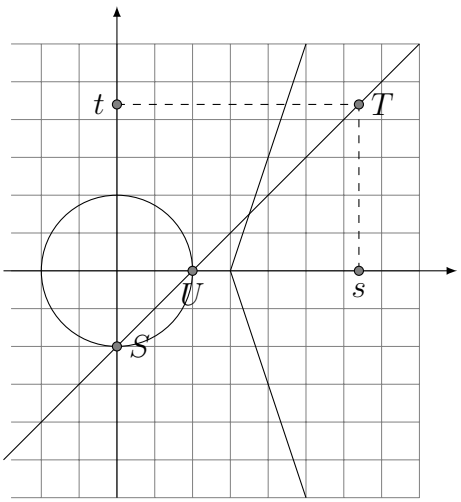

Рис. 1. Геометрическая интерпретация в простейшем случае

Поскольку абонент А при зашифровании сообщения s выбирает значение k случайным образом, вырабатываемая им точка $U = [k]P$, а следовательно, и прямая $t = f(\alpha, y_U)s + h(\alpha, \beta, y_U)$ также являются случайными.

Для расшифрования полученного сообщения M абонент Б представляет его в виде тройки $t \in \mathbb{Z}_m$, $W = (x_W, y_W) \in \mathcal{E}$ и кода целостности $\xi \in \mathbb{Z}_r$. Далее абонент Б выполняет следующие шаги:

1) Проверяет, что точка W принадлежит эллиптической кривой $\mathcal{E}$. В противном случае сообщение t не принимается.
2) Вычисляет точку $U = [d]W$, где $U = (x_U, y_U)$.
3) Используя сравнения (2), вычисляет значения $\alpha, \beta \in \mathbb{F}_p$ и определяет открытый текст s сравнением

$$s \equiv (t - h(\alpha, \beta, y_U))f^{-1}(\alpha, y_U) \pmod m. \tag{5}$$

4) Вычисляет ключ $d_U = \mathrm{kdf}(x_U, S)$ и код целостности $\mathrm{mac}(d_U, s)$. Если $\mathrm{mac}(d_U, s) = \xi$, то сообщение принимается и считается корректно расшифрованным. В противном случае сообщение не принимается.

1.3. Некоторые замечания о выборе параметров схемы

Сделаем несколько замечаний по выбору параметров схемы, влияющих как на корректность её работы, так и на её эксплуатационные качества.

Выбор долговременного ключа S

Для корректной работы предложенной схемы асимметричного шифрования должно выполняться условие

$$U \neq \pm S. \tag{6}$$

В противном случае выполнено сравнение $x_S \equiv x_U \pmod p$, и величины $\alpha, \beta \in \mathbb{F}_p$, удовлетворяющие равенствам (2), не могут быть корректно определены.

Выполнение условия (6) может быть обеспечено двумя способами. В первом случае можно выбрать эллиптическую кривую $\mathcal{E}$ таким образом, чтобы порядок её группы $|\mathcal{E}|$ удовлетворял равенству

$$|\mathcal{E}| = cqq_1,$$

где $q_1 > 2$ — некоторое большое простое число и $q_1 \neq q$; $c \geqslant 1$ — произвольное натуральное число. Тогда, выбирая в качестве S точку порядка q_1, получим, что для любого целого k, такого, что $0 < k < q$, выполнено условие

$$S \neq \pm U = \pm [k]P.$$

Во втором случае, когда порядок кривой $\mathcal{E}$ удовлетворяет равенству $|\mathcal{E}| = cq$ для некоторого натурального числа $c \geqslant 1$, можно модифицировать процедуру зашифрования сообщения s и проверять выполнение условия $U \neq \pm S$ на первом шаге алгоритма зашифрования. В случае невыполнения этого условия необходимо выбрать новое значение k.

Следует отметить, что если k выбирается случайно равновероятно из интервала $0 < k < q$, то вероятность получить равенство $U = \pm S$ мала и равна $2/(q-1)$.

Выбор значения параметра m и отображений f и h

Отметим, что выполнение условия $U \neq \pm S$ влечёт за собой выполнение условия $y_S \neq y_U$. В этом случае из (2) следует, что $\alpha \not\equiv 0 \pmod p$. Аналогично, для величины β выполнено следующее утверждение.

Лемма 1. Пусть величина $\beta \in \mathbb{F}_p$ определена сравнением (2). Пусть x-координата точки $S = (x_S, y_S) \in \mathbb{E}$ удовлетворяет условию

$$\left(\frac{(ax_S + b)^2 + 4bx_S^3}{p} \right) = -1,$$

где $\left(\frac{\cdot}{\cdot}\right)$ есть символ Лежандра. Тогда $\beta \not\equiv 0 \pmod p$.

Доказательство. Из (2) следует, что выполнение условия $\beta \equiv 0 \pmod p$ эквивалентно выполнению сравнения

$$y_S x_U \equiv y_U x_S \pmod p. \tag{7}$$

В силу выбора параметров схемы порядки точек U и S больше двух, поэтому их y-координаты отличны от нуля. Далее, если одна из x-координат, скажем x_U, сравнима с нулем по модулю p, то из (7) следует, что и вторая x-координата x_S также сравнима с нулем, что невозможно в силу (6). Таким образом, выполнение сравнения $\beta \equiv 0 \pmod p$ влечёт за собой сравнение

$$y_U \equiv \frac{y_S}{x_S} x_U \pmod p, \quad x_S \not\equiv 0 \pmod p.$$

Поскольку $(x_U, y_U) \in \mathcal{E}$, из последнего сравнения следует, что величина x_U должна являться корнем многочлена

$$\varphi(x) = x^3 - \left(\frac{y_S}{x_S}\right)^2 x^2 + ax + b$$

по модулю простого числа p. Легко проверить, что $\varphi(x_S) \equiv 0 \pmod p$; тогда можно записать сравнение

$$\varphi(x) \equiv (x - x_S)\left(x^2 - \frac{(ax_S + b)}{x_S^2}x - \frac{b}{x_S}\right) \pmod p. \tag{8}$$

В силу утверждения леммы, многочлен второй степени, входящий в произведение в правой части сравнения (8), не имеет корней в поле $\mathbb{F}_p$, поскольку его дискриминант

$$D \equiv \left(\frac{ax_S + b}{x_S^2}\right)^2 + \frac{4b}{x_S} \equiv \frac{(ax_S + b)^2 + 4bx_S^3}{x_S^4} \pmod p$$

является квадратичным невычетом по модулю p. ■

Теперь можно дать точное определение введённых ранее отображений f и h. Ввиду того, что значение $f(\alpha, y_U) \in \mathbb{Z}_m$ должно быть обратимо по модулю m, отображения f и h должны зависеть от значений параметра m, задающего длину шифруемого сообщения s.

Рассмотрим несколько вариантов.

1) Пусть m есть простое число или $m = p_1p_2$ есть произведение двух нечётных простых чисел, для которых выполнены неравенства $p < p_1 < p_2$. Поскольку вырабатываемая в алгоритме зашифрования величина α удовлетворяет соотношению $\alpha \not\equiv 0 \pmod p$, можно определить

$$f(\alpha, y_U) \equiv \alpha y_U \pmod m. \tag{9}$$

Порядок точки U равен q, поэтому $y_U \not\equiv 0 \pmod p$,

$$0 < \alpha y_U < m, \quad (\alpha, m) = 1.$$

Следовательно, значение $f(\alpha, y_U) = \alpha y_U$ обратимо по модулю m. Поскольку должно выполняться неравенство $m = p_1p_2 < 2p^2$, можно предъявить следующие оценки на величины p_1, p_2. Определим действительные величины γ_1, γ_2 неравенством $p_i < p + p^{\gamma_i}$, где $i = 1, 2$, и будем считать, что выполнено неравенство

$$0 < \gamma_1 < \gamma_2 < 1 - \log_p 3. \tag{10}$$

Тогда, учитывая, что из (10) следует неравенство $1 + \gamma_2 > 2\gamma_2$, получим

$$m = p_1p_2 < p^2 + p(p^{\gamma_1} + p^{\gamma_2}) + p^{\gamma_1+\gamma_2} < p^2 + 2p^{1+\gamma_2} + p^{2\gamma_2} < p^2 + 3p^{1-\log_p 3} = 2p^2.$$

2) Пусть $m = 2^n$ для некоторого натурального n и $m > 4p + 1$. Тогда можно определить

$$f(\alpha, y_U) \equiv 2(\alpha + y_U) + 1 \pmod m. \tag{11}$$

Поскольку $0 < \alpha < p$, $0 < y_U < p$, то получаем, что выполнено неравенство $1 < < f(\alpha, y_U) < 4p + 1 < m$; значение $f(\alpha, y_U)$ нечётно, следовательно, $f(\alpha, y_U)$ обратимо по модулю m.

Легко видеть, что отображение h действует в (3) как аддитивная маска. Следовательно, можно определить

$$h(\alpha, \beta, y_U) \equiv f^{-1}(\alpha, y_U)\beta \pmod{m}.$$

Отметим, что из леммы 1 вытекает, что значение $h(\alpha, \beta, y_U)$ отлично от нуля.

2. Краткий анализ предложенной схемы

Далее рассмотрим несколько атак на предложенную схему асимметричного шифрования и покажем, что при некоторых допущениях схема может считаться стойкой. Будем считать, что у желающего скомпрометировать схему нарушителя могут быть следующие цели:

— определение секретного ключа абонента Б;
— дешифрование переданного сообщения;
— навязывание абоненту Б ложного сообщения.

Предполагаем, что нарушитель обладает открытыми параметрами схемы, может перехватывать все передаваемые сообщения и проводить так называемый «пассивный» анализ. Более того, предполагаем, что нарушитель может активно воздействовать на канал связи и использовать абонента Б в качестве «оракула» для расшифрования специально подобранных сообщений [6]. Данные возможности нарушителя в англоязычной литературе принято называть возможностями, используемыми при проведении CCA и CCA2 атак.

Будем считать, что нарушитель может получать расшифрованные сообщения только в том случае, если сообщение расшифровано абонентом Б корректно, в частности, содержит корректный код целостности. Кроме того, упростим задачу нарушителю и будем предполагать, что ему известны координаты точки S, рассматривавшейся ранее как долговременный ключ.

2.1. Сведение задачи определения секретного ключа к задаче дискретного логарифмирования

Легко видеть, что сложность определения секретного ключа d абонента Б основывается на трудоёмкости решения задачи дискретного логарифмирования в группе точек эллиптической кривой $\mathcal{E}$. Действительно, поскольку нарушителю известны все открытые параметры схемы, в частности точка P порядка q и открытый ключ Y абонента Б, то секретный ключ может быть найден из уравнения

$$Y = [d]P, \quad d \in \mathbb{Z}_q^*.$$

Аналогично, если нарушителю каким-либо образом удалось определить точку U, используемую для зашифрования и расшифрования сообщений, то он может найти секретный ключ d из уравнения

$$U = [d]W, \quad d \in \mathbb{Z}_q^*.$$

Известно, что решение задачи дискретного логарифмирования в группе точек эллиптической кривой, определённой над конечным простым полем $\mathbb{F}_p$, является сложной задачей, трудоёмкость которой оценивается величиной $\mathrm{O}(\sqrt{q})$ [7, 8]. Это не позволяет, при больших значениях q, на практике найти значение d.

2.2. Сведение к задаче Диффи — Хеллмана

Перейдём к рассмотрению вопросов о дешифровании передаваемого сообщения. Предположим, что нарушитель умеет находить решение задачи Диффи — Хеллмана

в группе точек эллиптической кривой $\mathcal{E}$. Другими словами, по заданным точкам P, $W = [k]P$, $Y = [d]P$, $P, W, Y \in \mathcal{E}$, нарушитель может определить точку $U \in \mathcal{E}$, удовлетворяющую равенству

$$U = [kd]P.$$

Поскольку мы предполагаем, что нарушителю известна точка S, он может воспользоваться сравнениями (2), определить значения $\alpha, \beta \in \mathbb{F}_p$ и расшифровать передаваемое сообщение с использованием сравнения (5). Таким образом, нарушитель, который умеет решать задачу Диффи — Хеллмана в группе точек эллиптической кривой $\mathcal{E}$, может дешифровывать передаваемые сообщения. Следует отметить, что в настоящее время задача Диффи — Хеллмана в группе точек эллиптической кривой считается трудноразрешимой, а наиболее эффективный способ её решения заключается в сведении к задаче дискретного логарифмирования [8].

В случае, когда нарушитель умеет решать задачу Диффи — Хеллмана, но не знает точного значения координат точки S, он может предложить атаку для их определения. Действительно, пусть $l \geqslant 2$ — натуральное число, тогда, воспользовавшись абонентом Б как «оракулом» расшифрования, нарушитель может получить значения открытых текстов $s_1, \ldots, s_l \in \mathbb{Z}_m$ для некоторых произвольных корректно расшифрованных абонентом Б шифртекстов $M_1, \ldots, M_l$ вида (4). После этого нарушитель может составить систему уравнений

$$\begin{cases} \alpha_i \equiv \dfrac{y_{U_i} - y_S}{x_{U_i} - x_S} \pmod p, \\ \beta_i \equiv \dfrac{y_S x_{U_i} - x_S y_{U_i}}{x_{U_i} - x_S} \pmod p, \\ t_i \equiv f(\alpha_i, y_{U_i}) s_i + h(\alpha_i, \beta_i, y_{U_i}) \pmod m, \quad i = 1, \ldots, l. \end{cases} \tag{12}$$

Данная система состоит из $3l$ уравнений и зависит от $2l + 2$ неизвестных $\alpha_1, \ldots, \alpha_l, \beta_1, \ldots, \beta_l, x_S, y_S$ (значения $x_{U_1}, \ldots, x_{U_l}, y_{U_1}, \ldots, y_{U_l}$ известны нарушителю). В силу построения решение системы (12) существует, следовательно, нарушитель может найти это решение и определить неизвестные ему значения x_S, y_S.

2.3. Понятие разового ключа

Можно считать, что величина $k \in \mathbb{Z}_q^*$, вырабатываемая на первом шаге алгоритма зашифрования, является *разовым* ключом, поскольку её раскрытие приводит к эффективному дешифрованию.

Действительно, пусть $M = t||W||\operatorname{mac}(d_U, s)$ — шифртекст, выработанный под сообщением $s \in \mathbb{Z}_m$ с использованием величины k. Тогда нарушитель, зная величину k и открытый ключ Y абонента Б, может вычислить точку $U = [k]Y$. Далее, используя (2) и зная долговременный ключ S, нарушитель может определить параметры $\alpha, \beta \in \mathbb{F}_p$ и расшифровать передаваемое сообщение с использованием сравнения (5).

Добавим, что если нарушитель имеет доступ к $l \geqslant 2$ различным разовым ключам $k_1, \ldots, k_l$, а также может использовать абонента Б в качестве «оракула» расшифрования, вычисляющего по шифртекстам M_1, …, M_l, выработанным с использованием указанных разовых ключей, соответствующие корректно расшифрованные открытые тексты $s_1, \ldots, s_l$, то он может определить точное значение долговременного ключа S. Для этого нарушителю достаточно решить систему сравнений (12).

2.4. Атака при шифровании на одинаковых разовых ключах

Рассмотрим ситуацию, при которой нарушитель перехватывает $l \geqslant 2$ шифртекстов $M_1, \ldots, M_l$, выработанных с использованием одного и того же неизвестного нарушите-

лю разового ключа k. Для этого нарушителю достаточно отобрать из множества всех перехваченных шифртекстов те, у которых совпадают координаты точки W.

В этом случае, если нарушитель может использовать абонента Б как «оракула» для корректного расшифрования двух открытых текстов, скажем s_1 и s_2, он может при $l \geqslant 3$ эффективно дешифровать оставшиеся сообщения $s_3, \ldots, s_l$.

Действительно, параметры $\alpha, \beta \in \mathbb{F}_p$, определяемые равенствами (2) при одинаковых значениях $k \in \mathbb{Z}_q^*$, точка U и, следовательно, значения $f(\alpha, y_U)$, $h(\alpha, \beta, y_U)$ одинаковы для всех перехваченных сообщений $M_1, \ldots, M_l$. Тогда значения $f(\alpha, y_U)$, $h(\alpha, \beta, y_U)$ могут быть эффективно вычислены нарушителем. Пусть $t_1, t_2 \in \mathbb{Z}_m$ — фрагменты шифртекстов M_1 и M_2 соответственно. Тогда нарушитель может решить систему сравнений

$$\begin{cases} t_1 \equiv f(\alpha, y_U)s_1 + h(\alpha, \beta, y_U) \pmod m, \\ t_2 \equiv f(\alpha, y_U)s_2 + h(\alpha, \beta, y_U) \pmod m \end{cases} \tag{13}$$

относительно неизвестных значений $f(\alpha, y_U)$ и $h(\alpha, \beta, y_U)$, после чего воспользоваться равенствами (5) и дешифровать открытые тексты $s_3, \ldots, s_l$.

2.5. Атака на основе адаптивно подобранных шифртекстов

Известно [9], что классическая схема Эль-Гамаля является уязвимой относительно атаки с адаптивно подобранным шифртекстом. Рассмотрим возможность применения данной атаки к нашей схеме.

Будем считать, что нарушитель хочет дешифровать шифртекст

$$M = t||(x_W, y_W)||\operatorname{mac}(d_U, s)$$

и определить сообщение s. Для этого он пользуется абонентом Б как «оракулом» расшифрования и направляет ему на расшифрование два шифртекста специального вида

$$M_1 = 0||(x_W, y_W)||\operatorname{mac}(d_U, s), \quad M_2 = 1||(x_W, y_W)||\operatorname{mac}(d_U, s).$$

Легко видеть, что шифртексты M, M_1, M_2 выработаны с одним и тем же значением разового ключа k. Используя рассуждения выше и соответствующие шифртекстам M_1 и M_2 открытые тексты s_1, s_2, нарушитель может определить значения величин $f(\alpha, y_U)$ и $h(\alpha, \beta, y_U)$ из равенств (13):

$$f(\alpha, y_U) \equiv \frac{1}{s_2 - s_1} \pmod m, \quad h(\alpha, \beta, y_U) \equiv \frac{s_1}{s_1 - s_2} \pmod m. \tag{14}$$

Теперь величина s определяется из сравнения (3). Отметим, что для проведения атаки значения t_1 и t_2 могут принимать произвольные отличные друг от друга значения. Значения $t_1 = 0$ и $t_2 = 1$ выбраны для минимизации формул (14).

Однако возможность осуществления приведённой атаки возникает только в том случае, когда абонент Б при расшифровании шифртекстов M_1, M_2 не проверяет код целостности сообщения. Действительно, направляемый в шифртекстах M_1, M_2 код целостности $\operatorname{mac}(d_U, s)$ соответствует сообщению s и для корректного расшифрования должен изменяться при замене фрагмента t на t_1 или t_2. Таким образом, данная атака осуществима нарушителем в одном из двух случаев:

1) Для двух произвольных отличных друг от друга заранее заданных значений t_0, t_1 нарушитель может вычислить значения

$$\operatorname{mac}(d_U, s_i), \quad s_i \equiv (t_i - h(\alpha, \beta, y_U))f^{-1}(\alpha, y_U) \pmod m, \quad i = 1, 2,$$

при неизвестных значениях $f(\alpha, y_U)$, $h(\alpha, \beta, y_U)$ и ключа d_U.

2) Для двух произвольных отличных друг от друга заранее заданных значений ξ_1, ξ_2 нарушитель может определить два значения t_1 и t_2, такие, что

$$\mathrm{mac}(d_U, s_i) = \xi_i,\ s_i \equiv (t_i - h(\alpha, \beta, y_U))f^{-1}(\alpha, y_U) \pmod m,\ i = 1, 2,$$

при неизвестных значениях $f(\alpha, y_U)$, $h(\alpha, \beta, y_U)$ и ключа d_U.

Если для функции mac перечисленные предположения не выполняются, то предложенная схема может считаться стойкой относительно атаки с адаптивно подобранными шифртекстами (CCA2).

2.6. Использование геометрических особенностей схемы для её компрометации

Легко заметить, что предложенная схема обладает одной геометрической особенностью, которая может быть использована нарушителем для достижения целей компрометации. Действительно, из закона сложения на эллиптической кривой $\mathcal{E}$ вытекает, что в простейшем случае, когда $f(\alpha, y_U) \equiv \alpha \pmod m$ и $h(\alpha, \beta, y_U) \equiv \beta \pmod m$, прямая $t \equiv \alpha s + \beta$, используемая для зашифрования сообщения s, содержит в себе не только точки $U, S \in \mathcal{E}$, но и точку $-(U+S) \in \mathcal{E}$ (здесь, как и ранее, мы рассматриваем координаты точек как целые неотрицательные числа). Геометрически это изображено на рис. 2.

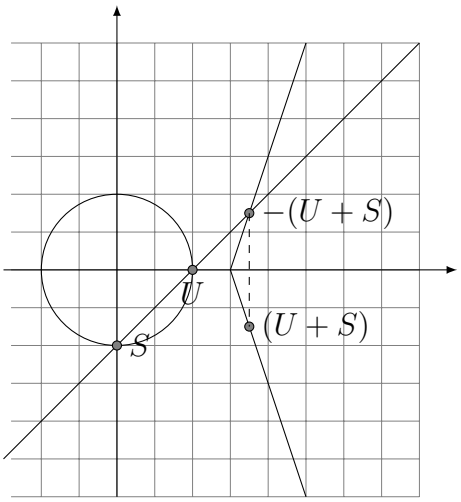

Рис. 2. Точки U, S и $-(U+S)$ на эллиптической кривой $\mathcal{E}$

Этот факт позволяет выразить значения параметров α и β через координаты точек U и $-(S+U)$. Более того, если $S, U \in \langle P \rangle$, то и $-(S+U) \in \langle P \rangle$, следовательно, найдется целое число k_0, такое, что $0 < k_0 < q$ и $-(U+S) = [k_0]P$. Если выполнено условие $S \neq [-2]U$, то $k_0 \neq k$ и получаем, что в схеме существуют два различных значения k, k_0, для которых будет выработано одно и то же значение параметров α и β.

Согласно (9) и (11), значение функции $f(\alpha, y_U)$ зависит не только от α, но и от x-координаты точки U, следовательно, значения $f(\alpha, y_U)$ и $f(\alpha, y_{-(U+S)})$, выработанные для точек U и $-(U+S)$ соответственно, различаются.

2.7. Навязывание сообщений

Высказанное ранее предположение о том, что нарушителю известен долговременный ключ S, позволяет предъявить простой алгоритм подделки передаваемого сообще-

ния. Действительно, для любого открытого текста $s_1 \in \mathbb{Z}_m$, $s_1 \not\equiv s \pmod m$, нарушитель может воспользоваться алгоритмом зашифрования и сформировать шифртекст

$$M_1 = t_1 || (x_W, y_W) || \operatorname{mac}(d_U, s_1),$$

который будет корректно расшифрован абонентом Б.

Поскольку $d_U = \operatorname{kdf}(x_U, S)$ и вычисление кода целостности $\operatorname{mac}(d_U, s_1)$ невозможно без знания долговременного ключа S, то навязывание абоненту Б ложного сообщения возможно только в двух случаях:

1) при компрометации долговременного ключа S;
2) если для заданных значений s и $\operatorname{mac}(d_U, s)$ нарушитель может определить секретный ключ d_U.

Для навязывания ложного сообщения при наличии второй уязвимости может быть применён вариант изложенной ранее атаки на одинаковых разовых ключах. Используя абонента Б в качестве «оракула расшифрования», нарушитель может получить для двух перехваченных шифртекстов M_1, M_2, выработанных на одном и том же разовом ключе k, соответствующие им открытые тексты s_1, s_2. Решая систему сравнений (13), нарушитель может найти значения $f(\alpha, y_U)$ и $h(\alpha, \beta, ty_U)$.

Теперь, используя уязвимость функции mac(), нарушитель может определить секретный ключ d_U, на котором был выработан код целостности сообщений s_1, s_2, и вычислить корректный шифртекст для произвольного сообщения s. Заметим, что в таком шифртексте будет присутствовать точка W, содержащаяся также в сообщениях M_1, M_2.

Легко заметить, что данная атака невозможна, если в распоряжении нарушителя не имеется двух шифртекстов M_1, M_2, выработанных на одном и том же разовом ключе.

Суммируем изложенные результаты в виде следующей теоремы.

Теорема 1. Предложенная схема асимметричного шифрования может считаться стойкой относительно угроз раскрытия секретного ключа, дешифрования и навязывания сообщений в случае, когда выполнены следующие условия:

1) для нарушителя являются трудоёмкими задачи дискретного логарифмирования и Диффи — Хеллмана в группе точек эллиптической кривой $\mathcal{E}$;
2) долговременный ключ S не известен нарушителю;
3) каждое сообщение шифруется с помощью уникального разового ключа k;
4) для функции выработки кода целостности mac() нарушитель не может решить задач, поставленных в п. 2.5 и 2.7;
5) расшифрованные сообщения, для которых неверен код целостности, не являются доступными нарушителю.

