Math-Net.Ru

Общероссийский математический портал

В. Н. Сачков, Комбинаторные свойства дифференциально 2-равномерных подстановок, *Матем. вопр. криптогр.*, 2015, том 6, выпуск 1, 159–179

DOI: <https://doi.org/10.4213/mvk156>

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

Параметры загрузки:

IP: 54.164.48.24

26 апреля 2023 г., 12:02:01

УДК: 519.719.2+519.12

Комбинаторные свойства дифференциально 2-равномерных подстановок

В. Н. Сачков

Академия криптографии Российской Федерации, Москва

Получено 23.IX.2014

Развивается комбинаторный подход к исследованию и методам построения дифференциально 2-равномерных подстановок векторного пространства над конечным полем F_2 . Приведены необходимые и достаточные условия, при которых ассоциированное с дифференциально 2-равномерной подстановкой семейство множеств является симметричной блок-схемой. Показано, что подстановка является дифференциально 2-равномерной тогда и только тогда, когда она является решением системы уравнений подобия, связывающих семейство трансляций с семейством разнovesных инволюций. Предложены способы построения дифференциально 2-равномерных подстановок с помощью таблицы Кэли аддитивной группы конечного поля F_{2^m} .

Ключевые слова: дифференциально 2-равномерные подстановки, семейство множеств, ассоциированное с подстановкой, (α, β) -конфигурации подстановки, разнovesные инволюции

Combinatorial properties of differentially 2-uniform substitutions

V. N. Sachkov

Academy of Cryptography of the Russian Federation, Moscow

Abstract. A combinatorial approach to the investigation and methods of construction of differentially 2-uniform substitutions of the vector space over the finite field F_2 is proposed. Necessary and sufficient conditions for the family of sets associated with a differentially 2-uniform substitution to be a symmetric block design are given. It is shown that a substitution is differentially 2-uniform if and only if it is a solution of a similarity equations system connecting a family of translations with a family of unequal weights involutions. We suggest methods of construction of differentially 2-uniform substitutions by means of the Cayley table of an additive group of finite field F_{2^m} .

Key words: differentially 2-uniform substitutions, family of sets associated with a substitution, (α, β) -configurations, unequal weights involutions

Citation: *Mathematical Aspects of Cryptography*, 2015, vol. 6, no. 1, pp. 159–179 (Russian).

Введение

В современных блочных шифрах, построенных, как правило, по итерационному принципу с R раундами, в r -м раунде, $1 \leq r \leq R$, процесс зашифрования и расшифрования информации связан с биективным преобразованием элементов группы $(E_{2^m}, +)$, являющейся аддитивной группой конечного поля F_{2^m} и состоящей из двоичных m -векторов, у которых сложение координат осуществляется в поле F_2 . Такое преобразование производится так называемым S-боксом и задается подстановкой S , действующей на множестве E_{2^m} . Специальный выбор этой подстановки проводится с целью обеспечения принципа «перемешивания» К.Шеннона и, в частности, уменьшения эффективности применения известного дифференциального (разностного) метода криптоанализа. В основе метода дифференциального криптоанализа блочных шифров лежит наличие в открытой информации пар элементов $x, x' \in E_{2^m}$, принадлежащих различным открытым сообщениям, причем эти элементы при одном и том же ключе подстановкой S преобразуются в пару $y, y' \in E_{2^m}$ элементов, принадлежащих зашифрованным сообщениям. Полагая $x' = x + \alpha$, $y' = y + \beta$, можно рассматривать «преобразование» подстановкой S разности α в разность β . Если $\alpha, \beta \in E_{2^m}$ и $\alpha \neq \theta$, где θ — нулевой элемент E_{2^m} , то имеем уравнение

$$S(x + \alpha) + S(x) = \beta, \quad x \in E_{2^m}. \quad (1)$$

Элементы группы E_{2^m} далее будем называть *точками*. В работах [2, 3] введено следующее понятие.

Определение 1. Подстановка S , действующая на группе E_{2^m} , определяет (α, β) -конфигурацию $[x, \alpha, \beta]$ в точке $x \in E_{2^m}$, если x является решением уравнения (1).

Заметим, что в определении 1 условие биективности преобразования S не используется. Поэтому аналогично можно определить понятие (α, β) -конфигураций для произвольного преобразования множества элементов группы E_{2^m} . Однако, поскольку основные результаты настоящей работы относятся именно к случаю, когда S — подстановка, далее понятие (α, β) -конфигураций для произвольных преобразований множества E_{2^m} не используется.

Ввиду многократного применения одного и того же биективного преобразования при заданном действующем ключе, число появлений пар блоков в открытых и зашифрованных сообщениях с указанными свойствами зависит от количества (α, β) -конфигураций в подстановке S . Отсюда следует зависимость объема зашифрованной информации, необходимого для

успешного применения дифференциального метода криптоанализа, от числа (α, β) -конфигураций.

Выбору преобразований для блочных шифров, в том числе с условием биективности, посвящен ряд работ. В статье [1] для произвольного преобразования $f : E_{2^m} \rightarrow E_{2^m}$ определено понятие дифференциальной δ -равномерности, состоящее в том, что для каждого ненулевого $\alpha \in E_{2^m}$ и каждого $\beta \in E_{2^m}$ уравнение $f(x + \alpha) + f(x) = \beta$ имеет не более δ решений. Если уравнение (1) совместно, то оно имеет не менее двух решений. Отсюда ясно, что эффективность дифференциального метода криптоанализа наименьшая, если $\delta = 2$.

В общем случае выбор преобразования для блочного шифра, в особенности с требованием биективности, отвечающего малым значениям δ , представляет собой трудную задачу. По этой причине широко используется частный подход к выбору преобразования, базирующийся на известных свойствах подстановки $x \rightarrow x^{-1}$ обращения ненулевых элементов конечного поля F_{2^m} . Этот подход позволяет для полученного преобразования одновременно исследовать и другие важные криптографические свойства: расстояние до множества аффинных функций, степень нелинейности соответствующих многочленов, алгебраическая иммунность и др. [5]. Вместе с тем этот подход не позволяет описать комбинаторную структуру (α, β) -конфигураций, определяющую криптографические свойства подстановок, включая дифференциальную 2-равномерность.

В данной статье используется другой подход, связанный с введенными в работе отношением эквивалентности на множестве (α, β) -конфигураций в подстановке и понятием семейства множеств, ассоциированного с подстановкой. С использованием этих понятий в работе получен критерий дифференциальной 2-равномерности подстановок, а также необходимые и достаточные условия того, чтобы ассоциированное семейство с дифференциально 2-равномерной подстановкой множеств являлось известной в комбинаторном анализе симметричной блок-схемой или (v, k, λ) -конфигурацией, с параметрами $v = 2^m - 1$, $k = 2^{m-1}$, $\lambda = 2^{m-2}$. Известно, что (v, k, λ) -конфигурации с такими параметрами можно построить для любого m на основе матриц Сильвестра–Адамара.

