Math-Net.Ru

Общероссийский математический портал

В. Н. Сачков, И. А. Круглов, Весовые дефициты инволюций и подстановок,
Матем. вопр. криптогр., 2016, том 7, выпуск 4, 95–116

DOI: <https://doi.org/10.4213/mvk206>

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: 34.227.88.159

26 апреля 2023 г., 05:20:49

Весовые дефициты инволюций и подстановок

В. Н. Сачков, И. А. Круглов

Академия криптографии Российской Федерации, Москва

Получено 30.V.2016

Аннотация. Пусть E_{2^m} — упорядоченная аддитивная группа конечного поля из 2^m элементов. Для подстановки $S : E_{2^m} \rightarrow E_{2^m}$ вводится и изучается понятие индекса весового дефицита инволюции, соответствующей подстановке S . Этот индекс позволяет оценивать стойкость S -боксов относительно дифференциального метода криптоанализа. Описаны перечислительные алгоритмы для инволюций с заданными значениями весовых дефицитов.

Ключевые слова: подстановки, инволюции, весовые дефициты, перечислительные задачи

Weight deficits of involutions and substitutions

V. N. Sachkov, I. A. Kruglov

Academy of Cryptography of the Russian Federation, Moscow

Abstract. Let E_{2^m} be an ordered additive group of the finite field with 2^m elements. For the substitution $S : E_{2^m} \rightarrow E_{2^m}$ we introduce and investigate the index of the weight deficit of involution corresponding to the substitution S . By means of this index the security of S -boxes against the differential method of cryptoanalysis may be estimated. Some enumeration algorithms for involutions with given values of weight deficits are described.

Keywords: subctitutions, involutions, weight deficit, enumeration problems

Citation: *Mathematical Aspects of Cryptography*, 2016, v. 7, № 4, pp. 95–116 (Russian)

© Академия криптографии Российской Федерации, 2016 г.

Введение

В статье для подстановок $S : E_{2^m} \rightarrow E_{2^m}$, где E_{2^m} — упорядоченная аддитивная группа конечного поля из 2^m элементов, вводится и изучается понятие весового дефицита. Предложен новый критерий определения криптографического качества подстановок на основе использования понятия индекса весовых дефицитов инволюций, соответствующих подстановке. При использовании подстановок в качестве S -блоков блочного шифратора индекс весовых дефицитов позволяет оценивать стойкость этого шифратора относительно дифференциального метода криптоанализа.

Основные результаты работы содержатся в теоремах, в которых изложены перечислительные алгоритмы для получения инволюций, принадлежащих различным классам, отличающимся возможными значениями весовых дефицитов. В качестве следствий этих теорем получены формулы для определения чисел инволюций в указанных классах.

1. Суппорты, диагонали и весовые дефициты

Рассмотрим аддитивную группу $(E_{2^m}, +)$ конечного поля из 2^m элементов относительно групповой операции покоординатного сложения двоичных векторов. Будем предполагать, что $m \geq 3$, элементы группы $E_{2^m} = \{u_0, u_1, \dots, u_{2^m-1}\}$ упорядочены некоторым образом, причем u_0 — нулевой вектор. Равенства

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

определяют парноцикловые подстановки $L_j, j = 1, 2, \dots, 2^m - 1$, действующие на группе E_{2^m} . Эти парноцикловые подстановки будем называть *трансляциями*. Каждую трансляцию L_j можно рассматривать как последовательность 2^{m-1} двоичных циклов, т. е. упорядоченных пар элементов группы E_{2^m} , причем пары в j -й последовательности не имеют общих элементов и состоят из элементов, сумма которых в группе E_{2^m} равна u_j .

Далее в работе, если не оговорено противное, инволюцией называем произвольную парноцикловую подстановку на группе E_{2^m} .

Рассмотрим произвольную подстановку S , действующую на группе E_{2^m} . Для любого $j = 1, 2, \dots, 2^m - 1$ подстановка S отображает пары j -й последовательности, соответствующей L_j , в некоторые пары элементов группы E_{2^m} . Эти пары образуют j -ю последовательность пар образов, которые определяют двоичные циклы инволюции

$$J_j = (a_{j,1}, b_{j,1})(a_{j,2}, b_{j,2}) \cdots (a_{j,2^{m-1}}, b_{j,2^{m-1}}).$$

Двоичным циклам произвольной инволюции

$$J = (u_{a_1}, u_{b_1}) (u_{a_2}, u_{b_2}) \cdots (u_{a_{2^m-1}}, u_{b_{2^m-1}})$$

соответствует *весовой вектор*

$$w = (w_1, w_2, \dots, w_{2^m-1})$$

с координатами (*весами двоичных циклов*)

$$w_s = u_{a_s} + u_{b_s}, \quad j, s = 1, 2, \dots, 2^m - 1.$$

О п р е д е л е н и е 1. Если k — число различных координат весового вектора w , $0 < k \leq 2^{m-1}$, то величина $r = 2^{m-1} - k$ называется *весовым дефицитом* инволюции J . Если весовой дефицит инволюции J равен нулю, то J называется *разновесной инволюцией* (см. [1]).

О п р е д е л е н и е 2. Если подстановке S и трансляции L_j соответствует инволюция J_j , имеющая весовой дефицит r_j , то будем говорить, что подстановка S имеет *частичный весовой дефицит* r_j , $j = 1, 2, \dots, 2^m - 1$.

О п р е д е л е н и е 3. Если подстановке S и последовательности трансляций $L_1, L_2, \dots, L_{2^m-1}$ соответствует последовательность инволюций $J_1, J_2, \dots, J_{2^m-1}$, то вектор $r(S) = (r_1, r_2, \dots, r_{2^m-1})$ будем называть *индикатором весовых дефицитов* подстановки S .

Справедлива следующая лемма.

Лемма 1. Подстановка $S : E_{2^m} \rightarrow E_{2^m}$ является дифференциально 2-равномерной тогда и только тогда, когда ее индикатор весовых дефицитов удовлетворяет условию

$$r(S) = (0, 0, \dots, 0).$$

Таким образом, индикатор весовых дефицитов подстановки S можно рассматривать как меру близости S к дифференциально 2-равномерной подстановке, позволяющую оценивать криптографические качества S относительно дифференциального метода криптоанализа.

Изучение инволюций будем проводить, используя латинские треугольники таблицы Кэли группы E_{2^m} .

Предположим, что строки и столбцы таблицы Кэли группы E_{2^m} занумерованы векторами $u_0, u_1, \dots, u_{2^m-1}$ в выбранном порядке. Клетку таблицы Кэли в строке с номером u_k и в столбце с номером u_l обозначим через $v(u_k, u_l)$, в данной клетке содержится элемент $u_k + u_l$ группы E_{2^m} (вес клетки $v(u_k, u_l)$).

Латинский треугольник таблицы Кэли представляет собой совокупность клеток $v(u_k, u_l)$, $1 \leq k < l \leq 2^m - 1$. Латинский треугольник состоит из $2^m - 1$ серий по 2^{m-1} клеток, все клетки k -й серии имеют вес u_k , $1 \leq k \leq 2^m - 1$.