3. Обобщения базовой схемы

Изложенная базовая схема допускает несколько различных модификаций, позволяющих изменить её функциональные особенности без изменения стойкости. Далее рассмотрим несколько вариантов, приведя, для краткости, лишь алгоритм зашифрования сообщений.

3.1. Вариант с зашифрованием кода целостности

Передаваемый абоненту Б шифртекст M содержит в себе три составляющих: зашифрованное сообщение t, точку эллиптической кривой W и код целостности открытого текста s. При этом код целостности может рассматриваться как некоторая информация о передаваемом сообщении. Эта информация может привести к появлению

атак на функцию выработки кода целостности с целью определения сообщения s по его коду целостности.

Для предотвращения подобного рода атак схема может быть модифицирована следующим образом. Определим целое число c_m равенством

$$c_m = \lfloor \log_2 m \rfloor - \lceil \log_2 r \rceil.$$

Будем шифровать сообщения $s \in \mathbb{Z}_{2^{c_m}}$. Для этого абонент А выполняет сначала шаги 1, 2 базовой схемы (см. п. 1.1), затем следующие шаги:

3) Определяет ключ $d_U = \mathrm{kdf}(x_U, S)$, затем вычисляет код целостности $\mathrm{mac}(d_U, s)$ и формирует сообщение $s' = s || \mathrm{mac}(d_U, s)$.
4) Вычисляет точку $W = [k]P$, $W = (x_W, y_W)$, определяет

$$t \equiv f(\alpha, y_U)s' + h(\alpha, \beta, y_U) \pmod{m}$$

и направляет абоненту Б шифртекст $M = t||(x_W, y_W)$.

В данном варианте схемы шифрования длина открытого текста s равна c_m бит, а длина соответствующего ему шифртекста M равна $\log_2 m + 2\log_2 p$ бит.

Легко видеть, что мы зашифровываем код целостности сообщения вместе с самим сообщением. Это позволяет скрыть от нарушителя информацию об открытом тексте s. Взамен мы уменьшаем размер открытого текста на $\lceil \log_2 r \rceil$ бит.

3.2. Вариант с аутентификацией отправителя

Изложенная базовая схема, в общем случае, не обеспечивает аутентификацию отправляющего сообщения абонента А. Действительно, точка S может являться долговременным ключом, известным нескольким абонентам, скажем $\mathrm{A}_1, \ldots, \mathrm{A}_l$, отправляющим сообщения абоненту Б. В этом случае абонент Б не может произвести различия между абонентами $\mathrm{A}_1, \ldots, \mathrm{A}_l$. Кроме того, это позволяет им навязывать от имени друг друга сообщения абоненту Б.

В случае, когда подобная ситуация является недопустимой, можно воспользоваться механизмом аутентификации отправляемых сообщений на основе цифровой подписи. Идея схемы асимметричного шифрования с аутентификацией отправителя была ранее высказана первым автором в [10].

Для реализации механизма аутентификации отправителя сообщения абонент А должен обладать парой персональных ключей — открытым ключом e_A и секретным ключом d_A цифровой подписи. Для выработки и проверки цифровой подписи может быть использована схема, регламентируемая национальным стандартом РФ ГОСТ Р 34.10-2012 [11].

В связи с использованием механизма цифровой подписи алгоритмы mac() и kdf() не используются. Кроме того, мы можем считать точку S общеизвестным открытым параметром схемы.

Как и для базовой схемы, будем считать, что абонент А зашифровывает сообщение $s \in \mathbb{Z}_m$. Для зашифрования абонент А выполняет шаги 1–3 базовой схемы (см. п. 1.1), а последний шаг выполняется следующим образом:

4) С использованием секретного ключа цифровой подписи d_A абонент А вычисляет цифровую подпись $\mathrm{sign}(d_A, s)$ под сообщением s и формирует сообщение

$$M = t||(x_W, y_W)||\,\mathrm{sign}(d_A, s).$$

Сообщение M является шифртекстом, который отправляется абоненту Б.

Длина открытого текста s равна $\log_2 m$ бит, а длина соответствующего ему шифртекста M равна $\log_2 m + 2\log_2 p + z$ бит, где z — размер цифровой подписи.

При получении шифртекста абонент Б должен расшифровать сообщение s и, используя открытый ключ e_A абонента А, проверить цифровую подпись. Если подпись верна, то абонент Б принимает решение о корректном расшифровании сообщения s.

В заключение отметим, что при неизвестном нарушителю значении S схема с аутентификацией отправителя сообщения может быть модифицирована для передачи цифровой подписи в зашифрованном виде так, как это было сделано в предыдущем пункте.

3.3. Вариант с шифрованием длинных сообщений

Изложенная базовая схема, а также два её варианта предназначены для шифрования сообщений короткой длины. Следующий вариант позволяет зашифровывать более длинные сообщения. Для его реализации отправитель и получатель сообщения, помимо определённых в п. 1.1 открытых параметров, должны иметь отображение $g : \mathbb{F}_q^* \to \mathbb{F}_q^*$, которое также может быть известно нарушителю.

Пусть абонент А хочет зашифровать сообщение, представленное в виде конечной последовательности $s_1, \ldots, s_l \in \mathbb{Z}_m$ при $l \geqslant 2$. Для его зашифрования абонент выполняет следующие шаги:

1. Вычисляет случайное целое число k_0, удовлетворяющее неравенствам $0<k_0<q$.
2. Вычисляет точку $W = [k_0]P$, где $W = (x_W, y_W)$.
3. Для всех индексов i от 1 до l:
   а) вычисляет значение $k_i = g(k_{i-1}) \in \mathbb{F}_q^*$;
   б) вычисляет точку $U_i = [k_i]Y$, $U_i = (x_{U_i}, y_{U_i})$ и, используя (2), определяет параметры $\alpha, \beta \in \mathbb{F}_p$;
   в) определяет $t_i \equiv f(\alpha, y_{U_i})s_i + h(\alpha, \beta, y_{U_i}) \pmod m$.
4. Определяет ключ $d_U = \mathrm{kdf}(x_{U_1}, S)$, затем вычисляет код целостности $\mathrm{mac}(d_U, s_1||\cdots||s_l)$ и формирует сообщение

$$M = t_1||\cdots||t_l||(x_W, y_W)||\,\mathrm{mac}(d_U, s_1||\cdots||s_l).$$

Сообщение M является шифртекстом, который отправляется абоненту Б.

В данном варианте длина открытого текста s равна $l\log_2 m$ бит, а длина соответствующего ему шифртекста M равна $l\log_2 m + 2\log_2 p + \log_2 r$ бит.

Легко видеть, что этот вариант схемы асимметричного шифрования представляет собой последовательность из l зашифрований в соответствии с базовой схемой; мы лишь минимизировали объём передаваемых данных за счёт использования отображения g, порождающего последовательность разовых ключей.

Надо добавить, что допустимый объём данных, зашифровываемый изложенным вариантом схемы, существенно зависит от свойств отображения g. Поскольку оно действует на конечном множестве из $q-1$ элементов, то оно порождает циклические последовательности разовых ключей, что, как говорилось в п. 2.4, является небезопасным.

Пусть τ — минимальная длина цикла последовательности, порождаемой отображением g, а λ — минимальная длина подхода к циклу. Тогда для каждого уникального значения k количество блоков открытого текста l должно удовлетворять неравенству $l < \lambda + \tau$.

3.4. Вариант со случайным многочленом

Базовая схема асимметричного шифрования допускает ещё одно обобщение, использующее геометрические особенности схемы и позволяющее зашифровывать более

длинные сообщения. Действительно, в базовой схеме для зашифрования используется случайная прямая, задаваемая сравнением (3). Однако можно использовать для зашифрования случайный многочлен некоторой заранее фиксированной степени l.

Рассмотрим этот процесс более детально. Будем считать, что абонентам А и Б известна не одна общая точка S, а некоторый набор точек $S_1, \ldots, S_l \in \mathcal{E}$, для которых выполнено условие

$$S_i \neq [\pm]S_j, \quad 1 \leqslant i < j \leqslant l, \quad l \geqslant 2.$$

Будем предполагать, что данный набор точек является известным не только абонентам, участвующим в передаче сообщения, но и нарушителю.

Будем считать, что абонент А, как и в схеме, описанной в п. 3.2, обладает парой персональных ключей — открытым ключом e_A и секретным ключом d_A цифровой подписи. Тогда для зашифрования последовательности сообщений $s_1, \ldots, s_l \in \mathbb{Z}_m$ абонент А выполняет следующие шаги:

1) Вычисляет случайное целое число k, удовлетворяющее неравенствам $0 < k < q$.
2) Вычисляет точку $S_{l+1} = [k]Y$ эллиптической кривой $\mathcal{E}$. Если найдётся индекс $i \in \{1, \ldots, l\}$, такой, что $S_{l+1} = [\pm]S_i$, то абонент возвращается на шаг 1.
3) Строит интерполяционный многочлен [12]

$$g(x) \equiv \sum_{i=1}^{l+1} y_{S_i} \prod_{j \neq i} \frac{x - x_{S_j}}{x_{S_i} - x_{S_j}} \pmod m, \ \deg g(x) = l, \ g(x) \in \mathbb{Z}_m[x].$$

   Если коэффициент при старшем мономе многочлена $g(x)$ не взаимно прост с модулем m, то абонент возвращается на шаг 1.
4) Для каждого $i = 1, \ldots, l$ вычисляет произвольный вычет $t_i \in \mathbb{Z}_m$, удовлетворяющий сравнению

$$g(t_i) \equiv s_i \pmod m.$$

5) Вычисляет точку $W = [k]P$, где $W = (x_W, y_W)$.
6) Используя свой секретный ключ d_A, вычисляет цифровую подпись $\operatorname{sign}(d_A, s_1 || \cdots || s_l)$ и формирует сообщение

$$M = t_1 || \cdots || t_l || (x_W, y_W) || \operatorname{sign}(d_A, s_1 || \cdots || s_l).$$

   Сообщение M является шифртекстом, который отправляется абоненту Б.

Длина открытого текста равна $l \log_2 m$ бит, а длина соответствующего ему шифртекста M равна $l \log_2 m + 2 \log_2 p + z$ бит, где z — размер цифровой подписи.

Легко видеть, что на 3-м шаге алгоритма зашифрования абонент А вычисляет случайный многочлен $g(x) \in \mathbb{Z}_m[x]$ степени l, коэффициенты которого определяются по $l + 1$ точкам эллиптической кривой $\mathcal{E}$. При этом, как и в базовой схеме, открытый текст s_i есть абсцисса некоторой точки, принадлежащей многочлену $g(x)$, а шифртекст t_i — ордината этой точки.

Основная алгоритмическая сложность при реализации данной схемы на практике заключается в вычислении на 4-м шаге алгоритма зашифрования значений шифртекстов $t_1, \ldots, t_l$ — корней многочленов вида $g(x) - s_i \in \mathbb{Z}_m[x]$, $i = 1, \ldots, l$. Для нахождения корней можно использовать вероятностный алгоритм [13, § 6.6].

4. Результаты практической реализации

Для оценки возможности эффективной реализации предложенной базовой схемы написана программа на языке C++. Эксперименты проводились на персональной ЭВМ

с процессором AMD A6-3410MX с тактовой частотой 1,6 МГц. Результаты вычислений сведены в таблицу.

Размер p	512	1024	2048	4096	8192
Величина n	1024	2048	4096	8192	16384
Скорость, байт/с	5418	1809	628	204	80

Размеры простых чисел p приведены в битах, параметр n определяет длину блока шифруемых данных $m = 2^n$, скорость зашифрования — среднее значение объёма информации (в байтах), зашифрованной в течение одной секунды.

Из приведённых результатов видно, что максимальная скорость шифрования предложенной базовой схемой существенно ниже скорости шифрования симметричными алгоритмами шифрования. Кроме того, увеличение длины блока шифруемых данных приводит к снижению скорости шифрования.

ЛИТЕРАТУРА

1. *Menezes A. J., van Oorschot P. C., and Vanstone S. A.* Handbook of Applied Cryptography. CRC Press, 1996. 816 p.
2. ISO/IEC 18033-2:2006. Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers. 2006.
3. ISO/IEC 9797-2:2011. Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function. 2011.
4. ГОСТ Р 34.13-2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. М.: Стандартинформ, 2015.
5. Рекомендации по стандартизации. Использование криптографических алгоритмов, сопутствующих применению стандартов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012. М.: Технический комитет 26 «Криптографическая защита информации», 2014.
6. *Bellare M., Desai A., Pointcheval D., and Rogaway P.* Relations among notions of security for public-key encryption schemes // Crypto'98. LNCS. 1998. V. 1462. P. 26–46.
7. *Nesterenko A. Yu.* Cycle detection algorithms and their applications // J. Math. Sci. 2012. V. 182. No. 4. P. 518–526.
8. *Blake I., Seroussi G., and Smart N.* Elliptic Curves in Cryptography. Cambridge University Press, 1999.
9. *Mao W.* Modern Cryptography: Theory and Practice. Prentice Hall PTR, 2003. 648 p.
10. *Аносов В. Д., Нестеренко А. Ю.* Схема асимметричного шифрования, основанная на отечественных криптографических примитивах // Материалы IX Междунар. конф. «Интеллектуальные системы и компьютерные науки» (23–27 окт. 2006 г.). Т. 1. Ч. 1. М.: МГУ, 2006. С. 45–47.
11. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. М.: Стандартинформ, 2013.
12. *Бахвалов Н. С., Жидков Н. П., Кобельков Г. М.* Численные методы. М.: Наука, 1987.
13. *Василенко О. Н.* Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2003. 328 с.

REFERENCES

1. *Menezes A. J., van Oorschot P. C., and Vanstone S. A.* Handbook of Applied Cryptography. CRC Press, 1996. 816 p.

2. ISO/IEC 18033-2:2006. Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers. 2006.
3. ISO/IEC 9797-2:2011. Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function. 2011.
4. GOST R 34.13-2015. Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Rezhimy raboty blochnykh shifrov [Information technology. Cryptographic protection of information. Operating modes of block ciphers]. Moscow, Standartinform, 2015. (in Russian)
5. Rekomendatsii po standartizatsii. Ispol'zovanie kriptograficheskikh algoritmov, soputstvuyushchikh primeneniyu standartov GOST R 34.10-2012 i GOST R 34.11-2012 [Recommendations for standardization. The use of cryptographic algorithms, concomitant use of GOST R 34.10-2012 and GOST R 34.11-2012]. Moscow, Technical Committee 26, 2014. (in Russian)
6. *Bellare M., Desai A., Pointcheval D., and Rogaway P.* Relations among notions of security for public-key encryption schemes. Crypto'98, LNCS, 1998, vol. 1462, pp. 26–46.
7. *Nesterenko A. Yu.* Cycle detection algorithms and their applications. J. Math. Sci., 2012, vol. 182, no. 4, pp. 518–526.
8. *Blake I., Seroussi G., and Smart N.* Elliptic Curves in Cryptography. Cambridge University Press, 1999.
9. *Mao W.* Modern Cryptography: Theory and Practice. Prentice Hall PTR, 2003. 648 p.
10. *Anosov V. D., Nesterenko A. Yu.* Skhema asimmetrichnogo shifrovaniya, osnovannaya na otechestvennykh kriptograficheskikh primitivakh [Asymmetric encryption scheme based on domestic cryptographic primitives]. Proc. IX Mezhdunar. konf. «Intellektual'nye sistemy i komp'yuternye nauki», vol. 1, part 1. Moscow, MSU Publ., 2006, pp. 45–47. (in Russian)
11. GOST R 34.10-2012. Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Protsessy formirovaniya i proverki elektronnoy tsifrovoy podpisi [Information technology. Cryptographic protection of information. The formation and checking of digital signature]. Moscow, Standartinform, 2013. (in Russian)
12. *Bakhvalov N. S., Zhidkov N. P., Kobel'kov G. M.* Chislennye metody [Numerical Methods]. Moscow, Nauka Publ., 1987. (in Russian)
13. *Vasilenko O. N.* Teoretiko-chislovye algoritmy v kriptografii [Number-Theoretical Algorithms in Cryptography]. Moscow, MCCME Publ., 2003. 328 p. (in Russian)

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

УДК 004.94

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ УПРАВЛЕНИЯ ВЕБ-БРАУЗЕРАМИ НА ОСНОВЕ ФРЭЙМВОРКА BeEF И ОБЛАЧНОГО СЕРВИСА Google Drive[1]

Д. Н. Колегов, О. В. Брославский, Н. Е. Олексов

Национальный исследовательский Томский государственный университет, г. Томск, Россия

Текущая реализация средства для анализа защищённости веб-приложений Browser Exploitation Framework (BeEF) предполагает прямое сетевое взаимодействие контролируемых браузеров с сервером управления, что не позволяет обеспечить высокий уровень неотслеживаемости и необнаруживаемости такого взаимодействия в компьютерной сети. В работе показывается, как может быть реализован механизм сетевого взаимодействия между сервером управления BeEF и контролируемыми браузерами с помощью скрытого канала через облачный файловый сервис Google Drive, позволяющий выдать сетевые потоки управления контролируемыми браузерами за стандартные пользовательские запросы к файловому сервису Google Drive.

Ключевые слова: *компьютерная безопасность, HTTP, скрытые каналы, безопасность веб-приложений, безопасность веб-браузеров, бот-сети.*

DOI 10.17223/20710410/30/6

HOOKED-BROWSER NETWORK WITH BeEF AND Google Drive

D. N. Kolegov, O. V. Broslavsky, N. E. Oleksov

National Research Tomsk State University, Tomsk, Russia

E-mail: d.n.kolegov@gmail.com, o.v.broslavsky@gmail.com, n.e.oleksov@gmail.com

At the present time, Browser Exploitation Framework (BeEF) supports experimental WebRTC-based mechanism for implementing a hooked browser meshed-network. The main purpose of this solution is to avoid tracking post-exploitation communication back to BeEF command and control server. We propose an alternate method to provide more anonymity and undetectability for BeEF hooked browser communications. The main idea is to use covert channel communications over known and popular cloud web services, for example Google Drive, by using it as shared resources between BeEF server and hooked browsers. In this case, there is no direct communication between BeEF server and hooked browsers, all of them communicate only with Google API servers. The implementation is based on Google Drive file system primitives and

[1]Работа представлялась на международной конференции по практическим аспектам информационной безопасности «Zero Nights 2015».

its API. We consider practical issues of this implementation and show how this can be implemented in BeEF.

Keywords: *computer security, HTTP, covert channels, web application security, web browsers security, botnets.*

Введение

Одним из наиболее известных средств для инструментального анализа защищенности веб-приложений, использующих методы реализации ботнетов для сетевого взаимодействия с исследуемыми браузерами, является Browser Exploitation Framework [1].

После получения контроля над браузером в результате эксплуатации какой-либо уязвимости веб-приложения одной из основных задач яляется обеспечение постоянного коммуникационного канала между браузером и командным сервером (command and control server) [2]. В случае внедрения контролирующего JavaScript-сценария в браузер жертвы коммуникационный канал, как правило, реализуется с помощью механизмов XMLHttpRequest, WebSocket или WebRTC. Вместе с тем ни один из этих механизмов, применённый для связи контролируемых браузеров напрямую с командным сервером, не обеспечивает решения задачи неотслеживаемости и необнаруживаемости командного сервера. На конференции Kiwicon в 2014 г. Кристианом Фричатом (Christian Frichot), одним из главных разработчиков BeEF, был представлен механизм построения сети контролируемых браузеров на основе технологии WebRTC [3]. В этом случае контролируемые браузеры могут взаимодействовать не только с сервером BeEF, но и друг с другом. При этом часть контролируемых браузеров все равно ваимодействует с сервером BeEF напрямую.

Другим подходом к решению данной задачи является реализация взаимодействия с командным сервером не напрямую, а через промежуточные узлы популярных сервисов (например, Google, Twitter, Yandex и др.). Как правило, крупные облачные хостинги, такие, как Google Drive и Dropbox, имеют высокий уровень доверия и, что важно, предоставляют программный интерфейс (API) для доступа к функционалу хостинга средствами JavaScript. В случае реализации такого сетевого взаимодействия средства анализа смогут фиксировать лишь сетевые информационные потоки между браузерами пользователей и сервисами, неотличимые от разрешённых потоков. Даный подход используется, например, в прототипах Gcat [4] и Twittor [5].

В данной работе демонстрируется возможность реализации механизма сетевого взаимодействия между сервером управления BeEF и контролируемыми браузерами с помощью скрытого канала через облачный файловый сервис Google Drive, позволяющий выдать сетевые потоки управления контролируемыми браузерами за стандартные пользовательские запросы к файловому сервису Google Drive.

1. Принципы работы BeEF

Для более детального понимания задачи ознакомимся с основными элементами, используемыми в BeEF. *Зомби* — вредоносный JavaScript-код, выполняемый в браузере жертвы. *Командный сервер* — основная часть инструментального средства, ответственная за отправку команд браузерам-зомби, а также за получение, обработку и хранение результатов выполнения команд. *Идентификатор «Hook session»* — уникальный идентификатор зомби, присваиваемый ему командным сервером.

Процесс захвата контроля над браузером, который моделирует действия злоумышленника, происходит следующим образом: в результате эксплуатации уязвимости бра-

узер жертвы загружает вредоносный JavaScript-код, который немедленно начинает исполняться в контексте заражённой страницы. В первую очередь данный вредоносный код собирает информацию о браузере жертвы и отправляет её командному серверу, после чего вредоносным кодом инициируются процедуры получения команд от сервера BeEF и логирования событий.

Для получения команды браузер жертвы с определённой периодичностью совершает HTTP-запросы к командному серверу и в теле HTTP-ответа получает JavaScript-код команд, поставленных в очередь на исполнение. О результатах выполнения должна сообщить сама команда, используя механизм отправки результатов командному серверу через функцию *beef.net.send*. Механизм логирования записывает все события, происходящие на заражённой странице, и с определённой периодичностью отправляет записанные события командному серверу.

Командный сервер BeEF неоднороден по своей структуре и состоит из множества обработчиков запросов вида /, */init*, */event*, а также обработчиков, уникальных для каждого конкретного модуля или расширения BeEF. Первый из запросов заражённого браузера, содержащий информацию о нём, предназначен для обработчика */init*. В данном обработчике полученная от браузера информация анализируется и заносится в базу данных. С этого момента заражённый браузер становится зомби, а нарушитель получает возможность отправлять этому зомби команды, используя интерфейс командного сервера. Обработчики / и */event* ответственны за выдачу команд зомби-браузерам и за сохранение результатов работы модуля регистрации событий.

2. Реализация коммуникационного канала через сервис Google Drive

Исходя из описанного процесса функционирования, первым шагом в решении задачи реализации коммуникационного канала между зомби-браузерами и сервером BeEF является переход от их прямого сетевого взаимодействия к непрямому сетевому взаимодействию с использованием функциональности облачных хостингов для временного размещения команд для зомби и результатов их выполнения для командного сервера.

Для минимально приемлемой реализации такого хранения команд и ответов достаточно разработать систему уникальных имён для файлов и хранить их в одном каталоге облачного хостинга. В некоторых случаях уникальности данных имён не требуется. Например, в Google Drive файлы различаются при помощи идентификаторов, самостоятельно генерируемых сервисом, а не их именами. Однако такое представление не является достаточно наглядным, поэтому предлагается разделить все хранимые файлы на несколько логических групп и использовать для каждой из групп отдельную директорию. Так, директория *Init* содержит информацию о только что заражённых браузерах, ожидающих обработки отосланной информации и подключения к серверу BeEF; директория *Answers* содержит данные выполнения команд в следующем формате:

— идентификатор команды в базе данных командного сервера;
— имя обработчика, ответственного за дальнейшую обработку результатов;
— непосредственно данные, предназначенные для этого обработчика;
— уникальный идентификатор зомби, выполнившего команду.

Кроме того, для каждого зомби создаётся отдельная директория с именем, соответствующим его идентификатору *hook_session*. Данная директория содержит команды, отправленные командным сервером BeEF и ожидающие загрузки их зомби-браузером (рис. 1).