В статье также определено понятие разнovesных инволюций над аддитивной группой E_{2^m} конечного поля F_{2^m} и предложен способ их построения с использованием таблицы Кэли группы E_{2^m} . Исходя из определения биекции множества трансляций в множество разнovesных попарно противоречивых инволюций установлена комбинаторная структура дифференциально 2-равномерной подстановки. На этой основе показано, что подстанов-

ка S является дифференциально 2-равномерной тогда и только тогда, когда S является решением системы уравнений подобия, связывающих семейство трансляций с семейством разностных попарно противоречивых инволюций.

С использованием этих критериев предложены способы построения дифференциально 2-равномерных подстановок.

1. Семейства множеств, ассоциированные с подстановками, и классы эквивалентности конфигураций подстановок

Для подстановки S , действующей на множестве E_{2^m} , определим разложимую матрицу, называемую иногда XOR -матрицей:

$$XOR = \begin{pmatrix} 2^m & \vec{0} \\ 0^\downarrow & C_S \end{pmatrix}_{2^m \times 2^m}, \quad (2)$$

где элементы матрицы

$$C_S = (c_{\alpha, \beta})_{(2^m-1) \times (2^m-1)}, \alpha, \beta \in E_{2^m} \setminus \{\theta\} \quad (3)$$

определяются равенствами

$$c_{\alpha, \beta} = |\{x \in E_{2^m} | S(x + \alpha) + S(x) = \beta\}|. \quad (4)$$

В соответствии с приведенным выше определением δ -равномерности подстановок можно дать следующее определение.

Определение 2. Подстановка

$$S : E_{2^m} \rightarrow E_{2^m}$$

называется *дифференциально 2-равномерной*, если матрица C_S , определяемая соотношениями (2), (3) и (4), имеет элементы, равные либо 0, либо 2. Если соответствующая некоторому $\alpha \in E_{2^m} \setminus \{\theta\}$ строка матрицы C_S имеет элементы, равные 0 либо 2, то мы будем называть подстановку S *дифференциально 2-равномерной относительно элемента α* .

В случаях $m = 1$ и $m = 2$ дифференциально 2-равномерных подстановок не существует. Поэтому далее мы предполагаем, что $m \geq 3$.

На множестве всех (α, β) -конфигураций в подстановке S введем отношение эквивалентности.

Определение 3. Две конфигурации $[x, \alpha, \beta]$ и $[x', \alpha', \beta']$ в подстановке S будем называть *эквивалентными*, если $\beta = \beta'$.

Нетрудно видеть, что введенное бинарное отношение на множестве всех конфигураций в подстановке S действительно является отношением эквивалентности. Отсюда следует, что на любом непустом множестве конфигураций в подстановке S также определено соответствующее отношение эквивалентности, и это множество разбивается на непустые попарно не пересекающиеся классы взаимно эквивалентных конфигураций.

В дальнейшем (α, β) -конфигурации при заданном $\alpha \neq \theta$ и различных β будем называть α -*строчными* или просто *строчными*. Для любого $\alpha \neq \theta$ на множестве всех α -строчных конфигураций в подстановке S выше определено отношение эквивалентности, которое мы обозначим через ϱ_α . А именно, при заданном $\alpha \in E_{2^m} \setminus \{\theta\}$ и любых $x, x' \in E_{2^m}$ конфигурации $[x, \alpha, \beta]$ и $[x', \alpha, \beta']$ являются ϱ_α -эквивалентными, если $\beta = \beta'$, т. е. если выполнено равенство

$$S(x + \alpha) + S(x) = S(x' + \alpha) + S(x') = \beta. \quad (5)$$

Значение β из соотношения (5) определяет класс отношения эквивалентности ϱ_α , содержащий (α, β) -конфигурацию в точке x .

Отношения ϱ_α , $\alpha \neq \theta$ будем называть *отношениями строчной эквивалентности*.

При любых заданных $\alpha, \beta \neq \theta$ уравнение (1) имеет решение $x \in E_{2^m}$ тогда и только тогда, когда оно имеет решение $x + \alpha$. Отсюда вытекает следующая лемма.

Лемма 1. Для любого $\alpha \in E_{2^m} \setminus \{\theta\}$ минимально возможное число элементов в любом классе строчной эквивалентности ϱ_α равно двум. Все классы строчной эквивалентности ϱ_α содержат минимальное число элементов тогда и только тогда, когда их общее число максимально и равно 2^{m-1} . Это условие эквивалентно свойству дифференциальной 2-равномерности подстановки S относительно элемента α .

Используя свойства уравнений вида (1), дадим комбинаторное описание числа классов строчных эквивалентностей ϱ_α для всех $\alpha \in E_{2^m} \setminus \{\theta\}$. Для этого представим группу E_{2^m} в следующем виде:

$$E_{2^m} = \{u_0, u_1, \dots, u_{2^m-1}\}, \quad (6)$$

где элементы группы записаны в порядке возрастания двоичных представлений u_i как чисел от 0 до $2^m - 1$, т. е.

$$u_0 = \theta = (0, 0, \dots, 0), u_1 = (0, 0, \dots, 1), \dots, u_{2^m-1} = (1, 1, \dots, 1).$$

Для любой заданной подстановки S , действующей на группе E_{2^m} , используя равенство (1), можно записать $2^m - 1$ систем равенств вида

$$\begin{aligned} S(u_0 + u_i) + S(u_0) &= \beta_0^{(i)}, \\ S(u_1 + u_i) + S(u_1) &= \beta_1^{(i)}, \\ &\dots\dots\dots \\ S(u_{2^m-1} + u_i) + S(u_{2^m-1}) &= \beta_{2^m-1}^{(i)}, \\ i &= 1, 2, \dots, 2^m - 1. \end{aligned} \quad (7)$$

Ясно, что ϱ_{u_i} -эквивалентным конфигурациям соответствуют равенства i -й системы (7) с совпадающими значениями правых частей. Рассмотрим мультимножество, состоящее из значений правых частей равенств i -й системы (7):

$$B_i = \left\{ \left\{ \beta_0^{(i)}, \beta_1^{(i)}, \dots, \beta_{2^m-1}^{(i)} \right\} \right\}, \quad i = 1, 2, \dots, 2^m - 1.$$

Если подстановке S соответствуют r_i классов строчной эквивалентности ϱ_{u_i} , то множество попарно различных элементов мультимножества B_i содержит r_i элементов и имеет вид

$$W_i = \left\{ w_1^{(i)}, w_2^{(i)}, \dots, w_{r_i}^{(i)} \right\}, \quad i = 1, 2, \dots, 2^m - 1, \quad (8)$$

где $w_1^{(i)}, w_2^{(i)}, \dots, w_{r_i}^{(i)}$ — попарно различные ненулевые элементы группы E_{2^m} . Отсюда следует, что при любом $i = 1, 2, \dots, 2^m - 1$ первичная спецификация мультимножества B_i имеет вид

$$[B_i] = \left[\left(w_1^{(i)} \right)^{\delta_1}, \left(w_2^{(i)} \right)^{\delta_2}, \dots, \left(w_{r_i}^{(i)} \right)^{\delta_{r_i}} \right], \quad (9)$$

где числа $\delta_1, \dots, \delta_{r_i}$ равны количествам элементов в классах эквивалентности ϱ_{u_i} и удовлетворяют условию $\delta_j \geq 2, j = 1, \dots, r_i$.

