Math-Net.Ru

Общероссийский математический портал

В. Н. Сачков, Инволюции с данным весовым дефицитом, соответствующие таблице Кэли конечной абелевой группы, *Матем. вопр. криптогр.*, 2017, том 8, выпуск 4, 117–134

DOI: <https://doi.org/10.4213/mvk236>

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: 54.198.187.58

26 апреля 2023 г., 15:10:32

**Инволюции с данным весовым дефицитом,
соответствующие таблице Кэли
конечной абелевой группы**

В. Н. Сачков

Академия криптографии Российской Федерации, Москва

Получено 11.V.2017

Аннотация. Изучаются весовые характеристики инволюций над конечными абелевыми группами G_n порядка $n \geq 3$. Для случайной равновероятной инволюции найдено точное распределение числа ее двоичных циклов, совпадающих с двоичными циклами фиксированной инволюции, доказано, что при $n \rightarrow \infty$ это распределение сходится к распределению Пуассона с параметром $\lambda = \frac{1}{2}$. Найдено среднее значение дефицита случайной равновероятной инволюции.

Ключевые слова: инволюции над группами, таблица Кэли, весовой дефицит

Involutions with given weight deficit corresponding to the Cayley table of the finite Abelian group

V. N. Sachkov

Academy of Cryptography of the Russian Federation, Moscow

Abstract. We investigate the weight characteristics of involutions over finite Abelian groups G_n of order $n \geq 3$. For random equiprobable involution the distribution of the number of its binary cycles coinciding with binary cycles of fixed involution is found, the convergence of this distribution to the Poisson distribution with the parameter $\lambda = \frac{1}{2}$ as $n \rightarrow \infty$ is proved. Mean value of the deficit of random equiprobable convolution is computed.

Key words: involutions over groups, Cayley table, weight deficit

Citation: *Mathematical Aspects of Cryptography*, 2017, v. 8, № 4, pp. 117–134 (Russian)

© Академия криптографии Российской Федерации, 2017 г.

Введение

В работе продолжены начатые в [1, 2] исследования весовых характеристик инволюций над конечными абелевыми группами G_n порядка $n \geq 3$, включая аддитивную группу поля из $n = 2^m$ элементов и группу вычетов по модулю n относительно операции сложения. Изучение таких характеристик представляет интерес для оценивания криптографических качеств подстановок над абелевыми группами, определяющих S -боксы в блочных шифрах и преобразования в шифрах колонной замены. Эти качества характеризуются весовыми свойствами систем инволюций, соответствующих подстановкам.

Предлагается алгоритм построения инволюций над группой G_n , основанный на использовании понятия парной неколлинеарности элементов ее таблицы Кэли. Получены формулы для общего числа инволюций для четных и нечетных n .

Для серий одинаковых элементов таблицы Кэли определена система равновесных инволюций над группой G_n . Для случайной равновероятной инволюции J над группой G_n вводится случайная величина ξ_n , равная числу двоичных циклов J , совпадающих с двоичными циклами фиксированной инволюции из системы. Найдено точное распределение ξ_n и доказано, что при $n \rightarrow \infty$ это распределение сходится к распределению Пуассона с параметром $\lambda = \frac{1}{2}$.

Дано описание множества инволюций над группой G_n с заданным значением весового дефицита. При случайном равновероятном выборе инволюции найдено среднее значение ее дефицита, которое при $n \rightarrow \infty$ имеет порядок $n/\sqrt{e}$.

1. Инволюции, соответствующие таблице Кэли конечной абелевой группы

Рассмотрим две абелевы группы, представляющие интерес для криптографии: E_{2^m} — аддитивная группа поля из $n = 2^m$ элементов и C_n — аддитивная группа кольца вычетов из n элементов. Эти группы имеют специфику, которая будет отмечаться при изучении их свойств. Вместе с тем они обладают важными общими свойствами, при изучении которых будем рассматривать произвольную абелеву группу $(G_n, +)$ с множеством элементов $G_n = \{0, 1, \dots, n-1\}$ и нейтральным элементом 0 (нулевой элемент группы).

Рассмотрим таблицу Кэли группы G_n . Будем предполагать, что строки и столбцы таблицы Кэли группы G_n занумерованы ее элементами, т. е. числами $0, 1, \dots, n-1$. В клетке таблицы Кэли в строке с номером i и в столбце с номером j содержится элемент $i+j = a_{i,j}$ группы G_n (*вес клетки*). Таким образом, таблица Кэли группы G_n имеет вид

$$A_n = (a_{i,j}), \quad i, j = 0, 1, \dots, n-1.$$

Симметричные относительно главной диагонали элементы таблицы Кэли $a_{i,j}$ и $a_{j,i}$, $i \neq j$, определяют симметричную пару $\langle a_{i,j}, a_{j,i} \rangle$. Соответствующие индексы i, j назовем *входами* данной пары. Входы каждой симметричной пары определяют двоичный цикл (i, j) с весом $i+j = a_{i,j} = a_{j,i}$.

Будем говорить, что симметричные пары $\langle a_{i,j}, a_{j,i} \rangle$ и $\langle a_{s,t}, a_{t,s} \rangle$ обладают *свойством парной неколлинеарности*, если соответствующие номера строк и столбцов i, j, s, t попарно различны, т. е. $i \neq s, i \neq t, j \neq s, j \neq t$.

Далее будем называть инволюцией произвольную неединичную подстановку J из симметрической группы подстановок $S(G_n)$, для которой $J^2 = \varepsilon$ — единичная подстановка. Каждая инволюция либо является двоичным циклом, либо представляется в виде произведения двух или более (попарно) независимых двоичных циклов, и такое представление единственно с точностью до перестановки сомножителей. Кроме того, любое произведение независимых двоичных циклов является инволюцией. В связи с этим будем при необходимости отождествлять инволюции с непустыми множествами независимых двоичных циклов. Элементы такого множества будем называть *двоичными циклами* соответствующей инволюции.

Непосредственно из определений вытекает следующая лемма.