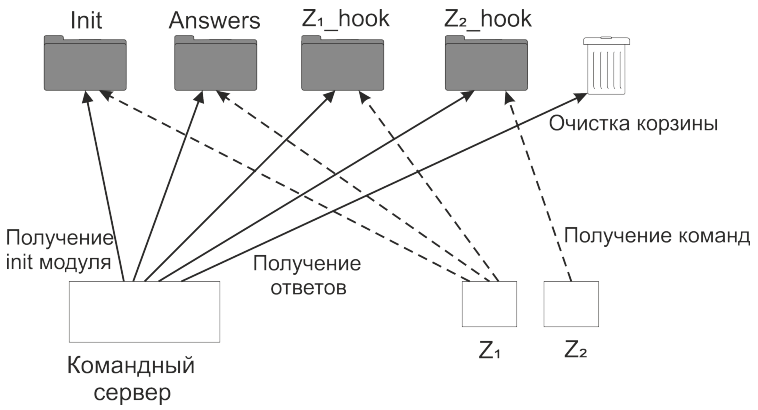

Рис. 1. Схема размещения ресурсов на Google Drive

Для авторизации доступа к сервису Google Drive необходим ряд ключей доступа. Ключ *api_key* используется зомби и позволяет запрашивать данные у программного интерфейса Google Drive, авторизуя доступ на чтение. Этот ключ используется для регулярного получения актуального значения ключа *auth_key*. Ключ *auth_key* используется командным сервером и зомби-браузерами для создания и удаления файлов, которые хранятся на облачном сервисе. Данный ключ действителен в течение ограниченного интервала времени и требует регулярного обновления. Для обновления данного ключа командный сервер использует ключ *master_key*, который может быть получен при помощи аутентификации по протоколу *OAuth* на сервисах Google. Обновлённый *auth_key* помещается сервером BeEF в специальную сущность-файл *keychain*, откуда он может быть загружен браузером-зомби при помощи ключа *api_key*.

Так как зомби в классической архитектуре BeEF для получения команд от сервера BeEF использует метод *polling*, то есть периодически опрашивает командный сервер о наличии новых команд, необходимые изменения на клиенте минимальны. Помимо реализации механизмов взаимодействия с программным интерфейсом Google Drive, необходимо, чтобы зомби осуществлял следующую логику. После инфицирования и сбора сведений о браузере полученные результаты загружаются в директорию *Init* и зомби начинает периодически проверять наличие новых команд в своей директории с именем, соответствующим идентификатору *hook_session*.

Для проверки обновлений используется стандартный механизм проверки обновлений с модифицированной функцией запроса. При обнаружении новых файлов в командной директории их содержимое выгружается и добавляется в очередь на исполнение, а сами файлы с командами помещаются в корзину.

Результаты выполнения команд помещаются в директорию *Answers* по готовности в формате, описанном выше. Результаты логирования событий загружаются в директорию *Answers* по мере накопления так, что в одном файле содержатся события, произошедшие в зомби-браузере за определённый интервал времени. Важным моментом является то, что одним из идентификаторов зомби на командном сервере является IP-адрес. В оригинальной архитектуре значение IP-адреса получается из соответствующего поля HTTP-запроса. Очевидно, при непрямом сетевом взаимодействии такой подход невозможен, поэтому в этом случае IP-адрес опрделяется запросом к внешнему сервису, а затем добавляется к первичной информации о заражённом браузере.

Командный сервер лишён какой бы то ни было активности и работает в классической клиент-серверной архитектуре. Таким образом, для работы в новой архитектуре

командный сервер нуждается в схожем с зомби *polling*-механизме. Опрос директорий Google Drive реализован в виде расширения BeEF и происходит в трёх независимых потоках выполнения. Поток *init_server* с заданной периодичностью проверяет содержимое директории *Init*, выполняет предварительную обработку полученных данных и передаёт их одноимённому обработчику командного сервера. Поток *command_server* занимается обработкой очереди команд, оформляя элементы очереди необходимым образом и сохраняя их в командных директориях зомби-браузеров. Поток *data_server* отвечает за получение и обработку результатов выполнения команд: один раз в течение заданного временного интервала *data_server* выгружает все накопившиеся в директории *Answers* ответы, записывает информацию о полученных ответах в базу данных и передаёт результаты соответствующим обработчикам.

Ещё один служебный поток выполнения описываемого расширения занимается регулярным обновлением ключа *auth_key* при помощи ключа *master_key* и интерфейса, предоставляемого сервисами Google. Отдельные функции расширения следят за созданием директорий для зомби-браузеров и за очисткой корзины, в которую помещаются все файлы, «считанные» зомби-браузерами и командным сервером.

Таким образом, в работе продемонстрирована возможность реализации сетевого взаимодействия между сервером управления BeEF и контролируемыми браузерами с помощью скрытого канала через облачный файловый сервис Google Drive.

ЛИТЕРАТУРА

1. The Browser Exploitation Framework Project. `http://beefproject.com/`
2. *Alkorn W., Frichot C., and Orru M.* The Browser Hacker's Handbook. Indianapolis: John & Wiley Sons, 2014. 648 p.
3. Hooked-Browser Meshed-Networks with WebRTC. `http://blog.beefproject.com/2015/01/hooked-browser-meshed-networks-with.html`
4. The Gcat Project. `https://github.com/byt3bl33d3r/gcat`
5. The Twittor Project. `https://github.com/PaulSec/twittor`

REFERENCES

1. The Browser Exploitation Framework Project. `http://beefproject.com/`
2. *Alkorn W., Frichot C., and Orru M.* The Browser Hacker's Handbook. Indianapolis, John & Wiley Sons, 2014. 648 p.
3. Hooked-Browser Meshed-Networks with WebRTC. `http://blog.beefproject.com/2015/01/hooked-browser-meshed-networks-with.html`
4. The Gcat Project. `https://github.com/byt3bl33d3r/gcat`
5. The Twittor Project. `https://github.com/PaulSec/twittor`

ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ

УДК 519.72

СРАВНЕНИЕ КОДА ГОЛЕЯ С АЛГЕБРОГЕОМЕТРИЧЕСКИМ КОДОМ

П. М. Ширяев

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

Рассматриваются два двоичных кода, код Голея $\mathcal{G} = [23, 12, 7]_2$ и предложенный автором алгеброгеометрический код C, для кодирования информации в двоичном симметричном канале с шириной $W = 50\,\text{КБ/с}$, тактовой частотой кодера/декодера $1\,\text{ГГц}$, вероятностью битовой ошибки $p = 0{,}005$ и требуемой вероятностью успешного декодирования передаваемого кодового слова не менее 0,9999. Показывается, что оба кода подходят под эти условия и что скорость передачи по этому каналу информации, закодированной по коду C, примерно в 1,12 раз выше, чем для информации, закодированной по коду $\mathcal{G}$. Показано также, как за счёт выбора дивизора D и базиса $L(D)$ при построении кода C можно ускорить стандартный алгоритм декодирования.

Ключевые слова: *AG-код, код Голея, L-конструкция, эллиптическая кривая.*

DOI 10.17223/20710410/30/7

COMPARISON OF THE BINARY GOLAY CODE WITH THE ALGEBRO-GEOMETRIC CODE

P. M. Shiriaev

Lomonosov Moscow State University, Moscow, Russia

E-mail: shiryaev.petr@gmail.com

The binary Golay code $\mathcal{G} = [23, 12, 7]_2$ and a binary algebro-geometric code C, proposed by the author, are considered for coding information in a binary symmetric channel with bandwidth $W = 50\,\text{KB/s}$, coder/decoder clock rate $1\,\text{GHz}$, bit error ratio $p = 0.005$, and required decoding probability 0.9999. It is shown that both codes fit this channel and the code C rate is $12\,\%$ greater than the code $\mathcal{G}$ rate. It is also shown how you can increase the decoding speed of the standard decoding algorithm by a proper choice of a divisor D and the basis of $L(D)$ for constructing C. The decoding complexity of C is estimated and the message transmission durations for C and $\mathcal{G}$ are compared.

Keywords: *AG-code, Golay code, L-construction, elliptic curve.*

Введение

Введём следующие обозначения:

— $\mathcal{G} = [23, 12, 7]_2$ — двоичный код Голея;

— $\mathbb{F} = \mathbb{Z}_2[t]/(t^4 + t^3 + 1)$ — поле из 16 элементов;
— C — алгеброгеометрический $[24, 14, 10]_{16}$-код;
— $L(D) = \{0\} \cup \{f \in k(\mathbb{X})^* : (f) + D \geqslant 0\}$ — пространство Римана — Роха дивизора D кривой $\mathbb{X}$ над полем k;
— $l(D)$ — размерность $L(D)$.

Для передачи информации в некоторых случаях требуются коды с вероятностью успешного декодирования не меньше 0,9999 при условии вероятности битовой ошибки 0,005 — например, код Голея $\mathcal{G} = [23, 12, 7]_2$. Опишем способ построения алгеброгеометрического кода на эллиптической кривой с параметрами $[24, 14, 10]_{16}$, который удовлетворяет этому условию и быстрее $\mathcal{G}$ примерно в 1,12 раз. Для декодирования полученного кода воспользуемся стандартным алгоритмом [1, с. 279]. Алгоритм декодирования использует базис пространства Римана — Роха $L(D)$ дивизора D, где D задаётся при построении кода. Выбор в качестве базиса множества, построенного в [2, теорема 3.3], позволяет уменьшить количество арифметических операций в алгоритме декодирования по сравнению с произвольным базисом. Вычислим сложность алгоритма декодирования и проверим, что указанный алгоритм гарантирует требуемую вероятность успешного декодирования. Все рассматриваемые дивизоры являются приведёнными [2, с. 48] и имеют положительную степень, поэтому для вычисления размерности пространства Римана — Роха будем пользоваться равенством $l(D) = \deg D + 1$ [1, 2.2.23] (род эллиптической кривой равен 1).

В ходе построений используются определённые на кривой $\mathbb{X}$ рациональные функции, в частности базис $L(D)$. Стоит отметить, что при этом используются не сами функции, а наборы их значений на некотором множестве точек $\mathcal{P}$, иными словами, векторы длины $|\mathcal{P}|$.

1. Построение АГ-кода

Многочлен t^4+t^3+1 неприводим над $\mathbb{Z}_2$, следовательно, $\mathbb{F} = \mathbb{Z}_2[t]/(t^4+t^3+1)$ является полем $\mathrm{GF}(2^4)$. Элементы этого поля будем интерпретировать как числа в двоичной записи. В частности, $t^3 + t + 1 \to 1011_2 = 11$, $t^2 + t + 1 \to 0111_2 = 7$. Рассмотрим над $\mathbb{F}$ эллиптическую кривую

$$\mathbb{X} = \{\infty\} \cup \{(x, y) : y^2 + y = x^3 + 11x + 7\},\ x, y \in \mathbb{F}.$$

Введём обозначение $\mathcal{P} = \mathbb{X}\backslash\infty$. Отметим, что $\mathcal{P}$ разбивается на пары сопряжённых точек [3, def. 5]. В дальнейшем нам понадобится зависимость координат сопряжённой точки от координат исходной. По определению, для $\mathbb{X}$ эта зависимость устроена следующим образом.

Замечание 1. Если $P = (x_P, y_P)$, то $\overline{P} = (x_P, y_P + 1)$.

Зафиксируем дивизор [3, def. 31] $D = 10 \cdot \infty$. Составим матрицу

$$H_D = (f_i(P))_{\substack{i=1\ldots l(D),\\ P\in\mathcal{P}}}$$

где $\{f_i\}$ — базис $L(D)$, и рассмотрим задаваемый ею код

$$C = \{c \in \mathbb{F}^{24} : H_D \cdot c = 0\}.$$

Согласно [1, теоремы 4.1.1 и 4.1.25], C является кодом с параметрами

$$[24, 24 - \deg(D), \deg(D)]_{16} = [24, 14, 10]_{16}.$$

Поскольку минимальное расстояние C равно 10, рассматриваемый код может исправить до четырёх произвольных ошибок. Ниже приведён алгоритм, исправляющий такое количество ошибок.

2. Скорость декодирования

По следствию 4.1.42 [1], стандартный алгоритм исправления ошибок [1, с. 279] позволяет декодировать до $\min(l(D'), \deg(D) - \deg(D')) - 1 = 4$ ошибок.

Опишем стандартный алгоритм. В качестве вспомогательного дивизора зафиксируем $D' = 5 \cdot \infty$. Для каждого шага алгоритма вычислим требуемое количество операций над элементами $\mathbb{F}$. Для краткости будем записывать операции как тройку чисел: количество (сложений, умножений, делений). Входящий вектор обозначим v, искомый вектор ошибок — e.

1) Обозначим базисы $L(D')$ и $L(D - D')$ как $\{g_j\}$ и $\{h_k\}$ соответственно. По теореме 3.3 из [2] для рассматриваемых дивизоров можно выбрать следующие базисы:

$$\{f_i\} = \{1, x, x^2, x^3, x^4, x^5, y, yx, yx^2, yx^3\}; \tag{1}$$

$$\{g_j\} = \{h_k\} = \{1, x, x^2, y, yx\}. \tag{2}$$

Замечание 2. Матрица $H_{D'} = (g_j(P))_{\substack{j=1\ldots l(D') \\ P \in \mathcal{P}}}$, используемая в алгоритме, получается из H_D вычёркиванием строк, поскольку базис (2) является подмножеством базиса (1).

2) Вычислим синдромы (вектор и матрицу)

$$s = H_D \cdot v = \left(\sum_{P \in \mathcal{P}} f_i(P) v_P \right)_{i=1\ldots l(D)}, \quad S = \left(\sum_{P \in \mathcal{P}} g_j(P) h_k(P) v_P \right)_{\substack{j=1\ldots l(D') \\ k=1\ldots l(D')}}.$$

Как упоминалось выше, $\mathcal{P}$ является объединением пар сопряжённых точек. Используем это для ускорения вычисления синдромов. Для упрощения записи введём обозначение $\alpha_n(P) = \begin{pmatrix} 1 \\ x_P \\ \cdots \\ x_P^n \end{pmatrix}$ и рассмотрим два столбца H_D, соответствующие паре сопряжённых точек P и $\overline{P}$. Их вклад в s выглядит следующим образом:

$$\begin{pmatrix} \alpha_5(P) & \alpha_5(P) \\ y_P \alpha_3(P) & (y_P + 1)\alpha_3(P) \end{pmatrix} \begin{pmatrix} v_P \\ v_{\overline{P}} \end{pmatrix} = \begin{pmatrix} \alpha_5(P) \\ y_P \alpha_3(P) \end{pmatrix} (v_P + v_{\overline{P}}) + \begin{pmatrix} 0 \\ \alpha_3(P) \end{pmatrix} v_{\overline{P}} =$$

$$= \begin{pmatrix} (v_P + v_{\overline{P}})\alpha_5(P) \\ (v_P + v_{\overline{P}}) y_P \alpha_3(P) \end{pmatrix} + \begin{pmatrix} 0 \\ v_{\overline{P}} \alpha_3(P) \end{pmatrix}.$$

Векторы $\alpha_5(P)$ и $y_P\alpha_3(P)$ составляют столбец матрицы H_D и потому известны; $\alpha_3(P)$ является подвектором $\alpha_5(P)$ и потому тоже известен. Отметим, что в $\alpha_3(P)$ и $\alpha_5(P)$ количество отличных от 1 координат не превосходит 3 и 5 соответственно.

За одно сложение вычислим $(v_P + v_{\overline{P}})$. Теперь координаты $\begin{pmatrix} (v_P + v_{\overline{P}})\alpha_5(P) \\ (v_P + v_{\overline{P}}) y_P \alpha_3(P) \end{pmatrix}$ можно найти за $5 + 4$ умножений, а $\begin{pmatrix} 0 \\ v_{\overline{P}} \alpha_3(P) \end{pmatrix}$ — за 3 умножения. На вычисление суммы векторов нужно ещё 4 сложения. Таким образом, вклад точек P и $\overline{P}$ может быть найден за $(5, 12, 0)$ операций. Такие вычисления нужно проделать 12 раз и сложить все

результаты, что даёт итоговую сложность в $12 \cdot (5, 12, 0) + 11 \cdot (10, 0, 0) = (170, 144, 0)$ операций для вычисления s.

Из очевидного равенства $D = D' + (D - D')$ следует, что $g_j h_k \in L(D)$. Значит, можно разложить $g_j h_k$ по базису $L(D)$, что позволяет выразить S через s:

$$\sum_{P \in \mathcal{P}} g_j(P) h_k(P) = \sum_i a_i f_i(P) \Rightarrow$$
$$\Rightarrow S_{jk} = \sum_{P \in \mathcal{P}} g_j(P) h_k(P) v_P = \sum_{P \in \mathcal{P}} \sum_i a_i f_i(P) v_P = \sum_i a_i \sum_{P \in \mathcal{P}} f_i(P) v_P = \sum_i a_i s_i.$$

Посмотрим, какие именно функции требуется так выразить. Запишем

$$(g_j h_k) = \begin{pmatrix} 1 & x & x^2 & y & yx \\ x & x^2 & x^3 & yx & yx^2 \\ x^2 & x^3 & x^4 & yx^2 & yx^3 \\ y & yx & yx^2 & y^2 & y^2 x \\ yx & yx^2 & yx^3 & y^2 x & y^2 x^2 \end{pmatrix}.$$

Все функции, за исключением y^2, $y^2 x$, $y^2 x^2$, уже принадлежат (1), поэтому результаты их скалярного произведения с v являются компонентами s. Из уравнения кривой имеем

$$y^2 = y + x^3 + 11x + 7,$$
$$y^2 x = yx + x^4 + 11x^2 + 7x,$$
$$y^2 x^2 = yx^2 + x^5 + 11x^3 + 7x^2,$$

где правые части равенств являются линейными комбинациями функций из (1). Таким образом, для вычисления каждой линейной комбинации понадобится не более $(3, 2, 0)$ операций, что в сумме даёт $(9, 6, 0)$.

3) Найдём z — произвольное нетривиальное решение однородной линейной системы уравнений

$$z^T S = 0\,.$$

Решение будем искать методом Гаусса. Для системы размера 5×5 возьмём оценку в $(50, 50, 15)$ операций [4, с. 17].

4) Найдём множество $I = \{P : \sum z_j g_j(P) = 0, P \in \mathcal{P}\}$ нулевых компонент вектора $z^T H_{D'}$. Для этого воспользуемся разбиением $\mathcal{P}$ на пары сопряжённых точек.

Вычислить $\sum\limits_{j=1}^{5} z_j g_j(P)$ можно за $(4, 5, 0)$ операций. Воспользовавшись замечанием 1, запишем условие для $\overline{P}$ следующим образом:

$$\sum_{j=1}^{5} z_j g_j(\overline{P}) = 0 \Leftrightarrow \sum_{j=1}^{5} z_j g_j(P) = z_4 \cdot 1 + z_5 \cdot x_P.$$

Левая часть последнего равенства уже найдена при проверке точки P, а правую можно вычислить за $(1, 1, 0)$ операций. Таким образом, $z^T H_{D'}$ можно найти за $12 \cdot (5, 6, 0) = (60, 72, 0)$ операций.

5) Найдём e как решение системы

$$\sum_{i=1}^{10} f_i(P) e_i = s_i, P \in I\,.$$

Для оценки размера системы докажем следующую лемму.

Лемма 1. $|I| \leqslant 5$.

Доказательство. По теореме 4.1.25 в [1] $H_{D'}$ можно рассматривать как порождающую матрицу для кода $C_{D'}$ с параметрами

$$[24, \deg(D'), 24 - \deg(D')]_{16} = [24, 5, 19]_{16}.$$

Тогда для всякого $z \in \mathbb{F}^5$ вектор $z^T H_{D'}$ является словом $C_{D'}$ и имеет не меньше 19 ненулевых компонент. Следовательно, нулевых компонент не больше $24 - 19$. Поскольку I есть обозначение множества нулевых компонент $z^T H_{D'}$, получаем $|I| \leqslant 24 - 19 = 5$. ■

Эту систему также будем решать методом Гаусса. По лемме 1 матрица системы состоит из не более чем 5 столбцов. Для системы размера 10×5 воспользуемся оценкой $(375, 375, 55) - (50, 50, 0) = (325, 325, 55)$ операций; $(375, 375, 55)$ — оценка [4, с. 17] для системы 10×10, при этом 5 столбцов можно считать нулевыми, поэтому на обнуление каждого элемента не потребуется тратить как минимум одно сложение и одно умножение, что и даёт $(50, 50, 0)$.

Суммарное количество операций равно

$$(170, 144, 0) + (9, 6, 0) + (50, 50, 15) + (60, 72, 0) + (325, 325, 55) = (614, 597, 70).$$

3. Сравнение C и $\mathcal{G}$

Убедимся, что код Голея удовлетворяет требованиям данной модели. Вероятность правильного декодирования сообщения не меньше вероятности того, что при передаче произойдёт не более 3 ошибок, то есть

$$\sum_{t=0}^{3} C_{23}^t p^t (1-p)^{23-t} \approx 0{,}999997.$$

Передадим сообщение размером $T = 50\,\text{КВ}$. Если передавать без кодирования, то на передачу уйдёт 1 с. Если же передавать кодом $\mathcal{G}$, то потребуется $23/12 \approx 1{,}92$ с.

Для кодирования одного блока требуется 84 операции `xor`, по одной на единичный элемент порождающей матрицы [5, рис. 2.13], поэтому на кодирование T при скорости вычислений 1 ГГц уйдёт $\dfrac{84 \cdot 50 \cdot 8 \cdot 2^{10}}{23} \cdot 10^{-9}$ с.

Декодирование можно осуществлять, например, методом вылавливания ошибок [1, с. 267–268]. Метод требует выполнить до $2 \cdot 23$ операций `xor`. Значит, на декодирование потребуется $\dfrac{46 \cdot 50 \cdot 8 \cdot 2^{10}}{23} \cdot 10^{-9}$ с. Общее время кодирования и декодирования составляет $\dfrac{130 \cdot 50 \cdot 8 \cdot 2^{10}}{23} \cdot 10^{-9} \approx 0{,}002\,\text{с}$. Общее время на передачу сообщения, таким образом, составит $\approx 1{,}922\,\text{с}$.

Поскольку для передачи информации достаточно хранить порождающую матрицу размера $23 \cdot 12 = 276$ бит [5, рис. 2.13], затратами памяти можно пренебречь.

Теперь проделаем то же самое для кода C. Сначала убедимся, что вероятность успешного декодирования достаточно высока. Поскольку каждый элемент $\mathbb{F}$ записывается четырьмя битами, число $\hat{p} = 1 - (1-p)^4$ естественно интерпретировать как вероятность возникновения ошибки в элементе $\mathbb{F}$. Тогда вероятность правильного декодирования сообщения произвольным кодом с $n = 24$, $d \geqslant 9$ над GF(16) равна

$$\sum_{t=0}^{4} \mathrm{C}_{24}^t \, \hat{p}^t (1-\hat{p})^{24-t} \approx 0{,}999904.$$

Будем считать, что известны таблицы умножения и деления элементов $\mathbb{F}$ (операция сложения элементов поля эквивалентна `xor` и потому выполняется за одну операцию без таблиц). Далее, поскольку конкретный вид порождающей матрицы C значения не имеет, будем считать, что в ней выделена единичная матрица, то есть $G_C = (I_{14}|A)$ для некоторой матрицы A.

Передадим сообщение размера T с помощью C. На передачу уйдёт $24/14 \approx 1{,}71$ с. Сложность декодирования одного блока длины $24{\cdot}4$ бита вычислена выше и составляет $(614, 597, 70)$ операций сложения, умножения и деления элементов поля соответственно. Кодирование информационного сообщения k заключается в вычислении $k^T A$, которое можно выполнить за $(140, 140, 0)$ операций. Таким образом, время на кодирование и декодирование сообщения составит $\dfrac{50 \cdot 8 \cdot 2^{10}}{96}(614{+}597{+}70{+}140{+}140){\cdot}10^{-9} \approx 0{,}007$ с. Общее время на передачу сообщения составит $\approx 1{,}717$ с.

Для кодирования требуется хранить матрицу A размером $14 \cdot 10 = 140$ байт, для декодирования, согласно замечанию 2, — матрицу H_D размером $24 \cdot 10 = 240$ байт. Дополнительно на таблицы умножения и деления достаточно выделить $2 \cdot 16 \cdot 16$ байт, поэтому затратами памяти для C также можно пренебречь.

Таким образом, в рамках данной модели код C оказывается быстрее в $\dfrac{1{,}922}{1{,}717} \approx$ $\approx 1{,}12$ раз при пренебрежимо малых для обоих кодов затратах памяти.

ЛИТЕРАТУРА

1. *Влэдуц С. Г., Ногин Д. Ю., Цфасман М. А.* Алгеброгеометрические коды. Основные понятия. М.: МЦНМО, 2002. 504 с.
2. *Семеновых Д. Н.* О теоретико-числовых вопросах в теории кодирования: дис. ... канд. физ.-мат. наук. М.: МГУ, 2005. 60 с.
3. *Menezes A., Wu Y.-H., and Zuccherato R.* An Elementary Introduction to Hyperelliptic Curves. Research report. Waterloo: Faculty of Mathematics, University of Waterloo, 1996. No. 19. 35 p.
4. *Богачев К. Ю.* Практикум на ЭВМ. Методы решения линейных систем и нахождения собственных значений. М.: МГУ, 1998. 79 с.
5. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979. 774 с.