Таким образом, имеем следующую лемму.

Лемма 2. Для любого $i = 1, 2, \dots, 2^m - 1$ число классов строчной эквивалентности ϱ_{u_i} совпадает с мощностью множества W_i . Все классы всех эквивалентностей ϱ_{u_i} минимальны (т. е. содержат по 2 элемента) тогда и только тогда, когда для любого $i = 1, 2, \dots, 2^m - 1$ число элементов множества W_i максимально и равно 2^{m-1} .

Определение 4. Семейство множеств

$$W_1, W_2, \dots, W_{2^m-1}, \quad (10)$$

являющихся подмножествами группы E_{2^m} и определенных равенствами (8), будем называть *семейством множеств, ассоциированным с подстановкой S* .

Из приведенных лемм вытекает следующий критерий дифференциальной 2-равномерности подстановки S в терминах семейства (10) и строчных эквивалентностей.

Теорема 1. Для любой подстановки S , действующей на группе E_{2^m} , следующие условия эквивалентны:

- а) подстановка S является дифференциально 2-равномерной;
- б) для любого $\alpha \in E_{2^m} \setminus \{\theta\}$ все классы строчной эквивалентности ϱ_α минимальны и содержат по 2 элемента;
- с) любое множество семейства (10) содержит максимальное число элементов, равное 2^{m-1} .

Если условия данной теоремы выполнены, то множества (10) семейства, ассоциированного с подстановкой S , будут обозначаться символами

$$V_1, V_2, \dots, V_{2^m-1}. \quad (11)$$

Все множества семейства (11) содержат по 2^{m-1} элементов. Кроме того, равенства (7) разбиваются на пары, в которых правые части совпадают, а левые части отличаются только перестановкой слагаемых. Из каждой пары оставим одно равенство. В результате при любом $i = 1, 2, \dots, 2^m - 1$ получим приведенную систему равенств вида

$$\begin{aligned} S(u_{\nu_0^{(i)}}) + S(u_{\nu_1^{(i)}}) &= w_1^{(i)}, \\ S(u_{\nu_2^{(i)}}) + S(u_{\nu_3^{(i)}}) &= w_2^{(i)}, \\ &\dots\dots\dots \\ S(u_{\nu_{2^m-2}^{(i)}}) + S(u_{\nu_{2^m-1}^{(i)}}) &= w_{2^m-1}^{(i)}. \end{aligned} \quad (12)$$

Для любого $i = 1, 2, \dots, 2^m - 1$ в приведенной системе (12) в левых частях равенств аргументы $u_{\nu_0^{(i)}}, u_{\nu_1^{(i)}}, \dots, u_{\nu_{2^m-1}^{(i)}}$ подстановки S попарно различны и, следовательно, образуют множество E_{2^m} , а множество индексов

$\{\nu_0^{(i)}, \nu_1^{(i)}, \dots, \nu_{2^m-1}^{(i)}\} = \{0, 1, \dots, 2^m - 1\}$. Отсюда следует, что в результате сложения равенств (12) для любого $i = 1, 2, \dots, 2^m - 1$ можно получить равенство

$$\omega_1^{(i)} + \omega_2^{(i)} + \dots + \omega_{2^m-1}^{(i)} = \theta. \quad (13)$$

Равенство вида (13) будем называть *условием обнуления*.

Далее из построения систем (12) следует, что для любого $i = 1, 2, \dots, 2^m - 1$ имеем выражение для множества V_i семейства (11):

$$V_i = \{\omega_1^{(i)}, \omega_2^{(i)}, \dots, \omega_{2^m-1}^{(i)}\}, \quad (14)$$

а также выражение для первичной спецификации (9):

$$[B_i] = \left[\left(\omega_1^{(i)} \right)^2, \left(\omega_2^{(i)} \right)^2, \dots, \left(\omega_{2^m-1}^{(i)} \right)^2 \right], \quad 1 \leq i \leq 2^m - 1.$$

Эти замечания обосновывают следующую лемму.

Лемма 3. Если подстановка S дифференциально 2-равномерна и определяет при каждом $i = 1, 2, \dots, 2^m - 1$ приведенную систему равенств (12), то любое множество V_i семейства, ассоциированного с подстановкой S , имеет вид (14) и необходимо удовлетворяет условию обнуления (13).

Обозначим через B мультимножество с минимальным порождающим множеством $E_{2^m} \setminus \{\theta\}$, равное объединению мультимножеств $B_i, i = 1, \dots, 2^m - 1$. Из способа построения систем (7) для первичной спецификации мультимножества B следует равенство

$$[B] = \left[(u_1)^{2^m}, (u_2)^{2^m}, \dots, (u_{2^m-1})^{2^m} \right].$$

При любом $j = 1, \dots, 2^m - 1$ для числа n_j множеств (14) семейства (11), которым принадлежит элемент u_j , имеем равенство $2n_j = 2^m$, то есть $n_j = 2^{m-1}$. Таким образом, доказана следующая лемма.

Лемма 4. Матрица инцидентности A_S семейства (11), соответствующего дифференциально 2-равномерной подстановке S , является квадратной $(0, 1)$ -матрицей порядка $2^m - 1$, у которой в каждой строке и в каждом столбце имеется ровно 2^{m-1} единиц.

Заметим, что в иных терминах содержание данной леммы установлено в работе [6].

Из теоремы Биркгофа следует, что при выполнении условий леммы 4 матрица A_S является суммой 2^{m-1} подстановочных матриц, а семейство (11) имеет трансверсаль. Из равенств (7) следует, что одной из таких трансверсалей является последовательность

$$S(u_i) + S(u_0), \quad i = 1, 2, \dots, 2^m - 1.$$

Свойствами, указанными в лемме 4, обладают матрицы инцидентности симметричных блок-схем или (v, k, λ) -конфигураций с параметрами $v = 2^m - 1$, $k = 2^{m-1}$. Поэтому естественно возникает задача определения условий на дифференциально 2-равномерную подстановку S , при выполнении которых семейство (11) является (v, k, λ) -конфигурацией. Из известного соотношения $k(k-1) = \lambda(v-1)$ для параметров симметричных блок-схем следует, что в этом случае число элементов в любом пересечении $V_i \cap V_j$, $1 \leq i < j \leq 2^m - 1$, равно $\lambda = 2^{m-2}$.