О п р е д е л е н и е 4. Для произвольного $k = 1, 2, \dots, 2^m - 1$ и любого набора индексов $1 \leq j_1 < j_2 < \dots < j_k \leq 2^m - 1$ объединение k серий клеток с весами $u_{j_1}, u_{j_2}, \dots, u_{j_k}$ назовем *суппортом* и обозначим через

$$[j_1, j_2, \dots, j_k].$$

В дальнейшем будем рассматривать последовательности из 2^{m-1} клеток латинского треугольника вида

$$d = v(u_{a_1}, u_{b_1}), v(u_{a_2}, u_{b_2}), \dots, v(u_{a_{2^{m-1}}}, u_{b_{2^{m-1}}}), a_i < b_i, i = 1, \dots, 2^{m-1}. \quad (1)$$

О п р е д е л е н и е 5. Назовем 2^{m-1} -диагональю суппорта $[j_1, j_2, \dots, j_k]$ последовательность (1) попарно неколлинеарных (не лежащих в одной строке и в одном столбце) клеток этого суппорта, удовлетворяющую условию

$$a_1 < a_2 < \dots < a_{2^{m-1}}. \quad (2)$$

Отметим, что в произвольном суппорте $[j_1, j_2, \dots, j_k]$ для любого $i = 1, \dots, k$ имеется серия вида (1), (2), состоящая из 2^{m-1} клеток латинского треугольника фиксированного веса

$$u_{j_i} = u_{a_1} + u_{b_1} = u_{a_2} + u_{b_2} = \dots = u_{a_{2^{m-1}}} + u_{b_{2^{m-1}}},$$

и эта серия является 2^{m-1} -диагональю данного суппорта.

О п р е д е л е н и е 6. Назовем 2^{m-1} -диагональю латинского треугольника таблицы Кэли группы E_{2^m} произвольную 2^{m-1} -диагональ некоторого суппорта в данном треугольнике.

Введем понятия сильных и слабых клеток по отношению к данной клетке латинского треугольника. Для этого латинскому треугольнику таблицы Кэли группы E_{2^m} поставим в соответствие числовой треугольник. При этом соответствии каждой клетке $v(u_i, u_j)$ латинского треугольника соответствует элемент (i, j) числового треугольника. При этом из условия $i < j$ следует, что $i \in \{0, 1, \dots, 2^m - 2\}$, $j \in \{1, 2, \dots, 2^m - 1\}$.

Клетка $v(u_k, u_l)$ называется *слабой* по отношению к клетке $v(u_i, u_j)$, если выполнено хотя бы одно из двух условий

- (a) $l = i, k \neq j$ и $k < i < j$,
- (b) $k = j, l \neq i$ и $i < j < l$.

Клетка $v(u_k, u_l)$ называется *сильной* по отношению к клетке $v(u_i, u_j)$, если она не является слабой, т. е. выполнено условие

- (c) $l \neq i, k \neq j$.

Для любых клеток $v(u_i, u_j)$ и $v(u_k, u_l)$, лежащих на некоторой 2^{m-1} -диагонали в латинском треугольнике, транспозиции (u_i, u_j) и (u_k, u_l) являются двоичными циклами некоторой инволюции тогда и только тогда, когда клетка $v(u_k, u_l)$ является сильной по отношению к клетке $v(u_i, u_j)$.

Будем называть 2^{m-1} -диагональ d вида (1) в латинском треугольнике *слабой*, если существуют такие $1 \leq \mu < \nu \leq 2^{m-1}$, что клетка диагонали $v(a_\nu, b_\nu)$ является слабой по отношению к клетке диагонали $v(a_\mu, b_\mu)$.

Будем называть 2^{m-1} -диагональ d вида (1) в латинском треугольнике *сильной*, если для любых $1 \leq \mu < \nu \leq 2^{m-1}$ клетка $v(a_\nu, b_\nu)$ является сильной по отношению к клетке $v(a_\mu, b_\mu)$.

Для любой 2^{m-1} -диагонали d вида (1) в латинском треугольнике последовательность двоичных циклов

$$(u_{a_1}, u_{b_1})(u_{a_2}, u_{b_2}) \cdots (u_{a_{2^{m-1}}}, u_{b_{2^{m-1}}}) \quad (3)$$

образует инволюцию на группе E_{2^m} тогда и только тогда, когда диагональ d является сильной.

Если для 2^{m-1} -диагонали d латинского треугольника вида (1) число различных элементов множества $\{u_{a_1} + u_{b_1}, u_{a_2} + u_{b_2}, \dots, u_{a_{2^{m-1}}} + u_{b_{2^{m-1}}}\}$ равно k , $0 < k \leq 2^{m-1}$, то число $r = 2^{m-1} - k$ называется *весовым дефицитом* диагонали d .

Будем называть 2^{m-1} -диагональ d латинского треугольника вида (1) *разновесной*, если ее весовой дефицит равен нулю, т. е. веса $u_{a_1} + u_{b_1}, u_{a_2} + u_{b_2}, \dots, u_{a_{2^{m-1}}} + u_{b_{2^{m-1}}}$ входящих в нее клеток попарно различны. Отметим, что если для некоторого k -суппорта $[j_1, j_2, \dots, j_k]$ существуют разновесные 2^{m-1} -диагонали, то необходимо выполнено неравенство $k \geq 2^{m-1}$.

Будем называть 2^{m-1} -диагональ d вида (1) некоторого $(2^{m-1} - r)$ -суппорта $[j_1, j_2, \dots, j_{2^{m-1}-r}]$, $0 \leq r < 2^{m-1}$, *трансверсалью серий* этого суппорта, если весовой дефицит диагонали d равен r .

Любая разновесная 2^{m-1} -диагональ вида (1) является трансверсалью серий 2^{m-1} -суппорта $[j_1, j_2, \dots, j_{2^{m-1}}]$, определяемого равенством

$$\{u_{a_1} + u_{b_1}, u_{a_2} + u_{b_2}, \dots, u_{a_{2^{m-1}}} + u_{b_{2^{m-1}}}\} = \{u_{j_1}, u_{j_2}, \dots, u_{j_{2^{m-1}}}\}. \quad (4)$$

Сильная 2^{m-1} -диагональ вида (1) является трансверсалью серий 2^{m-1} -суппорта $[j_1, j_2, \dots, j_{2^{m-1}}]$, определяемого равенством (4), тогда и только тогда, когда соответствующая инволюция (3) — разновесная.

2. Многочлены формального пересчисления

2^{m-1} -диагоналей

В данном параграфе рассматриваются многочлены с целыми коэффициентами от многих переменных, а в качестве формальных переменных используются упорядоченные пары элементов группы E_{2^m} вида (u_a, u_b) , $0 \leq a < b \leq 2^m - 1$. Любой 2^{m-1} -диагонали d вида (1) в латинском треугольнике таблицы Кэли группы E_{2^m} , удовлетворяющей условию (2), поставим в соответствие моном

$$(u_{a_1}, u_{b_1}) \cdot (u_{a_2}, u_{b_2}) \cdots (u_{a_{2^{m-1}}}, u_{b_{2^{m-1}}}). \quad (5)$$

Будем говорить, что многочлен M пересчисляет диагонали из (возможно, пустого) множества D диагоналей латинского треугольника группы E_{2^m} , если ненулевые коэффициенты при мономах M равны единице, мономы с коэффициентом 1 имеют вид (5) и находятся во взаимно однозначном соответствии с диагоналями из множества D . В частности, нулевой многочлен пересчисляет диагонали из пустого множества.