Лемма 1. *Совокупности симметричных пар таблицы Кэли A_n*

$$\langle a_{i_1, j_1}, a_{j_1, i_1} \rangle, \dots, \langle a_{i_k, j_k}, a_{j_k, i_k} \rangle, \quad k \geq 1,$$

соответствует инволюция $(i_1, j_1) \cdot \dots \cdot (i_k, j_k)$ тогда и только тогда, когда любые две различные пары совокупности удовлетворяют свойству парной неколлинеарности.

Совокупность всех элементов таблицы Кэли A_n , равных фиксированному ненулевому элементу $k \in \{0, 1, \dots, n-1\}$, называется *серией веса k* . Каждой таблице Кэли A_n соответствует n серий с n элементами в серии. Так как группа G_n коммутативная, то элементы каждой серии, не лежащие на главной диагонали таблицы Кэли A_n , разбиваются на парно неколлинеарные симметричные пары. В свою очередь, каждой такой симметричной паре соответствует двоичный цикл. Из леммы 1 вытекает следующая лемма.

Лемма 2. Совокупности симметричных пар любой серии веса k в таблице Кэли A_n соответствует инволюция, за исключением случая $G_n = E_{2^m}$, $k = 0$.

Инволюции из леммы 2 будем называть *равновесными*.

Теорема 1. 1°. Если

$$n = 2^m, \quad G_n = E_{2^m},$$

то каждой из $n-1$ серий ненулевого веса в таблице Кэли A_{2^m} соответствует равновесная инволюция с 2^{m-1} двоичными циклами.

2°. При

$$G_n = C_n, \quad n - \text{нечетное число},$$

каждой из n серий таблицы Кэли соответствует равновесная инволюция с $(n-1)/2$ двоичными циклами.

3°. При

$$G_n = C_n, \quad n - \text{четное число},$$

каждой из $n/2$ серий с нечетным весом соответствует равновесная инволюция с $n/2$ двоичными циклами, а каждой из $n/2$ серий с четным весом соответствует инволюция с $n/2 - 1$ двоичными циклами.

Доказательство. 1°. Если $G_n = E_{2^m}$, то серия нулевых элементов группы образует главную диагональ таблицы Кэли A_{2^m} . Следовательно, серии ненулевого веса разбиваются на симметричные пары клеток, т. е. каждой такой серии соответствует инволюция из 2^{m-1} двоичных циклов.

2°, 3°. Если $G_n = C_n$, то для любых $i, k = 0, 1, \dots, n-1$ равенство $a_{i,i} = k$ выполняется тогда и только тогда, когда имеет место сравнение $2i \equiv k \pmod{n}$. Если n нечетное, то для любого $k = 0, 1, \dots, n-1$ данное сравнение имеет ровно одно решение $i \in \{0, 1, \dots, n-1\}$. Этому решению соответствует единичный цикл инволюции. Остальные элементы серии веса k разбиваются на симметричные пары, и серии веса k соответствует инволюция из $(n-1)/2$ двоичных циклов. Отсюда следует утверждение п. 2°.

Аналогично, если n четное, то для любого четного $k = 0, 2, \dots, n-2$ указанное сравнение имеет ровно два решения $i \in \{0, 1, \dots, n-1\}$, а для любого нечетного $k = 1, 3, \dots, n-1$ решений нет. Отсюда следует утверждение п. 3°. Теорема доказана. $\square$

Таким образом, при любых $n \geq 3$ и $k = 0, 1, \dots, n-1$, за исключением случая $n = 2^m$, $k = 0$, серии веса k таблицы Кэли A_n ставится в соответствие инволюция I_k , все двоичные циклы которой имеют вес k . В случае $n = 2^m$, $k = 0$ будем считать, что $I_0 = \varepsilon$.

Выбор подстановки S в качестве S -блока блочного шифра или преобразования в шифре колонной замены зависит от свойства близости к равномерному для следующего преобразования множества пар различных элементов из множества $\{0, 1, \dots, n-1\}$:

$$S(l, t) = (S(l), S(t)), \quad 0 \leq l < t \leq n-1. \quad (1)$$

Для каждой инволюции I_k совокупность образов $S(l, t)$ ее двоичных циклов снова образует множество независимых двоичных циклов. Этому множеству соответствует инволюция J_k . Эффективность применения дифференциального метода криптоанализа определяется числом различных весов двоичных циклов инволюций J_k .

В случае $n = 2^m$, $j = 0$ будем считать, что $J_0 = \varepsilon$. Каждая подстановка J_k получается из подстановки I_k трансформацией циклов подстановкой S , поэтому имеем следующую лемму.

Лемма 3. Для любой подстановки S , действующей на абелевой группе G_n , система $J_0, J_1, \dots, J_{n-1}$ связана с системой $I_0, I_1, \dots, I_{n-1}$ равенствами

$$S^{-1} \cdot I_k \cdot S = J_k, \quad k = 0, 1, \dots, n-1. \quad (2)$$

При заданных $J_0, J_1, \dots, J_{n-1}$ систему равенств (2) можно рассматривать как систему уравнений подобия для определения неизвестной подстановки S , обладающей требуемыми весовыми свойствами [1].

В случае $G_n = E_{2^m}$, $n = 2^m$, инволюцией, соответствующей таблице Кэли A_{2^m} , будем называть любую инволюцию из симметрической группы $S(E_{2^m})$, имеющую 2^{m-1} двоичных циклов.

В случае $G_n = C_n$, n — нечетное, инволюцией, соответствующей таблице Кэли A_n , будем называть любую инволюцию из симметрической группы $S(C_n)$, имеющую $(n-1)/2$ двоичных циклов (и один единичный цикл).

В случае $G_n = C_n$, n — четное, инволюцией, соответствующей таблице Кэли A_n , будем называть либо любую инволюцию из симметрической группы $S(C_n)$, имеющую $n/2$ независимых двоичных циклов, либо любую инволюцию из симметрической группы $S(C_n)$, имеющую $(n-2)/2$ независимых двоичных циклов (и два единичных цикла).