Для описания свойств пересечений множеств семейства (10), ассоциированного с произвольной подстановкой S при любых $\alpha, \alpha' \in E_{2^m} \setminus \{\theta\}$, $\alpha \neq \alpha'$, рассмотрим множество, содержащее все α -строчные и α' -строчные конфигурации в подстановке S . На этом множестве, согласно определению 3, также задано отношение эквивалентности конфигураций, которое мы обозначим через $\sigma_{\alpha, \alpha'}$. Отношения $\sigma_{\alpha, \alpha'}$, $\alpha \neq \alpha'$ будем называть *отношениями междустрочной эквивалентности*.

Из определения непосредственно следует, что для любых $\alpha, \alpha' \in E_{2^m} \setminus \{\theta\}$ любые ϱ_α -эквивалентные и любые $\varrho_{\alpha'}$ -эквивалентные конфигурации подстановки S являются $\sigma_{\alpha, \alpha'}$ -эквивалентными. Кроме того, при любых $x, x' \in E_{2^m}$ конфигурации $[x, \alpha, \beta]$ и $[x', \alpha', \beta']$ подстановки S будут $\sigma_{\alpha, \alpha'}$ -эквивалентными при выполнении равенства $\beta = \beta'$, т. е. при

$$S(x + \alpha) + S(x) = S(x' + \alpha') + S(x') = \beta.$$

В частности из приведенных рассуждений следует, что любой класс отношения эквивалентности $\sigma_{\alpha, \alpha'}$ содержит не менее 2 элементов. Классы отношения междустрочной эквивалентности $\sigma_{\alpha, \alpha'}$ из 2 элементов будем называть *тривиальными* классами, классы более чем из 2 элементов — *нетривиальными* классами.

Лемма 5. *Предположим, что для подстановки S и некоторых $\alpha, \alpha' \in E_{2^m} \setminus \{\theta\}$, $\alpha \neq \alpha'$ все классы отношений строчной эквивалентности ϱ_α и $\varrho'_{\alpha'}$ минимальны и содержат по 2 элемента. Тогда любой нетривиальный класс отношения междустрочной эквивалентности $\sigma_{\alpha, \alpha'}$ содержит*

ровно 4 элемента и является объединением некоторого класса отношения строчной эквивалентности ϱ_α и некоторого класса отношения строчной эквивалентности $\varrho_{\alpha'}$.

При доказательстве без ограничения общности можно считать, что элементом нетривиального класса K является некоторая α -строчная конфигурация $[x, \alpha, \beta]$ в подстановке S . В этом случае $x + \alpha \neq x$ и $[x + \alpha, \alpha, \beta] \in K$. Так как K — нетривиальный класс, то существует элемент $x' \in E_{2^m}$, для которого либо $x \neq x'$, $x + \alpha \neq x'$ и $[x', \alpha, \beta] \in K$, либо $[x', \alpha', \beta] \in K$.

В первом случае нетрудно получить противоречие с условием минимальности классов отношения эквивалентности ϱ_α . Во втором случае K содержит следующие 4 попарно различные конфигурации в подстановке S :

$$[x, \alpha, \beta], [x + \alpha, \alpha, \beta], [x', \alpha', \beta], [x' + \alpha', \alpha', \beta] \quad (15)$$

и не содержит конфигураций $[x_1, \alpha_1, \beta]$, отличных от конфигураций (15). Таким образом лемма 5 доказана.

В условиях леммы 5 рассмотрим нетривиальные классы отношения междустрочной эквивалентности $\sigma_{\alpha, \alpha'}$. Каждый нетривиальный класс содержит некоторый класс отношения эквивалентности ϱ_α и некоторый класс отношения эквивалентности $\varrho_{\alpha'}$, при этом элементы правых частей i -й и j -й приведенных систем (12), определяющие эти классы отношений строчной эквивалентности, совпадают и принадлежат пересечению $V_i \cap V_j$. Отсюда следует справедливость следующей леммы.

Лемма 6. Если подстановка S дифференциально 2-равномерна, то эквивалентны следующие условия:

а) для любых $\alpha, \alpha' \in E_{2^m} \setminus \{\theta\}$, где $\alpha \neq \alpha'$, число нетривиальных классов междустрочной эквивалентности $\sigma_{\alpha, \alpha'}$ равно 2^{m-2} ;

б) семейство множеств вида (14) удовлетворяет условиям

$$|V_i \cap V_j| = \begin{cases} 2^{m-1}, & i = j, \\ 2^{m-2}, & i \neq j, \end{cases}$$

т. е. является (v, k, λ) -конфигурацией с параметрами

$$v = 2^m - 1, \quad k = 2^{m-1}, \quad \lambda = 2^{m-2}. \quad (16)$$

Следующая теорема устанавливает связь дифференциально 2-равномерных подстановок с классическими симметричными блок-схемами частного вида и вытекает из приведенных выше лемм.

Теорема 2. Пусть S — произвольная подстановка, действующая на группе E_{2^m} . Тогда следующие условия эквивалентны:

а) семейство множеств (14), ассоциированное с подстановкой S , образует (v, k, λ) -конфигурацию с параметрами (16) и дополнительным условием обнуления (13) в блоках (14);

б) подстановка S дифференциально 2-равномерна, и для любых $\alpha, \alpha' \in E_{2^m} \setminus \{\theta\}$, где $\alpha \neq \alpha'$, ровно 2^{m-2} из 2^{m-1} классов строчной эквивалентности ϱ_α образуют тривиальные классы междустрочной эквивалентности $\sigma_{\alpha, \alpha'}$.

При выполнении указанных условий матрица C_S , определяемая подстановкой S и соотношениями (3), (4), при соответствующей нумерации строк и столбцов связана с матрицей инцидентности A_S некоторой (v, k, λ) -конфигурации с блоками (14) равенством

$$C_S = 2 \cdot A_S.$$

Отметим, что (v, k, λ) -конфигурации с параметрами $v = 2^m - 1$, $k = 2^{m-1}$, $\lambda = 2^{m-2}$ существуют для любого $m \geq 3$. Примеры таких (v, k, λ) -конфигураций можно построить на основе матриц Сильвестра–Адамара [4].