Для произвольного $k = 1, 2, \dots, 2^m - 1$ и любого набора индексов $1 \leq j_1 < j_2 < \dots < j_k \leq 2^m - 1$ обозначим через

$$M[j_1, j_2, \dots, j_k]$$

многочлен, который пересчисляет 2^{m-1} -диагонали k -суппорта $[j_1, j_2, \dots, j_k]$.

Для любых $r \in \{0, 1, \dots, 2^{m-1} - 1\}$, $k \in \{2^{m-1} - r, \dots, 2^m - 1\}$ и любого k -суппорта $[j_1, j_2, \dots, j_k]$ обозначим через

$$M_r[j_1, j_2, \dots, j_k]$$

многочлен, который пересчисляет 2^{m-1} -диагонали этого k -суппорта, имеющие весовой дефицит, равный r .

Докажем следующую общую теорему.

Теорема 1. Для любого $r \in \{0, 1, \dots, 2^{m-1} - 1\}$, любого $k \in \{2^{m-1} - r, \dots, 2^m - 1\}$ и любого k -суппорта $[j_1, j_2, \dots, j_k]$ имеет место формула

$$\begin{aligned} M_r[j_1, j_2, \dots, j_k] &= \\ &= \sum_{t=1}^{2^{m-1}-r} (-1)^{r+t} \binom{k-t}{k-2^{m-1}+r} \sum_{1 \leq \mu_1 < \mu_2 < \dots < \mu_t \leq k} M[j_{\mu_1}, j_{\mu_2}, \dots, j_{\mu_t}]. \end{aligned} \quad (6)$$

Доказательство. Для 2^{m-1} -диагоналей k -суппорта $[j_1, j_2, \dots, j_k]$ определим свойства $A_1, A_2, \dots, A_k$: свойство A_i означает, что 2^{m-1} -диагональ не содержит клеток с весом u_{j_i} . Весовой дефицит 2^{m-1} -диагонали равен r тогда и только тогда, когда она обладает ровно $k - (2^{m-1} - r)$ свойствами из набора $A_1, A_2, \dots, A_k$. Для любого $l = k - (2^{m-1} - r), k - (2^{m-1} - r) + 1, \dots, k$ и любого набора номеров $1 \leq \nu_1 < \nu_2 < \dots < \nu_l \leq k$ многочлен, перечисляющий 2^{m-1} -диагонали, обладающие свойствами $A_{\nu_1}, A_{\nu_2}, \dots, A_{\nu_l}$, есть

$$M[j_{\mu_1}, j_{\mu_2}, \dots, j_{\mu_{k-l}}],$$

где набор номеров $1 \leq \mu_1 < \mu_2 < \dots < \mu_{k-l} \leq k$ определяется условием

$$\{\mu_1, \mu_2, \dots, \mu_{k-l}\} \cup \{\nu_1, \nu_2, \dots, \nu_l\} = \{1, 2, \dots, k\}.$$

Из общей формулы включения-исключения следует равенство

$$\begin{aligned} M_r[j_1, j_2, \dots, j_k] &= \\ &= \sum_{l=k-(2^{m-1}-r)}^{k-1} (-1)^{l-k+2^{m-1}+r} \binom{l}{k-(2^{m-1}-r)} \sum_{1 \leq \nu_1 < \dots < \nu_l \leq k} M(j_{\mu_1}, \dots, j_{\mu_{k-l}}) = \\ &= \sum_{l=k-(2^{m-1}-r)}^{k-1} (-1)^{l-k+r} \binom{l}{k-(2^{m-1}-r)} \sum_{1 \leq \mu_1 < \dots < \mu_{k-l} \leq k} M(j_{\mu_1}, \dots, j_{\mu_{k-l}}). \end{aligned} \quad (7)$$

Сделаем в сумме (7) замену переменного $t = k - l$. Используя тот факт, что числа $(-t + r)$ и $(r + t)$ одинаковой четности, получим равенство (6). $\square$

Из теоремы 1 в качестве частных случаев получаем следующие формулы.

Теорема 2. (1) Для любого $r = 0, 1, \dots, 2^{m-1} - 1$ и любого $(2^{m-1} - r)$ -суппорта $[j_1, j_2, \dots, j_{2^{m-1}-r}]$ многочлен, который перечисляет трансверсали серий данного $(2^{m-1} - r)$ -суппорта, имеет вид

$$\begin{aligned} M_r [j_1, j_2, \dots, j_{2^{m-1}-r}] &= \\ &= \sum_{t=1}^{2^{m-1}-r} (-1)^{r+t} \sum_{1 \leq \mu_1 < \mu_2 < \dots < \mu_t \leq 2^{m-1}-r} M [j_{\mu_1}, j_{\mu_2}, \dots, j_{\mu_t}]. \end{aligned} \quad (8)$$

(2) Для многочлена, перечисляющего разнovesные 2^{m-1} -диагонали любого заданного 2^{m-1} -суппорта $[j_1, j_2, \dots, j_{2^{m-1}}]$, справедлива формула

$$\begin{aligned} M_0 [j_1, j_2, \dots, j_{2^{m-1}}] &= \\ &= \sum_{t=1}^{2^{m-1}} (-1)^t \sum_{1 \leq \mu_1 < \mu_2 < \dots < \mu_t \leq 2^{m-1}} M [j_{\mu_1}, j_{\mu_2}, \dots, j_{\mu_t}]. \end{aligned} \quad (9)$$

(3) Многочлен, который перечисляет разнovesные 2^{m-1} -диагонали латинского треугольника группы E_{2^m} , выражается формулой

$$\begin{aligned} M_0 [1, 2, \dots, 2^m - 1] &= \\ &= \sum_{t=1}^{2^{m-1}} (-1)^t \binom{2^m - t - 1}{2^{m-1} - 1} \sum_{1 \leq \mu_1 < \mu_2 < \dots < \mu_t \leq 2^m - 1} M [\mu_1, \mu_2, \dots, \mu_t]. \end{aligned} \quad (10)$$

Приведем аналогичные формулы для перечисления инволюций. В случае когда d — сильная 2^{m-1} -диагональ, моному (5) естественным образом соответствует инволюция на группе E_{2^m} с двоичными циклами $(u_{a_1}, u_{b_1}), (u_{a_2}, u_{b_2}), \dots, (u_{a_{2^{m-1}-1}}, u_{b_{2^{m-1}-1}})$. Эту инволюцию будем отождествлять с мономом (5), определяемым сильной 2^{m-1} -диагональю d .

Для произвольного $k = 1, 2, \dots, 2^m - 1$ и любого набора индексов $1 \leq j_1 < j_2 < \dots < j_k \leq 2^m - 1$ обозначим через

$$M^{(s)} [j_1, j_2, \dots, j_k]$$

многочлен, перечисляющий инволюции, у которых веса двоичных циклов содержатся в множестве $\{u_{j_1}, u_{j_2}, \dots, u_{j_k}\}$.

Для любого $r = 0, 1, \dots, 2^{m-1} - 1$, любого $k = 2^{m-1} - r, \dots, 2^m - 1$ и любого k -суппорта $[j_1, j_2, \dots, j_k]$ обозначим через

$$M_r^{(s)} [j_1, j_2, \dots, j_k]$$

многочлен, перечисляющий инволюции с весовым дефицитом r , у которых веса двоичных циклов содержатся в множестве $\{u_{j_1}, u_{j_2}, \dots, u_{j_k}\}$.