Для множества всех инволюций, соответствующих таблице Кэли A_n конечной абелевой группы G_n и имеющих ω единичных циклов, $\omega \in \{0, 1, 2\}$, будем использовать обозначения

$$\mathcal{F}_\omega(A_n), \quad N_\omega(A_n) = |\mathcal{F}_\omega(A_n)|.$$

2. Перечисление инволюций для таблицы Кэли абелевой группы

Перечисление инволюций, соответствующих таблице Кэли абелевой группы G_n , основано на перечислении симметричных пар, при этом используются все $\binom{n}{2}$ симметричные пары таблицы A_n .

Рассмотрим алгоритмы, которые на каждом шаге позволяют получить двоичный цикл инволюции степени n . Каждому шагу алгоритма соответствует выбор подматрицы в таблице Кэли A_n и выбор значения веса используемой симметричной пары, определяющей двоичный цикл инволюции. Варьируя выбор подматриц и значения весов симметричных пар на шагах алгоритма, можно получить все инволюции, соответствующие таблице Кэли группы G_n . Описание алгоритмов имеет отличия для различных случаев, определяемых количеством двоичных циклов искомым инволюции.

Рассмотрим случай, когда либо $G_n = E_{2^m}$, $n = 2^m$, либо $G_n = C_n$, n — четное, и искомая инволюция имеет $n/2$ двоичных циклов. Если $G_n = E_{2^m}$, то в качестве элемента группы с номером $i \in \{0, 1, \dots, n-1\}$ рассматриваем двоичный вектор $(i_{n-1}, \dots, i_1, i_0)$, для которого $i_{n-1} \cdot 2^{n-1} + \dots + i_1 \cdot 2 + i_0 = i$.

Алгоритм 1.1

Шаг 1. В строке и в столбце матрицы A_n с номером 0 выбирается одна из $n-1$ симметричных пар $\langle \mu_1, \mu_1 \rangle$ с весом μ_1 , входы которой в матрице A_n определяют двоичный цикл $(i_1, j_1) = (0, \mu_1)$. В матрице A_n вычеркиваются строки и столбцы с номерами из множества $\{i_1, j_1\}$ и тем самым определяется подматрица $A_n[i_1, j_1]$ размеров $(n-2) \times (n-2)$.

Шаг 2. В строке и в столбце матрицы $A_n[i_1, j_1]$ с минимальным номером выбирается одна из $n-3$ симметричных пар $\langle \mu_2, \mu_2 \rangle$ веса μ_2 , входы которой в матрице A_n определяют двоичный цикл (i_2, j_2) , $i_2 + j_2 = \mu_2$. В матрице $A_n[i_1, j_1]$ вычеркиваются строки и столбцы с номерами из множества $\{i_2, j_2\}$ и тем самым определяется подматрица $A_n[i_1, j_1; i_2, j_2]$ размеров $(n-4) \times (n-4)$.

Шаг k . В матрице $A_n[i_1, j_1; \dots; i_{k-1}, j_{k-1}]$ размеров $(n-2(k-1)) \times (n-2(k-1))$ в строке и в столбце с минимальным номером выбирается одна из $(n-2(k-1)-1)$ симметричных пар $\langle \mu_k, \mu_k \rangle$ веса μ_k , входы которой в матрице A_n определяют двоичный цикл (i_k, j_k) , $i_k + j_k = \mu_k$. В матрице $A_n[i_1, j_1; \dots; i_{k-1}, j_{k-1}]$ вычеркиваются строки и столбцы с номерами из множества $\{i_k, j_k\}$ и тем самым определяется подматрица $A_n[i_1, j_1; \dots; i_k, j_k]$ размеров $(n-2k) \times (n-2k)$.

Шаг $n/2$. Матрица $A_n[i_1, j_1; \dots; i_{n/2-1}, j_{n/2-1}]$ имеет размеры 2×2 , ее симметричные элементы вне главной диагонали определяют двоичный цикл $(i_{n/2}, j_{n/2})$.

В результате алгоритм 1.1 строит инволюцию

$$J = (i_1, j_1) (i_2, j_2) \dots (i_{n/2}, j_{n/2}).$$

Рассмотрим случай, когда $G_n = C_n$, n — нечетное.

Алгоритм 1.2

Шаг 1. На главной диагонали матрицы A_n произвольно выбирается элемент, входы которого в матрице A_n определяют единичный цикл (i_0) . В матрице A_n вычеркиваются строка и столбец с номером i_0 и тем самым определяется подматрица $A_n[i_0]$ размеров $(n-1) \times (n-1)$.

Шаг 2. В строке и в столбце матрицы $A_n[i_0]$ с минимальным номером выбирается одна из $n-2$ симметричных пар $\langle \mu_1, \mu_1 \rangle$ с весом μ_1 , входы которой в матрице A_n определяют двоичный цикл (i_1, j_1) . В матрице $A_n[i_0]$ вычеркиваются строки и столбцы с номерами из множества $\{i_1, j_1\}$ и тем самым определяется подматрица $A_n[i_0; i_1, j_1]$ размеров $(n-3) \times (n-3)$.

Шаг k . В матрице $A_n[i_0; i_1, j_1; \dots; i_{k-2}, j_{k-2}]$ размеров $(n-2(k-2)-1) \times (n-2(k-2)-1)$ в строке и в столбце с минимальным номером выбирается одна из $(n-2(k-1))$ симметричных пар $\langle \mu_{k-1}, \mu_{k-1} \rangle$ веса μ_{k-1} , входы которой в матрице A_n определяют двоичный цикл (i_{k-1}, j_{k-1}) , $i_{k-1} + j_{k-1} = \mu_{k-1}$. В матрице $A_n[i_0; i_1, j_1; \dots; i_{k-2}, j_{k-2}]$ вычеркиваются строки и столбцы с номерами из множества $\{i_{k-1}, j_{k-1}\}$ и тем самым определяется подматрица $A_n[i_0; i_1, j_1; \dots; i_{k-1}, j_{k-1}]$ размеров $(n-2(k-1)-1) \times (n-2(k-1)-1)$.

Шаг $(n+1)/2$. Матрица $A_n[i_0; i_1, j_1; \dots; i_{(n-1)/2-1}, j_{(n-1)/2-1}]$ имеет размеры 2×2 , ее симметричные элементы вне главной диагонали определяют двоичный цикл $(i_{(n-1)/2}, j_{(n-1)/2})$.