REFERENCES

1. *Vleduts S. G., Nogin D. Yu., Tsfasman M. A.* Algebrogeometricheskie kody. Osnovnye ponyatiya [Algebro-Geometric Codes. Basic Concepts]. Moscow, MCCME Publ., 2002. 504 p. (in Russian)
2. *Semenovykh D. N.* O teoretiko-chislovykh voprosakh v teorii kodirovaniya [On Number-Theoretic Problems in Coding Theory]. PhD Thesis, Moscow, MSU Publ., 2005. 60 p. (in Russian)
3. *Menezes A., Wu Y.-H., and Zuccherato R.* An Elementary Introduction to Hyperelliptic Curves. Research report. Waterloo, Faculty of Mathematics, University of Waterloo, 1996, no. 19. 35 p.
4. *Bogachev K. Yu.* Praktikum na EVM. Metody resheniya lineynykh sistem i nakhozhdeniya sobstvennykh znacheniy [Workshop on the Computer. Methods for Linear Systems Solving and Eigenvalues Finding]. Moscow, MSU Publ., 1998. 79 p. (in Russian)
5. *Mak-Vil'yams F. Dzh., Sloen N. Dzh. A.* Teoriya kodov, ispravlyayushchikh oshibki [The Theory of Error-Correcting Codes]. Moscow, Svyaz' Publ., 1979. 774 p. (in Russian)

ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

УДК 519.1

О НЕКОТОРЫХ КЛАССАХ ЭКСТРЕМАЛЬНЫХ ОРИЕНТИРОВАННЫХ ГРАФОВ

А. Ю. Зубов

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

Изучаются ориентированные графы, обладающие свойством транзитивности и имеющие ограниченные степени вершин. Указываются классы экстремальных графов.

Ключевые слова: *теорема Турана, экстремальный ориентированный граф.*

DOI 10.17223/20710410/30/8

ABOUT SOME CLASSES OF EXTREMAL ORIENTED GRAPHS

A. Yu. Zubov

Lomonosov Moscow State University, Moscow, Russia

E-mail: Zubovanatoly@yandex.ru

Some classes of extremal directed graphs with the transitivity property and limited vertices degrees are studied.

Keywords: *Turan's theorem, extremal directed graph.*

1. Задачи экстремальной теории графов

Одно из направлений теории графов составляет класс задач, связанных с оценкой максимального числа рёбер графа, не содержащего подграфов определённого вида. Это направление, получившее название «*экстремальная теория графов*», возникло в начале XX века после доказательства теоремы Мантеля (1907 г.), в которой утверждается, что связный граф порядка $n \geqslant 3$ и размера $m > \lfloor n^2/4 \rfloor$ содержит треугольник [1]. *Порядком* и *размером* графа называется соответственно число его вершин и рёбер. Теорема Мантеля обобщается теоремой Турана (1941 г.), в которой доказано, что максимальный размер графа порядка $n \geqslant 3$, не содержащего полного подграфа K_k порядка k, равен $\left[\dfrac{k-2}{k-1} \cdot \dfrac{n^2-r^2}{2} + \binom{r}{2}\right]$, где r — остаток от деления n на $k-1$. Теорема Турана даёт также полное описание экстремальных графов $T_{n,k}$ такого размера [2]. Турановский граф $T_{n,k}$ — это k-дольный полный граф, такой, что его доли $V_1, \ldots, V_k$ имеют возможно близкие к друг другу мощности (r долей мощности $\lceil n/k \rceil$ и $k-r$ долей мощности $\lfloor n/k \rfloor$).

Известно большое число других подобных результатов [2–4]. Например, если порядок $n \geqslant 4$ и размер m графа связаны соотношением $m \geqslant (n + n\sqrt{4n-3})/4 + 1$, то граф содержит цикл C_4 длины 4. В теореме Поша (1952 г.) утверждается, что

граф порядка n, не содержащий путей длины k, имеет размер m, не меньший чем $n(k-1)/2$. Эта оценка достижима в том и только в том случае, когда все компоненты связности графа есть полные подграфы K_k. П. Туран поставил общую задачу (the problem of forbidden subgraphs — проблема запрещённых подграфов): найти максимальный размер графа порядка n, который не содержит заданного подграфа F. Пусть $ex(n,F)$ — такой максимальный размер и $EX(n,F)$ — множество соответствующих экстремальных графов. В этих терминах теорему Турана формулируют в виде равенства $EX(n,F) = T_{n,k}$. Один из фундаментальных результатов экстремальной теории графов сформулирован в теореме Эрдёша — Стоуна (1946 г.): для графа F, содержащего не менее одного ребра, выполняется равенство

$$\lim_{n\to\infty} \frac{ex(n,F)}{\binom{n}{2}} = \frac{\chi(F)-2}{\chi(F)-1},$$

где $\chi(F)$ — хроматическое число графа F. Аналогичные задачи возникают и для ориентированных графов без петель, обладающих свойством транзитивности: если граф содержит ориентированные рёбра (a,b) и (b,c), то он содержит и ребро (a,c). Такие графы ассоциируются с частично упорядоченными множествами. Так, в [5] для решения некоторых уравнений в группе подстановок G на множестве $\Omega_n = \{1,2,\ldots,n\}$ вводится отношение порядка $\prec_\sigma$, определяемое произвольной подстановкой $\sigma = \begin{pmatrix} c \\ \sigma c \end{pmatrix}_{c\in\Omega_n}$:

$$a \prec_\sigma b \Leftrightarrow [\sigma a, a] \subset [\sigma b, b],$$

где

$$[\sigma c, c] = \begin{cases} \{c\}, & \text{если } \sigma c = c, \\ \{\sigma^{-1}c, \sigma^{-1}c+1, \ldots, c+1, c\}, & \text{если } \sigma c \neq c, \end{cases}$$

и решается экстремальная задача относительно величин

$$\Delta_\sigma = |\{(a,b) : a,b \in \Omega_n, a \prec_\sigma b\}|, \quad \sigma \in G.$$

Такая задача оказывается эквивалентной задаче нахождения максимального размера ориентированного графа без петель с n вершинами, обладающего свойствами транзитивности и ограниченности для каждой вершины чисел предшествующих (полустепень захода) и последующих (полустепень исхода) вершин. Этому вопросу посвящён п. 3 данной работы.

Отметим, что теорема Турана верна и для ориентированных графов без петель со свойством транзитивности. При этом условие отсутствия полных подграфов порядка k заменяется условием отсутствия в графе ориентированных путей длины k. В данной работе изучаются ориентированные графы порядка n со свойством транзитивности, для которых степень каждой вершины не превосходит $k < n$. В зависимости от чётности чисел k, n приводятся примеры экстремальных графов, размер которых достигает величины $[n(k-1)/2]$.

2. Ориентированные графы с ограниченными степенями вершин

Введём следующие обозначения. Пусть Γ_n — ориентированный граф без петель с множеством вершин Ω_n, обладающий свойством транзитивности, и $\overline{\Gamma}_n$ — соответствующий неориентированный граф; v_c — степень вершины $c \in \Omega_n$; $\Gamma_{n,k}$ — граф Γ_n, степень каждой вершины которого меньше k; $|\Gamma_{n,k}|$ — число рёбер графа $\Gamma_{n,k}$; $\Gamma_{n,k}^{\max}$ — граф $\Gamma_{n,k}$ максимального размера.

Подсчитывая число рёбер графа, степень каждой вершины которого равна $k-1$, получаем следующее неравенство.

Утверждение 1. Для любого графа $\Gamma_{n,k}$

$$|\Gamma_{n,k}| \leqslant \left[\frac{n(k-1)}{2}\right]. \tag{1}$$

Замечание 1. Граф $\Gamma_{n,k}$ не содержит (ориентированных) путей длины k. Вместе с тем неравенство (1) не следует из приведённой выше теоремы Поша, поскольку в графе $\overline{\Gamma}_{n,k}$ могут содержаться пути длины, большей чем $k-1$.

Покажем, что оценка (1) достижима.

Утверждение 2. При $k \in \{1,2\}$, $k \leqslant n$, и при $k=3$, $3 \leqslant n$, $n \neq 5$, имеет место равенство

$$|\Gamma^{\max}_{n,k}| = \left[\frac{n(k-1)}{2}\right]. \tag{2}$$

Доказательство. При $k=1$ имеем $|\Gamma_{n,1}| = 0$. Граф $\Gamma_{n,2}$ не содержит путей длины 2. При чётном n экстремальным является граф, рёбра которого исчерпываются элементами множества

$$\{(i, n/2+i) : i = 1, 2, \ldots, n/2\},$$

а при нечётном n — элементами множества

$$\{(i, [n/2]+i) : i = 1, 2, \ldots, [n/2]\}.$$

Поэтому $|\Gamma^{\max}_{n,k}| = [n/2]$.

Граф $\Gamma_{n,3}$ не содержит путей длины 3. Легко видеть, что при чётном n экстремальным является граф C_n, представляющий собой цикл, составленный рёбрами

$$(1,2), (3,2), (3,4), (5,4), \ldots, (n-1,n), (1,n)$$

с чередующимися направлениями, а при нечётном n — граф из двух компонент C_{n-3} и C_3, составленных рёбрами $(1,2), (3,2), (3,4), (5,4), \ldots, (n-4,n-3), (1,n-3)$ и $(n-2,n-1), (n-1,n), (n-2,n)$. Отсюда следует, что $|\Gamma^{\max}_{n,3}| = n$. Исключение составляет случай, когда $n=5$, $k=3$. Легко проверить, что $|\Gamma^{\max}_{5,3}| = 4$. ■

Утверждение 3. При любом чётном n и любом k, $3 \leqslant k \leqslant n/2+1$, выполняется равенство (2).

Доказательство. Рассмотрим граф C_n из доказательства утверждения 2. Его вершины, представленные нечётными числами, являются истоками графа (их полустепени захода равны 0), а вершины, представленные чётными числами, являются стоками графа (их полустепени исхода равны 0). Можно рассматривать такой граф как двудольный, степень каждой вершины которого равна 2. Одной долей графа служит $\{1, 3, \ldots, n-1\}$, второй — $\{2, 4, \ldots, n\}$. Все рёбра графа начинаются в первой доле и заканчиваются во второй.

Аналогично можно построить и двудольный граф $\Gamma_{n,k}$ с теми же долями, степень каждой вершины которого равна k, где $3 \leqslant k \leqslant n/2+1$. Таким, например, является граф с множеством рёбер

$$\{(2i+1, 2i+2j+2 \bmod n),\ i = 1, 2, \ldots, n/2-1,\ j = 0, 1, \ldots, k-2\}.$$

Для построенного графа выполняется равенство (2). ■

Заметим, что для любых нечётного n и чётного k не существует графа Γ_n, степень каждой вершины которого равна $k-1$. В таком случае экстремальным является граф $\Gamma_{n,k}$, степени $n-1$ вершин которого равны $k-1$, а степень одной вершины равна $k-2$. Однако попытки построить такой ориентированный граф $\Gamma_{n,k}$, например при $n=7$, $k=4$, не приводят к успеху. Непосредственно проверяется, что для $\Gamma^{\max}_{7,4}$ равенство (2) не выполняется. Вместе с тем справедливо следующее утверждение.

Утверждение 4. При любом нечётном $n \geqslant 5$, $n \neq 7$, выполняется равенство

$$|\Gamma^{\max}_{n,4}| = [3n/2]\,.$$

Доказательство. Поскольку $n-5$ чётно, при $n \geqslant 11$ выполняются условия утверждения 3 и, следовательно, существует граф $\Gamma' = \Gamma_{n-5,4}$, для которого выполняется равенство (2). Заметим, что экстремален и граф $\Gamma'' = \Gamma_{5,4}$ с множеством рёбер

$$\{(1,2),(1,5),(3,2),(3,4),(3,5),(4,2),(4,5)\}.$$

Построим граф $\Gamma_{n,4}$, состоящий из компонент связности Γ' и Γ''. Непосредственно проверяется, что построенный граф экстремален. Аналогично граф $\Gamma_{9,4}$, компонентами которого служат Γ' и полный граф $\Gamma_{4,4}$, экстремален. ■

Утверждение 5. При любых нечётных k и $n \geqslant 3k-2$ выполняется равенство (2).

Доказательство. С учётом утверждения 3, достаточно заметить, что граф $\Gamma_{n,k}$, состоящий из компонент $\Gamma_{k,k}$ и $\Gamma^{\max}_{n-k,k}$, является экстремальным. ■

Известны примеры графов $\Gamma_{n,k}$, для которых выполняется равенство (2) и при других соотношениях между k и n, чем указанные в условиях утверждений 2–5. Таковым является, например, граф $\Gamma_{8,6}$ с множеством рёбер

$$(1,2),(1,4),(1,5),(1,6),(1,8),(3,2),(2,4),(5,2),(7,2),(3,4),$$
$$(3,6),(3,7),(3,8),(5,4),(7,4),(5,6),(5,8),(7,6),(8,6),(7,8).$$

3. Ориентированные графы с ограниченными полустепенями вершин

Пусть $G_{n,k}$ — ориентированный граф без петель со свойством транзитивности, с n вершинами, полустепени исхода и захода которых меньше k.

Утверждение 6. Справедлива оценка

$$|G^{\max}_{n,k}| < |T_{n,k+1}|. \tag{3}$$

Доказательство. Граф $G_{n,k}$ содержит истоки и стоки. Любой сток достижим из некоторого истока. По условию длина пути между истоком и стоком не превосходит $k-1$. Отсюда следует, что в $G_{n,k}$ нет путей длины k и полных подграфов на $k+1$ вершинах.

Заметим, что и неориентированный граф $\bar{G}_{n,k}$ не содержит полных подграфов K_{k+1}. В самом деле, если $\bar{G}_{n,k}$ содержит K_{k+1}, то граф $G_{n,k}$ обязан содержать путь длины k. Это легко доказать индукцией по k, учитывая, что имеет место цепочка включений $K_{k+1} \supset K_k \supset K_{k-1} \supset \ldots$ По теореме Турана отсюда следует, что

$$|G^{\max}_{n,k}| = |\bar{G}^{\max}_{n,k}| \leqslant |T_{n,k+1}|.$$

Если

$$|\bar{G}^{\max}_{n,k}| = |T_{n,k+1}|, \tag{4}$$

то $\bar{G}^{\max}_{n,k} = T_{n,k+1}$ в силу того, что $T_{n,k+1}$ — единственный экстремальный граф. Используя описание графа $T_{n,k+1}$, убеждаемся в том, что степени его вершин равны k или $k+1$. В частности, степень любого истока a графа $G^{\max}_{n,k}$ тогда не меньше k, что невозможно, поскольку по условию полустепень исхода вершины a не превосходит $k-1$. Следовательно, равенство (4) невозможно, откуда следует (3). ■

Заметим, что конструкции экстремальных графов типа $\Gamma_{n,k}$, рассмотренные в п. 2, являются и графами типа $G_{n,k}$. Это позволяет получить нижнюю оценку величины $|G^{\max}_{n,k}|$ для таких графов.

Утверждение 7. Для значений n, k, удовлетворяющих любому из условий утверждений 2–5, справедливо неравенство

$$\left[\frac{n(k-1)}{2}\right] \leqslant |G^{\max}_{n,k}|. \tag{5}$$

Оценки (3) и (5) для некоторых значений n, k дают близкие значения. Например, при $n = 2k$ получаем следующий результат.

Утверждение 8. Если $n = 2k$, то

$$\frac{n(n-2)}{4} \leqslant |G^{\max}_{n,k}| \leqslant \frac{n(n-2)}{2}. \tag{6}$$

В [5] доказано, что на самом деле в утверждении 8 нижняя оценка достигается. Вычислим точно величину $|G^{\max}_{n,k}|$ при $k = [(n+1)/2]$.

Утверждение 9. Имеет место равенство

$$|G^{\max}_{n,[(n+1)/2]}| = \left[\frac{n}{2}\right]\left[\frac{n-1}{2}\right]. \tag{7}$$

Доказательство. Граф $G = G_{n,k}$ определяет на своём множестве вершин $\Omega = \{1, 2, \ldots, n\}$ отношение порядка $\prec_G$, где $a \prec_G b$ для $a, b \in \Omega$, если и только если G содержит ребро (a, b). Это отношение обладает свойством транзитивности (но, в отличие от отношения частичного порядка, не обладает свойствами рефлексивности и антисимметричности). Пусть $U_{(\Omega,\prec_G)}(a)$ — множество элементов из Ω, предшествующих a согласно $\prec_G$, и $W_{(\Omega,\prec_G)}(a)$ — множество элементов из Ω, следующих за a согласно $\prec_G$. Из определения графа G следует, что для каждого $a \in \Omega$ выполняются неравенства

$$|U_{(\Omega,\prec_G)}(a)| \leqslant k-1, \;\; |W_{(\Omega,\prec_G)}(a)| \leqslant k-1. \tag{8}$$

Пусть

$$\Phi(\Omega, \prec_G) = \{(a, b) : a, b \in \Omega, a \prec_G b\}.$$

Тогда (7) равносильно равенству

$$\max_{G=G_{n,[(n+1)/2]}} |\Phi(\Omega, \prec_G)| = \left[\frac{n}{2}\right]\left[\frac{n-1}{2}\right]. \tag{9}$$

Докажем (9) индукцией по n.

При $n = 1$ и 2 утверждение очевидно. Предположим, что оно справедливо для $n \leqslant r-1$, и рассмотрим случай, когда $n = r$. Пусть сначала n чётно. По условию выполняются неравенства (8) при $k = n/2$. Так как $(\Omega, \prec_G)$ не содержит циклов, найдётся $b \in \Omega$, для которого $|U_{(\Omega,\prec_G)}(b)| = 0$. Удалив из Ω точку b, получим множество $\Omega' = \Omega\backslash\{b\}$ с тем же отношением порядка $\prec_G$, для которого выполняются неравенства

$$|U_{(\Omega',\prec_G)}(c)| \leqslant \left[\frac{n-1}{2}\right] = \left[\frac{n-2}{2}\right], \tag{10}$$

$$|W_{(\Omega',\prec_G)}(c)| \leqslant \left[\frac{n-1}{2}\right] = \left[\frac{n-2}{2}\right] \tag{11}$$

при любом $c \in \Omega'$. Поэтому для Ω' выполняются условия (8) и по предположению индукции

$$|\Phi(\Omega', \prec_G)| \leqslant \left[\frac{(n-1)^2}{2}\right].$$

Поскольку $|W_{(\Omega,\prec_G)}(c)| \leqslant n/2 - 1$, справедлива оценка

$$|\Phi(\Omega, \prec_G)| = |\Phi(\Omega', \prec_G)| + |W_{(\Omega,\prec_G)}(b)| \leqslant \left[\frac{n}{2}\right]\left[\frac{n-1}{2}\right],$$

что и требуется доказать.

Пусть n нечётно. Предположим, что на $(\Omega, \prec_G)$ достигается максимум величины $|\Phi(\Omega, \prec'_G)|$ по всем отношениям порядка $\prec'_G$, для которых выполняются условия (8). Если в Ω имеется не более одной точки b, для которой $|U_{(\Omega,\prec_G)}(b)| = [(n-1)/2]$ или $|W_{(\Omega,\prec_G)}(b)| = [(n-1)/2]$, то по предположению индукции

$$|\Phi(\Omega, \prec_G)| = |\Phi(\Omega\backslash\{b\}, \prec_G)| + |U_{(\Omega,\prec_G)}(b)| \leqslant \frac{(n-1)(n-3)}{4} + \left[\frac{n-1}{2}\right] = \left[\frac{n}{2}\right]\left[\frac{n-1}{2}\right],$$

что и требуется доказать.

Пусть $i_1, \ldots, i_t$ — все точки из Ω, для которых

$$|W_{(\Omega,\prec_G)}(i_\alpha)| = \left[\frac{n-1}{2}\right], \;\; \alpha = 1, \ldots, t, \;\; t \geqslant 0,$$

и $j_1, \ldots, j_s$ — все точки из Ω, для которых

$$|U_{(\Omega,\prec_G)}(j_\beta)| = \left[\frac{n-1}{2}\right], \;\; \beta = 1, \ldots, s, \;\; s \geqslant 0.$$

Предположим, что $s = 0$. Тогда по условию случая $t \geqslant 2$. Пусть j — одна из точек, для которых $|W_{(\Omega,\prec_G)}(j)| = 0$. Построим на Ω отношение порядка $\prec'$, совпадающее с $\prec = \prec_G$ на элементах множества $\Omega\backslash\{j\}$; $|U_{(\Omega,\prec')}(j)| = 0$, а $W_{(\Omega,\prec')}(j)$ содержит $[(n-1)/2]$ элементов из множества $\Omega\backslash\{i_1, \ldots, i_t, j\}$. Это можно сделать, поскольку $t \leqslant [(n-1)/2]$ (в противном случае получим противоречие с условием $s = 0$). Поскольку для любой точки $l \in \Omega$, для которой $|W_{(\Omega,\prec)}(l)| = 0$, имеет место

$$|U_{(\Omega,\prec)}(l)| \leqslant \left[\frac{n-1}{2}\right] - 1,$$

для $(\Omega, \prec')$ выполняются условия (9). Но $|\Phi(\Omega, \prec')| > |\Phi(\Omega, \prec)|$, что противоречит условию выбора отношения $\prec$. Аналогично приходим к противоречию в случае, когда $t = 0$.

Пусть теперь $t > 0,\ s > 0$. Тогда $i_\alpha \prec j_\beta$ для любых $\alpha \in \{1, \ldots, t\},\ \beta \in \{1, \ldots, s\}$. В самом деле, если $(i_\alpha, j_\beta) \notin \Phi(\Omega, \prec)$, то $W_{(\Omega,\prec)}(i_\alpha) \cap U_{(\Omega,\prec)}(j_\beta) = \varnothing$. Но тогда в объединении

$$W_{(\Omega,\prec)}(i_\alpha) \cup U_{(\Omega,\prec)}(j_\beta) \cup \{i_\alpha\} \cup \{j_\beta\}$$

содержится более n элементов, что невозможно. В таком случае, исключая из Ω две точки, например i_1 и j_1, получим множество $\Omega' = \Omega \backslash \{i_1, j_1\}$ с тем же отношением порядка $\prec$, удовлетворяющим условиям (8). Действительно,

$$|W_{(\Omega',\prec)}(i_\alpha)| < \left[\frac{n-1}{2}\right], \quad |U_{(\Omega',\prec)}(j_\beta)| < \left[\frac{n-1}{2}\right]$$

для $\alpha = 2, \ldots, t$, $\beta = 2, \ldots, s$. Вместе с точками i_1 и j_1 из множества $\Phi_\prec(\Omega)$ мы удалили $n-2$ пары элементов: $[(n-1)/2]$ пар, содержащих i_1, и $[(n-1)/2] - 1$ пар, содержащих j_1. По предположению индукции

$$|\Phi(\Omega, \prec)| = |\Phi(\Omega', \prec)| + |U_{(\Omega,\prec)}(i_1)| + |W_{(\Omega,\prec)}(j_1)| \leqslant \frac{(n-3)^2}{2} + n - 2 = \left[\frac{n}{2}\right]\left[\frac{n-1}{2}\right],$$

что и требуется доказать. ■

Следствие 1. Граф $G_{n,[(n+1)/2]}$, состоящий из двух компонент связности, представляющих собой полные графы $K_{n/2}$, $K_{n/2}$ при чётном n и $K_{(n+1)/2}$, $K_{(n+1/2}$ при нечётном n, является экстремальным.

В заключение отметим, что автору неизвестны точные значения $|\Gamma^{\max}_{n,k}|$ и $|G^{\max}_{n,k}|$ при произвольных n, k.

ЛИТЕРАТУРА

1. *Харари Ф.* Теория графов. М.: Мир, 1972.
2. *Llado A.* An Introduction to Extremal Graph Theory. CIMPA-UNESCO-Indonesia School on Extremal Problems and Hamiltonicity in Graphs. ITB, Bandung, 2–13 Febr. 2009.
3. *Simonovits M.* Introduction to Extremal Graph Theory. Budapest: Alfred Renyi Mathematical Institute, 2006.
4. *McClintock J.* Extremal Graphs Theory for Book-Embeddings. M. Sc. Thesis, University of Melbourne Department of Mathematics and Statistics, 2012.
5. *Зубов А. Ю.* О диаметре группы S_N относительно системы образующих, состоящей из полного цикла и транспозиции // Труды по дискретной математике. Т. 2. М.: ТВП, 1998. С. 112–150.

REFERENCES

1. *Harary F.* Graph Theory. Perseus Books, 1994.
2. *Llado A.* An Introduction to Extremal Graph Theory. CIMPA-UNESCO-Indonesia School on Extremal Problems and Hamiltonicity in Graphs. ITB, Bandung, 2–13 Febr. 2009.
3. *Simonovits M.* Introduction to Extremal Graph Theory. Budapest: Alfred Renyi Mathematical Institute, 2006.
4. *McClintock J.* Extremal Graphs Theory for Book-Embeddings. M. Sc. Thesis, University of Melbourne Department of Mathematics and Statistics, 2012.