Аналогично теоремам 1, 2 можно доказать следующие теоремы.

Теорема 1'. Для любого $r = 0, 1, \dots, 2^{m-1} - 1$, любого $k = 2^{m-1} - r, \dots, 2^m - 1$ и любого k -суппорта $[j_1, j_2, \dots, j_k]$ имеет место формула

$$\begin{aligned} & M_r^{(s)} [j_1, j_2, \dots, j_k] = \\ & = \sum_{t=1}^{2^{m-1}-r} (-1)^{r+t} \binom{k-t}{k-2^{m-1}+r} \sum_{1 \leq \mu_1 < \mu_2 < \dots < \mu_t \leq k} M^{(s)} [j_{\mu_1}, j_{\mu_2}, \dots, j_{\mu_t}]. \end{aligned} \quad (11)$$

Теорема 2'. (1) Для любого $r = 0, 1, \dots, 2^{m-1} - 1$ и любого $(2^{m-1} - r)$ -суппорта $[j_1, j_2, \dots, j_{2^{m-1}-r}]$ многочлен, перечисляющий инволюции, у которых множество весов двоичных циклов совпадает с множеством $\{u_{j_1}, u_{j_2}, \dots, u_{j_{2^{m-1}-r}}\}$, имеет вид

$$\begin{aligned} & M_r^{(s)} [j_1, j_2, \dots, j_{2^{m-1}-r}] = \\ & = \sum_{t=1}^{2^{m-1}-r} (-1)^{r+t} \sum_{1 \leq \mu_1 < \mu_2 < \dots < \mu_t \leq 2^{m-1}-r} M^{(s)} [j_{\mu_1}, j_{\mu_2}, \dots, j_{\mu_t}]. \end{aligned} \quad (12)$$

(2) Для многочлена, который перечисляет разнovesные инволюции с заданными попарно различными весами двоичных циклов $u_{j_1}, u_{j_2}, \dots, u_{j_{2^m-1}}$, справедлива формула

$$\begin{aligned} & M_0^{(s)} [j_1, j_2, \dots, j_{2^m-1}] = \\ & = \sum_{t=1}^{2^m-1} (-1)^t \sum_{1 \leq \mu_1 < \mu_2 < \dots < \mu_t \leq 2^m-1} M^{(s)} [j_{\mu_1}, j_{\mu_2}, \dots, j_{\mu_t}]. \end{aligned} \quad (13)$$

(3) Для многочлена, который перечисляет разнovesные инволюции на группе E_{2^m} , справедлива формула

$$\begin{aligned} M_0^{(s)} [1, 2, \dots, 2^m - 1] = \\ = \sum_{t=1}^{2^m-1} (-1)^t \binom{2^m - t - 1}{2^{m-1} - 1} \sum_{1 \leq \mu_1 < \mu_2 < \dots < \mu_t \leq 2^m-1} M^{(s)} [\mu_1, \mu_2, \dots, \mu_t]. \end{aligned} \quad (14)$$

Из приведенных теорем в качестве следствий получим формулы для числа 2^{m-1} -диагоналей (инволюций) с заданными весовыми характеристиками. Число 2^{m-1} -диагоналей (инволюций) в зависимости от весовых ограничений будем обозначать буквой N с соответствующими индексами. В частности, $N[j_1, j_2, \dots, j_k]$ есть число 2^{m-1} -диагоналей k -суппорта $[j_1, j_2, \dots, j_k]$. Аналогично, $N^{(s)}[j_1, j_2, \dots, j_k]$ есть число инволюций, у которых веса двоичных циклов содержатся в множестве $\{u_{j_1}, u_{j_2}, \dots, u_{j_k}\}$.

Предположим, что многочлен M перечисляет диагонали из некоторого множества D . В этом случае значение многочлена M при условии, что все переменные (u_a, u_b) , $0 \leq a < b \leq 2^m - 1$, принимают значение единица, равно числу мономов, входящих в многочлен M с ненулевым (т.е. единичным) коэффициентом. Это же число совпадает с числом элементов множества D . Из данного свойства и приведенных выше теорем получаем следствия.

Следствие 1. Для любых $r = 0, 1, \dots, 2^{m-1} - 1$, $k = 2^{m-1} - r, \dots, 2^m - 1$ и любого k -суппорта $[j_1, j_2, \dots, j_k]$ число 2^{m-1} -диагоналей этого суппорта, имеющих весовой дефицит r , выражается формулой

$$\begin{aligned} N_r[j_1, j_2, \dots, j_k] = \\ = \sum_{t=1}^{2^{m-1}-r} (-1)^{r+t} \binom{k-t}{k-2^{m-1}+r} \sum_{1 \leq \mu_1 < \mu_2 < \dots < \mu_t \leq k} N[j_{\mu_1}, j_{\mu_2}, \dots, j_{\mu_t}]. \end{aligned}$$

Следствие 2. (1) Для любого $r = 0, 1, \dots, 2^{m-1} - 1$ число трансверсалей серий любого заданного $(2^{m-1} - r)$ -суппорта $[j_1, j_2, \dots, j_{2^{m-1}-r}]$ выражается формулой

$$\begin{aligned} N_r[j_1, j_2, \dots, j_{2^{m-1}-r}] = \\ = \sum_{t=1}^{2^{m-1}-r} (-1)^{r+t} \sum_{1 \leq \mu_1 < \mu_2 < \dots < \mu_t \leq 2^{m-1}-r} N[j_{\mu_1}, j_{\mu_2}, \dots, j_{\mu_t}]. \end{aligned}$$

(2) Для числа разнovesных 2^{m-1} -диагоналей любого заданного 2^{m-1} -суппорта $[j_1, j_2, \dots, j_{2^{m-1}}]$ справедлива формула

$$\begin{aligned} N_0[j_1, j_2, \dots, j_{2^{m-1}}] &= \\ &= \sum_{t=1}^{2^{m-1}} (-1)^t \sum_{1 \leq \mu_1 < \mu_2 < \dots < \mu_t \leq 2^{m-1}} N[j_{\mu_1}, j_{\mu_2}, \dots, j_{\mu_t}]. \end{aligned}$$

(3) Для числа разнovesных 2^m -диагоналей латинского треугольника группы E_{2^m} имеет место формула

$$\begin{aligned} N_0[1, 2, \dots, 2^m - 1] &= \\ &= \sum_{t=1}^{2^{m-1}} (-1)^t \binom{2^m - t - 1}{2^{m-1} - 1} \sum_{1 \leq \mu_1 < \mu_2 < \dots < \mu_t \leq 2^m - 1} N[\mu_1, \mu_2, \dots, \mu_t]. \end{aligned}$$

Следствие 1'. Для любого $r = 0, 1, \dots, 2^{m-1} - 1$, любого $k = 2^{m-1} - r, \dots, 2^m - 1$ и любого k -суппорта $[j_1, j_2, \dots, j_k]$ число инволюций с весовым дефицитом r , у которых веса двоичных циклов содержатся в множестве $\{u_{j_1}, u_{j_2}, \dots, u_{j_k}\}$, определяется формулой

$$\begin{aligned} N_r^{(s)}[j_1, j_2, \dots, j_k] &= \\ &= \sum_{t=1}^{2^{m-1}-r} (-1)^{r+t} \binom{k-t}{k-2^{m-1}+r} \sum_{1 \leq \mu_1 < \mu_2 < \dots < \mu_t \leq k} N^{(s)}[j_{\mu_1}, j_{\mu_2}, \dots, j_{\mu_t}]. \end{aligned}$$