В качестве примера реализации условий теоремы 2 рассмотрим полноцикловую подстановку

$$S = (u_0, u_7, u_5, u_1, u_3, u_4, u_2, u_6)$$

элементов группы $E_8 = \{u_0, u_1, u_2, u_3, u_4, u_5, u_6, u_7\}$ (случай $m = 3$). Выпишем множества V_i системы (14), ассоциированной с подстановкой S :

$$\begin{aligned} V_1 &= \{u_4, u_2, u_3, u_5\}, & V_2 &= \{u_1, u_7, u_2, u_4\}, & V_3 &= \{u_3, u_5, u_7, u_1\}, \\ V_4 &= \{u_5, u_2, u_6, u_1\}, & V_5 &= \{u_6, u_1, u_3, u_4\}, & V_6 &= \{u_7, u_6, u_4, u_5\}, \\ V_7 &= \{u_2, u_3, u_7, u_6\}. \end{aligned}$$

Подстановка S является дифференциально 2-равномерной, семейство множеств $V_1, \dots, V_7$, ассоциированное с подстановкой S , есть $(7, 4, 2)$ -конфигурация. Для соответствующих матриц A_S и C_S имеем равенства:

$$A_S = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}, \quad C_S = \begin{pmatrix} 0 & 2 & 2 & 2 & 2 & 0 & 0 \\ 2 & 2 & 0 & 2 & 0 & 0 & 2 \\ 2 & 0 & 2 & 0 & 2 & 0 & 2 \\ 2 & 2 & 0 & 0 & 2 & 2 & 0 \\ 2 & 0 & 2 & 2 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 & 2 & 2 & 2 \\ 0 & 2 & 2 & 0 & 0 & 2 & 2 \end{pmatrix}.$$

2. Сцепления, разноравные инволюции и дифференциально 2-равноравные подстановки

В данном параграфе нам будет удобно отдельно выделить следующий частный случай строчной эквивалентности (α, β) -конфигураций в подстановке S , действующей на аддитивной группе E_{2^m} конечного поля F_{2^m} . Если для $x \in E_{2^m}$, $\alpha, \beta \in E_{2^m} \setminus \{\theta\}$ выполнено соотношение (1), то будем говорить, что подстановка S имеет (α, β) -сцепление (α, β) -конфигураций $[x, \alpha, \beta]$ и $[x + \alpha, \alpha, \beta]$. При этом элементы α, β в некотором (α, β) -сцеплении будем называть *верхним весом* и *нижним весом* соответственно.

Весом двоичного цикла (α, β) будем называть сумму $\alpha + \beta$ в группе E_{2^m} .

Лемма 7. Любому (α, β) -сцеплению (α, β) -конфигураций $[x, \alpha, \beta]$ и $[x + \alpha, \alpha, \beta]$ в подстановке S можно поставить в соответствие двоичные циклы $(x, x + \alpha)$ и $(S(x), S(x + \alpha))$, веса которых совпадают, соответственно, с верхним и нижним весами этого (α, β) -сцепления. При заданном верхнем весе сцепления α нижний вес определяется действием подстановки S в точках $x, x + \alpha \in E_{2^m}$.

Лемма 7 позволяет в терминах (α, β) -сцеплений описать дифференциально 2-равноравные подстановки.

Лемма 8. Если подстановка S дифференциально 2-равноравна, то для любого $\alpha \neq \theta$ все ее (α, β) -конфигурации исчерпываются 2^{m-1} различными (α, β) -сцеплениями, верхние веса которых равны α , а нижние 2^{m-1} весов являются различными ненулевыми элементами группы E_{2^m} .

В самом деле, в матрице C_S верхний вес α соответствует номеру строки, нижний вес определяет номер столбца элемента, а наличие двух решений уравнения (1) соответствует равенству $c_{\alpha, \beta} = 2$.

Определение 5. Подстановки $L_0, L_1, L_2, \dots, L_{2^m-1}$, действующие на группе E_{2^m} и определяемые равенствами

$$L_j(u_i) = u_i + u_j, \quad i = 0, 1, \dots, 2^m - 1, \quad j = 0, 1, 2, \dots, 2^m - 1,$$

называются *трансляциями*.

Трансляция L_0 есть единичная подстановка. Каждая трансляция L_j при $j = 1, 2, \dots, 2^m - 1$ является инволюцией, содержащей только двоичные циклы, т. е. существуют такие различные элементы $u_{i_1}^{(j)}, u_{i_2}^{(j)}, \dots, u_{i_{2^m-1}}^{(j)}$, что трансляция L_j может быть записана в виде

$$L_j = \left(u_{i_1}^{(j)}, u_{i_1}^{(j)} + u_j \right) \left(u_{i_2}^{(j)}, u_{i_2}^{(j)} + u_j \right) \dots \left(u_{i_{2^m-1}}^{(j)}, u_{i_{2^m-1}}^{(j)} + u_j \right). \quad (17)$$

Это означает, что каждая трансляция L_j , $j = 1, 2, \dots, 2^m - 1$, записывается в виде произведения 2^{m-1} двоичных циклов одинакового веса, равного u_j . Отсюда вытекает следующая лемма.

Лемма 9. Множество всех трансляций $L_0, L_1, \dots, L_{2^m-1}$ состоит из попарно противоречивых подстановок, действующих на группе E_{2^m} , и образует латинский квадрат

$$[L_0, L_1, \dots, L_{2^m-1}]_{2^m}. \quad (18)$$

Определение 6. Инволюцию J , состоящую из 2^{m-1} двоичных циклов, назовем *разновесной*, если двоичные циклы, входящие в J , имеют попарно различные веса. Семейство инволюций, действующих на группе E_{2^m} ,

[illegible]

называется *разновесным*, если каждая инволюция $J_0, J_1, \dots, J_{2^m-1}$ — разновесная и все $\binom{2^m}{2}$ двоичных циклов, входящих в инволюции (19), попарно различны.

Инволюцию J_0 будем считать равной единичной подстановке.

Лемма 10. Семейство разнovesных инволюций вида (19) вместе с единичной подстановкой есть семейство попарно противоречивых подстановок, действующих на группе E_{2m} и образующих латинский квадрат

$$[J_0, J_1, \dots, J_{2^m-1}]_{2^m} . \quad (20)$$

Определение 7. Цикловой биекцией инволюции L_i вида (17) в некоторую инволюцию J , состоящую из 2^{m-1} двоичных циклов, назовем подстановку элементов группы E_{2^m} , которая осуществляет суперпозицию некоторой биекции совокупности двоичных циклов L_i в совокупность двоичных циклов J и некоторых биекций элементов соответствующих двоичных циклов.

Общее число цикловых биекций L_i в J равно

$$2^{2^{m-1}} \cdot (2^{m-1})!$$

Из определения следует, что в случае, когда подстановка $S : E_{2^m} \rightarrow E_{2^m}$ дифференциально 2-равномерна относительно элемента $\alpha = u_i$, число ее (u_i, β) -сцеплений, верхние веса которых равны u_i , а нижние 2^{m-1} весов являются попарно различными ненулевыми элементами группы E_{2^m} , равно 2^{m-1} .

Лемма 11. Если подстановка $S : E_{2^m} \rightarrow E_{2^m}$ дифференциально 2-равномерна относительно элемента $\alpha = u_i$, то она является цикловой биекцией трансляции L_i в некоторую разностную инволюцию J , состоящую из 2^{m-1} двоичных циклов.

