Math-Net.Ru

Общероссийский математический портал

Б. А. Погорелов, М. А. Пудовкина, О расстояниях от подстановок до импримитивных групп при фиксированной системе импримитивности, *Дискрет. матем.*, 2013, том 25, выпуск 3, 78–95

DOI: <https://doi.org/10.4213/dm1249>

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: 44.207.124.84

26 апреля 2023 г., 16:53:48

О расстояниях от подстановок до импримитивных групп при фиксированной системе импримитивности

© 2013 г. Б. А. Погорелов, М. А. Пудовкина

В настоящей работе исследуются расстояния от подстановок степени $n = wr$ до сплетения групп $S_w \wr S_r$ с фиксированной системой импримитивности. В ряде случаев найдены величина максимального расстояния и множества максимально далеких подстановок.

1. Введение

Приближение сложных преобразований множества X более простыми, т.е. оставляющими инвариантными те или иные простые структуры (отношения, "геометрии и др.) на множестве X — один из важнейших способов исследования множеств преобразований. Наиболее распространено приближение линейными преобразованиями, например, в различных вариациях линейного криптоанализа. В этом случае множество X наделяется структурой векторного пространства. Близость преобразования к линейному преобразованию в криптографии выражается в разных терминах, в том числе через расстояние Хемминга до группы аффинных преобразований и через размерность пространства его линейных структур. Можно рассматривать приближения преобразований различными группами, сохраняющими те или иные отношения на множестве X .

Пример 1. Пусть задано нетривиальное разбиение множества X на равномошные подмножества. Множество всех подстановок, сохраняющих такое разбиение, является сплетением симметрических групп, а само разбиение называется системой импримитивности. На этом пути возникает метод гомоморфизмов.

Пример 2. Если на множестве X задана метрика, то ей соответствует группа изометрий, и можно рассматривать приближения преобразованиями, сохраняющими эту метрику.

Оказывается, указанные два случая имеют нечто общее, которое можно выразить в терминах сплетения групп. А именно, близость преобразования к линейному, выраженная в терминах линейных структур, может быть описана и в терминах сплетения групп (в импримитивном действии) [3]. Гомоморфизмы импримитивных групп опять влекут возможность вложения группы в сплетение групп. Наконец, группа изометрий метрического пространства Хемминга над алфавитом X , $|X| = n \geq 3$,

описывается экспоненцированием групп, т. е. той же группой сплетения, но в её примитивном действии. Кроме того, в [5] показано, что в некоторых случаях в разностном методе криптоанализа оценивается расстояние от функции зашифрования до смежного класса симметрической группы по сплетению некоторых групп. Отметим, что в [1] также рассмотрена проблема нахождения расстояния до группы сплетения при построении кодов на основе групп подстановок, но в метриках, отличных от метрик Хемминга.

В данной работе будет рассмотрен второй способ приближения подстановок — подстановками из множества G , являющегося сплетением групп $S_w \wr S_r$, соответствующим системе импримитивности $W = \{W_1, \dots, W_r\}$, где $S(X)$ — симметрическая группа на множестве X и $S_n = S(X)$ при $n = |X|$. Максимальную импримитивную группу подстановок, сохраняющую систему импримитивности $W \in W_{w,r}$, будем обозначать $IG_W = (S_w \wr S_r, W)$, где $W_{w,r}$ — множество всех таких нетривиальных систем импримитивности с параметрами w, r , $w \in \mathbb{N}$, $n = r \cdot w$.

В данной работе мера близости подстановок $g, h \in S_n$ определяется равенством

$$\chi(g, h) = n - \text{im}(gh^{-1}),$$

где $\text{im}(gh^{-1})$ — число неподвижных точек подстановки gh^{-1} . Другими словами, $\chi(g, h)$ — это расстояние Хемминга между табличными представлениями подстановок. Нас будет интересовать число

$$\chi_W(g) = \min\{\chi(g, h) \mid h \in IG_W\},$$

которое назовём порядком W -примитивности. Если соответствующие параметры больше нуля, то подстановку g будем называть W -примитивной. В противном случае — W -импримитивной.

При рассмотрении W -примитивности каждой подстановке ставится в соответствие матрица, характеризующая удалённость данной подстановки от группы IG_W . Через коэффициенты матрицы получено выражение для $\chi_W(g)$. Описаны максимально W -примитивные подстановки. Их можно считать "бент-подстановками" относительно системы импримитивности. Найдено число таких подстановок.

В работе рассмотрена ещё одна мера близости между произвольной подстановкой и группой IG_W . Она задаётся метрикой [6], сохраняемой группой IG_W , и названа коэффициентом изометричности. Приведены её оценки и описаны подстановки с максимальным значением коэффициента изометричности.