Следствие 2'. (1) Для любого $r = 0, 1, \dots, 2^{m-1} - 1$ число инволюций, у которых множество весов двоичных циклов совпадает с заданным множеством попарно различных элементов $\{u_{j_1}, u_{j_2}, \dots, u_{j_{2^{m-1}-r}}\}$, выражается формулой

$$\begin{aligned} N_r^{(s)}[j_1, j_2, \dots, j_{2^{m-1}-r}] &= \\ &= \sum_{t=1}^{2^{m-1}-r} (-1)^{r+t} \sum_{1 \leq \mu_1 < \mu_2 < \dots < \mu_t \leq 2^{m-1}-r} N^{(s)}[j_{\mu_1}, j_{\mu_2}, \dots, j_{\mu_t}]. \end{aligned}$$

(2) Для числа разнovesных инволюций, у которых веса двоичных циклов образуют множество $\{u_{j_1}, u_{j_2}, \dots, u_{j_{2^m-1}}\}$, справедлива формула

$$N_0^{(s)}[j_1, j_2, \dots, j_{2^m-1}] = \sum_{t=1}^{2^m-1} (-1)^t \sum_{1 \leq \mu_1 < \mu_2 < \dots < \mu_t \leq 2^m-1} N^{(s)}[j_{\mu_1}, j_{\mu_2}, \dots, j_{\mu_t}].$$

(3) Для числа разнovesных инволюций на группе E_{2^m} имеет место формула

$$N_0^{(s)}[1, 2, \dots, 2^m - 1] = \sum_{t=1}^{2^m-1} (-1)^t \binom{2^m - t - 1}{2^{m-1} - 1} \sum_{1 \leq \mu_1 < \mu_2 < \dots < \mu_t \leq 2^m-1} N^{(s)}[\mu_1, \mu_2, \dots, \mu_t].$$

3. Случай суппорта, определяемого аффинной гиперплоскостью

В этом разделе более подробно рассмотрим следующий частный случай 2^{m-1} -суппорта. Зафиксируем произвольное подпространство W векторного пространства E_{2^m} размерности $m - 1$. Множество $E_{2^m} \setminus W$ будем называть аффинной гиперплоскостью. Будем использовать следующую нумерацию элементов группы $E_{2^m} = \{u_0, u_1, \dots, u_{2^{m-1}-1}, u_{2^{m-1}}, \dots, u_{2^m-1}\}$. Полагаем u_0 равным нулевому вектору. Далее выбираем произвольный вектор $u_1 \in W \setminus \{u_0\}$ и фиксируем произвольную нумерацию элементов подпространства $W = \{u_0, u_1, \dots, u_{2^{m-1}-1}\}$, удовлетворяющую соотношению

$$u_{2i+1} = u_{2i} + u_1, \quad i = 0, 1, \dots, 2^{m-2} - 1. \quad (15)$$

Затем выбираем произвольный вектор $u_{2^{m-1}} \in E_{2^m} \setminus W$ и определяем нумерацию элементов аффинной гиперплоскости $E_{2^m} \setminus W = \{u_{2^{m-1}}, u_{2^{m-1}+1}, \dots, u_{2^m-1}\}$ соотношением

$$u_{2^{m-1}+i} = u_i + u_{2^{m-1}}, \quad i = 0, 1, \dots, 2^{m-1} - 1. \quad (16)$$

Теперь с учетом данного выбора нумерации рассмотрим суппорт $[2^{m-1}, 2^{m-1} + 1, \dots, 2^m - 1]$. Нетрудно проверить, что этот суппорт как совокупность клеток латинского треугольника таблицы Кэли группы E_{2^m} представляет собой квадратную подматрицу R таблицы Кэли порядка 2^{m-1} в первых 2^{m-1} строках (с номерами $0, 1, \dots, 2^{m-1} - 1$) и в последних 2^{m-1} столбцах (с номерами $2^{m-1}, 2^{m-1} + 1, \dots, 2^m - 1$).

Можно считать, что строки матрицы R занумерованы векторами пространства $W = \{u_0, u_1, \dots, u_{2^{m-1}-1}\}$. Присвоим столбцу матрицы R с номером u_j , где $u_j \in E_{2^m} \setminus W$, $j = 2^{m-1} + i$, $i \in \{0, 1, \dots, 2^{m-1} - 1\}$, новый номер u_i , где теперь $u_i \in W$.

Обозначим через J целочисленную квадратную матрицу порядка 2^{m-1} , все элементы которой равны единице. Матрица $u_{2^{m-1}} \cdot J$ есть квадратная матрица порядка 2^{m-1} , все элементы которой равны $u_{2^{m-1}}$. Из соотношения (16) следует, что с учетом новой нумерации строк и столбцов матрица $R + u_{2^{m-1}} \cdot J$ будет совпадать с таблицей Кэли аддитивной группы пространства W . Для любого $i = 0, 1, \dots, 2^{m-1} - 1$ обозначим через Π_i подстановочную $(0, 1)$ -матрицу порядка 2^{m-1} , соответствующую трансляции группы W

$$\pi_i(u_k) = u_k + u_i, \quad k = 0, 1, \dots, 2^{m-1} - 1. \quad (17)$$

Имеем равенство

$$R = u_{2^{m-1}} \cdot J + \sum_{i=0}^{2^{m-1}-1} u_i \cdot \Pi_i. \quad (18)$$

Далее, 2^{m-1} -диагонали суппорта $[2^{m-1}, 2^{m-1} + 1, \dots, 2^m - 1]$, определенные выше, являются диагоналями матрицы R (т.е. каждая диагональ суппорта есть последовательность из 2^{m-1} попарно неколлинеарных клеток матрицы). Таким образом, всего имеем $(2^{m-1})!$ диагоналей суппорта $[2^{m-1}, 2^{m-1} + 1, \dots, 2^m - 1]$ (матрицы R).

Так как множества номеров строк и номеров столбцов клеток суппорта не пересекаются, то любая его диагональ является сильной. Поэтому выполнено равенство

$$M^{(s)}[2^{m-1}, 2^{m-1} + 1, \dots, 2^{m-1} - 1] = M[2^{m-1}, 2^{m-1} + 1, \dots, 2^{m-1} - 1].$$

Таким образом, в данном случае перечисление диагоналей подматрицы R влечет перечисление соответствующих инволюций.

Для любых $i = 0, 1, \dots, 2^{m-1} - 1$, $j = 2^{m-1}, 2^{m-1} + 1, \dots, 2^{m-1} - 1$ заменим в клетке $v(u_i, u_j)$ подматрицы R (в исходной нумерации строк и столбцов) элемент $u_i + u_j$ упорядоченной парой (u_i, u_j) . В результате получим квадратную матрицу C порядка 2^{m-1} , элементами которой являются введенные в разделе 2 формальные переменные (u_i, u_j) , $i = 0, 1, \dots, 2^{m-1} - 1$, $j = 2^{m-1}, 2^{m-1} + 1, \dots, 2^{m-1} - 1$. Матрицу C можно рассматривать как квадратную матрицу над кольцом многочленов от многих переменных с целыми коэффициентами, и для нее стандартным образом определяется перманент $\text{per } C$.