5. *Zubov A. Yu.* O diametre gruppy S_N otnositel'no sistemy obrazuyushchikh, sostoyashchey iz polnogo tsikla i transpozitsii [On the diameter of the group S_N with respect to a system of generators consisting of a complete cycle and a transposition]. Tr. Diskr. Mat., 1998, vol. 2, pp. 112–150. (in Russian)

УДК 519.17

ВЕРХНЯЯ ОЦЕНКА КОЛИЧЕСТВА ДОПОЛНИТЕЛЬНЫХ РЁБЕР МИНИМАЛЬНЫХ РЁБЕРНЫХ 1-РАСШИРЕНИЙ СВЕРХСТРОЙНЫХ ДЕРЕВЬЕВ

Д. Д. Комаров

Саратовский государственный университет им. Н. Г. Чернышевского, г. Саратов, Россия

Минимальные рёберные расширения графов можно рассматривать как модель оптимальной рёберной отказоустойчивой реализации некоторой системы. Работа посвящена верхней оценке количества дополнительных рёбер минимальных рёберных 1-расширений для графов специального вида — сверхстройных деревьев. Приводятся две схемы построения рёберного 1-расширения для сверхстройного дерева произвольного вида и соответствующий алгоритм на основе этих схем.

Ключевые слова: *графы, минимальные расширения графов, сверхстройное дерево, отказоустойчивость.*

DOI 10.17223/20710410/30/9

UPPER BOUND FOR THE NUMBER OF ADDITIONAL EDGES IN MINIMAL 1-EDGE EXTENSIONS OF STARLIKE TREES

D. D. Komarov

Saratov State University, Saratov, Russia

E-mail: komarovdd@gmail.com

Minimal edge extension of graphs can be regarded as a model of optimal edge fault tolerant implementation of a system. This paper is about an upper bound for the number of additional edges in minimal 1-edge extensions for graphs of a special class — starlike trees. Two schemes for constructing 1-edge extensions for any kind starlike trees and an algorithm based on these schemes are proposed.

Keywords: *graphs, minimal extensions of graphs, fault tolerance, starlike trees.*

Введение

Задача распознавания рёберного расширения произвольного графа является NP-полной [1], поэтому представляет интерес нахождение классов графов, для которых возможно построить минимальное рёберное расширение аналитически или найти «хорошую» верхнюю (нижнюю) оценку количества дополнительных рёбер минимального расширения. Для минимальных вершинных 1-расширений графов существуют такие оценки. Так, например, тривиальное вершинное 1-расширение для произвольного графа может выступать в качестве верхней оценки. Для рёберных же расширений произвольного графа в качестве верхней оценки можно взять лишь полный граф, учитывая при этом, что в общем случае не для всех графов существуют рёберные расширения. Работа [2] посвящена нижней оценке числа дополнительных рёбер минимального рёберного 1-расширения произвольного сверхстройного дерева. В данной работе рассматривается верхняя оценка.

Актуальность задачи нахождения минимальных рёберных расширений графа рассматривается в контексте моделирования отказоустойчивых систем. Ф. Харари и Дж. Хейз рассматривают граф как модель некоторой технической системы [3]. Отказ связи системы рассматривается как удаление соответствующего этой связи ребра. При такой интерпретации минимальное рёберное k-расширение графа, моделирующего некоторую систему Σ, является моделью оптимальной рёберной k-отказоустойчивой реализации системы Σ.

Дадим основные определения, которые будут использованы в работе.

Назовём граф $G^* = (V^*, \alpha^*)$ *рёберным k-расширением* графа $G = (V, \alpha)$, если граф G вложим в каждый граф, получающийся из G^* удалением любых его k рёбер.

Граф $G^* = (V^*, \alpha^*)$ называется *минимальным рёберным k-расширением* графа $G = (V, \alpha)$, если выполняются следующие условия:

1) граф G^* является рёберным k-расширением G;

2) $|V^*| = |V|$;

3) α^* имеет минимальную мощность при выполнении условий 1 и 2.

Будем говорить, что минимальное рёберное k-расширение содержит $|\alpha^*| - |\alpha|$ дополнительных рёбер. Обозначим через $ec(G, k)$ число дополнительных рёбер минимального рёберного k-расширения графа G. При $k = 1$ будем записывать просто $ec(G)$.

Ациклический связный граф называется *деревом*; дерево с одной выделенной вершиной называется *корневым* деревом, а выделенная вершина — *корнем* дерева. В дереве вершины степени 1 называются *листьями*.

Сверхстройным деревом называется корневое дерево, где степень всех вершин, кроме корня, не превосходит 2, а степень корня больше 2.

Альтернативное определение: граф G называется *сверхстройным деревом*, если он является объединением $s > 2$ цепей с общей концевой вершиной (примеры сверхстройных деревьев показаны на рис. 1).

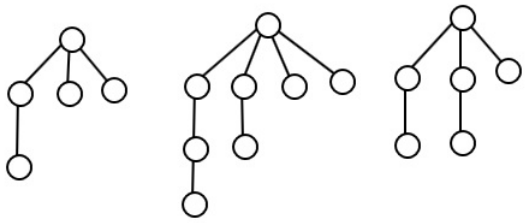

Рис. 1. Примеры сверхстройных деревьев

Будем задавать сверхстройное дерево с помощью вектора $(a_1, \ldots, a_s)$, где a_i — количество цепей длины i; s — длина максимальной цепи.

Пусть граф G — сверхстройное дерево, являющееся объединением $s > 2$ цепей P_1, $\ldots$, P_s с общей концевой вершиной и заданное вектором $(a_1, \ldots, a_t)$, $t > 1$. Назовём ребро цепи P_i *сложным ребром* цепи P_i, если при его удалении цепь P_i разбивается на две цепи длин k_i и l_i ($k_i + l_i + 1 = m_i$, m_i — длина цепи P_i), причём $a_{k_i} = 0$, $a_{l_i} = 0$, и ни k_i, ни l_i не равны 0. Ребро, не являющееся сложным, назовём *простым ребром*. Назовём *началом сложного ребра* вершину, инцидентную этому ребру и находящуюся ближе к корневой вершине. *Количеством сложных рёбер сверхстройного дерева* будем называть общее количество сложных рёбер цепей этого сверхстройного дерева.

Приведём некоторые результаты относительно верхней оценки количества дополнительных рёбер для сверхстройных деревьев специального вида.

Теорема 1. Пусть граф G — сверхстройное дерево, заданное вектором $(a_1, \ldots, a_s)$, $a_i \neq 0$ для $i = 1, \ldots, s$, причём если s чётно, то $a_{s/2} \geqslant 2$. Тогда существует граф G^* — рёберное 1-расширение графа G — с количеством дополнительных рёбер $ec(G)$, вычисляемым по формуле

$$ec(G) = a_s + \sum_{i=1}^{[s/2]} (|a_i - a_{s-i}| + \min(a_i, a_{s-i})). \tag{1}$$

Количество таких неизоморфных рёберных расширений равно

$$\prod_{i=1}^{[s/2]} T_{|a_i - a_{(s-i)}|}^{\min(a_i, a_{(s-i)})}, \tag{2}$$

где T_N^K можно вычислить с помощью рекуррентной формулы

$$T_N^K = T_{N-K}^K + T_N^{K-1}. \tag{3}$$

Здесь $T_N^0 = 0$, $T_0^k = 1$ и $T_N^K = T_N^N$, если $N > 0$, $K > N$.

Доказательство. Пусть граф G — сверхстройное дерево, заданное вектором $(a_1, \ldots, a_s)$, $a_i \neq 0$ для $i = 1, \ldots, s$, и если s чётно, то $a_{s/2} \geqslant 2$. Построим граф G^* из графа G следующим образом: листья цепей длины s соединим с корневой вершиной; лист цепи длины i, отличной от s, соединим с листом цепи длины $(s - i)$, не соединённым ни с каким другим листом, либо, если таких нет, с любым листом цепи длины $(s - i)$. Пример описанной схемы для $s = 3$ показан на рис. 2.

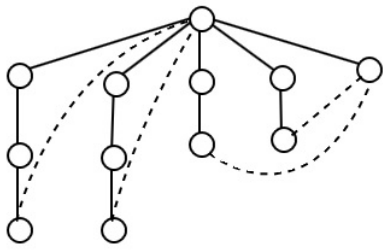

Рис. 2. Иллюстрация к теореме 1

Покажем, что граф G^* является рёберным 1-расширением графа G. Из построения очевидно, что граф G^* является объединением циклов длины $(s+1)$, причём все циклы имеют одну общую вершину (корневая вершина в дереве) и каждое ребро в G^* принадлежит, по крайней мере, одному из этих циклов. Построим граф G_1 из G^*, удалив произвольное ребро. Цикл, которому принадлежит это ребро, распадётся на две цепи с длинами l и $(s - l)$, $0 \leqslant l \leqslant s$. Пусть изначально этот цикл был образован цепями длин k и $(s - k)$, $0 \leqslant k \leqslant s$. Тогда при вложении G в G_1 цепи длин k и $(s - k)$ могут вложиться в цикл, образованный цепями длин l и $(s - l)$. Остальное вложение можно произвести естественным путём. Таким образом доказывается вложимость G_1 в G, из чего следует, что G^* — рёберное 1-расширение графа G. Количество дополнительных рёбер этого расширения даёт формула (1).

Соотношение для количества неизоморфных таких рёберных 1-расширений выводится из нижеследующих соображений. Если не для каждой цепи длины i найдется свободная пара — цепь длины $(s - i)$, то такие цепи можно соединить с любой занятой цепью длины $(s - i)$. Именно различные сочетания соединений «беспарных» цепей

с занятыми цепями обуславливают возможность получения неизоморфных рёберных 1-расширений по описанной схеме. Для конкретного i задачу о количестве различных способов соединения можно переформулировать следующим образом: сколькими различными способами можно разбить число n на сумму, где количество слагаемых не превышает k; в данном контексте под n подразумевается количество занятых цепей длины $(s-i)$, а под k — количество «беспарных» цепей длины i. Решение данной задачи описывается с помощью рекуррентной формулы (3). Для получения окончательного результата необходимо перемножить результаты для всех i от 1 до $[s/2]$, в результате чего и получится итоговая формула (2). ■

Сверхстройных деревьев, удовлетворяющих условию теоремы 1, относительно немного, поэтому представляет интерес построить оценку для сверхстройных деревьев произвольного вида.

1. Основной результат

Теорема 2. Пусть граф G — сверхстройное дерево, заданное вектором $(a_1, \ldots, a_s)$, при этом $a_1 = k$ и $a_2 = 0$, $k \neq 0$. Тогда существует граф G^* — рёберное 1-расширение графа G с количеством дополнительных рёбер $ec(G)$, вычисляемым по формуле

$$ec(G) = k + \sum_{i=1}^{s} (i-1)\, a_i.$$

Доказательство. Построим граф G^* из G. Для каждой из цепей графа G выполним следующие действия:

1. Если длина цепи не равна 1, то соединим вершину степени 1, принадлежащую этой цепи, со всеми вершинами этой цепи, не смежными с ней, в том числе и с корневой вершиной дерева (рис. 3).

2. Если длина цепи равна 1, то соединим вершину степени 1, принадлежащую этой цепи, с вершиной, смежной с вершиной степени 1 из любой другой цепи длины больше 1 (рис. 4).

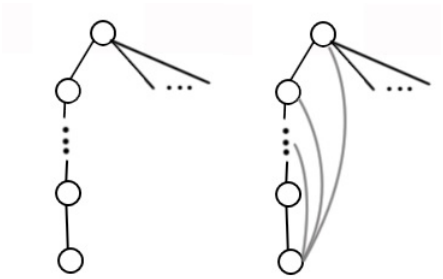

Рис. 3

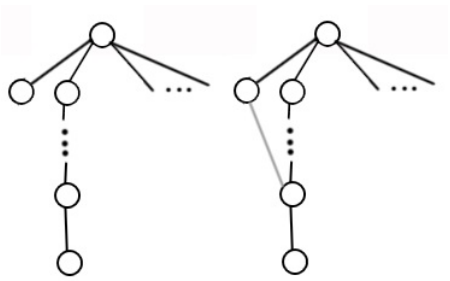

Рис. 4

Построенный граф G^* имеет $k + \sum_{i=1}^{s} (i-1)\, a_i$ дополнительных рёбер по сравнению с G. Покажем, что G^* является рёберным 1-расширением графа G. Очевидно, что при удалении любого из добавленных рёбер вложение осуществляется естественным путём.

Рассмотрим два случая: 1) удаление ребра из цепи длины больше 1 и 2) удаление ребра из цепи длины 1.

Для удаления ребра из цепи длины больше 1: схема вложения этой цепи представлена на рис. 5, остальные цепи можно вложить естественным путём. Для удаления ребра

из цепи длины 1: схема вложения этой цепи и цепи, с которой она соединена в процессе построения, представлена на рис. 6, остальные цепи можно вложить непосредственно.

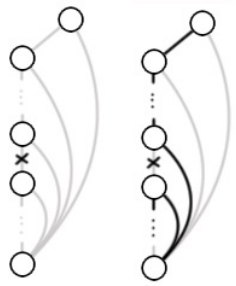

Рис. 5

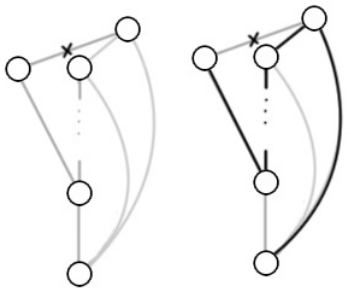

Рис. 6

Теорема доказана. ■

Схема из теоремы 2 имеет ограничения на сверхстройные деревья, к которым она применима. Рассмотрим ещё одну схему, дающую рёберное 1-расширение для сверхстройных деревьев произвольного вида.

Теорема 3. Пусть граф G — сверхстройное дерево, являющееся объединением $s > 2$ цепей $P_1, \ldots, P_s$ с общей концевой вершиной и заданное вектором $(a_1, \ldots, a_t)$, $t > 1$. Тогда существует граф G^* — рёберное 1-расширение графа G с количеством дополнительных рёбер $ec(G)$, вычисляемым по формуле

$$ec(G) = N_d + \frac{s + 1 + a_1}{2}(s - a_1),$$

где N_d — количество сложных рёбер графа G.

Доказательство. Построим граф G^* из графа G путём соединения каждой вершины степени 1 из цепи длины больше 1 со всеми вершинами степени 1 других цепей, корневой вершиной и всеми началами сложных рёбер цепи, которой принадлежит эта вершина. Схема построения графа G^* представлена на рис. 7.

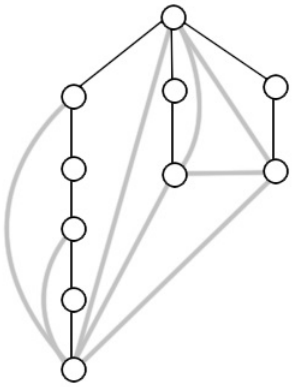

Рис. 7

Количество добавленных рёбер в G^* по сравнению с G можно вычислить по построению: $N_d + \frac{s - 1 + a_1}{2}(s - a_1) + (s - a_1) = N_d + \frac{s + 1 + a_1}{2}(s - a_1)$.

Покажем, что граф G^* является рёберным 1-расширением графа G. Очевидно, что при удалении любого из добавленных рёбер вложение осуществимо естественным путём.

Рассмотрим два случая: 1) удаление сложного ребра цепи и 2) удаление простого ребра. Для удаления сложного ребра из цепи: схема вложения этой цепи представлена на рис. 8, остальные цепи можно вложить естественным путём.

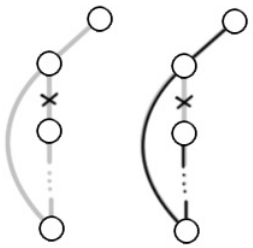

Рис. 8

При удалении простого ребра возможны четыре случая: при удалении ребра цепь P_i разбивается на две цепи длин k_i и l_i, при этом 1) $k_i = 0$; 2) $l_i = 0$; 3) $a_{k_i} > 0$; 4) $a_{l_i} > 0$.

С л у ч а й 1: $k_i = 0$. Схема вложения цепи, которой принадлежит удаляемое ребро, представлена на рис. 9, остальные цепи можно вложить естественным путём.

С л у ч а й 2: $l_i = 0$. Схема вложения цепи, которой принадлежит удаляемое ребро, представлена на рис. 10, остальные цепи можно вложить естественным путём, при этом корневая вершина вкладывается в вершину, которая была листом в исходном сверхстройном дереве.

С л у ч а й 3: $a_{k_i} > 0$. Схема вложения цепи, которой принадлежит удаляемое ребро, и цепи длины k_i представлена на рис. 11, остальные цепи можно вложить естественным образом.

Для с л у ч а я 4 ($a_{l_i} > 0$) схема аналогична, но корневая вершина вкладывается в вершину, которая была листом в исходном сверхстройном дереве.

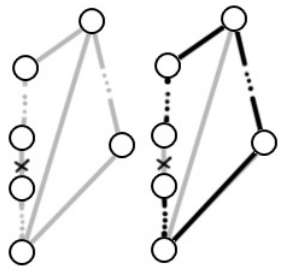

Рис. 9

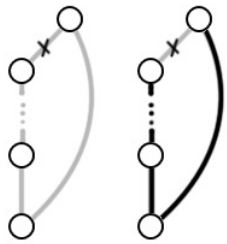

Рис. 10

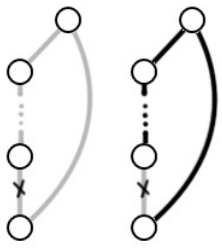

Рис. 11

Таким образом, теорема доказана. ■

Стоит отметить, что в некоторых случаях схема из теоремы 2 позволяет построить рёберное 1-расширение с меньшим количеством дополнительных рёбер по сравнению со схемой из теоремы 3, а в каких-то случаях схема из теоремы 3 оказывается оптимальней схемы из теоремы 2.

Например, на рис. 12 представлен граф, для которого схема из теоремы 2 даёт рёберное 1-расширение с шестью, а схема из теоремы 3 — с девятью дополнительными

рёбрами. Причём для данного графа минимальное рёберное 1-расширение имеет всего три дополнительных ребра. На рис. 13 представлен граф, для которого схема из теоремы 2 даёт рёберное 1-расширение с пятью, а схема из теоремы 3 — с четырьмя дополнительными рёбрами, причём в данном случае схема из теоремы 3 даёт минимальное рёберное 1-расширение [5].

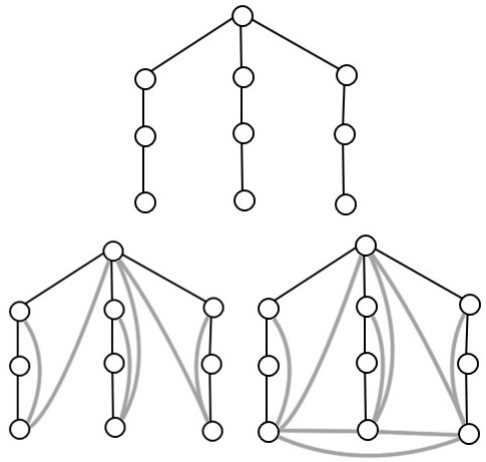

Рис. 12

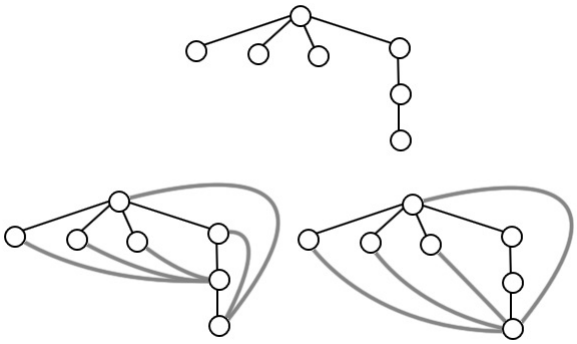

Рис. 13

Заметим, что в каждой из рассмотренных схем построение для одной конкретной цепи происходит изолированно и последовательно; это позволяет для каждой цепи независимо выбирать стратегию построения либо из теоремы 2, либо из теоремы 3. Единственным нюансом остаётся тот факт, что для схемы из теоремы 3 важным является, для какого количества цепей она будет использована (так как вершина степени 1 в этой схеме соединяется со всеми вершинами степени 1, а какие-то вершины степени 1 могут быть уже соединены). Минимизацию в данном случае можно выполнить с помощью итеративных повторений.

Сформулируем алгоритм 1 построения рёберного 1-расширения произвольного сверхстройного дерева, основанный на схемах из теорем 2 и 3. В алгоритме использованы вспомогательные переменные: i — счетчик цикла; h — признак того, что решение найдено (0 — не найдено, 1 — найдено); u — количество цепей, для которых стоит применить схему из теоремы 3.

Сложность алгоритма составляет $O(s^2)$, так как в худшем случае за каждый проход по s цепям добавляется ровно одна цепь, для которой стоит применить схему из теоремы 3; в таком случае понадобится не более s проходов.

На рис. 14 показан 14-вершинный граф и его рёберное 1-расширение, полученное с использованием алгоритма 1. Данное рёберное 1-расширение имеет 8 дополнительных рёбер; для двух цепей применена схема из теоремы 2 и для одной — схема из теоремы 3. При этом рёберное 1-расширение, полученное только по схеме из теоремы 2, имеет 10 дополнительных рёбер, а полученное по схеме из теоремы 3 — 9 дополнительных рёбер. Минимальное рёберное 1-расширение этого графа, полученное в результате вычислительного эксперимента, имеет всего 3 дополнительных ребра.

В заключение стоит отметить, что для любого графа с количеством вершин меньше 11, являющегося объединением цепи длины 3 и произвольного количества цепей длины 1 с общей концевой вершиной, алгоритм 1 даёт минимальное рёберное 1-рас-

Алгоритм 1. Построение рёберного 1-расширения произвольного сверхстройного дерева

Вход: граф G — объединение $s > 2$ цепей с длинами $m_1, \ldots, m_s$ и с общей концевой вершиной.

Выход: булев вектор $(f_1, \ldots, f_s)$, где $f_i = 0$, если для цепи i надо применять схему из теоремы 2, и $f_i = 1$, если для цепи i надо применять схему из теоремы 3.

1: **Для всех** $i = 1, \ldots, s$ положить $f_i := 0$;
2: $h := 0$, $u := 0$, s_1 положить равным количеству цепей длины 1;
3: **Если** $h = 1$ или $u = s$, переход к шагу 12;
4: $h := 1$, $i := 1$;
5: **Если** $i > s$, переход к шагу 3;
6: **Если** $f_i = 1$, переход к шагу 10;
7: **Если** $m_i < (s - u + r_i + 1 - s_1)$ и $m_i > 2$, где r_i — количество сложных рёбер цепи P_i, переход к шагу 10;
8: **Если** $m_i = 1$ и $u = 0$, переход к шагу 10;
9: $u := u + 1$; $h := 0$; $f_i := 1$; $s_1 := 0$;
10: $i := i + 1$;
11: переход к шагу 5;
12: **Вернуть** $(f_1, \ldots, f_s)$.

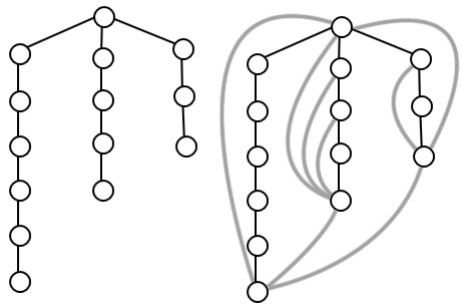

Рис. 14

ширение [5]. Таким образом, оценка количества дополнительных рёбер минимального рёберного 1-расширения произвольного сверхстройного дерева, которую можно получить с помошью алгоритма 1, является достижимой.

ЛИТЕРАТУРА

1. *Абросимов М. Б.* О сложности некоторых задач, связанных с расширениями графов // Матем. заметки. 2010. Т. 88. № 5. С. 643–650.
2. *Абросимов М. Б.* О нижней оценке числа ребер минимального реберного 1-расширения сверхстройного дерева // Изв. Сарат. ун-та. Нов. сер. Математика. Механика. Информатика. 2011. Т. 11. Вып. 3. Ч. 2. С. 111–117.
3. *Harary F. and Hayes J. P.* Edge fault tolerance in graphs // Networks. 1993. No. 23. P. 135–142.
4. *Абросимов М. Б.* Графовые модели отказоустойчивости. Саратов: Изд-во Сарат. ун-та, 2012. 192 с.
5. *Абросимов М. Б., Комаров Д. Д.* Минимальные реберные расширения сверхстройных деревьев с малым числом вершин. Саратов, 2010. 27 с. Деп. в ВИНИТИ 18.10.2010 № 589-В2010.