Работа состоит из следующих разделов. В разделе 2 получены оценки порядка W -примитивности для произвольных подстановок из S_n . В разделе 3 приведены определение коэффициента изометричности и его свойства. В разделе 4 получены оценки порядка W -примитивности для раундовой функции алгоритма блочного шифрования SMS4.

Будем придерживаться следующих обозначений: $\mathbb{N}$ — множество всех натуральных чисел, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$; $[a]$ — целая часть числа a ; $\lceil a \rceil$ — минимальное целое число b со свойством $b \geq a$; $\bar{g} \in S_r$ — образ подстановки $g \in IG_W$ при естественном гомоморфизме $IG_W \rightarrow S_r$; $\alpha^g = \alpha g = g(\alpha)$ — образ элемента $\alpha \in X$ при действии на него подстановкой $g \in S(X)$.

2. Расстояние от подстановки до группы IG_W относительно метрики Хемминга

Пусть X — произвольное конечное множество, $n = wr = |X|$, $w, r \in \mathbb{N} \setminus \{1\}$, $W = \{W_1, \dots, W_r\}$ — произвольная фиксированная нетривиальная (см. [4]) система импримитивности из множества $W_{w,r}$, $w = |W_i|$. Для подстановки $g \in S(X)$ рассмотрим $(r \times r)$ -матрицу $\mathbf{c}_W(g)$ с элементами $c_{ij}(g) \in \mathbb{N}_0$, где

$$c_{ij}(g) = |\{\alpha \in W_i | \alpha^g \in W_j\}| = |W_i^g \cap W_j|, \quad i, j \in \{1, \dots, r\}.$$

Очевидно, что

$$\sum_{t=1}^r c_{it}(g) = |W_i| = w, \quad \sum_{t=1}^r c_{tj}(g) = |W_j| = w. \quad (1)$$

Рассмотрим множество $C_{w,r}$ всех целых неотрицательных $(r \times r)$ -матриц $\mathbf{c} = \|c_{ij}\|$ со свойством

$$\sum_{t=1}^r c_{it} = \sum_{t=1}^r c_{tj} = w.$$

Пусть $\bar{g}$ — образ подстановки $g \in IG_W$ при естественном гомоморфизме импримитивной группы IG_W с системой импримитивности W . Легко видеть, что матрицы подстановок, принадлежащих правому смежному классу группы $S(X)$ по подгруппе IG_W , различаются только перестановками строк, а матрицы подстановок, принадлежащих левому смежному классу, различаются только перестановками столбцов. Поэтому справедливо следующее утверждение.

Утверждение 1. Пусть $g \in S(X)$, $W \in W_{w,r}$. Тогда для произвольных подстановок $h \in IG_W$ и индексов $i, j \in \{0, \dots, r-1\}$ справедливы равенства $c_{ij}(hg) = c_{ij}(g)$ при $l = i\bar{h}$ и $c_{ij}(gh) = c_{it}(g)$ при $t = j\bar{h}^{-1}$. $\square$

Опишем подстановки с одинаковой матрицей $\mathbf{c} \in C_{w,r}$.

Утверждение 2. Пусть $W \in W_{w,r}$. Тогда для каждой матрицы $\mathbf{c} \in C_{w,r}$ справедливо равенство

$$|\{g \in S(X) | \mathbf{c} = \mathbf{c}_W(g)\}| = \frac{(w!)^{2r}}{\prod_{i=1}^r \prod_{j=1}^r c_{ij}!}. \quad (2)$$

Доказательство. Найдём число $n_W(\mathbf{c})$ подстановок $g \in S(X)$, для которых $\mathbf{c} = \mathbf{c}_W(g)$. Подсчёт числа даст и конструктивный способ их перечисления. Пусть $n_W(\mathbf{c})$ — число таких разбиений W_i, W'_j множества X , что

$$W_i = (W_{i1}, \dots, W_{ir}), \quad W'_j = \begin{pmatrix} W'_{1j} \\ \vdots \\ W'_{rj} \end{pmatrix},$$

$$|W_{ij}| = |W'_{ij}| = c_{ij}, \quad W_{ij}^g = W'_{ij}, \quad i, j = 1, \dots, r,$$

умноженному на число биективных отображений множеств $W_{ij} \rightarrow W'_{ij}$. Поэтому

$$n_W(\mathbf{c}) = \prod_{i=1}^r \begin{pmatrix} w \\ c_{i1} \end{pmatrix} \begin{pmatrix} w - c_{i1} \\ c_{i2} \end{pmatrix} \dots \begin{pmatrix} w - c_{i1} - \dots - c_{jr-1} \\ c_{ir} \end{pmatrix} \times$$

$$\times \prod_{j=1}^r \binom{w}{c_{1j}} \binom{w - c_{1j}}{c_{2j}} \dots \binom{w - c_{1j} - \dots - c_{r-1,j}}{c_{rj}} = \frac{(w!)^{2r}}{\prod_{i,j \geq 1} c_{ij}!}. \square$$

Матрицы из множества $C_{w,r}$, у которых в каждой строке ровно один ненулевой элемент, соответствуют подстановкам из группы IG_W .