При этом имеет место равенство

$$\text{per } C = M [2^{m-1}, 2^{m-1} + 1, \dots, 2^{m-1} - 1]. \quad (19)$$

Для произвольного $t = 1, 2, \dots, 2^{m-1}$ и любого набора индексов $2^{m-1} \leq \mu_1 < \mu_2 < \dots < \mu_t \leq 2^m - 1$ обозначим через

$$C(\mu_1, \mu_2, \dots, \mu_t)$$

квадратную матрицу порядка 2^{m-1} , полученную из матрицы C заменой всех элементов (u_i, u_j) , для которых $u_i + u_j \notin \{u_{\mu_1}, u_{\mu_2}, \dots, u_{\mu_t}\}$, целым числом 0. В этих обозначениях имеет место равенство

$$\text{per } C(\mu_1, \mu_2, \dots, \mu_t) = M[\mu_1, \mu_2, \dots, \mu_t].$$

В качестве частного случая теоремы 1 получим следующее утверждение.

Теорема 3. Для любого $r = 0, 1, \dots, 2^{m-1} - 1$ многочлен, который перечисляет инволюции, имеющие весовой дефицит r и веса двоичных циклов из множества $E_{2^m} \setminus W$, имеет вид

$$\begin{aligned} M_r[E_{2^m} \setminus W] &= \\ &= \sum_{t=1}^{2^{m-1}-r} (-1)^{r+t} \binom{2^{m-1}-t}{r} \sum_{2^{m-1} \leq \mu_1 < \mu_2 < \dots < \mu_t \leq 2^m-1} \text{per } C(\mu_1, \mu_2, \dots, \mu_t). \end{aligned} \quad (20)$$

Используя соотношение (18), аналогично следствиям 1, 2, 1', 2' в качестве следствия теоремы 3 получаем формулу для числа $N_r[E_{2^m} \setminus W]$ инволюций, имеющих весовой дефицит $r = 0, 1, \dots, 2^{m-1} - 1$ и веса двоичных циклов из множества $E_{2^m} \setminus W$.

Следствие 3. Формула для числа инволюций, имеющих весовой дефицит $r = 0, 1, \dots, 2^{m-1} - 1$ и веса двоичных циклов из множества $E_{2^m} \setminus W$ имеет вид

$$\begin{aligned} N_r[E_{2^m} \setminus W] &= \\ &= \sum_{t=r}^{2^{m-1}-1} (-1)^{r+t} \binom{t}{r} \sum_{0 \leq \mu_1 < \mu_2 < \dots < \mu_t \leq 2^{m-1}-1} \text{per}(J - \Pi_{\mu_1} - \Pi_{\mu_2} - \dots - \Pi_{\mu_t}). \end{aligned} \quad (21)$$

В частности, количество $N_0[E_{2^m} \setminus W]$ разнovesных инволюций, имеющих веса двоичных циклов из множества $E_{2^m} \setminus W$, определяется выражением

$$\sum_{t=0}^{2^{m-1}-1} (-1)^t \sum_{0 \leq \mu_1 < \mu_2 < \dots < \mu_t \leq 2^{m-1}-1} \text{per}(J - \Pi_{\mu_1} - \Pi_{\mu_2} - \dots - \Pi_{\mu_t}). \quad (22)$$

Доказательство. Для доказательства формулы (21) приравняем единице все входящие в левую и правую части равенства (20) переменные вида (u_i, u_j) . Заметим также, что тогда для любых $t = 1, 2, \dots, 2^{m-1}$ и

$$2^{m-1} \leq \mu_1 < \mu_2 < \dots < \mu_t \leq 2^m - 1$$

матрица, получаемая из матрицы $C(\mu_1, \mu_2, \dots, \mu_t)$, будет совпадать с матрицей

$$\Pi_{\mu_1-2^{m-1}} + \Pi_{\mu_2-2^{m-1}} + \dots + \Pi_{\mu_t-2^{m-1}} = J - \Pi_{\nu_1} - \Pi_{\nu_2} - \dots - \Pi_{\nu_{2^{m-1}-t}},$$

где набор $0 \leq \nu_1 < \nu_2 < \dots < \nu_{2^{m-1}-t} \leq 2^{m-1} - 1$ определяется равенством

$$\begin{aligned} \{2^{m-1} + \nu_1, 2^{m-1} + \nu_2, \dots, 2^{m-1} + \nu_{2^{m-1}-t}\} \cup \{\mu_1, \mu_2, \dots, \mu_t\} = \\ = \{2^{m-1}, \dots, 2^m - 1\}. \end{aligned}$$

Следовательно,

$$\begin{aligned} N_r[E_{2^m} \setminus W] &= \sum_{t=1}^{2^{m-1}-r} (-1)^{r+t} \binom{2^{m-1}-t}{r} \times \\ &\times \sum_{0 \leq \nu_1 < \dots < \nu_{2^{m-1}-t} \leq 2^{m-1}-1} \text{per}(J - \Pi_{\nu_1} - \dots - \Pi_{\nu_{2^{m-1}-t}}). \end{aligned} \quad (23)$$

Заменив переменную суммирования во внешней сумме в правой части равенства (23), получим равенство (21). $\square$

На множестве всех $(2^{m-1})!$ инволюций, имеющих веса двоичных циклов из множества $E_{2^m} \setminus W$, зададим равномерное вероятностное распределение. Рассмотрим случайную величину η_m , равную весовому дефициту случайной равновероятной инволюции из указанного множества. Формулу для ее распределения получаем из следствия 3: при любом $r = 0, 1, \dots, 2^{m-1} - 1$

$$\mathbf{P}(\eta_m = r) = \frac{1}{(2^{m-1})!} N_r[E_{2^m} \setminus W] = \quad (24)$$

$$= \sum_{t=r}^{2^{m-1}-1} \frac{(-1)^{r+t}}{(2^{m-1})!} \binom{t}{r} \sum_{0 \leq \mu_1 < \mu_2 < \dots < \mu_t \leq 2^{m-1}-1} \text{per}(J - \Pi_{\mu_1} - \Pi_{\mu_2} - \dots - \Pi_{\mu_t}).$$

Для любого $s = 1, \dots, 2^{m-1} - 1$ обозначим через $B_{s,m}$ биномиальный момент порядка s случайной величины η_m . Из формул обращения в методе включения-исключения (см., например, [2]) следует, что для любого $s = 1, \dots, 2^{m-1} - 1$

$$B_{s,m} = \frac{1}{(2^{m-1})!} \sum_{0 \leq \mu_1 < \mu_2 < \dots < \mu_s \leq 2^{m-1} - 1} \text{per}(J - \Pi_{\mu_1} - \Pi_{\mu_2} - \dots - \Pi_{\mu_s}). \quad (25)$$

При $s = 1$ из равенства (25) следует формула для математического ожидания $M\eta_m$ случайной величины η_m . Для любого $0 \leq \mu \leq 2^{m-1} - 1$ величина $\text{per}(J - \Pi_{\mu})$ совпадает с числом подстановок на группе W , противоречивых с трансляцией π_{μ} (см. (17)), т. е.

$$\text{per}(J - \Pi_{\mu}) = (2^{m-1})! \sum_{\nu=1}^{2^{m-1}} \frac{(-1)^{\nu}}{\nu!}.$$