В результате алгоритм 1.2 строит инволюцию

$$J = (i_0) (i_1, j_1) (i_2, j_2) \dots (i_{(n-1)/2}, j_{(n-1)/2}).$$

Рассмотрим случай, когда $G_n = C_n$, n четное, и искомая инволюция имеет $(n-2)/2$ двоичных циклов и два единичных цикла.

Алгоритм 1.3

Шаг 1. На главной диагонали матрицы A_n произвольно выбираются два элемента, входы которых в матрице A_n определяют два единичных цикла $(i_0), (j_0)$, $0 \leq i_0 < j_0 \leq n-1$. В матрице A_n вычеркиваются строки и столбцы с номерами i_0, j_0 и тем самым определяется подматрица $A_n[i_0, j_0]$ размеров $(n-2) \times (n-2)$.

Шаг 2. В строке и в столбце матрицы $A_n[i_0, j_0]$ с минимальным номером выбирается одна из $n-3$ симметричных пар $\langle \mu_1, \mu_1 \rangle$ с весом μ_1 , входы которой в матрице A_n определяют двоичный цикл (i_1, j_1) . В матрице $A_n[i_0, j_0]$ вычеркиваются строки и столбцы с номерами из множества $\{i_1, j_1\}$, и тем самым определяется подматрица $A_n[i_0, j_0; i_1, j_1]$ размеров $(n-4) \times (n-4)$.

Шаг k. В матрице $A_n[i_0, j_0; i_1, j_1; \dots; i_{k-2}, j_{k-2}]$ размеров $(n-2(k-1)) \times (n-2(k-1))$ в строке и в столбце с минимальным номером выбирается одна из $(n-2(k-1)-1)$ симметричных пар $\langle \mu_{k-1}, \mu_{k-1} \rangle$ веса μ_{k-1} , входы которой в матрице A_n определяют двоичный цикл (i_{k-1}, j_{k-1}) , $i_{k-1} + j_{k-1} = \mu_{k-1}$. В матрице $A_n[i_0, j_0; i_1, j_1; \dots; i_{k-2}, j_{k-2}]$ вычеркиваются строки и столбцы с номерами из множества $\{i_{k-1}, j_{k-1}\}$ и тем самым определяется подматрица $A_n[i_0, j_0; i_1, j_1; \dots; i_{k-1}, j_{k-1}]$ размеров $(n-2k) \times (n-2k)$.

Шаг $n/2$. Матрица $A_n[i_0, j_0; i_1, j_1; \dots; i_{n/2-2}, j_{n/2-2}]$ имеет порядок 2×2 , ее симметричные элементы вне главной диагонали определяют двоичный цикл $(i_{n/2-1}, j_{n/2-1})$.

В результате алгоритм 1.3 строит инволюцию

$$J = (i_0)(j_0)(i_1, j_1)(i_2, j_2) \dots (i_{n/2-1}, j_{n/2-1}).$$

Приведенные выше алгоритмы построения инволюций, соответствующих таблице Кэли A_n конечной абелевой группы G_n , позволяют доказать следующую теорему.

Теорема 2. Для числа инволюций, соответствующих таблице Кэли конечной абелевой группы G_n , справедливы следующие формулы.

(1) В случае когда $\omega = 0$ и либо $G_n = E_{2^m}$, $n = 2^m$, либо $G_n = C_n$, n — четное,

$$N_0(A_n) = \frac{n!}{2^{n/2} \cdot (n/2)!}. \quad (3)$$

(2) В случае когда $\omega = 1$, $G_n = C_n$, n — нечетное,

$$N_1(A_n) = \frac{n!}{2^{(n-1)/2} \cdot ((n-1)/2)!}. \quad (4)$$

(3) В случае когда $\omega = 2$, $G_n = C_n$, n — четное,

$$N_2(A_n) = \frac{n!}{2^{n/2} \cdot (n/2 - 1)!}. \quad (5)$$

Доказательство. Действительно, в случае (1) имеем

$$N_0(A_n) = (n-1) \cdot (n-3) \cdot \dots \cdot (n-1-2(k-1)) \cdot \dots \cdot 3 \cdot 1.$$

В случае (2) имеем

$$N_1(A_n) = n \cdot (n-2) \cdot (n-4) \cdot \dots \cdot (n-2(k-1)) \cdot \dots \cdot 3 \cdot 1.$$

В случае (3) имеем

$$N_2(A_n) = \frac{n(n-1)}{2} \cdot (n-3) \cdot (n-5) \cdot \dots \cdot (n-1-2(k-1)) \cdot \dots \cdot 3 \cdot 1.$$

Во всех случаях после несложных преобразований получаем формулы (3), (4), (5), приведенные в теореме 2. Теорема доказана. $\square$

Отметим, что алгоритмы 1.1–1.3 можно использовать для перечисления инволюций, соответствующих таблице Кэли A_n , в которые входят двоичные циклы некоторой *наперед заданной* инволюции $\{(i_1, j_1), (i_2, j_2), \dots, (i_k, j_k)\}$ с $k \geq 1$ независимыми двоичными циклами.

Рассмотрим матрицу $A_n[i_1, j_1; \dots; i_k, j_k]$ размеров $(n-2k) \times (n-2k)$, полученную из таблицы Кэли A_n вычеркиванием строк и столбцов с номерами из множества $\{i_1, j_1, \dots, i_k, j_k\}$. Дополним указанную инволюцию с k двоичными циклами до инволюции, соответствующей таблице Кэли, применив один из алгоритмов 1.1–1.3 к матрице $A_n[i_1, j_1; \dots; i_k, j_k]$.

Обозначим через

$$N_\omega(A_n[i_1, j_1; \dots; i_k, j_k]), \quad \omega \in \{0, 1, 2\},$$

число инволюций, соответствующих таблице Кэли конечной абелевой группы G_n и имеющих фиксированные двоичные циклы некоторой инволюции $\{(i_1, j_1), (i_2, j_2), \dots, (i_k, j_k)\}$. Рассуждая аналогично доказательству теоремы 2, получим следующее утверждение.