REFERENCES

1. *Abrosimov M. B.* O slozhnosti nekotorykh zadach, svyazannykh s rasshireniyami grafov [On the complexity of some problems related to graph extensions]. Mat. Zametki, 2010, vol. 88, no. 5, pp. 643–650. (in Russian)
2. *Abrosimov M. B.* O nizhney otsenke chisla reber minimal'nogo rebernogo 1-rasshireniya sverkhstroynogo dereva [On lower bound of edge number of minimal edge 1-extension of starlike tree]. Izv. Saratov Univ. (N.S.), Ser. Math. Mech. Inform., 2011, vol. 11, iss. 3(2), pp. 111–117. (in Russian)
3. *Harary F. and Hayes J. P.* Edge fault tolerance in graphs. Networks, 1993, no. 23, pp. 135–142.
4. *Abrosimov M. B.* Grafovye modeli otkazoustoychivosti [Graph Model of Fault Tolerance]. Saratov, SSU Publ., 2012. 192 p. (in Russian)
5. *Abrosimov M. B., Komarov D. D.* Minimal'nye rebernye rasshireniya sverkhstroynykh derev'ev s malym chislom vershin [Minimal Edge 1-Extension of Starlike Trees with a Small Number of Vertices]. Saratov, 2010. 27 p. VINITI, 18.10.2010, No. 589-V2010. (in Russian)

ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

УДК 519.8

АНАЛИЗ И РЕШЕНИЕ ЗАДАЧ ДИСКРЕТНОЙ ОПТИМИЗАЦИИ С ЛОГИЧЕСКИМИ ОГРАНИЧЕНИЯМИ НА ОСНОВЕ L-РАЗБИЕНИЯ[1]

А. В. Адельшин, А. А. Колоколов

Институт математики им. С. Л. Соболева СО РАН, Омский филиал, г. Омск, Россия

Исследуются задачи дискретной оптимизации с логическими ограничениями на основе моделей целочисленного линейного программирования и метода регулярных разбиений. Получена верхняя оценка мощности произвольного L-комплекса многогранника задачи 2-выполнимости, использование которой позволяет более эффективно решать некоторые прикладные задачи проектирования сложных изделий с помощью рассматриваемых подходов.

Ключевые слова: *задача выполнимости, логические ограничения, целочисленное программирование, L-разбиение.*

DOI 10.17223/20710410/30/10

ANALYSIS AND SOLUTION OF DISCRETE OPTIMIZATION PROBLEMS WITH LOGICAL CONSTRAINTS ON THE BASE OF L-PARTITION APPROACH

A. V. Adelshin, A. A. Kolokolov

Omsk Branch of Sobolev Institute of Mathematics, Omsk, Russia,

E-mail: adelshin@ofim.oscsbras.ru, kolo@ofim.oscsbras.ru

In the paper, we analize discrete optimization problems with logical constraints based on integer linear programming models and L-partition approach. We obtain an upper bound for the power of any L-complex of the 2-SAT polytope. The use of this evaluation allows to solve some applied problems of designing complex products by these approaches much more efficiently.

Keywords: *satisfiability problem, logical constraints, integer programming, L-partition.*

Введение

Во многих задачах управления, планирования, проектирования и других областях возникают логические ограничения, которые необходимо учитывать в процессе принятия решений. Указанные ограничения часто описываются с помощью логических формул и приводят к задаче выполнимости, одной из центральных в теории сложности, а также к задаче максимальной выполнимости и смешанной задаче с логическими

[1]Работа поддержана грантом РФФИ № 13-01-00862.

условиями. Широкое практическое применение этих задач является стимулом для разработки алгоритмов их решения [1 – 6]. В ряде работ проводились исследования указанных задач на основе моделей целочисленного линейного программирования (ЦЛП) и L-разбиения [7], получены структурные свойства многогранников задач и предложены семейства трудных задач для определённых классов алгоритмов [8 – 10]. Кроме того, для задачи выполнимости разработан алгоритм, основанный на методе перебора L-классов [5]. В дальнейшем с его использованием предложены алгоритмы решения задачи максимальной выполнимости и смешанной задачи максимальной выполнимости. В данной работе продолжены исследования структуры многогранника задачи выполнимости, получено новое свойство его L-структуры, которое может оказаться полезным при анализе и разработке алгоритмов решения рассматриваемых задач, основанных на методах целочисленного программирования и аппарате непрерывной оптимизации.

Рассмотрим постановку задачи выполнимости (SAT). Пусть $x_1, \ldots, x_n$ — переменные, принимающие значение *истина* или *ложь*. Под литералом понимается либо переменная x_j, $j = 1, \ldots, n$, либо её отрицание. Пусть логическая формула F представляет собой конъюнкцию формул (скобок) C_i, $i = 1, \ldots, m$, каждая из которых является дизъюнкцией литералов. Требуется определить, выполнима ли формула F, т. е. существует ли такой набор значений переменных, при котором F принимает значение *истина*. Известно, что задача SAT является NP-полной, а в случае, когда каждая скобка содержит не более двух литералов, задача полиномиально разрешима [11]. Многие известные задачи теории графов, построения расписаний, криптографии могут быть сформулированы как задача выполнимости некоторой логической формулы в конъюнктивной нормальной форме [12 – 14].

Важным обобщением задачи SAT является задача максимальной выполнимости (MAX SAT). Предположим, что каждой скобке C_i соответствует неотрицательный вес c_i, тогда задача MAX SAT состоит в отыскании набора значений логических переменных, при котором суммарный вес выполненных скобок будет наибольшим.

Перейдём далее к рассмотрению моделей ЦЛП рассматриваемых задач. Приведём сначала модель для задачи выполнимости. Введём булевы переменные $y_1, \ldots, y_n$, такие, что y_j соответствует переменной x_j, а $(1 - y_j)$ — её отрицанию, т. е. $y_j = 1$ тогда и только тогда, когда переменная x_j принимает значение *истина*, $j = 1, \ldots, n$. Нетрудно показать, что условие выполнимости логической формулы F эквивалентно существованию решения системы

$$\sum_{j \in C_i^+} y_j - \sum_{j \in C_i^-} y_j \geqslant 1 - |C_i^-|, \ i = 1, \ldots, m; \tag{1}$$

$$0 \leqslant y_j \leqslant 1, \ j = 1, \ldots, n; \tag{2}$$

$$y_j \in \mathbb{Z}, \ j = 1, \ldots, n, \tag{3}$$

где C_i^- и C_i^+ — множества индексов переменных, входящих в скобку C_i с отрицанием и без него соответственно; величина $|C_i^-|$ — мощность множества C_i^-.

Для получения задачи ЦЛП необходимо ввести целевую функцию. В качестве такой функции может быть выбрана, например, $f(y) = y_1 \to \max$ или $f(y) = \sum_{j=1}^{n} y_j \to \max$, где $y = (y_1, \ldots, y_n)$. В данной работе рассматривается лексикографическая постановка задачи ЦЛП, т. е. ищется лексикографически максимальный вектор y, удовлетворяющий системе ограничений (1) — (3).

Модель ЦЛП задачи максимальной выполнимости выглядит следующим образом:

$$y_0 = \sum_{i=1}^{m} c_i z_i \to \max; \tag{4}$$

$$\sum_{j \in C_i^-} y_j - \sum_{j \in C_i^+} y_j + z_i \leqslant |C_i^-|, \quad i = 1, \ldots, m; \tag{5}$$

$$0 \leqslant y_j \leqslant 1,\ j = 1, \ldots, n; \tag{6}$$

$$0 \leqslant z_i \leqslant 1,\ i = 1, \ldots, m; \tag{7}$$

$$y_j,\ z_i \in \mathbb{Z},\ j = 1, \ldots, n,\ i = 1, \ldots, m. \tag{8}$$

Здесь каждой скобке C_i поставлена в соответствие переменная z_i, причём в любом допустимом целочисленном решении $z_i = 1$ только в том случае, когда C_i выполнена. Таким образом, оптимальное значение целевой функции равно наибольшему суммарному весу выполненных скобок. Отметим, что если в последнюю модель добавить ограничения вида (1), то получим модель ЦЛП для смешанной задачи с «жесткими» ограничениями (1) и «мягкими» ограничениями (5).

1. О методе регулярных разбиений

Для исследования структуры задач целочисленного программирования, построения и анализа методов их решения А. А. Колоколовым предложен подход, идея которого заключается в выделении семейства специальных разбиений релаксационного множества задачи. Особенности данного подхода подробно описаны в [7].

Приведём необходимые для дальнейшего изложения определения и обозначения. В первую очередь потребуется понятие лексикографического порядка. Для этого рассмотрим функцию

$$\eta(x, y) = \min\{i : x_i \neq y_i,\ i = 1, \ldots, n\},\ x, y \in \mathbb{R}^n,\ x \neq y.$$

Вектор x *лексикографически больше* (*меньше*) вектора y, т. е. $x \succ y$ ($x \prec y$), если $x \neq y$ и $x_w > y_w$ ($x_w < y_w$) для $w = \eta(x, y)$. Отношение $\succ$ представляет собой отношение строгого линейного порядка. Запись $x \succeq y$ означает, что либо $x \succ y$, либо $x = y$. Аналогично понимается $x \preceq y$.

Для множеств $X, Y \subset \mathbb{R}^n$ полагаем: $X \succ Y$ ($X \prec Y$), если $x \succ y$ ($x \prec y$) для любых $x \in X$ и $y \in Y$.

Пусть $x, y \in \mathbb{R}^n$ и $x \succ y$. Будем говорить, что точки x и y *отделимы*, если найдётся точка $z \in \mathbb{Z}^n$, для которой выполняется $x \succeq z \succeq y$. Точку z назовём *отделяющей*.

Дадим определение L-разбиения. Точки $x, y \in \mathbb{R}^n$ ($x \succ y$) называются *L-эквивалентными*, если не существует отделяющей их точки $z \in \mathbb{Z}^n$. Это отношение эквивалентности порождает разбиение любого множества $X \subset \mathbb{R}^n$ на непересекающиеся *L-классы*. Фактор-множество X/L называется *L-разбиением* множества X. Указанное разбиение обладает рядом полезных свойств, применяемых при разработке и исследовании алгоритмов целочисленного программирования, в частности алгоритмов перебора L-классов. Отметим некоторые из них:

1) каждая точка $z \in \mathbb{Z}^n$ образует отдельный L-класс, остальные классы состоят из нецелочисленных точек и называются *дробными*;
2) если X — ограниченное множество, то фактор-множество X/L конечно;
3) любой дробный L-класс $V \in X/L$ можно представить в виде

$$V = X \cap \{x :\ x_1 = a_1, \ldots, x_{r-1} = a_{r-1}, a_r < x_r < a_r + 1\},$$

где $a_i \in \mathbb{Z}$, $i = 1, \ldots, r$; $1 \leqslant r \leqslant n$.

Рангом L-класса V называется величина

$$r(V) = \begin{cases} \min\{i:\ x_i \neq [x_i],\ i = 1, \ldots, n,\ x \in V\}, & \text{если } V - \text{дробный}, \\ n+1 \quad \text{в противном случае.} \end{cases}$$

Подмножество K дробных L-классов из X/L называется *комплексом* (L-*комплексом*), если для любых $V, V' \in K$, $V \succ V'$, не существует точки $z \in X \cap \mathbb{Z}^n$, отделяющей V и V', т. е. $V \succ z \ \succ V'$.

Далее рассмотрим лексикографическую задачу ЦЛП следующего вида: найти лексикографически максимальную точку y^* множества $(M \cap \mathbb{Z}^n)$, т. е.

$$\text{найти } y^* = \operatorname{lexmax}(M \cap \mathbb{Z}^n), \tag{9}$$

где M — некоторый выпуклый многогранник. Важную роль в исследовании задачи (9) и методов её решения играет множество

$$M_* = \{y \in M : \forall z \in M \cap \mathbb{Z}^n\ (y \succ z)\},$$

которое называется *дробным накрытием* задачи (9). Фактор-множество M_*/L называется L-*накрытием* задачи.

Выделение этой части релаксационного множества задачи связано с тем, что в некоторых методах ЦЛП (методах отсечения, перебора L-классов) происходит последовательное исключение точек из M_*, т. е. эти методы можно рассматривать как определённые способы «снятия» дробных накрытий.

С использованием метода регулярных разбиений получен ряд теоретических результатов при исследовании задач с логическими условиями [5, 8 – 10]. Проведён анализ L-структуры многогранников (1) — (2) и (5) — (7) задач выполнимости и максимальной выполнимости. Построены семейства логических формул, для которых мощности L-накрытий задач выполнимости и максимальной выполнимости растут экспоненциально с увеличением числа переменных. Получены оценки числа итераций некоторых алгоритмов целочисленного линейного программирования при решении задач из построенных семейств.

2. Задача 2-выполнимости

Пусть каждая скобка в логической формуле F содержит не более двух литералов. В этом случае задачу выполнимости называют *задачей 2-выполнимости*. В работе [9] проведён анализ структуры задачи 2-выполнимости и доказана следующая

Лемма 1 [9]. Если многогранник M задачи 2-выполнимости, содержащий целочисленную точку, пересекается с некоторой k-мерной гранью куба $B^n = \{x \in \mathbb{R}^n : 0 \leqslant \leqslant x_j \leqslant 1, j = 1, \ldots, n\}$, то M содержит вершину этой грани.

С помощью этой леммы получена верхняя оценка мощности L-накрытия лексикографического варианта (9) задачи 2-выполнимости

Теорема 1. Если многогранник M задачи 2-выполнимости содержит целочисленную точку, то для мощности L-накрытия выполняется $|M_*/L| \leqslant n - 1$.

Далее приводятся результаты исследований структуры многогранника данной задачи, обобщающие ранее полученную оценку теоремы 1.

Лемма 2. Пусть существуют $a = (a_1, \ldots, a_n) \in M \cap \mathbb{Z}^n$ и $b = (b_1, \ldots, b_n) \in M \cap \mathbb{Z}^n$, такие, что $a \succ b$ и не существует $c \in M \cap \mathbb{Z}^n$ со свойством $a \succ c \succ b$. Тогда для $\Omega = \{y \in M :\ a \succ y \succ b\}$ справедливо $|\Omega/L| \leqslant n - 1$.

Доказательство.

I. Допустим, L-комплекс Ω/L содержит L-класс V ранга n. Пусть $V = \{(v_1, \ldots, v_{n-1}, v_n) : 0 < v_n < 1\}$, где $v_j \in \{0, 1\}$, $j = 1, \ldots, n-1$. Покажем, что $(v_1, \ldots, v_{n-1}, 0) \in M$ и $(v_1, \ldots, v_{n-1}, 1) \in M$. Заметим, что в системе ограничений (1) задачи возможны четыре вида неравенств, содержащих переменную y_n: $y_j + y_n \leqslant 1$, $y_j + y_n \geqslant 1$, $y_j - y_n \leqslant 0$ и $y_j - y_n \geqslant 0$. Учитывая множества возможных значений координат $v_1, \ldots, v_{n-1}, v_n$, легко видеть, что в любом из перечисленных неравенств значение v_n можно положить равным 0 или 1, при этом полученное решение останется допустимым.

Следовательно, если L-комплекс Ω/L содержит L-класс V ранга n, то $a = (v_1, \ldots, v_{n-1}, 1) \in M$, $b = (v_1, \ldots, v_{n-1}, 0) \in M$, а значит, $|\Omega| = 1$.

II. Теперь докажем, что Ω/L не может содержать два L-класса одного ранга.

Предположим обратное: пусть существуют $V_1, V_2 \in \Omega/L$ ранга k и $V_1 \succ V_2$. Нетрудно показать, что они имеют следующий вид:

$$V_1 = \{(a_1, \ldots, a_{k-1}, \alpha_k, \ldots, \alpha_n) : \ 0 < \alpha_k < 1, \ 0 \leqslant \alpha_j \leqslant 1, \ j = k+1, \ldots, n\},$$
$$V_2 = \{(b_1, \ldots, b_{k-1}, \beta_k, \ldots, \beta_n) : \ 0 < \beta_k < 1, \ 0 \leqslant \beta_j \leqslant 1, \ j = k+1, \ldots, n\}.$$

Это вытекает из леммы 1 и того, что между a и b нет других целочисленных точек.

Покажем, что существует целочисленная точка $d \in M$, такая, что $a \succ d \succ b$, и построим её алгоритмически.

Определим следующие множества. Пусть F — множество всех ограничений задачи, $Q^t \subseteq F$, $I = \{1, \ldots, n\}$ — множество всех индексов переменных формулы, $J^t \subseteq \{j : j \geqslant k\}$. Будем рассматривать различные целочисленные точки $d^t = (d_1^t, \ldots, d_n^t)$: для всех $j \in I$

$$d_j^t = \begin{cases} a_j, & \text{если } j \notin J^t, \\ b_j, & \text{если } j \in J^t. \end{cases}$$

Положим $Q^0 = \varnothing$, $J^0 = \{k\}$, $d^0 = (a_1, \ldots, a_{k-1}, 0, a_{k+1}, \ldots, a_n)$. Нетрудно показать, что $a_k = 1$, $b_k = 0$, $\alpha_k \neq a_k$.

Пусть после итерации t имеются Q^t, J^t и соответствующая точка d^t, такие, что выполнены следующие свойства:

— ограничения из Q^t содержат только литералы с индексами из J^t;
— $\forall j \in J^t$ $(\alpha_j \neq a_j)$.

Покажем, что если $d^t \notin M$, то можно построить множества $Q^{t+1} \supset Q^t$, $J^{t+1} \supset J^t$ и соответствующую точку d^{t+1}, для которых данные свойства также будут выполнены. Пусть d^t удовлетворяет любому ограничению из Q^t. Значит, должно существовать ограничение $g(y_i, y_j) \in F \backslash Q^t$, которому точка d^t не удовлетворяет, но удовлетворяют точки a, b и L-класс V_1. Попробуем его найти.

Возможны несколько вариантов такого ограничения:

1) $i \notin J^t$, $j \notin J^t$. Но тогда данному ограничению не удовлетворяет точка a. Противоречие.
2) $i \in J^t$, $j \in J^t$. Но тогда данному ограничению не удовлетворяет точка b. Противоречие.
3) $i < k$, $j \in J^t$. Возможны четыре вида ограничений: $y_i + y_j \leqslant 1$, $y_i + y_j \geqslant 1$, $y_i - y_j \leqslant 0$ и $y_i - y_j \geqslant 0$.

Рассмотрим первое из них $y_i + y_j \leqslant 1$:

$$\begin{cases} d_i^t + d_j^t > 1, \\ a_i + a_j \leqslant 1, \\ a_i + \alpha_j \leqslant 1 \end{cases} \Rightarrow \begin{cases} a_i + d_j^t > 1, \\ a_i + a_j \leqslant 1, \\ a_i + \alpha_j \leqslant 1 \end{cases} \Rightarrow \begin{cases} a_i = 1, d_j^t = 1, \\ a_i + a_j \leqslant 1, \\ a_i + \alpha_j \leqslant 1 \end{cases} \Rightarrow \begin{cases} a_i = 1, d_j^t = 1, \\ 1 + a_j \leqslant 1, \\ 1 + \alpha_j \leqslant 1 \end{cases} \Rightarrow$$

$$\Rightarrow \begin{cases} a_i = 1, d_j^t = 1, \\ a_j = 0, \\ \alpha_j = 0 \end{cases} \Rightarrow \text{противоречие с } \alpha_j \neq a_j.$$

Аналогично рассматриваются оставшиеся ограничения, которые приводят к таким же противоречиям.

Таким образом, ограничения задачи, удовлетворяющие свойствам 1–3, не являются искомыми. Остаётся последний вариант:

4) $j \in J^t$, $i \notin J^t$ и $i > k$. Возможны те же четыре вида ограничений.

Рассмотрим первое $y_i + y_j \leqslant 1$:

$$\begin{cases} d_i^t + d_j^t > 1, \\ a_i + a_j \leqslant 1, \\ \alpha_i + \alpha_j \leqslant 1 \end{cases} \Rightarrow \begin{cases} a_i + b_j > 1, \\ a_i + a_j \leqslant 1, \\ \alpha_i + \alpha_j \leqslant 1 \end{cases} \Rightarrow \begin{cases} a_i = 1, b_j = 1, \\ a_i + a_j \leqslant 1, \\ \alpha_i + \alpha_j \leqslant 1 \end{cases} \Rightarrow \begin{cases} a_i = 1, b_j = 1, \\ 1 + a_j \leqslant 1, \\ \alpha_i + \alpha_j \leqslant 1 \end{cases} \Rightarrow$$

$$\Rightarrow \begin{cases} a_i = 1, b_j = 1, \\ a_j = 0, \\ \alpha_i + \alpha_j \leqslant 1 \end{cases} \Rightarrow (\alpha_j \neq a_j) \Rightarrow \begin{cases} a_i = 1, b_j = 1, \\ a_j = 0, \alpha_j > 0 \\ \alpha_i + \alpha_j \leqslant 1 \end{cases} \Rightarrow \begin{cases} a_i = 1, b_j = 1, \\ a_j = 0, \alpha_j > 0 \\ \alpha_i < 1 \end{cases} \Rightarrow$$

$$\Rightarrow \alpha_i \neq a_i.$$

Аналогично можно рассмотреть оставшиеся виды ограничений и получить такие же результаты.

Теперь рассмотрим множества $Q^{t+1} = Q^t \cup \{g(y_i, y_j)\}$, $J^{t+1} = J^t \cup \{i\}$ и соответствующую точку d^{t+1}, где $d_i^{t+1} = b_i$. Очевидно, что:

— ограничения из Q^{t+1} содержат только литералы с индексами из J^{t+1};
— $\forall j \in J^{t+1}$ $(\alpha_j \neq a_j)$.

Таким образом, мы построили множества $Q^{t+1} \supset Q^t$, $J^{t+1} \supset J^t$ и соответствующую точку d^{t+1}, для которых выполнены те же условия, что и для d^t. А значит, можно строить последовательность пар таких множеств (Q^{t+2}, J^{t+2}), (Q^{t+3}, J^{t+3}), …, до тех пор, пока не найдём $d^s \in M$. Конечность данного процесса вытекает из конечности множеств F и I. А поскольку $a \succ d^s \succ b$ по построению, получаем противоречие. Следовательно, L-комплекс Ω/L не может содержать два L-класса одного ранга.

Таким образом, либо L-комплекс Ω/L содержит L-класс ранга n, и тогда $|\Omega/L| = 1$, либо не содержит, и тогда $|\Omega/L| \leqslant n - 1$. ■

Приведём пример формулы, для которой данная оценка достигается.

Пример 1. Рассмотрим логическую формулу

$$F = \bigwedge_{i<j\leqslant n} (\overline{x}_i \vee \overline{x}_j) \bigwedge_{i=2}^{n-1} (\overline{x}_i \vee x_{i+1}) \wedge (x_{n-1} \vee \overline{x}_n).$$

Нетрудно показать, что многогранник M содержит только две целочисленные точки: $z_1 = (1, 0, \ldots, 0)$ и $z_2 = (0, 0, \ldots, 0)$, а также в нём содержатся полуцелочисленные

точки вида

$$y^{(k)} = (\underbrace{0,\ldots,0}_{k-1}, 1/2,\ldots,1/2),\ k = 1,\ldots,n-1,$$

причём $z_1 \succ y^{(k)} \succ z_2$. Каждая точка $y^{(k)}$ является представителем L-класса

$$V^{(k)} = \{(\underbrace{0,\ldots,0}_{k-1}, v_k,\ldots,v_n),\ 0 < v_k < 1,\ 0 \leqslant v_j \leqslant 1,\ j = k+1,\ldots,n\},$$

причём $r(V^{(k)}) = k$. Таким образом, $|\{y \in M : z_1 \succ y \succ z_2\}/L| = n-1$.

Лемма 3. Пусть существует $a \in M \cap Z$ и не существует $c \in M \cap Z$, что $a \succ c$. Тогда для $\Omega = \{y \in M : a \succ y\}$ справедливо $|\Omega/L| \leqslant n-1$.

Доказательство. Легко показать (аналогично п. I доказательства леммы 2), что L-комплекс Ω/L не содержит L-класса ранга n, поскольку в противном случае существует точка $c \in M \cap Z$, для которой $a \succ c$.

Допустим, существуют $V_1, V_2 \in \Omega/L$ ранга $k < n$ и $V_1 \succ V_2$:

$$V_1 = \{(\alpha_1,\ldots,\alpha_{k-1},\alpha_k,\ldots,\alpha_n) :\ 0 < \alpha_k < 1,\ 0 \leqslant \alpha_j \leqslant 1,\ j = k+1,\ldots,n\},$$

где $\alpha_j \in \{0,1\}$, $j = 1,\ldots,k-1$, — фиксированные;

$$V_2 = \{(\beta_1,\ldots,\beta_{k-1},\beta_k,\ldots,\beta_n) :\ 0 < \beta_k < 1,\ 0 \leqslant \beta_j \leqslant 1,\ j = k+1,\ldots,n\},$$

где $\beta_j \in \{0,1\}$, $j = 1,\ldots,k-1$, — фиксированные.