Действительно, для каждого сцепления (u_i, β) -конфигураций в подстановке S элементам $x, x + u_i$ соответствует единственный двоичный цикл трансляции L_i , а образам $S(x), S(x + u_i)$ — единственный двоичный цикл $(S(x), S(x + u_i))$ инволюции J . Из условия дифференциальной 2-равномерности S следует, что инволюция J — разностная.

На основе леммы 11 можно доказать следующие утверждения.

Лемма 12. Подстановка $S : E_{2^m} \rightarrow E_{2^m}$ является дифференциально 2-равномерной относительно элемента $\alpha = u_i$, $1 \leq i \leq 2^m - 1$, тогда и только тогда, когда S является одним из решений следующего уравнения подобия

$$X^{-1} \cdot L_i \cdot X = J_i, \quad (21)$$

где J_i — некоторая разностная инволюция, состоящая из 2^{m-1} двоичных циклов. Число решений уравнения (21) равно

$$2^{2^{m-1}} \cdot (2^{m-1})!$$

Для доказательства заметим, что условие дифференциальной 2-равномерности S относительно элемента $\alpha = u_i$ равносильно выполнению соотношения вида

$$\begin{aligned} (S(u_{i_1}^{(i)}), S(u_{i_1}^{(i)} + u_j)) \dots (S(u_{i_{2^{m-1}}}^{(i)}), S(u_{i_{2^{m-1}}}^{(i)} + u_j)) = \\ = (a_1^{(i)}, b_1^{(i)}) \dots (a_{2^{m-1}}^{(i)}, b_{2^{m-1}}^{(i)}) \end{aligned} \quad (22)$$

с некоторой разностной инволюцией в правой части. Соотношение (22), в свою очередь, равносильно уравнению (21).

Каждое уравнение подобия (21) решается с использованием оператора Коши и имеет $2^{2^{m-1}} \cdot (2^{m-1})!$ решений. Эти решения совпадают с множеством подстановок, полученных цикловыми биекциями.

Лемма 13. Подстановка $S : E_{2^m} \rightarrow E_{2^m}$ является дифференциально 2-равномерной тогда и только тогда, когда S является одним из решений системы уравнений подобия

$$\begin{aligned} X^{-1} \cdot L_1 \cdot X &= J_1, \\ X^{-1} \cdot L_2 \cdot X &= J_2, \\ &\dots\dots\dots \\ X^{-1} \cdot L_{2^m-1} \cdot X &= J_{2^m-1}, \end{aligned} \tag{23}$$

где $L_1, L_2, \dots, L_{2^m-1}$ — трансляции (17) и $J_1, J_2, \dots, J_{2^m-1}$ — некоторое семейство разнoвесных инволюций.

Действительно, для того чтобы при любом $i = 1, 2, \dots, 2^m - 1$ подстановка S удовлетворяла уравнению $X^{-1} \cdot L_i \cdot X = J_i$, необходимо и достаточно существование 2^{m-1} сцеплений подстановки S , верхние веса которых равны u_i , а нижние веса различны. Последнее условие равносильно свойству дифференциальной 2-равномерности подстановки S .

Проверка совместности системы вида (23) при заданном семействе разнoвесных инволюций $J_1, J_2, \dots, J_{2^m-1}$ сводится к перебору $2^{2^{m-1}} \cdot (2^{m-1})!$ подстановок S , удовлетворяющих равенству $S^{-1} \cdot L_1 \cdot S = J_1$, и к проверке того, что опробуемый вариант подстановки S может быть получен некоторой цикловой биекцией трансляции L_i в разнoвесную инволюцию J_i для всех $i = 1, 2, \dots, 2^m - 1$. Стало быть, этот алгоритм проверки совместности системы (23) фактически совпадает с алгоритмом отыскания одного из ее решений.

Алгоритм проверки того, является ли заданная подстановка S дифференциально 2-равномерной, более простой. Для этого следует проверить наличие в подстановке S всех сцеплений, у которых верхний вес принимает значения $u_1, \dots, u_{2^m-1}$, и при фиксированном верхнем весе все нижние веса различны. Число сцеплений при фиксированном верхнем весе равно 2^{m-1} , и верхние веса принимают $2^m - 1$ значений. Значит, число операций проверки равно $\binom{2^m}{2}$.

Из леммы 13 вытекает следующее утверждение.

Следствие 1. Если система (23) совместна и имеет решение S , являющееся дифференциально 2-равномерной подстановкой, то латинские квадраты (18) и (20) связаны соотношением

$$S^{-1} \cdot [L_0, L_1, \dots, L_{2^m-1}]_{2^m} \cdot S = [J_0, J_1, \dots, J_{2^m-1}]_{2^m}.$$

3. Способы построения разнovesных инволюций и дифференциально 2-равномерных подстановок

Выше был указан способ построения разнovesных инволюций с использованием сцеплений дифференциально 2-равномерных подстановок. Однако этот способ неприменим, если такая подстановка неизвестна. Поэтому укажем другой способ построения разнovesных инволюций, соответствующих определению 6. Для этого используем таблицу Кэли группы E_{2^m} , представляющую собой латинский квадрат, симметричный относительно главной диагонали, состоящей из клеток с повторяющимся элементом u_0 . Клетку таблицы Кэли в строке с номером a и в столбце с номером b , $a, b \in E_{2^m}$, содержащую элемент $u_i = a + b$, будем обозначать через $u_i(a, b)$ и называть a и b входами клетки. Ввиду симметрии будем использовать только треугольную часть латинского квадрата, расположенную выше главной диагонали и содержащую клетки $u_i(a, b)$ с входами $a < b$. Эту часть будем называть латинским треугольником.

Определение 8. Максимальное подмножество клеток латинского треугольника, содержащих один и тот же элемент группы E_{2^m} , будем называть *серией*. Число клеток называется *длиной серии*.

Каждому ненулевому элементу группы $u_i \in E_{2^m}$ в латинском треугольнике соответствует серия D_{u_i} длины 2^{m-1} . Общее число серий в латинском треугольнике равно $2^m - 1$. Для различных ненулевых элементов E_{2^m} , определенных произвольным вектором

$$(u_{\nu_1}, u_{\nu_2}, \dots, u_{\nu_{2^m-1}}), 1 \leq \nu_1 < \nu_2 < \dots < \nu_{2^m-1} \leq 2^m - 1, \quad (24)$$

с условием обнуления

$$u_{\nu_1} + u_{\nu_2} + \dots + u_{\nu_{2^m-1}} = u_0, \quad (25)$$

рассмотрим упорядоченное семейство серий

$$(D_{u_{\nu_1}}, D_{u_{\nu_2}}, \dots, D_{u_{\nu_{2^m-1}}}). \quad (26)$$

Элементы семейства (26) попарно не пересекаются, поэтому для него существуют трансверсали. Нам потребуется следующее уточнение понятия трансверсали.