Таким образом, из (25) получим формулу

$$M\eta_m = 2^{m-1} \sum_{\nu=1}^{2^{m-1}} \frac{(-1)^{\nu}}{\nu!}.$$

Если $m \rightarrow +\infty$, то

$$M\eta_m = 2^{m-1} e^{-1} \left(1 + O\left(\frac{1}{(2^{m-1} + 1)!}\right) \right). \quad (26)$$

Для дисперсии случайной величины η_m имеем равенство

$$D\eta_m = 2B_{2,m} + M\eta_m - (M\eta_m)^2. \quad (27)$$

Проведем оценку величины $B_{2,m}$. Для любых $0 \leq \mu_1 < \mu_2 \leq 2^{m-1} - 1$ величина $\text{per}(J - \Pi_{\mu_1} - \Pi_{\mu_2})$ равна числу подстановок элементов группы W , противоречивых с трансляциями π_{μ_1}, π_{μ_2} . Согласно [4], последняя величина зависит только от цикловой структуры подстановки $\pi_{\mu_1}^{-1} \cdot \pi_{\mu_2} = \pi_{\nu}$, где индекс ν определяется из условия $u_{\nu} = u_{\mu_1} + u_{\mu_2}$. Так как $\mu_1 < \mu_2$, то $\nu > 0$. Таким образом, трансляция π_{ν} имеет 2^{m-2} циклов длины 2.

Итак, в сумме из правой части равенства (25) при $s = 2$ слагаемые одинаковы и

$$B_{2,m} = \frac{2^{m-1} (2^{m-1} - 1)}{2} \cdot \frac{\text{per}(J - \Pi_0 - \Pi_1)}{(2^{m-1})!}. \quad (28)$$

Согласно нумерации (15) элементов группы W матрица $\Pi_0 + \Pi_1$ есть квадратная блочно-диагональная матрица порядка 2^{m-1} , на диагонали которой расположено 2^{m-2} квадратных блоков порядка 2, каждый блок состоит из единиц. Для оценки величины $\text{per}(J - \Pi_0 - \Pi_1)$ можно воспользоваться результатами, приведенными в [4, с. 210–211, пример 7]. Частным случаем этих результатов является следующее асимптотическое равенство при $m \rightarrow \infty$:

$$\text{per}(J - \Pi_0 - \Pi_1) = (2^{m-1})! e^{-2} \left[1 - \frac{1}{2^{m-1} - 1} + O\left(\frac{1}{2^{2m}}\right) \right]. \quad (29)$$

Из соотношений (27), (26), (28) и (29) получаем асимптотическую оценку для дисперсии при $m \rightarrow \infty$:

$$D\eta_m \sim 2^{m-1} \frac{e - 2}{e^2}.$$

Отметим, что главные члены в асимптотических оценках среднего и дисперсии случайных величин η_m совпадают с соответствующими главными членами в асимптотических оценках среднего и дисперсии дефицита случайной равновероятной подстановки степени $\sim 2^{m-1}$ (см. [3]).

4. Число диагоналей латинского треугольника и алгоритм построения разнovesных инволюций

Аналогично понятию 2^{m-1} -диагонали k -диагональю ($k = 1, 2, \dots, 2^m - 1$) латинского треугольника таблицы Кэли группы E_{2^m} назовем последовательность из k попарно не коллинеарных клеток

$$d = v(u_{a_1}, u_{b_1}), v(u_{a_2}, u_{b_2}), \dots, v(u_{a_k}, u_{b_k}), \quad a_i < b_i, \quad i = 1, 2, \dots, k,$$

удовлетворяющую условию $a_1 < a_2 < \dots < a_k$.

Теорема 4. Для любого $k = 1, 2, \dots, 2^m - 1$ число $(2^m - k)$ -диагоналей латинского треугольника таблицы Кэли группы E_{2^m} равно числу Стирлинга второго рода $\sigma(2^m, k)$:

$$\sigma(2^m, k) = \frac{1}{k!} \sum_{j=0}^k (-1)^j \binom{k}{j} (k-j)^{2^m}.$$

В частности, число (2^{m-1}) -диагоналей латинского треугольника таблицы Кэли группы E_{2^m} равно $\sigma(2^m, 2^{m-1})$.

Доказательство. Используем результаты Риордана и Капланского по теории ладейных многочленов [4]. Ладейные многочлены являются производящими функциями чисел диагоналей некоторых матриц, соответствующих обобщенным шахматным доскам. Совокупность клеток латинского треугольника таблицы Кэли группы E_{2^m} является равнобедренным прямоугольным треугольником с катетом из $2^m - 1$ элементов.

В общем случае обозначим через $T_q(x)$ производящую функцию чисел всех диагоналей равнобедренного прямоугольного треугольника с катетом из q элементов, а через $T_{2,q}(x)$ — соответствующую производящую функцию чисел диагоналей прямоугольной трапеции, полученной из прямоугольного треугольника удалением элемента на пересечении одного катета и гипотенузы. Из разложения по удаленному элементу имеем соотношение

$$T_{2,q}(x) = T_{q+1}(x) - x T_q(x).$$

Разлагая $T_{2,q}(x)$ по числу элементов диагоналей на наклонной боковой стороне трапеции, получаем

$$T_{2,q}(x) = \sum_{k=0}^q \binom{q}{k} x^k T_{q-k}(x).$$

Рассмотрим производящую функцию для последовательности $\{T_q(x)\}_{q=0}^{\infty}$:

$$T(x, y) = \sum_{q=0}^{\infty} T_q(x) \frac{y^q}{q!}.$$

Для частной производной $T_q(x, y)$ по y имеем уравнение

$$T'_y(x, y) = (x + e^{xy}) T(x, y)$$

при начальных условиях

$$T(x, 0) = T_0(x) = 1.$$

Это уравнение имеет решение

$$T(x, y) = \exp \left\{ xy + \frac{1}{x} (e^{xy} - 1) \right\}.$$

Отсюда следует, что

$$e^{-xy} T(x, y) = \sum_{k=1}^{\infty} \frac{(e^{xy} - 1)^k}{x^k k!} = \sum_{q=0}^{\infty} \frac{y^q}{q!} \sum_{k=0}^q \sigma(q, k) x^{q-k}.$$

С другой стороны,

$$e^{-xy}T(x, y) = \sum_{q=0}^{\infty} \frac{y^q}{q!} \sum_{k=0}^q (-1)^k \binom{q}{k} x^k T_{q-k}(x).$$

Следовательно, для любого $q \geq 1$

$$\sum_{k=0}^q (-1)^k \binom{q}{k} x^k T_{q-k}(x) = \sum_{k=0}^q \sigma(q, k) x^{q-k}. \quad (30)$$

Из соотношения

$$\sum_{q=0}^{\infty} T_q(x) \frac{y^q}{q!} = \sum_{q=0}^{\infty} \frac{y^q}{q!} \sum_{k=0}^{q+1} (-1)^k \binom{q+1}{k} x^k T_{q+1-k}(x)$$

следует, что

$$T_q(x) = \sum_{k=0}^{q+1} (-1)^k \binom{q+1}{k} x^k T_{q+1-k}(x).$$

Отсюда и из равенства (30) имеем

$$T_q(x) = \sum_{k=0}^{q+1} \sigma(q+1, q+1-k) x^k.$$

Теорема доказана. $\square$

Число Стирлинга второго рода $\sigma(2^m, 2^{m-1})$ определяет количество разбиений множества из 2^m элементов на 2^{m-1} блоков. В это множество разбиений входят все разбиения на 2^{m-1} блоков, каждый из которых содержит два элемента. Таким разбиениям соответствуют инволюции с 2^{m-1} циклами длины два.