Тогда V_1 содержится в $(n-k+1)$-мерной грани

$$S^1 = \{(\alpha_1,\ldots,\alpha_{k-1},y_k,\ldots,y_n) :\ 0 \leqslant y_j \leqslant 1,\ j = k,\ldots,n\},$$

V_2 содержится в $(n-k+1)$-мерной грани

$$S^2 = \{(\beta_1,\ldots,\beta_{k-1},y_k,\ldots,y_n) :\ 0 \leqslant y_j \leqslant 1,\ j = k,\ldots,n\}$$

и $S^1 \succ S^2$. Согласно лемме 1, в каждой из этих граней есть вершина, принадлежащая M. Обозначим их $c_1 \in S_1$ и $c_2 \in S_2$. Но поскольку $a \succeq S_1 \succ S_2$, получается, что $a \succ c_2$. Противоречие. ■

Приведём пример формулы, для которой данная оценка достигается.

Пример 2. Рассмотрим логическую формулу

$$F = \bigwedge_{i=1}^{n-1} (x_i \vee x_{i+1}) \bigwedge_{i=1}^{n-1} (x_i \vee \overline{x}_{i+1})\,.$$

Многогранник M содержит только две целочисленные точки: $z_1 = (1,\ldots,1,1)$ и $z_2 = (1,\ldots,1,0)$, а также в нём содержатся полуцелочисленные точки вида

$$y^{(k)} = (\underbrace{1,\ldots,1}_{k-1}, 1/2,\ldots,1/2),\ k = 1,\ldots,n-1,$$

причём $z_2 \succ y^{(k)}$. Каждая точка $y^{(k)}$ является представителем L-класса

$$V^{(k)} = \{(\underbrace{1,\ldots,1}_{k-1}, v_k,\ldots,v_n) :\ 0 < v_k < 1,\ 0 \leqslant v_j \leqslant 1,\ j = k+1,\ldots,n\},$$

причём $r(V^{(k)}) = k$.

Таким образом, $|\{y \in M : z_2 \succ y\}/L| = n-1$.

Из лемм 2 и 3 следует верхняя оценка мощности произвольного L-комплекса многогранника задачи 2-SAT.

Теорема 2. Мощность любого L-комплекса многогранника задачи 2-SAT, содержащего целочисленную точку, не превосходит $n - 1$.

Полученные свойства полезны при анализе и разработке алгоритмов решения задачи выполнимости и смешанной задачи максимальной выполнимости. В частности, в работе [6] предложен алгоритм решения последней, в котором используется процедура перехода от одного допустимого решения к другому в порядке лексикографического убывания. Эта процедура основана на переборе L-классов и её трудоёмкость определяется числом дробных L-классов между соседними целочисленными решениями. В некоторых прикладных задачах (например, проектирования [5]) набор логических ограничений представляет собой задачу 2-выполнимости, а значит, теорема 2 гарантирует, что перебор допустимых решений в указанной процедуре будет осуществляться достаточно быстро. Таким образом, представляется целесообразным построение алгоритмов, использующих перебор L-классов, для рассматриваемых постановок.

ЛИТЕРАТУРА

1. *Колоколов А. А., Адельшин А. В., Ягофарова Д. И.* Решение задачи выполнимости с использованием метода перебора L-классов // Информационные технологии. 2009. № 2. С. 54–59.
2. *Gu J., Purdom P., Franco J., and Wah B.* Algorithms for the satisfiability (SAT) problem: a survey // DIMACS Series in Discrete Mathematics and Theoretical Computer Science. American Mathematical Society, 1996. P. 19–152.
3. *Hamadi Y., Jabbour S., and Sais L.* ManySAT: a parallel SAT solver // J. Satisfiability, Boolean Modeling and Comput. 2009. No. 6. P. 245–262.
4. *Thornton J., Bain S., Sattar A., and Pham D. N.* A two level local search for MAX-SAT Problems with hard and soft constraints // Proc. 15th Australian Joint Conference on Artificial Intelligence, AustAI-2002. Canberra, Australia, 2002. P. 603–614.
5. *Колоколов А. А., Адельшин А. В., Ягофарова Д. И.* Исследование задач дискретной оптимизации с логическими ограничениями на основе метода регулярных разбиений // Прикладная дискретная математика. 2013. № 1(19). С. 99–109.
6. *Адельшин А. В., Кучин А. К.* Разработка алгоритмов решения смешанной задачи максимальной выполнимости // Материалы V Всерос. конф. «Проблемы оптимизации и экономические приложения». Омск, 2012. С. 99.
7. *Колоколов А. А.* Регулярные разбиения и отсечения в целочисленном программировании // Сиб. журнал исследования операций. 1994. № 2. С. 18–39.
8. *Адельшин А. В.* Исследование задач максимальной и минимальной выполнимости с использованием L-разбиения // Автоматика и телемеханика. 2004. № 3. С. 35–42.
9. *Ягофарова Д. И.* Анализ L-структуры задачи 2-выполнимость // Материалы конф. «Под знаком ‘Сигма’». Омск, 1994. С. 71–77.
10. *Kolokolov A., Adelshin A., and Yagofarova D.* Analysis and solving SAT and MAX-SAT problems using an L-partition approach // J. Math. Modeling Algorithm. 2013. No. 12(2). P. 201–212.
11. *Cook S. A.* The complexity of theorem-proving procedure // Proc. 3rd Annual ACM Symp. Theory of Computing. N. Y.: ACM, 1971. P. 151–159.
12. *Колоколов А. А., Ярош А. В.* Автоматизация проектирования сложных изделий с использованием дискретной оптимизации и информационных технологий // Омский научный вестник. 2010. № 2(90). С. 234–238.

13. *Посыпкин М. А., Заикин О. С., Беспалов Д. В., Семенов А. А.* Решение задач криптоанализа поточных шифров в распределенных вычислительных средах // Труды ИСА. 2009. Т. 46. С. 119–137.
14. *Massacci F. and Marraro L.* Logical cryptanalysis as a SAT problem // J. Automated Reasoning. 2000. No. 24. P. 165–203.

REFERENCES

1. *Kolokolov A. A., Adelshin A. V., Yagofarova D. I.* Reshenie zadachi vypolnimosti s ispol'zovaniem metoda perebora L-klassov [Solving SAT problem using L-class enumeration method]. Informatsionnye Tekhnologii, 2009, no. 2, pp. 54–59. (in Russian)
2. *Gu J., Purdom P., Franco J., and Wah B.* Algorithms for the satisfiability (SAT) problem: a survey. DIMACS Series in Discrete Mathematics and Theoretical Computer Science. American Mathematical Society, 1996, pp. 19–152.
3. *Hamadi Y., Jabbour S., and Sais L.* ManySAT: a parallel SAT solver. J. Satisfiability, Boolean Modeling and Comput., 2009, no. 6, pp. 245–262.
4. *Thornton J., Bain S., Sattar A., and Pham D. N.* A two level local search for MAX-SAT Problems with hard and soft constraints. Proc. 15th Australian Joint Conference on Artificial Intelligence, AustAI-2002. Canberra, Australia, 2002, pp. 603–614.
5. *Kolokolov A. A., Adelshin A. V., Yagofarova D. I.* Issledovanie zadach diskretnoy optimizatsii s logicheskimi ogranicheniyami na osnove metoda regulyarnykh razbieniy [Study of discrete optimization problems with logical constraints based on regular partitions]. Prikladnaya Diskretnaya Matematika, 2013, no. 1(19), pp. 99–109. (in Russian)
6. *Adelshin A. V., Kuchin A. K.* Razrabotka algoritmov resheniya smeshannoy zadachi maksimal'noy vypolnimosti [Development of algorithms for solving a mixed problem of maximal satisfiability]. Materialy V Vseross. konf. «Problemy optimizatsii i ekonomicheskie prilozheniya», Omsk, 2012, p. 99. (in Russian)
7. *Kolokolov A. A.* Regulyarnye razbieniya i otsecheniya v tselochislennom programmirovanii [Regular partitions and truncations in integer programming]. // Sibirsk. Zh. Issled. Oper., 1994, no. 2, pp. 18–39. (in Russian)
8. *Adelshin A. V.* Issledovanie zadach maksimal'noy i minimal'noy vypolnimosti s ispol'zovaniem L-razbieniya [Investigation of maximum and minimum satisfiability problems using L-partition]. Avtomat. i Telemekh., 2004, no. 3, pp. 35–42. (in Russian)
9. *Yagofarova D. I.* Analiz L-struktury zadachi 2-vypolnimost' [Analysis of the L-structure for 2-SAT problem]. Materialy konf. «Pod znakom 'Sigma'». Omsk, 1994, pp. 71–77. (in Russian)
10. *Kolokolov A., Adelshin A., and Yagofarova D.* Analysis and solving SAT and MAX-SAT problems using an L-partition approach. J. Math. Modeling Algorithm, 2013, no. 12(2), pp. 201–212.
11. *Cook S. A.* The complexity of theorem-proving procedure. Proc. 3rd Annual ACM Symp. Theory of Computing. N. Y., ACM, 1971, pp. 151–159.
12. *Kolokolov A. A., Yarosh A. V.* Avtomatizatsiya proektirovaniya slozhnykh izdeliy s ispol'zovaniem diskretnoy optimizatsii i informatsionnykh tekhnologiy [Computer-aided design of complex products using discrete optimization and information technologies]. Omskiy nauchnyy vestnik, 2010, no. 2(90), pp. 234–238. (in Russian)
13. *Posypkin M. A., Zaikin O. S., Bespalov D. V., Semenov A. A.* Reshenie zadach kriptoanaliza potochnykh shifrov v raspredelennykh vychislitel'nykh sredakh [Cryptanalysis of stream ciphers in distributed computing systems]. Trudy ISA, 2009, vol. 46, pp. 119–137. (in Russian)
14. *Massacci F. and Marraro L.* Logical cryptanalysis as a SAT problem. J. Automated Reasoning, 2000, no. 24, pp. 165–203.

ДИСКРЕТНЫЕ МОДЕЛИ РЕАЛЬНЫХ ПРОЦЕССОВ

УДК 519.168

МЕТОД ОЦЕНКИ СТЕПЕНИ СВЯЗИ БИНАРНОГО И НОМИНАЛЬНОГО ПОКАЗАТЕЛЕЙ

С. В. Дронов, И. Ю. Бойко

Алтайский государственный университет, г. Барнаул, Россия

При обработке современных статистических данных всё чаще появляется необходимость исследовать связь между числовым (номинальным) и бинарным показателями. В работе рассмотрен новый коэффициент для оценивания силы связи между такими показателями, названный ледж-коэффициентом и ориентированный на выявление связей типа «ступеньки», означающей существование заранее неизвестных, но постоянных границ для числового показателя, при попадании в которые бинарный показатель в основном принимает только одно из своих значений. Предлагаются алгоритмы для вычисления ледж-коэффициента, а также для перебора всех случаев, в которых связь оказывается слабейшей и сильнейшей из возможных. Приведены сравнительные примеры оценивания силы связи по ледж-коэффициенту и коэффициентам корреляции Пирсона и Кендалла.

Ключевые слова: *бинарные и номинальные переменные, нормативные интервалы, связь типа «ступенька», бинарные цепочки.*

DOI 10.17223/20710410/30/11

METHOD FOR ESTIMATING CONNECTION POWER OF BINARY AND NOMINAL VARIABLES

S. V. Dronov, I. Yu. Boyko

Altai State University, Barnaul, Russia

E-mail: dsv@math.asu.ru

Nowadays, one of the common connection types in statistical data processing is the connection between numerical (nominal) and binary variables. We propose a new coefficient for evaluation of this type connection. It is quite different from Pearson's correlation coefficient and focused at the "ledge" type of connection, which means that the binary variable is expected to take one of its values only within some unknown but fixed boundaries for the the numerical variable. We call it ledge-coefficient. Application scope for the proposed coefficient is discussed. Algorithms for calculating ledge-coefficient and for searching all cases when the ledge connection is extremely weak or strong are proposed. Comparative examples for estimating connection power by ledge-coefficient and by Pearson's correlation coefficient or by Kendall's tau are shown.

Keywords: *binary and nominal variables, normative intervals, ledge connection, binary string.*

Введение

Практически любая обработка данных эксперимента имеет одной из своих целей установления факта связи определённых показателей, а также оценку степени (силы) этой связи. Сегодня достаточно активно разрабатываются современные методы решения этой задачи для случая, когда показатели измеряются в шкалах разных типов (к примеру, аппараты качественной и логистической регрессий, модель Раша в тестологии и многие другие). Тем не менее в практических расчетах проблема все ещё часто решается с помощью коэффициента корреляции Пирсона между показателями, что фактически ограничивает исследование лишь линейными связями. Исследователь-практик объясняет такой выбор метода, как правило, тем, что он склонен считать распределения нужных ему показателей нормальными, тем самым оправдывая законность изучения только связей, имеющих существенную линейную составляющую. Однако в одном из случаев ясно, что предположения нормальности показателя заведомо не отвечают объективной структуре данных: это ситуация, когда показатель бинарен и может принимать только значения 0 или 1. Случай, когда один из показателей принимает числовые значения (номинальный), а второй бинарен, рассматривается в настоящей работе.

Описанная ситуация является довольно обычной, особенно в медицине, которая сегодня все чаще использует в своих моделях математику [1, 2]. Номинальными являются числовые медицинские показатели (кровяное давление, температура тела и пр.), бинарными — наличие или отсутствие определённых признаков. В медицинских работах используют либо уже упомянутый коэффициент Пирсона, либо коэффициенты бисериальной или точечно-бисериальной корреляции. Однако внимательное изучение этих коэффициентов показывает, что они являются лишь вариантами коэффициента Пирсона, а значит, применение их также не вполне законно.

Действительно, линейная связь, наличие которой обеспечивает значимая величина коэффициента корреляции, предполагает, что все точки поля корреляции выборочных данных довольно хорошо аппроксимируются некоторой прямой линией, что, как правило, невозможно, когда одна из координат принимает только два различных значения. Таким образом, даже в случае очень сильно выраженной связи аппроксимирующая линия должна быть иной.

Один из видов такой линии выявляется в медицинской практике. Так, большинство числовых показателей в медицине имеют нормативные интервалы, при выходе за которые возникает подозрение на заболевание. Если X — значение такого числового показателя, то при некоторых a, b признак здоровья пациента Y должен в случае наличия предельно сильной связи задаваться, таким образом, формулой

$$Y_{a,b}(X) = \begin{cases} 1, & a \leqslant X \leqslant b, \\ 0 & \text{иначе.} \end{cases} \tag{1}$$

Далее такую функцию будем называть ступенькой, а соответствующую связь (при её установлении) связью типа «ступенька». Как правило, интервал $[a, b]$ будем считать неизвестным. Этот тип связи впервые, по-видимому, изучался в работах [3, 4].

Исходными данными для оценки силы связи служат две связанные выборки объёма n каждая: $X = (x_1, \ldots, x_n)$ и $Y = (y_1, \ldots, y_n)$, где вторая состоит из 0 и 1. Требуется выяснить, насколько точно облако точек (x_i, y_i), $i = 1, \ldots, n$, при наилучшем выборе границ a, b аппроксимируется графиком (1), при этом оценив степень аппроксимации некоторым числовым коэффициентом.

Отметим, что в силу характера задачи сами значения первого показателя нам не нужны, а важно лишь расположение точек (x_i, y_i), $i = 1, \ldots, n$, относительно какой-нибудь ступеньки. Значит, без ограничения общности (меняя, если нужно, одновременно порядок следования элементов в обеих выборках) условимся далее считать, что $x_1, \ldots, x_n$ расположены в выборке в порядке неубывания. Более того, можно заменить эти значения их последовательными номерами (рангами), тем самым сведя задачу лишь к рассмотрению нужным образом упорядоченной второй выборки. Теперь можно поставить задачу строго.

1. Постановка задачи

Будем рассматривать цепочки Y длины n (из нулей и единиц) с целью определить степень их соответствия зависимости (1) при наилучшем возможном выборе границ a, b, где в роли X выступает номер соответствующего элемента Y. Для этого в фиксированной цепочке Y будем минимизировать величину ошибок аппроксимации

$$S_{[a,b]}(Y) = \sum_{j=1}^{n} \left(y_j - Y_{a,b}(j)\right)^2 \tag{2}$$

путём подбора границ a, b. Если a и b заданы, то $S_{[a,b]}(Y)$ равно сумме числа нулей внутри отрезка $[a, b]$ и числа единиц вне него. За критерий качества соответствия для цепочки Y примем

$$S(Y) = \min_{a,b} S_{[a,b]}(Y). \tag{3}$$

Тот отрезок $[a, b]$, на котором достигается минимум, назовём оптимальным. Оптимальных отрезков может быть несколько.

Выделим класс $A_{k,m}$ цепочек, в которых $k > 0$ единиц и $m > 0$ нулей $(k + m = n)$. Минимальное и максимальное значения $S(Y)$ среди всех цепочек из $A_{k,m}$ были ранее найдены в [3], но непосредственное вычисление величины наименьшего возможного количества ошибок $S(Y)$ для заданной цепочки Y выделенного класса по всем возможным значениям границ отрезка $[a, b]$ внутри неё вызывает серьёзные затруднения. В связи с этим ставится задача создания относительно простых алгоритмов поиска наименьшего возможного количества ошибок $S(Y)$ для заданной цепочки $Y \in A_{k,m}$, а также перечисления всех оптимальных отрезков в ней.

При более подробном изучении ситуации оказывается, что цепочки из $A_{k,m}$, в которых $S(Y)$ максимально, устроены довольно сложно. Поэтому предлагается алгоритм, позволяющий последовательно конструировать все такие цепочки. Отметим, что в [3] сформулировано лишь достаточное условие того, что конкретная цепочка даёт максимально возможное количество ошибок и, как следствие, указаны только некоторые из таких цепочек.

После решения поставленных задач практическое оценивание силы связи показателей изучаемого типа не будет вызывать затруднений.

2. Наилучший и наихудший случаи

Предположим, что $Y \in A_{k,m}$, т. е. в бинарной цепочке длины n имеется k единиц и m нулей $(k + m = n)$. Пусть $a, b \in \{1, \ldots, n\}$, $b \geqslant a$, — границы отрезка внутри цепочки Y. Оптимальным является тот отрезок $[a, b]$, для которого $S_{[a,b]}(Y) = S(Y)$.

Лемма 1. Оптимальный отрезок начинается и заканчивается единицами.

Доказательство. Если это не так, то, исключая крайний 0 из отрезка, мы уменьшим число ошибок, что противоречит его оптимальности. ■

Далее оценим наибольшее возможное число ошибок в классе цепочек $A_{k,m}$:

$$\overline{S}(A_{k,m}) = \max_{Y \in A_{k,m}} S(Y).$$

Для любой цепочки $Y \in A_{k,m}$ справедливо $0 \leqslant S(Y) \leqslant \overline{S}(A_{k,m})$. Цепочки, для которых $S(Y) = 0$, будем называть наилучшими, а те, для которых $S(Y)$ максимально — наихудшими в классе $A_{k,m}$.

Очевидно, что наилучшими в $A_{k,m}$ являются те и только те цепочки, в которых все k единиц идут подряд. Поэтому число наилучших цепочек равно $m + 1$.

При определении количества наихудших цепочек важно различать случаи достаточно большого и достаточно малого количества единиц. Назовём цепочку насыщенной, если $k \geqslant m + 1$, и ненасыщенной иначе.

Лемма 2. В насыщенном случае $\overline{S}(A_{k,m}) = m$.

Доказательство. Нетрудно заметить, что $S_{[1,n]}(Y) = m$ для любой из рассматриваемых цепочек, откуда всегда $S(Y) \leqslant m$ и, следовательно, $\overline{S}(A_{k,m}) \leqslant m$. Рассмотрим цепочку, начинающуюся с 1, и такую, что следом за каждым нулём идёт единица (такие существуют в силу определения насыщенного случая). Начнём с отрезка $[1, 1]$ и будем расширять его вправо так, чтобы при включении в него очередного нуля вместе с ним добавлялась бы и идущая следом единица. Тогда число ошибок в расширенном отрезке не станет больше, чем до расширения. Поэтому минимальное число ошибок достигается на наиболее широком отрезке:

$$S(Y) = S_{[1,n]}(Y) = m.$$

Итак, верхняя граница числа ошибок достигается. ■

Лемма 3. Для ненасыщенного случая $\overline{S}(A_{k,m}) = k - 1$.

Доказательство. В произвольной цепочке Y выберем j так, чтобы $y_j = 1$. Получаем оценку $S(Y) \leqslant S_{[j,j]}(Y) = k-1$. Рассмотрим далее такую цепочку Y, в которой имеется подцепочка длины $2k - 1$ вида $1010\ldots01$, где между любыми единицами размещается ровно один нуль. В этой подцепочке содержатся все единицы данной цепочки. Возьмём произвольный отрезок данной цепочки, начинающийся и заканчивающийся единицей (по лемме 1 оптимальный отрезок содержится среди таких). Пусть выбранный отрезок содержит s единиц и, следовательно, $(s - 1)$ нуль. Тогда для него $S_{[a,b]}(Y) = (k - s) + (s - 1) = k - 1$, а значит, таково это число и для оптимального отрезка. Оценка сверху для $S(Y)$ достигнута. ■

Таким образом, получено иное доказательство результата из [3]:

Теорема 1.

$$\overline{S}(A_{k,m}) = \begin{cases} k - 1, & k < m + 1, \\ m, & k \geqslant m + 1. \end{cases} \tag{4}$$

3. Строение и количество наихудших цепочек

Для наилучших цепочек вопрос об их количестве и устройстве оказался простым. Для наихудших разберём отдельно ненасыщенный и насыщенный случаи. Пусть сначала $k < m + 1$ (ненасыщенный случай). Обозначим через W_1 множество таких цепочек, в которых никакие две единицы не расположены рядом.

Теорема 2. Множество наихудших ненасыщенных цепочек совпадает с W_1.

Доказательство. Пусть $Y \in W_1$, j — номер позиции любой единицы в ней, находящейся внутри оптимального отрезка. Заметим, что $S_{[j,j]}(Y) = k-1$. При расширении отрезка $[j, j]$ в любую сторону вместе с каждой единицей в него будет добавляться хотя бы один нуль (добавление только одного нуля запретим, ориентируясь на лемму 1). Таким образом, при расширении отрезка число ошибок не уменьшается, а значит, $S(Y) \geqslant k - 1$. Из леммы 3 следует, что строгое неравенство здесь невозможно, и Y является наихудшей.

Обратно, пусть Y — наихудшая цепочка. Если она не принадлежит W_1, то в ней есть две единицы, расположенные на соседних позициях. Пусть номера этих позиций j и $j + 1$. Тогда

$$S(Y) \leqslant S_{[j,j+1]}(Y) = k - 2 < \overline{S}(A_{k,m}),$$

а значит, эта цепочка не наихудшая. ■

Следствие 1. Имеется ровно C^k_{m+1} наихудших ненасыщенных цепочек.

Доказательство. Согласно теореме 2, это количество равно числу способов расставить в ряд k единиц и m нулей так, чтобы никакие две единицы не располагались рядом. Решение такой задачи широко известно и приведено, например, в [5]: расставим m нулей в ряд. Между ними и по краям образуется $m + 1$ место для возможного расположения k единиц. Выбирая положение для каждой из них, что можно сделать C^k_{m+1} способами, переберём все существующие возможности. ■

Перейдём к рассмотрению насыщенного случая: $k \geqslant m + 1$. Обозначим через W_2 множество цепочек такого типа, обладающих следующим свойством: для каждого нуля и слева, и справа от него число единиц строго больше, чем число расположенных с этой же стороны нулей.

Теорема 3. Множество наихудших насыщенных цепочек совпадает с W_2.

Доказательство. Возьмём $Y \in W_2$. Выберем границы a, b произвольно. При расширении выбранного отрезка до $[1, b]$ в него добавится больше единиц, чем нулей, а значит, число ошибок может лишь уменьшиться. Те же соображения работают при расширении отрезка с произвольными границами вправо, поэтому

$$m = S_{[1,n]}(Y) \leqslant S_{[1,b]}(Y) \leqslant S_{[a,b]}(Y).$$

Таким образом, и для оптимального отрезка число ошибок не меньше m. Согласно лемме 2, строгое неравенство невозможно, значит, $S(Y) = m = \overline{S}(A_{k,m})$, т. е. рассматриваемая цепочка является наихудшей.