Определение 9. Последовательность клеток вида

$$\left(u_{\nu_1}(a_1, b_1), u_{\nu_2}(a_2, b_2), \dots, u_{\nu_{2^m-1}}(a_{2^m-1}, b_{2^m-1}) \right), \quad u_{\nu_i}(a_i, b_i) \in D_{u_{\nu_i}} \quad (27)$$

называется *трансверсалью семейства серий* (26) с условием *неколлинеарности*, если члены каждой из последовательностей $(a_1, a_2, \dots, a_{2^m-1})$ и $(b_1, b_2, \dots, b_{2^m-1})$ элементов группы E_{2^m} попарно различны.

Отметим, что так как в последовательности (27) $a_i < b_j$ для любых $i, j = 1, \dots, 2^m-1$, то в условиях определения 9 множество $\{a_1, a_2, \dots, a_{2^m-1}, b_1, b_2, \dots, b_{2^m-1}\} = E_{2^m}$.

Из определения трансверсали с условием неколлинеарности (27) следует, что ее клетки находятся в разных строках и разных столбцах латинского треугольника таблицы Кэли группы E_{2^m} . В дальнейшем для краткости мы будем использовать термин «трансверсаль», *всегда имея в виду, что она удовлетворяет условию неколлинеарности*.

Если задана трансверсаль вида (27), то ее можно использовать для последовательного построения вариантов подстановок и за счет проверки совместности системы (23) получать дифференциально 2-равномерные подстановки S . Для этого полагаем $J_1 = (a_1, b_1)(a_2, b_2) \dots (a_{2^m-1}, b_{2^m-1})$ и получаем разностную инволюцию, соответствующую выбранной трансверсали семейства серий (26). С использованием цикловых биекций трансляции L_1 в инволюцию J_1 получаем $2^{2^m-1} \cdot (2^m-1)!$ вариантов решения уравнения $S^{-1} \cdot L_1 \cdot S = J_1$. Каждый из полученных вариантов подстановки S используется для последовательного проведения процесса проверки совместности системы (23). Варианты подстановки S , не удовлетворяющие условию совместности, отклоняются. В этом случае выбирается другой вариант решения уравнения $S^{-1} \cdot L_1 \cdot S = J_1$ и проводится очередная проверка совместности системы (23). Вариант подстановки S , удовлетворяющий условию совместности (23), является дифференциально 2-равномерной подстановкой.

Отметим одно важное свойство трансверсалей семейств серий.

Теорема 3. Трансверсали латинского треугольника вида (27) для $2^m - 1$ семейств серий не имеют пересечений, если их входы в таблицу Кэли соответствуют разностным инволюциям $J_1, J_2, \dots, J_{2^m-1}$, для которых система уравнений (23) совместна и определяет дифференциально 2-равномерную подстановку S . В этом случае трансверсали полностью без перекрытий покрывают весь латинский треугольник таблицы Кэли группы E_{2^m} .

Действительно, каждый из векторов вида (24) определяется одной из разноресных инволюций $J_1, J_2, \dots, J_{2^m-1}$, которые в случае совместности системы (23) вместе с J_0 образуют латинский квадрат. Число возможных представителей от каждой серии равно 2^{m-1} , а число серий равно $2^m - 1$. Отсюда следует, что трансверсали определяются без пересечений всей совокупностью из $\binom{2^m}{2}$ возможных неупорядоченных пар различных элементов группы E_{2^m} .

Следует заметить, что трансверсали могут пересекаться по значениям координат вектора (24). Однако при совпадении координат векторов (24) соответствующие входы клеток таблицы Кэли являются различными.

Отыскание одной трансверсали для семейства из 2^{m-1} серий в латинском треугольнике не является особенно трудоемкой задачей. Но определение достаточно большого их числа требует рассмотрения специального алгоритма. Этот алгоритм основывается на общей идее нахождения в некоторой таблице заданного числа попарно не коллинеарных клеток. Такая идея используется, в частности, в работах Риордана и Капланского (см. [7]) по перечислению числа способов расстановки различных взаимно не атакующих фигур на шахматной доске произвольной конфигурации. Однако в указанных работах основным требованием допустимого расположения фигур является только требование их неколлинеарности. В нашем случае для определения входов клеток трансверсали возникают два дополнительных требования, связанные с тем, что заполнения клеток попарно различны и удовлетворяют условию аннулирования (25).

В латинском треугольнике таблицы Кэли группы E_{2^m} любую непустую совокупность клеток будем называть *доской* и обозначать через $M_{\mu,\nu}$, где μ и ν — минимальные числа строк и столбцов латинского треугольника, в которых расположены все клетки доски. Совокупность всех клеток, соответствующих элементам серий (26), назовем *серийной доской* и также обозначим через $M_{\mu,\nu}$. В этом случае μ и ν — минимальные числа строк и столбцов латинского треугольника, в которых расположены клетки всех серий (26).

Для формализации построения трансверсалей для заданной серийной доски определим *операцию разложения произвольной доски $M_{\mu,\nu}$ по некоторой клетке этой доски*. Используем тот факт, что если клетка $u_{\nu_j}(a_j, b_j)$, $1 \leq j \leq 2^{m-1}$, является элементом трансверсали, то никакие другие клетки, расположенные в a_j -й строке и в b_j -м столбце доски $M_{\mu,\nu}$, не могут быть элементами этой трансверсали. Отсюда следует возможность разложения доски $M_{\mu,\nu}$ по клетке $u_{\nu_j}(a_j, b_j)$ следующего вида:

$$M_{\mu,\nu} = u_{\nu_j}(a_j, b_j) M'_{\mu-1,\nu-1} + M''_{\mu,\nu}, \quad (28)$$

где $M'_{\mu-1,\nu-1}$ — усеченная доска, полученная из доски $M_{\mu,\nu}$ вычеркиванием a_j -й строки и b_j -го столбца, а $M''_{\mu,\nu}$ — сокращенная доска, полученная из доски $M_{\mu,\nu}$ удалением клетки с элементом $u_{\nu_j}(a_j, b_j)$. Аналогично соотношению (28), доски $M'_{\mu-1,\nu-1}$ и $M''_{\mu,\nu}$ разлагаются по своим элементам. В результате многократного применения операции разложения число клеток во вновь полученных досках уменьшается, а число слагаемых, содержащих такие доски, увеличивается.

Процесс разложения доски $M_{\mu,\nu}$ завершается, когда усеченные и сокращенные доски становятся либо пустыми, либо содержат одну клетку. После завершения процесса разложения в правой части равенства вида (28) получается объединение соединенных знаком $+$ мономов, представляющих собой формальные произведения клеток доски $M_{\mu,\nu}$. При этом в некоторых полученных мономах веса сомножителей-клеток могут совпадать, такие мономы на завершающем этапе не учитываются.