Следствие 1. *Справедливы следующие формулы.*

(1) В случае когда $\omega = 0$ и либо $G_n = E_{2^m}$, $n = 2^m$, либо $G_n = C_n$, n — четное, $1 \leq k \leq n/2$,

$$N_0(A_n[i_1, j_1; \dots; i_k, j_k]) = \frac{(n-2k)!}{2^{n/2-k} \cdot (n/2-k)!}. \quad (6)$$

(2) В случае когда $\omega = 1$, $G_n = C_n$, n нечетное, $1 \leq k \leq (n-1)/2$,

$$N_1(A_n[i_1, j_1; \dots; i_k, j_k]) = \frac{(n-2k)!}{2^{(n-1)/2-k} \cdot ((n-1)/2-k)!}. \quad (7)$$

(3) В случае когда $\omega = 2$, $G_n = C_n$, n — четное, $1 \leq k \leq n/2 - 1$,

$$N_2(A_n[i_1, j_1; \dots; i_k, j_k]) = \frac{(n-2k)!}{2^{n/2-k} \cdot (n/2-1-k)!}. \quad (8)$$

Кроме того, в дальнейшем будем использовать алгоритмы 1.1–1.3 для перечисления инволюций при наличии заданных ограничений на веса двоичных циклов, входящих в искомые инволюции. Предположим, что задано множество $\{\nu_1, \dots, \nu_k\} \subset G_n$, $k \geq 1$. Обозначим через $A_n^{(\nu_1, \dots, \nu_k)}$ матрицу, полученную из таблицы Кэли A_n конечной абелевой группы G_n путем замены ее элементов, принадлежащих множеству $\{\nu_1, \dots, \nu_k\}$, на «пустой» вес $\emptyset$. Обозначим через $\mathcal{F}_\omega(A_n; \nu_1, \dots, \nu_k)$ множество инволюций, соответствующих таблице Кэли A_n , у которых вес любого двоичного цикла не содержится в множестве $\{\nu_1, \dots, \nu_k\}$ и имеющих ω единичных циклов. Множество $\mathcal{F}_\omega(A_n; \nu_1, \dots, \nu_k)$ может быть получено путем применения модификации одного из алгоритмов 1.1–1.3, соответствующего выбору группы G_n и значению ω , к матрице $A_n^{(\nu_1, \dots, \nu_k)}$. Модификация будет заключаться в следующем: наличие пустого веса в элементах симметричной пары матрицы означает запрет на использование этой симметричной пары для выбора двоичного цикла инволюции на каждом шаге алгоритма. Отметим также, что при вычеркивании в ходе работы алгоритма строки (столбца) матрицы A_n вычеркиваются в том числе клетки веса $\emptyset$ в этой строке (столбце).

3. Случайные инволюции, имеющие заданное число общих двоичных циклов с разнovesной инволюцией

Основная цель данного раздела заключается в доказательстве теоремы 3, для формулировки которой введем обозначения.

Предположим, что задан некоторый элемент $\nu \in G_n$, удовлетворяющий условию: если $n = 2^m$ и $G_n = E_{2^m}$, то $\nu \neq 0$. Рассмотрим равновесную инволюцию I_ν , соответствующую серии элементов веса ν в таблице Кэли A_n абелевой группы G_n . Обозначим через $\omega(\nu)$ число единичных циклов инволюции I_ν .

В случае когда $n = 2^m$ и $G_n = E_{2^m}$, для любого $\nu \in E_{2^m} \setminus 0$ имеем $\omega = 0$. Рассмотрим случайную инволюцию J , выбранную равномерно из множества $\mathcal{F}_0(A_n)$ инволюций, соответствующих таблице Кэли A_n группы E_{2^m} . Обозначим через $\xi_n^{(\nu,0)}$ случайную величину, равную числу общих двоичных циклов инволюций I_ν и J , а через $B_{k,n}^{(\nu,0)}$ — k -й биномиальный момент случайной величины $\xi_n^{(\nu,0)}$, $k = 0, 1, \dots$

В случае когда $n = 2m+1$ нечетно и $G_n = C_{2m+1}$, для любого $\nu \in C_{2m+1}$ имеем $\omega = 1$. Рассмотрим случайную инволюцию J , выбранную равномерно из множества $\mathcal{F}_1(A_{2m+1})$ инволюций, соответствующих таблице Кэли группы C_{2m+1} . Обозначим через $\xi_{2m+1}^{(\nu,1)}$ случайную величину, равную числу общих двоичных циклов инволюций I_ν и J , а через $B_{k,2m+1}^{(\nu,1)}$ — k -й биномиальный момент случайной величины $\xi_{2m+1}^{(\nu,1)}$, $k = 0, 1, \dots$

В случае когда $n = 2m$ четно и $G_n = C_{2m}$, для элементов $\nu \in C_{2m}$, в зависимости от четности, возможны два значения $\omega = \omega(\nu) \in \{0, 2\}$. Для каждого $\rho \in \{0, 2\}$ рассмотрим случайную инволюцию J , выбранную равномерно из множества $\mathcal{F}_\rho(A_{2m})$ инволюций, соответствующих таблице Кэли группы C_{2m} . Обозначим через $\xi_{2m}^{(\nu,\omega,\rho)}$ случайную величину, равную числу общих двоичных циклов инволюций I_ν и J , а через $B_{k,2m}^{(\nu,\omega,\rho)}$ — k -й биномиальный момент случайной величины $\xi_{2m}^{(\nu,\omega,\rho)}$, $k = 0, 1, \dots$. Ниже $(l)_k = l(l-1)\dots(l-k+1)$ — символ Жордана.