Обратно, пусть Y наихудшая. Тогда она начинается с единицы, так как иначе

$$S(Y) \leqslant S_{[2,n]}(Y) = m - 1 < \overline{S}(A_{k,m}).$$

Аналогично доказывается, что и заканчиваться такая цепочка должна единицей. Если $Y \notin W_2$, то в ней, например, найдётся некоторый нуль, справа от которого единиц не больше, чем нулей. Обозначим номер позиции этого нуля j, число единиц справа от него t, число нулей с той же стороны q. Ясно, что

$$S(Y) \leqslant S_{[1,j-1]}(Y) = m - (1 + q) + t \leqslant m - 1,$$

так как вне указанного отрезка $1 + q$ нулей, а значит, внутри него $m - (1 + q)$ нулей. Полученное неравенство в силу леммы 2 доказывает, что рассматриваемая цепочка

не может быть наихудшей. Случай нарушения соотношения нулей и единиц слева разбирается аналогично. ■

В насыщенном случае структура множества наихудших цепочек существенно сложнее. Для подсчёта их количества и последовательной генерации всех таких цепочек предлагается следующий способ.

Изобразим на координатной плоскости прямоугольник из k клеток по горизонтали и m клеток по вертикали. Построение каждой наихудшей цепочки насыщенного типа соответствует движению по точкам с целыми координатами в этом прямоугольнике, которое начинается в его левом нижнем углу (0 единиц и 0 нулей) и заканчивается в верхнем правом (k единиц и m нулей).

Каждый шаг ломаной вправо означает появление в цепочке единицы, а шаг вверх — нуля. Условия, которые обеспечивают попадание цепочки в множество W_2, выясним следующим образом. Обозначим через (x, y) текущие координаты точки, движущейся по целочисленным узлам прямоугольника. Рассмотрим момент, когда появился очередной нуль (y увеличился на 1). Здесь имеется $y-1$ нуль и x единиц слева от нового нуля, поэтому из теоремы 3 вытекает ограничение $y - 1 < x$. Условие на соотношение нулей и единиц справа имеет вид $m - y < k - x$. Выписанное строгое неравенство должно выполняться только при появлении на текущем шаге нуля, а значит, на предыдущем шаге вместо него могло быть выполнено равенство. Но поскольку после появления очередного нуля y увеличивается лишь на единицу, то противоположное неравенство ($m - y > k - x$) ни для одной точки ломаной недопустимо.

Окончательно, ограничения на движение точки, траектория которой соответствует цепочке из W_2, записываются в виде системы неравенств

$$\begin{cases} y < x + 1, \\ y \geqslant x + m - k. \end{cases} \tag{5}$$

Следующий алгоритм позволяет вычислить количество наихудших насыщенных цепочек по заданным k и m.

Алгоритм 1. Расчёт числа наихудших цепочек в $A_{k,m}$

1: Проверка условий и подготовка к работе. Если $k \leqslant m$, то отказ. Иначе формируем массив H размера $(m+1) \times (k+1)$, нумерации строк и столбцов которого начинаются с 0. Заполняем его нулями. Для каждого $x \leqslant k - m$ полагаем $H(x, 0) = 1$.
2: **Для** $y = 1, \ldots, m$
3: **Для** $x = y, y + 1, \ldots, y + k - m$
$H(x, y) := H(x - 1, y) + H(x, y - 1)$.
4: **Вернуть** $H(k, m)$.

Графически работа алгоритма 1 при $k = 8, m = 5$ представлена на рис. 1.

Выделенная на рис. 1 линия соответствует одной из наихудших насыщенных цепочек (1011010010111). Светлая полоса на чертеже показывает границы, за которые траектории движения заходить не могут (правда, нижнего края полосы они могут касаться). На рисунке видно, что искомое число наихудших цепочек $H(8, 5) = 144$.

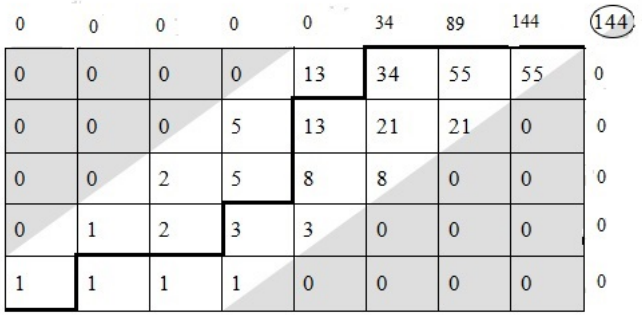

Рис. 1. Графическая иллюстрация алгоритма 1

4. Коэффициент L_E и алгоритм его расчёта

В работе [3] введён коэффициент, который по заданной цепочке нулей и единиц позволяет оценивать силу связи типа «ступенька»:

$$L_E(X,Y) = 1 - \frac{S(Y)}{\overline{S}(A_{k,m})}, \tag{6}$$

где $\overline{S}(A_{k,m})$ определяется формулой (4), а $S(Y)$ — формулой (3) для цепочки Y после её упорядочения по неубыванию соответствующих элементов X. Будем называть его ледж-коэффициентом (от ledge — ступенька).

В силу доказанных лемм $0 \leqslant L_E(X,Y) \leqslant 1$, и его возрастание возможно трактовать как увеличение степени связи соответствующих показателей.

Одним из недостатков, мешающих широкому применению ледж-коэффициента, является трудность вычисления $S(Y)$ для конкретной цепочки Y. Следующая очевидная лемма даёт возможность обосновать приводимый далее алгоритм этого вычисления. Введя обозначения $k(a,b)$, $m(a,b)$ соответственно для количеств единиц и нулей внутри отрезка $[a,b]$, рассмотрим

$$Q[a,b] = k(a,b) - m(a,b).$$

Лемма 4.

1) Если $a < b < c$, то $Q[a,c] = Q[a,b-1] + Q[b,c]$.
2) $S_{[a,b]}(Y) = k - Q[a,b]$. В частности, отрезок $[a_0,b_0]$ оптимален тогда и только тогда, когда $Q[a_0,b_0] = \max Q[a,b]$.

Алгоритм 2. Вычисление ледж-коэффициента

1: Под каждым из элементов цепочки нулей и единиц подпишем число $q(j)$ по следующему правилу. Пусть номер очередного элемента цепочки j. Если этот элемент равен 0 и единиц до него не встречалось, то $q(j) = 0$. Для первой из единиц в цепочке $q(j) = 1$, для всех последующих $q(j) = q(j-1) + 1$. Если элемент равен 0 и перед ним были единицы, то полагаем

$$q(j) = \begin{cases} q(j-1) - 1, & q(j-1) \neq 0, \\ 0, & q(j-1) = 0. \end{cases}$$

2: Находим $q = \max\limits_{j=1,\ldots,n} q(j)$. Тогда $S(Y) = k - q$. Вычислим $\overline{S}(A_{k,m})$ по формуле (4) и $L_E(X,Y)$ согласно (6).

Число $q(j)$ представляет собой величину $Q[i,j]$, где i — ближайшая слева от j граница, такая, что отрезок $[i,j]$ начинается с 1 и не содержит внутри себя ни одного отрезка $[a,b]$ с условием $Q[a,b]=0$. Ясно, что если отрезок $[i,j]$ оптимален, то $q(i)=1$, $q(j)=q$, а если $q(j)=0$, то обязательно $y_j=0$.

Например, для цепочки на рис. 1 значения чисел $q(j)$ получаются равными $1;0;1;2;1;2;1;0;1;0;1;2;3$. Максимальное $q=3$, откуда $S(Y)=8-3=5$. При этом цепочка является насыщенной, следовательно, $\overline{S}(A_{k,m})$ равно числу нулей в соответствии с (4) и $L_E(X,Y)=0$, что подтверждает тот факт, что цепочка наихудшая. Коэффициент корреляции ρ между значениями Y и их рангами для такой цепочки равен 0,127. Это, как и при использовании нашего метода, может быть интерпретировано как отсутствие связи. Те же численные значения и выводы получаются и при расчёте коэффициента бисериальной корреляции. Если, учитывая непараметрический характер изучаемой связи, привлечь к исследованию τ-коэффициент Кендалла, то его значение (0,56) показывает здесь, напротив, наличие статистически значимой ранговой связи. В то же время для наилучшей цепочки 0011111000 ($L_E=1$) значение ρ равно $-0{,}17$, а $\tau=0{,}45$. Следовательно, оба эти коэффициента указывают на отсутствие значимой связи между показателями. Это даёт повод констатировать некорректность выводов классических методик в рассматриваемой ситуации.

5. Поиск оптимальных отрезков

Оптимальных отрезков внутри изучаемой цепочки может быть несколько. Непересекающиеся оптимальные отрезки следует, вероятно, рассматривать, как до определённой степени парадоксальную ситуацию с точки зрения медицинских приложений, хотя чисто математически исключить такую возможность нельзя. Тем не менее случай, когда имеются два вложенных друг в друга оптимальных отрезка, является довольно обычным.

При этом возникает вопрос, какой из двух отрезков выбрать — больший или меньший? Конечно, всё зависит от решаемой задачи. В медицинских задачах, где значения $Y=1$ интерпретируются как признак здоровья человека, интересен наиболее короткий отрезок, если нужно выбрать тех пациентов, которые наверняка здоровы. Если же значение 1 означает наличие некоторого опасного заболевания, то следует предпочесть более длинный отрезок, чтобы оставить за его пределами как можно меньше больных. Понятно, что приведённые рассуждения близки к дискуссии о том, какую из двух возможных ошибок, первого или второго рода, следует считать более серьёзной при проверке статистических гипотез. Отметив это, решим далее обе поставленные задачи — приведём алгоритмы поиска самого короткого и самого длинного из оптимальных отрезков. Сначала докажем несколько утверждений о строении набора всех оптимальных отрезков в данной бинарной цепочке.

Лемма 5. Если пересечение двух оптимальных отрезков не пусто, то оно само является оптимальным отрезком.

Доказательство. Пусть $a<c<b<d$ и отрезки $[a,b]$ и $[c,d]$ оба оптимальны. Если $Q[a,c-1]<0$, то из утверждения 1 леммы 4 получим $Q[c,b]>Q[a,b]$. Это противоречит оптимальности $[a,b]$. Более того, случай $Q[a,c-1]>0$ также невозможен, иначе $Q[a,d]=Q[a,c-1]+Q[c,d]>Q[c,d]$, а значит, не оптимален отрезок $[c,d]$. При помощи этих рассуждений убеждаемся, что $Q[a,c-1]=0$, откуда по лемме 4 получаем $Q[c,b]=Q[a,b]-Q[a,c-1]=Q[a,b]$, что означает оптимальность пересечения $[c,b]$. ■

Из леммы 5 следует, что можно построить систему попарно непересекающихся минимальных по длине оптимальных отрезков Ψ, такую, что каждый оптимальный отрезок изучаемой цепочки содержит внутри себя хотя бы один из отрезков системы Ψ. Поскольку ни один из отрезков системы Ψ не содержит внутри себя других оптимальных отрезков, будем называть их атомарными. Отрезок $[a, b]$ назовём нейтральным, если $Q[a, b] = 0$.

Утверждение 1. Произвольный неатомарный оптимальный отрезок получается из некоторого атомарного добавлением к нему одного или двух (с разных сторон) нейтральных отрезков.

Доказательство. Пусть $[c, d]$ — оптимальный неатомарный отрезок. Внутри него расположен $[a, b] \in \Psi$. Пусть, например, $c < a$ (добавлен левый отрезок). Тогда нейтральность добавленного отрезка немедленно вытекает из соотношения

$$Q[a, b] = Q[c, b] = Q[c, a - 1] + Q[a, b],$$

справедливого в силу лемм 4 и 5. Поскольку рассуждения для добавляемого правого отрезка полностью аналогичны, утверждение доказано. ■

Следовательно, укоротить оптимальный отрезок можно, лишь отыскав нейтральный, расположенный внутри него и примыкающий к одному из его краев, что соответствует появлению 0 в наборе соответствующих чисел $q(j)$.

Алгоритм 3. Поиск самого короткого оптимального отрезка

1: Выполняем первый шаг алгоритма 2.
2: Пусть $q = \max\limits_{j=1,\ldots,n} q(j)$. Проходим набор чисел $q(j)$ слева направо, находя все отрезки, начинающиеся с 1 и заканчивающиеся q, такие, что внутри них нет нулей.
3: Если на шаге 2 найдено несколько отрезков, то находим из них тот, что имеет наименьшую длину.

Проиллюстрируем работу алгоритма 3 следующей таблицей ($k = 12, m = 10$). По третьей строке таблицы видим, что $q = 4$. По второму утверждению леммы 4 число ошибок для оптимального отрезка $S(Y) = k - q = 8$. Интервалы, обнаруживаемые на втором шаге алгоритма, — $[5, 10]$, $[5, 14]$ и $[19, 22]$. Наименьшую длину имеет последний из них. Атомарными являются отрезки $[5, 10]$ и $[19, 22]$.

X	01	02	03	04	05	06	07	08	09	10	11
Y	0	0	1	0	1	1	1	0	1	1	0
$q(j)$	0	0	1	0	1	2	3	2	3	4	3
X	12	13	14	15	16	17	18	19	20	21	22
Y	0	1	1	0	0	0	0	1	1	1	1
$q(j)$	2	3	4	3	2	1	0	1	2	3	4

Утверждение 2. Если для некоторых $j_0 < j_1$ верно $q(j) = 0$, $j_0 \leqslant j \leqslant j_1$, то отрезок $[j_0, j_1]$ не содержится ни в каком оптимальном.

Доказательство. Предположим противное. Пусть нашлись такие индексы i, j, что $[j_0, j_1] \subset [i, j]$, и отрезок $[i, j]$ оптимален. Заметим, что $y_{j_0} = y_{j_1} = 0$. Поэтому включение отрезков является строгим, так как по лемме 1 $y_i = y_j = 1$. Без ограничения общности можно считать, что $[j_0, j_1]$ — максимальный по включению отрезок, внутри

которого все числа $q(j)$ равны 0, что по определению этих чисел означает $q(j_0 - 1) = q(j_1 + 1) = 1$. Ясно, что тогда отрезок $[i, j_0]$ нейтрален, $Q[j_0 + 1, j_1] < 0$. В силу оптимальности $[i, j]$ выполнено $q(j) = q$, а значит, $Q[i, j] = Q[i, j_0] + Q[j_0 + 1, j_1] + Q[j_1 + 1, j] < q$, что противоречит оптимальности $[i, j]$. ■

Утверждение 2 означает, что в наборе чисел $q(j)$, когда j пробегает оптимальный отрезок, два нуля не могут следовать подряд, что обосновывает алгоритм 4.

Алгоритм 4. Поиск самого длинного оптимального отрезка

1: Выполняем первый шаг алгоритма 2.
2: Пусть $q = \max\limits_{j=1,\ldots,n} q(j)$. Проходим набор чисел $q(j)$ слева направо, находя все отрезки, начинающиеся с 1 и заканчивающиеся q, такие, что внутри них содержится не более одного нуля подряд.
3: Среди всех обнаруженных на шаге 2 отрезков выбираем тот, который имеет наибольшую длину.

В примере (см. таблицу) на втором шаге будут обнаружены отрезки $[3, 10]$, $[3, 14]$, $[3, 22]$, $[5, 10]$, $[5, 14]$, $[5, 22]$, $[17, 22]$ и $[19, 22]$. Ответ — $[3, 22]$.

Заключение

Рассмотрен новый вид связи («ступенька») между номинальным и бинарным показателями. Он является естественным и часто встречается в приложениях, особенно медицинских, но описание и анализ связей такого вида на основе классических методов не являются вполне удовлетворительными и корректными по причине отсутствия информации о распределении выборок.

С помощью предлагаемых алгоритмов может быть оценена сила связи типа «ступенька» и найдены границы, в которых должен изменяться числовой показатель, чтобы оказаться наиболее сильно связанным с бинарным. Эти алгоритмы делают расчёт ледж-коэффициента L_E, а также поиск нормативных интервалов изучаемых показателей в предположении, что они неизвестны, доступными даже при работе без привлечения компьютера. Ранее (в работе [3]) предлагалось производить эти вычисления методом полного перебора, что предполагало написание специальной компьютерной программы (особенно при объёмах выборок больше 20).

Можно рекомендовать изучаемый в работе ледж-коэффициент для использования оценки силы связи показателей описанных типов как альтернативу традиционно используемым разного рода коэффициентам корреляции. Он также может быть полезен, когда вместо номинального показателя используется порядковая переменная.

Результаты работы можно также использовать для оценки качества разбиения объектов на два кластера [6].

ЛИТЕРАТУРА

1. *Straus Sh. E., Richardson W. S., Glasziou P., and Haynes R. B.* Evidence Based Medicine. Elsevier Churchhill Livingstone, 2011. 295 p.
2. *Дударева Ю. А., Гуръева В. А., Дронов С. В., Шойхет Я. Н.* Сравнительная оценка состояния здоровья потомков лиц, проживавших на территории с неблагоприятной экологической обстановкой // Клиническая медицина. 2014. Т. 92. № 5. С. 66–70.
3. *Дронов С. В., Петухова Р. В.* Один вид связи между номинальной и бинарной переменными // Известия АлтГУ. 2010. Т. 65. № 1/2. С. 34–36.

4. *Мирмоминов Р. М.* Один вид связи между номинальной и бинарной переменными // Сб. научных статей Междунар. конф. «Ломоносовские чтения на Алтае: фундаментальные проблемы науки и образования». Барнаул, 11–14 ноября 2014. Барнаул: Изд-во АлтГУ, 2014. С. 171–173.
5. *Виленкин Н. Я., Виленкин А. Н., Виленкин П. А.* Комбинаторика. М.: ФИМА, МЦНМО, 2006. 400 с.
6. *Dronov S. V. and Dementjeva E. A.* A new approach to post-hoc problem in cluster analysis // Model Assisted Statistics and Applications. 2012. V. 7. No. 1. P. 49–55.

REFERENCES

1. *Straus Sh. E., Richardson W. S., Glasziou P., and Haynes R. B.* Evidence Based Medicine. Elsevier Churchhill Livingstone, 2011. 295 p.
2. *Dudareva Yu. A., Gur'eva V. A., Dronov S. V., Shoykhet Ya. N.* Sravnitel'naya otsenka sostoyaniya zdorov'ya potomkov lits, prozhivavshikh na territorii s neblagopriyatnoy ekologicheskoy obstanovkoy [Comparative evaluation of the health status of descendants of people residing in environmentally unfriendly regions by means of mathematical modeling]. Klinicheskaya meditsina, 2014, vol. 92, no 5, pp. 66–70. (in Russian)
3. *Dronov S. V., Petukhova R. V.* Odin vid svyazi mezhdu nominal'noy i binarnoy peremennymi [One type of connection between nominal and binary variables]. Izvestiya AltSU, 2010, vol. 65, no. 1/2, pp. 34–36. (in Russian)
4. *Mirmominov R. M.* Odin vid svyazi mezhdu nominal'noy i binarnoy peremennymi [One type of connection between nominal and binary variables]. Proc. conf. «Lomonosovskie chteniya na Altae: fundamental'nye problemy nauki i obrazovaniya». Barnaul, 11–14 November 2014. Barnaul, AltSU Publ., 2014, pp. 171–173. (in Russian)
5. *Vilenkin N. Ya., Vilenkin A. N., Vilenkin P. A.* Kombinatorika [Combinatorics]. Moscow, MCCME Publ., 2006. 400 p. (in Russian)
6. *Dronov S. V. and Dementjeva E. A.* A new approach to post-hoc problem in cluster analysis // Model Assisted Statistics and Applications, 2012, vol. 7, no. 1, pp. 49–55.

СВЕДЕНИЯ ОБ АВТОРАХ

АДЕЛЬШИН Александр Владимирович — кандидат физико-математических наук, доцент, старший научный сотрудник Омского филиала Института математики им. С. Л. Соболева СО РАН, г. Омск. E-mail: **adelshin@ofim.oscsbras.ru**

БОЙКО Илья Юрьевич — студент 4 курса факультета математики и информационных технологий Алтайского государственного университета, г. Барнаул. E-mail: **boyan.94@mail.ru**

БРОСЛАВСКИЙ Олег Викторович — студент кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск. E-mail: **o.v.broslavsky@gmail.com**

БУГРОВ Алексей Дмитриевич — специалист ООО «Центр сертификационных исследований», г. Москва. E-mail: **Bugrovalexey1@yandex.ru**

ДРОНОВ Сергей Вадимович — кандидат физико-математических наук, доцент, доцент кафедры математического анализа Алтайского государственного университета, г. Барнаул. E-mail: **dsv@math.asu.ru**

ЗУБОВ Анатолий Юрьевич — кандидат физико-математических наук, доцент, старший научный сотрудник Московского государственного университета им. М. В. Ломоносова, г. Москва. E-mail: **zubovanatoly@yandex.ru**

КОЛЕГОВ Денис Николаевич — кандидат технических наук, доцент кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, старший специалист отдела защиты приложений ЗАО «Позитив Текнолоджис», г. Томск. E-mail: **d.n.kolegov@gmail.com**

КОЛОКОЛОВ Александр Александрович — доктор физико-математических наук, профессор, заведующий лабораторией Омского филиала Института математики им. С. Л. Соболева СО РАН, г. Омск. E-mail: **kolo@ofim.oscsbras.ru**

КОМАРОВ Дмитрий Дмитриевич — аспирант, ассистент кафедры теоретических основ компьютерной безопасности и криптографии Саратовского государственного университета им. Н. Г. Чернышевского, г. Саратов. E-mail: **komarovdd@gmail.com**

КОЧЕРГИН Вадим Васильевич — доктор физико-математических наук, профессор кафедры дискретной математики механико-математического факультета МГУ им. М. В. Ломоносова, ведущий научный сотрудник Института теоретических проблем микромира им. Н. Н. Боголюбова МГУ, г. Москва. E-mail: **vvkoch@yandex.ru**

МЕДВЕДЕВА Наталья Валерьевна — кандидат физико-математических наук, доцент, доцент Уральского государственного университета путей сообщения, г. Екатеринбург. E-mail: **medvedeva_n_v@mail.ru**

МИХАЙЛОВИЧ Анна Витальевна — кандидат физико-математических наук, доцент общеуниверситетской кафедры высшей математики Национального исследовательского университета «Высшая школа экономики», г. Москва. E-mail: **anna@mikhaylovich.com**

НЕСТЕРЕНКО Алексей Юрьевич — кандидат физико-математических наук, доцент кафедры компьютерной безопасности Московского института электроники и математики Национального исследовательского университета «Высшая школа экономики», г. Москва. E-mail: **nesterenko_a_y@mail.ru**

ОЛЕКСОВ Никита Евгеньевич — студент кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск. E-mail: **n.e.oleksov@gmail.com**

ПУГАЧЕВ Андрей Васильевич — преподаватель кафедры информационной безопасности Московского государственного университета информационных технологий, радиотехники и электроники, г. Москва. E-mail: **a_pugachev@mirea.ru**

ТИТОВ Сергей Сергеевич — доктор физико-математических наук, профессор, профессор Уральского государственного университета путей сообщения, г. Екатеринбург. E-mail: **stitov@usaaa.ru**

ТРИШИН Андрей Евгеньевич — кандидат физико-математических наук, ведущий специалист ООО «Центр сертификационных исследований», г. Москва.
E-mail: **Trishin17@yandex.ru**

ШИРЯЕВ Петр Михайлович — аспирант Московского государственного университета им. М. В. Ломоносова, г. Москва. E-mail: **shiryaev.petr@gmail.com**

Журнал «Прикладная дискретная математика» включен в перечень ВАК рецензируемых российских журналов, в которых должны быть опубликованы основные результаты диссертаций, представляемых на соискание учёной степени кандидата и доктора наук, в базу данных Web of Science (Russian Science Citation Index — RSCI), а также в перечень журналов, рекомендованных УМО в области информационной безопасности РФ в качестве учебной литературы по специальности «Компьютерная безопасность».

Журнал «Прикладная дискретная математика» распространяется по подписке; его подписной индекс 38696 в объединённом каталоге «Пресса России». Полнотекстовые электронные версии вышедших номеров журнала доступны на его сайте journals.tsu.ru/pdm и на Общероссийском математическом портале www.mathnet.ru. На сайте журнала можно найти также и правила подготовки рукописей статей в журнал.

Тематика публикаций журнала:

- *Теоретические основы прикладной дискретной математики*
- *Математические методы криптографии*
- *Математические методы стеганографии*
- *Математические основы компьютерной безопасности*
- *Математические основы надёжности вычислительных и управляющих систем*
- *Прикладная теория кодирования*
- *Прикладная теория автоматов*
- *Прикладная теория графов*
- *Логическое проектирование дискретных автоматов*
- *Математические основы информатики и программирования*
- *Вычислительные методы в дискретной математике*
- *Дискретные модели реальных процессов*
- *Математические основы интеллектуальных систем*
- *Исторические очерки по дискретной математике и её приложениям*