Данную формальную сумму мономов будем называть *формальным многочленом доски* $M_{\mu,\nu}$ и обозначать $R(M_{\mu,\nu})$. Формальные многочлены досок обладают следующим свойством, облегчающим их определение методом разложения досок.

Утверждение 1. Если доска $M_{\mu,\nu}$ представляется в виде объединения досок $M_{\mu_1,\nu_1}^{(1)}$ и $M_{\mu_2,\nu_2}^{(2)}$, не имеющих общих строк и столбцов, то

$$R(M_{\mu,\nu}) = R(M_{\mu_1,\nu_1}^{(1)}) \cdot R(M_{\mu_2,\nu_2}^{(2)}).$$

На завершающем этапе определения трансверсалей серий латинского треугольника используется следующее свойство.

Утверждение 2. Мономы формального многочлена $R(M_{\mu,\nu})$ серийной доски семейства (26), содержащие по 2^{m-1} неколлинеарных сомножителей с различными весами, соответствуют трансверсалиям (27) этого семейства.

Рассмотрим пример при $m = 3$. Вектор

$$(u_2, u_3, u_4, u_5)$$

вида (24) удовлетворяет условию обнуления (25). Выделим клетки серийной доски $M_{6,6}$ в латинском треугольнике таблицы Кэли группы E_8 для семейства

серий $(D_{u_2}, D_{u_3}, D_{u_4}, D_{u_5})$:

u_0	u_1	u_2	u_3	u_4	u_5	u_6	u_7
u_0		$u_2(0, 2)$	$u_3(0, 3)$	$u_4(0, 4)$	$u_5(0, 5)$		
u_1		$u_3(1, 2)$	$u_2(1, 3)$	$u_5(1, 4)$	$u_4(1, 5)$		
u_2						$u_4(2, 6)$	$u_5(2, 7)$
u_3						$u_5(3, 6)$	$u_4(3, 7)$
u_4						$u_2(4, 6)$	$u_3(4, 7)$
u_5						$u_3(5, 6)$	$u_2(5, 7)$
u_6							
u_7							

Имеем разложение доски вида

$$M_{6,6} = M_{2,4} \cup M_{4,2}, \quad M_{2,4} \cap M_{4,2} = \emptyset.$$

Следовательно, серийный многочлен равен произведению

$$R(M_{6,6}) = R(M_{2,4}) \cdot R(M_{4,2}).$$

Последовательно раскладывая доски, получим выражения для многочленов-сомножителей:

$$\begin{aligned} R(M_{2,4}) &= u_2(0, 2) [u_2(1, 3) + u_5(1, 4) + u_4(1, 5)] + \\ &\quad + u_3(1, 2) [u_3(0, 3) + u_4(0, 4) + u_5(0, 5)] + \\ &\quad + u_3(0, 3) [u_5(1, 4) + u_4(1, 5)] + u_2(1, 3) [u_4(0, 4) + u_5(0, 5)] + \\ &\quad + u_4(0, 4)u_4(1, 5) + u_5(1, 4)u_5(0, 5) + u_5(0, 5) + u_4(1, 5), \\ R(M_{4,2}) &= u_4(2, 6) [u_4(3, 7) + u_3(4, 7) + u_2(5, 7)] + \\ &\quad + u_5(2, 7) [u_5(3, 6) + u_2(4, 6) + u_3(5, 6)] + \\ &\quad + u_5(3, 6) [u_3(4, 7) + u_2(5, 7)] + u_4(3, 7) [u_2(4, 6) + u_3(5, 6)] + \\ &\quad + u_2(4, 6)u_2(5, 7) + u_3(4, 7)u_3(5, 6) + u_3(5, 6) + u_2(5, 7). \end{aligned}$$

Перемножая эти многочлены и выделяя мономы с неколлинеарными сомножителями различного веса, в результате получим следующие семь трансверсалий семейства серий $(D_{u_2}, D_{u_3}, D_{u_4}, D_{u_5})$, а также семь соответствующих развесных инволюций с весами циклов u_2, u_3, u_4, u_5 :

$$\begin{aligned} &(u_2(1, 3), u_3(4, 7), u_4(2, 6), u_5(0, 5)), \quad (u_1, u_3)(u_4, u_7)(u_2, u_6)(u_0, u_5); \\ &(u_2(5, 7), u_3(0, 3), u_4(2, 6), u_5(1, 4)), \quad (u_5, u_7)(u_0, u_3)(u_2, u_6)(u_1, u_4); \\ &(u_2(4, 6), u_3(0, 3), u_4(1, 5), u_5(2, 7)), \quad (u_4, u_6)(u_0, u_3)(u_1, u_5)(u_2, u_7); \\ &(u_2(0, 2), u_3(4, 7), u_4(1, 5), u_5(3, 6)), \quad (u_0, u_2)(u_4, u_7)(u_1, u_5)(u_3, u_6); \end{aligned}$$

$$\begin{aligned}
 & (u_2(5, 7), u_3(1, 2), u_4(0, 4), u_5(3, 6)), \quad (u_5, u_7)(u_1, u_2)(u_0, u_4)(u_3, u_6); \\
 & (u_2(4, 6), u_3(1, 2), u_4(3, 7), u_5(0, 5)), \quad (u_4, u_6)(u_1, u_2)(u_3, u_7)(u_0, u_5); \\
 & (u_2(0, 2), u_3(5, 6), u_4(3, 7), u_5(1, 4)), \quad (u_0, u_2)(u_5, u_6)(u_3, u_7)(u_1, u_4).
 \end{aligned}$$

Список литературы

1. Nyberg K. Differentially uniform mappings for cryptography // EUROCRYPT'93. Lect. Notes Comput. Sci. — 1994. — Vol. 765. — P. 55–64.
2. Sachkov V.N. Probability distributions of number of configurations and discordances of random permutations from regular cyclic classes // Probabilistic methods in Discrete Mathematics. — Utreht: VSP, 2002. — P. 23–40.
3. Сачков В.Н. Цепи Маркова итерационных систем преобразований // Труды по дискретной математике. — 2002. — Т. 6. — М.: Физматлит, 2002. — С. 165–183.
4. Сачков В.Н. Комбинаторные методы дискретной математики. — М.: Наука, 1977.
5. Tang D., Carlet C., Tang X. Differentially 4-uniform bijections by permuting the inverse functions // Cryptology ePrint Archive, rep. 2013/639 (to appear in Designs, Codes and Cryptography).
6. Carlet C., Charpin P., Zinoviev V. Codes, bent functions and permutations suitable for DES-like cryptosystems // Designs, Codes and Cryptography. — 1998. — V. 15. № 2. — P. 125–156.
7. Риордан Дж. Введение в комбинаторный анализ. — М.: Изд-во иностранной литературы, 1963.