Теорема 3. Для распределений случайных величин $\xi_n^{(\nu,\omega)}$, $\xi_n^{(\nu,\omega,\rho)}$ имеют место формулы

$$\mathbf{P}\{\xi_n^{(\nu,\omega)} = r\} = \sum_{k=r}^{\lfloor \frac{n}{2} \rfloor} (-1)^{k-r} \cdot \binom{k}{r} \cdot B_{k,n}^{(\nu,\omega)}, \quad r = 0, 1, \dots, \quad (9)$$

$$\mathbf{P}\{\xi_n^{(\nu,\omega,\rho)} = r\} = \sum_{k=r}^{\frac{n}{2}} (-1)^{k-r} \cdot \binom{k}{r} \cdot B_{k,n}^{(\nu,\omega,\rho)}, \quad r = 0, 1, \dots \quad (10)$$

При этом:

(1) Если $n = 2^m$, $G_n = E_{2^m}$, $\nu \in E_{2^m} \setminus 0$, то

$$B_{k,2^m}^{(\nu,0)} = \frac{2^k}{k!} \cdot \frac{((2^{m-1})_k)^2}{(2^m)_{2k}}, \quad k = 0, 1, \dots, 2^{m-1}, \quad (11)$$

$$\mathbf{P}\{\xi_{2^m}^{(\nu,0)} = 0\} = \sum_{k=0}^{2^{m-1}} (-1)^k \cdot \frac{2^k}{k!} \cdot \frac{((2^{m-1})_k)^2}{(2^m)_{2k}}. \quad (12)$$

(2) Если $n = 2m + 1$, $m = 0, 1, 2, \dots$, $G_n = C_{2m+1}$, то при любом $\nu \in C_{2m+1}$

$$\mathbf{B}_{k,2m+1}^{(\nu,1)} = \frac{2^k}{k!} \cdot \frac{((m)_k)^2}{(2m+1)_{2k}}, \quad k = 0, 1, \dots, m, \quad (13)$$

$$\mathbf{P}\{\xi_{2m+1}^{(\nu,1)} = 0\} = \sum_{k=0}^m (-1)^k \cdot \frac{2^k}{k!} \cdot \frac{((m)_k)^2}{(2m+1)_{2k}}. \quad (14)$$

(3) Если $n = 2m$, $m = 1, 2, \dots$, $G_n = C_{2m}$, то при любом $\nu \in C_{2m}$ и для любого $\rho = 0, 2$

$$\mathbf{B}_{k,2m}^{(\nu,\omega,\rho)} = \frac{2^k}{k!} \cdot \frac{(m-\omega/2)_k \cdot (m-\rho/2)_k}{(2m)_{2k}}, \quad k = 0, 1, \dots, m, \quad (15)$$

$$\mathbf{P}\{\xi_{2m}^{(\nu,\omega,\rho)} = 0\} = \sum_{k=0}^m (-1)^k \cdot \frac{2^k}{k!} \cdot \frac{(m-\omega/2)_k \cdot (m-\rho/2)_k}{(2m)_{2k}}. \quad (16)$$

Доказательство. Приведем доказательство теоремы для случайных величин $\xi_n^{(\nu,\omega)}$ в случаях (1) и (2). Для случайных величин $\xi_n^{(\nu,\omega,\rho)}$ в случае (3) рассуждения аналогичны. Воспользуемся обозначениями из теоремы 2 и ее следствия. По формуле включения-исключения при любом $r = 0, 1, \dots, \lfloor n/2 \rfloor$ получим формулу для числа $N_{\omega,r}(A_n)$ инволюций $J \in \mathcal{F}_\omega(A_n)$, имеющих с I_ν ровно r общих двоичных циклов:

$$N_{\omega,r}(A_n) = \sum_{k=r}^{\lfloor \frac{n}{2} \rfloor} (-1)^{k-r} \cdot \binom{k}{r} \cdot S_{k,n}^{(\nu)}, \quad (17)$$

где

$$S_{k,n}^{(\nu)} = \sum_{(i_1,j_1); \dots; (i_k,j_k)} N_\omega(A_n[i_1, j_1; \dots; i_k, j_k]), \quad (18)$$

суммирование в (18) осуществляется по всем k -сочетаниям двоичных циклов инволюции I_ν .

Справедливы формулы для распределения случайной величины $\xi_n^{(\nu,\omega)}$:

$$\mathbf{P}\{\xi_n^{(\nu,\omega)} = r\} = \frac{N_{\omega,r}(A_n)}{|\mathcal{F}_\omega(A_n)|}, \quad r = 0, 1, \dots, \left\lfloor \frac{n}{2} \right\rfloor, \quad (19)$$

и для ее биномиальных моментов:

$$\mathbf{B}_{k,n}^{(\nu)} = \frac{S_{k,n}^{(\nu)}}{|\mathcal{F}_\omega(A_n)|}, \quad k = 0, 1, \dots, \left\lfloor \frac{n}{2} \right\rfloor. \quad (20)$$

Из (19), (17), (20) следует формула (9).

Далее, используя дополнительно соотношения (18) и (3)–(8), после несложных преобразований получим формулы (11), (13), (15). Теорема доказана. $\square$

Заметим, что любое $\nu \geq 0$ можно рассматривать в качестве элемента группы G_n при каждом значении $n > \nu$. Теорема 3 позволяет получить доказательство следующей теоремы.

Теорема 4. Для любого $\nu \geq 1$ и для аддитивной группы E_{2^m} поля F_{2^m} распределения случайных величин $\xi_{2^m}^{(\nu,0)}$ при $m \rightarrow \infty$ сходятся к распределению Пуассона с параметром $\lambda = \frac{1}{2}$, т. е.

$$\mathbf{P}\{\xi_{2^m}^{(\nu,0)} = r\} \rightarrow \frac{\left(\frac{1}{2}\right)^r}{r!} \cdot e^{-1/2}, \quad r = 0, 1, \dots \quad (21)$$

Для любого $\nu \geq 0$ и для аддитивной группы C_{2m+1} кольца вычетов по нечетному модулю $2m+1$ распределения случайных величин $\xi_{2m+1}^{(\nu,1)}$ при $m \rightarrow \infty$ сходятся к распределению Пуассона с параметром $\lambda = \frac{1}{2}$, т. е.

$$\mathbf{P}\{\xi_{2m+1}^{(\nu,1)} = r\} \rightarrow \frac{\left(\frac{1}{2}\right)^r}{r!} \cdot e^{-1/2}, \quad r = 0, 1, \dots \quad (22)$$

Для любого $\nu \geq 0$ и для аддитивной группы C_{2m} кольца вычетов по четному модулю $2m$ распределения случайных величин $\xi_{2m}^{(\nu,\omega,\rho)}$, $\rho = 0, 2$, при $m \rightarrow \infty$ сходятся к распределению Пуассона с параметром $\lambda = \frac{1}{2}$, т. е.

$$\mathbf{P}\{\xi_{2m}^{(\nu,\omega,\rho)} = r\} \rightarrow \frac{\left(\frac{1}{2}\right)^r}{r!} \cdot e^{-1/2}, \quad r = 0, 1, \dots \quad (23)$$

Действительно, из формул (11), (13), (15) следует, что при выполнении каждого из условий (1)–(3) теоремы 3 соответствующие биномиальные моменты сходятся при $m \rightarrow \infty$ к биномиальным моментам распределения Пуассона с параметром $\lambda = \frac{1}{2}$.