Таким образом, если установить биекцию между всеми 2^{m-1} -диагоналями латинского треугольника и разбиениями множества из 2^m элементов на 2^{m-1} блоков, то сильным диагоналям будут соответствовать разбиения на 2^{m-1} блоков, каждый из которых содержит два элемента, т. е. инволюции с 2^{m-1} циклами длины два. Число таких разбиений равно

$$R(2^m, 2^{m-1}) = \frac{(2^m)!}{2^{2^{m-1}} (2^{m-1})!}.$$

Следовательно, среди всех $\sigma(2^m, 2^{m-1})$ диагоналей латинского треугольника имеется $R(2^m, 2^{m-1})$ сильных диагоналей.

Поэтому вероятность того, что случайная равновероятная 2^{m-1} -диагональ латинского треугольника является сильной, равна

$$P_m = \frac{(2^m)!}{2^{2^{m-1}} (2^{m-1})! \sigma(2^m, 2^{m-1})} = \frac{(2^m)!}{2^{2^{m-1}}} \frac{1}{\sum_{j=0}^{2^{m-1}} (-1)^j \binom{2^{m-1}}{j} (2^{m-1} - j)^{2^m}}. \quad (31)$$

Для чисел Стирлинга $\sigma(n, r)$ имеет место следующая асимптотическая оценка (см. [5, с. 169]). Если

$$r < \frac{(n+1)^{\frac{2}{3}}}{\pi + (n+1)^{-\frac{1}{3}}},$$

то

$$\sigma(n, r) = \frac{1}{r!} (e^u - 1)^r \left(\frac{n}{eu} \right)^n \left(1 - \frac{u}{e^u - 1} \right)^{-\frac{1}{2}} (1 + o(1)), \quad n \rightarrow \infty. \quad (32)$$

В соотношении (32) число u — корень некоторого трансцендентного уравнения, для которого имеет место двусторонняя оценка

$$\frac{n+1}{r} - 1 < u < \frac{n+1}{r}.$$

Используя оценку (32) в (31), получим, что для некоторого $1 < u < 2$ при $m \rightarrow \infty$

$$P_m = \sqrt{\pi 2^{m+1}} \left(1 - \frac{u}{e^u - 1} \right) \left(\frac{u^2}{2(e^u - 1)} \right)^{2^{m-1}} (1 + o(1)). \quad (33)$$

Из (33) следует, что при $m \rightarrow \infty$ вероятность $P_m \rightarrow 0$.

С использованием метода включения-исключения в теореме 2 был предложен перечислительный алгоритм построения разнovesных 2^{m-1} -диагоналей латинского треугольника, в частности трансверсалей серий для различных 2^{m-1} -суппортов. Алгоритм рассмотрен в частном случае 2^{m-1} -суппорта $[2^{m-1}, 2^{m-1} + 1, \dots, 2^m - 1]$ (теорема 3), когда все трансверсали соответствуют сильным диагоналям, и, следовательно, алгоритм позволяет одновременно строить разнovesные инволюции.

Этот же алгоритм может быть применен и в общем случае для построения трансверсалий серий суппортов и латинского треугольника в целом. Однако в результате применения алгоритма могут быть получены трансверсали, являющиеся слабыми диагоналями. Поэтому для получения сильных трансверсалий, соответствующих разновесным инволюциям, требуется дополнительный этап отбраковки слабых трансверсалий.

Алгоритм для перечисления разновесных инволюций состоит из двух этапов. На первом этапе формулой (9) определяется многочлен $M_0[j_1, j_2, \dots, j_{2^m-1}]$, перечисляющий мономы, соответствующие трансверсалиям серий произвольного 2^{m-1} -суппорта. Многочлен $M_0[1, 2, \dots, 2^m - 1]$, перечисляющий трансверсалии серий для всех возможных 2^{m-1} -суппортов (т. е. разновесные диагонали латинского треугольника таблицы Кэли группы E_{2^m}), определяется по формуле (10).

На втором этапе алгоритма применяется перебор с использованием памяти и устраняются мономы, соответствующие слабым трансверсалиям. Оставшиеся после второго этапа мономы соответствуют сильным трансверсалиям, определяющим разновесные инволюции.

Для любого заданного монома

$$(u_{a_1}, u_{b_1}) (u_{a_2}, u_{b_2}) \cdots (u_{a_{2^m-1}}, u_{b_{2^m-1}}) \quad (34)$$

рассмотрим последовательность $\{w_j\}_{j=1}^{2^m}$ элементов группы E_{2^m} , где для любого $j = 1, 2, \dots, 2^{m-1}$

$$w_{2j-1} = u_{a_j}, \quad w_{2j} = u_{b_j}.$$

Отметим, что моном (34) соответствует сильной трансверсали тогда и только тогда, когда все члены последовательности $\{w_j\}_{j=1}^{2^m}$ попарно различны. Это свойство мы используем следующим образом.

Будем использовать память на 2^m ячеек, занумерованных элементами группы E_{2^m} , содержимое каждой ячейки — либо 0, либо 1. Вначале присвоим всем ячейкам значение 0. Будем последовательно перебирать $j = 1, 2, \dots, 2^m$. Для каждого значения j обращаемся в память по адресу w_j . Если содержимое ячейки с адресом w_j равно 1, то трансверсаль (34) является слабой, алгоритм заканчивает свою работу. Если содержимое ячейки с адресом w_j равно 0, то заменяем значение данной ячейки на 1. Если $j = 2^m$, то трансверсаль (34) является сильной, алгоритм заканчивает свою работу. Если $j < 2^m - 1$, то переходим к следующему значению j .

При случайном независимом и равновероятном выборе диагоналей латинского треугольника рассмотрим случайную величину z , равную количеству шагов до получения сильной диагонали. Случайная величина z равна числу испытаний до первого успеха в схеме испытаний Бернулли, она имеет геометрическое распределение

$$P(z = k) = P_m (1 - P_m)^{k-1}, \quad k = 1, 2, \dots$$

Отсюда следует, что среднее число шагов на втором этапе алгоритма до первого получения сильной диагонали равно

$$Mz = \frac{1}{P_m} = \left(\pi 2^{m+1} \left(1 - \frac{u}{e^u - 1} \right) \right)^{-\frac{1}{2}} \left(\frac{2(e^u - 1)}{u^2} \right)^{2^{m-1}} (1 + o(1)), \quad m \rightarrow \infty.$$

Список литературы

- [1] Сачков В.Н., “Комбинаторные свойства дифференциально 2-равномерных подстановок”, *Математические вопросы криптографии*, **6:1** (2015), 159–180.
- [2] Сачков В.Н., *Курс комбинаторного анализа*, М.–Ижевск: НИЦ «Регулярная и хаотическая динамика», 2013, 336 pp.
- [3] Сачков В.Н., “Цепи Маркова итерационных систем преобразований”, *Труды по дискретной математике*, **6** (2002), 165–183.
- [4] Риордан Дж., *Введение в комбинаторный анализ*, М.: ИЛ, 1963, 287 pp.
- [5] Сачков В.Н., *Комбинаторные методы дискретной математики*, М.: Наука, 1977, 319 pp.