4. Инволюции над абелевой группой с данным дефицитом

Для конечной абелевой группы G_n введем понятие дефицита $d(J)$ инволюции $J \in \mathcal{F}_\omega[A_n]$ с ω единичными циклами.

В случае аддитивной группы конечного поля $G_n = E_{2^m}$, $n = 2^m$,

$$d(J) = 2^m - 1 - v(J),$$

где $v(J)$ — число различных весов двоичных циклов J . Тогда для любой инволюции $J \in \mathcal{F}_0[A_{2^m}]$ выполнены неравенства

$$2^{m-1} - 1 \leq d(J) \leq 2^m - 2.$$

В случае аддитивной группы кольца вычетов $G_n = C_n$

$$d(J) = n - v(J),$$

где $v(J)$ — число различных весов двоичных циклов J . Тогда при нечетном n для любой инволюции $J \in \mathcal{F}_1[A_n]$ выполнены неравенства

$$\frac{n+1}{2} \leq d(J) \leq n-1.$$

При четном n и $\omega = 0, 2$ для любой инволюции $J \in \mathcal{F}_\omega[A_n]$ выполнены неравенства

$$\frac{n+\omega}{2} \leq d(J) \leq n-1.$$

Введем общее обозначение для множества инволюций, соответствующих таблице Кэли A_n конечной абелевой группы G_n , имеющих ω единичных циклов и дефицит, равный r :

$$\mathcal{F}_\omega[A_n, G_n]^{(r)}.$$

Теорема 5. Число инволюций с заданным весовым дефицитом, соответствующих таблице Кэли A_n группы G_n , определяется следующими формулами.

(1) В случае $G_n = E_{2^m}$, $n = 2^m$ для любого $r = 2^{m-1} - 1, \dots, 2^m - 2$

$$\begin{aligned} |\mathcal{F}_0[A_{2^m}, E_{2^m}]^{(r)}| &= \\ &= \sum_{k=r}^{2^m-2} (-1)^{k-r} \cdot \binom{k}{r} \cdot \sum_{1 \leq \nu_1 < \dots < \nu_k \leq 2^m-1} |\mathcal{F}_0[A_{2^m}; \nu_1, \dots, \nu_k]|. \end{aligned} \quad (24)$$

(2) В случае $G_n = C_n$, при нечетном n и $\omega = 1$, а также при четном n и $\omega = 0, 2$ для любого $r = (n+\omega)/2, \dots, n-1$

$$\begin{aligned} |\mathcal{F}_\omega[A_n, C_n]^{(r)}| &= \\ &= \sum_{k=r}^{n-1} (-1)^{k-r} \cdot \binom{k}{r} \cdot \sum_{0 \leq \nu_1 < \dots < \nu_k \leq n-1} |\mathcal{F}_\omega[A_n; \nu_1, \dots, \nu_k]|. \end{aligned} \quad (25)$$

Приведем доказательство теоремы для случая $G_n = C_n$, в случае $G_n = E_{2^m}$ доказательство аналогично. Определим свойства $B_j, j = 0, 1, \dots, n-1$, инволюций $J \in \mathcal{F}_\omega[A_n]$: инволюция J обладает свойством B_j , если все веса ее двоичных циклов отличны от j . Для любой инволюции J значение $d(J)$ равно числу свойств из набора $B_j, j = 0, 1, \dots, n-1$, которым удовлетворяет эта инволюция. Применив формулы метода включения-исключения, получим равенства (24), (25).

На множестве $\mathcal{F}_\omega[A_n]$ инволюций с ω единичными циклами зададим равновероятное распределение и рассмотрим случайную величину $\zeta_n^{(\omega)}$, равную весовому дефициту случайной равновероятной инволюции $J \in \mathcal{F}_\omega[A_n]$. В качестве следствия теоремы 5 имеем следующую теорему.

Теорема 6. Вероятностное распределение весового дефицита $\zeta_n^{(\omega)}$ случайной равновероятной инволюции $J \in \mathcal{F}_\omega[A_n]$ имеет следующий вид:

(1) В случае $G_n = E_{2^m}$, $n = 2^m$, для любого $r = 2^{m-1}-1, \dots, 2^m-2$

$$\begin{aligned} \mathbf{P}\{\zeta_{2^m}^{(0)} = r\} &= \\ &= \sum_{k=r}^{2^m-2} (-1)^{k-r} \cdot \binom{k}{r} \cdot \sum_{1 \leq \nu_1 < \dots < \nu_k \leq 2^m-1} \frac{|\mathcal{F}_0[A_{2^m}; \nu_1, \dots, \nu_k]|}{N_0[A_n]}. \end{aligned} \quad (26)$$

(2) В случае $G_n = C_n$ при нечетном n и $\omega = 1$, а также при четном n и $\omega = 0, 2$ для любого $r = (n+\omega)/2, \dots, n-1$

$$\begin{aligned} \mathbf{P}\{\zeta_n^{(\omega)} = r\} &= \\ &= \sum_{k=r}^{n-1} (-1)^{k-r} \cdot \binom{k}{r} \cdot \sum_{0 \leq \nu_1 < \dots < \nu_k \leq n-1} \frac{|\mathcal{F}_\omega[A_n; \nu_1, \dots, \nu_k]|}{N_\omega[A_n]}. \end{aligned} \quad (27)$$

Используя известные формулы для биномиальных моментов вероятностного распределения, полученные методом включения-исключения [3], нетрудно доказать следующую теорему.

Теорема 7. Биномиальные моменты $\tilde{B}_{k,n}^{(\omega)}$ случайной величины $\zeta_n^{(\omega)}$, равной весовому дефициту случайной равновероятной инволюции $J \in \mathcal{F}_\omega[A_n]$, имеют следующие выражения:

(1) В случае $G_n = E_{2^m}$, $n = 2^m$, для любого $k = 1, \dots, 2^m - 2$

$$\tilde{B}_{k,2^m}^{(0)} = \sum_{1 \leq \nu_1 < \dots < \nu_k \leq 2^m - 1} \frac{|\mathcal{F}_0[A_{2^m}; \nu_1, \dots, \nu_k]|}{N_0[A_{2^m}]}. \quad (28)$$

(2) В случае $G_n = C_n$ при нечетном n и $\omega = 1$, а также при четном n и $\omega = 0, 2$ для любого $k = 1, 2, \dots, n-1$

$$\tilde{B}_{k,n}^{(\omega)} = \sum_{0 \leq \nu_1 < \dots < \nu_k \leq n-1} \frac{|\mathcal{F}_\omega[A_n; \nu_1, \dots, \nu_k]|}{N_\omega[A_n]}. \quad (29)$$

Из теоремы 7 при $k = 1$ следуют выражения для среднего значения случайной величины $\zeta_n^{(\omega)}$:

(1) Если $G_n = E_{2^m}$, $n = 2^m$, то

$$\mathbf{E} \zeta_{2^m}^{(0)} = \sum_{1 \leq \nu \leq 2^m - 1} \frac{|\mathcal{F}_0[A_{2^m}; \nu]|}{N_0[A_{2^m}]}. \quad (30)$$

(2) Если $G_n = C_n$, то при нечетном n и $\omega = 1$, а также при четном n и $\omega = 0, 2$

$$\mathbf{E} \zeta_n^{(\omega)} = \sum_{0 \leq \nu \leq n-1} \frac{|\mathcal{F}_\omega[A_n; \nu]|}{N_\omega[A_n]}. \quad (31)$$

Величина

$$\frac{|\mathcal{F}_\omega[A_n; \nu]|}{N_\omega[A_n]}$$

равна вероятности того, что случайная равновероятная инволюция $J \in \mathcal{F}_\omega[A_n]$ не имеет общих двоичных циклов с инволюцией I_ν . Из формул (12), (14), (16) следует, что слагаемые в правой части равенств (30), (31) либо одинаковы, либо принимают два различных значения. Используя указанные формулы, а также соотношения (22), (23), получим два следствия.

Следствие 2. Для среднего значения $\mathbf{E} \zeta_n^{(\omega)}$ весового дефицита случайной равновероятной инволюции $J \in \mathcal{F}_\omega [A_n]$ справедливы следующие выражения:

(1) Если $n = 2^m$, $G_n = E_{2^m}$, то

$$\mathbf{E} \zeta_{2^m}^{(0)} = (2^m - 1) \cdot \left(\sum_{k=0}^{2^m-1} (-1)^k \cdot \frac{2^k}{k!} \cdot \frac{((2^{m-1})_k)^2}{(2^m)_{2k}} \right). \quad (32)$$

(2) Если $G_n = C_{2m+1}$, $n = 2m+1$, $m=0, 1, 2, \dots$, то

$$\mathbf{E} \zeta_{2m+1}^{(1)} = (2m+1) \cdot \sum_{k=0}^m (-1)^k \cdot \frac{2^k}{k!} \cdot \frac{((m)_k)^2}{(2m+1)_{2k}}.$$

(3) Если $G_n = C_{2m}$, $n = 2m$, $m=1, 2, \dots$, то при $\omega = 0, 2$

$$\mathbf{E} \zeta_{2m}^{(\omega)} = m \cdot \left(\sum_{k=0}^m (-1)^k \cdot \frac{2^k}{k!} \cdot \frac{((m - \omega/2)_k)^2}{(2m)_{2k}} + \sum_{k=0}^{m-1} (-1)^k \cdot \frac{2^k}{k!} \cdot \frac{(m)_k \cdot (m-1)_k}{(2m)_{2k}} \right).$$

Следствие 3. Для среднего значения $\mathbf{E} \zeta_n^{(\omega)}$ весового дефицита случайной равновероятной инволюции $J \in \mathcal{F}_\omega [A_n]$ справедливы следующие асимптотические соотношения:

(1) Если $n = 2^m$, $G_n = E_{2^m}$, то при $m \rightarrow \infty$

$$\mathbf{E} \zeta_{2^m}^{(0)} = \frac{2^m}{\sqrt{e}} \cdot (1 + o(1)). \quad (33)$$

(2) Если $G_n = C_n$, то при $\omega = 1$ и нечетных $n \rightarrow \infty$, а также при $\omega = 0, 2$ и четных $n \rightarrow \infty$

$$\mathbf{E} \zeta_n^{(\omega)} = \frac{n}{\sqrt{e}} \cdot (1 + o(1)).$$

Пусть S — случайная равновероятная подстановка, действующая на группе $G_n = E_{2^m}$, $n = 2^m$, и $J_1, \dots, J_{2^m-1}$ — система инволюций, определенная в разделе 1 действием S на двоичных циклах инволюций $I_1, \dots, I_{2^m-1}$, см. (1). Весовой индикатор [2] подстановки S является случайным вектором $(d_{1,2^m}, d_{2,2^m}, \dots, d_{2^m-1,2^m})$, где $d_{k,2^m}$ — весовой дефицит J_k , $1 \leq k \leq 2^m-1$. Среднее значение $d_{k,2^m}$ определяется формулой (32), асимптотика при $m \rightarrow \infty$ — формулой (33).

Список литературы

- [1] Сачков В. Н., “Комбинаторные свойства дифференциально 2-равномерных подстановок”, *Математические вопросы криптографии*, **6:1** (2015), 159–180.
- [2] Сачков В. Н., Круглов И. А., “Весовые дефициты инволюций и подстановок”, *Математические вопросы криптографии*, **7:4** (2016), 95–116.
- [3] Сачков В. Н., *Курс комбинаторного анализа*, М.—Ижевск: НИЦ «Регулярная и хаотическая динамика», 2013, 336 с.