Следствие 1. Пусть $W \in W_{w,r}$ и матрица $\mathbf{c} \in C_{w,r}$ такова, что для каждого $i \in \{1, \dots, r\}$ существует элемент $t_i \in \{1, \dots, r\}$, удовлетворяющий равенству $c_{it_i} = w$. Тогда

$$\{g \in S(X) | \mathbf{c} = \mathbf{c}_W(g)\} \subseteq IG_W,$$

$$|\{g \in S(X) | \mathbf{c} = \mathbf{c}_W(g)\}| = (w!)^r.$$

Доказательство очевидно. $\square$

Элементы матрицы $\mathbf{c}_W(g)$ позволяют найти порядок W -примитивности $\chi_W(g)$ и оценить сверху и снизу расстояние Хемминга до произвольной подстановки $s \in IG_W$. Для этого нам понадобятся следующие понятия:

– $[t_1, \dots, t_r]$ — остов матрицы $\mathbf{c} = \|c_{ij}\|$, где c_{it_i} — максимальный элемент в i -й строке; остов называется подстановочным, если $[t_1, \dots, t_r] = \{1, \dots, r\}$;

– $v(\mathbf{c}) = v([t_1, \dots, t_r]) = \sum_{i=1}^r c_{it_i}$ — вес остова (веса всех остовов одинаковы).

Теорема 1. Пусть $W \in W_{w,r}$, $s \in IG_W$, $g \in S(X)$. Тогда:

$$(1) \quad \chi(g, s) \geq |X| - v(\mathbf{c}(g)).$$

(2)

$$\chi_W(g) = |X| - \max \left\{ \sum_{i=1}^r c_{ii^h}(g) \mid h \in S_r \right\}. \quad (3)$$

(3) Если существует подстановочный остов $\bar{\mathbf{c}}(g) = [t_1, \dots, t_r]$, то

$$\chi_W(g) = |X| - v([t_1, \dots, t_r]).$$

Доказательство. Пусть W_i — произвольный блок непримитивности системы W , $W_i^s = W_j$. Тогда

$$|\{\alpha \in W_i | \alpha^s = \alpha^g\}| \leq c_{ij}(g)$$

и для любой подстановки $s \in IG_W$ справедливы соотношения

$$|\{\alpha \in W_i | \alpha^s = \alpha^g\}| \leq \max \{c_{ij}(g) \mid j = 1, \dots, r\},$$

$$|X| - \chi(g, s) = \sum_{i=1}^r |\{\alpha \in W_i | \alpha^s = \alpha^g\}| \leq v(\mathbf{c}(g)).$$

Укажем алгоритм построения подстановки $b \in IG_W$ со свойством

$$\chi(g, b) = |X| - \max \left\{ \sum_{i=1}^r c_{ii^h}(g) \mid h \in S_r \right\}.$$

(1) Находим подстановку $f \in S_r$, для которой

$$\sum_{i=1}^r c_{iif}(g) = \max \left\{ \sum_{i=1}^r c_{iifh}(g) \mid h \in S_r \right\}.$$

(2) Для каждого $i \in \{1, \dots, r\}$ выполняем:

- для каждого $\beta \in W_{f(i)}^{g^{-1}} \cap W_i$ полагаем $\beta^b = \beta^g$;
- выбираем произвольную биекцию

$$t_i : W_i \setminus W_{f(i)}^{g^{-1}} \mapsto W_{f(i)} \setminus W_i^g$$

и полагаем $\beta^b = \beta^{t_i}$ для любого $\beta \in W_i \setminus W_{f(i)}^{g^{-1}}$.

Из построения следует, что $b \in \text{IG}_W$ и

$$\chi(g, b) = |X| - \max \left\{ \sum_{i=1}^r c_{iifh}(g) \mid h \in S_r \right\}.$$

Так как $\chi(g, s) \geq \chi(g, b)$ для $s \in \text{IG}_W$, то

$$\chi_W(g) = |X| - \max \left\{ \sum_{i=1}^r c_{iifh}(g) \mid h \in S_r \right\}.$$

Теперь из существования подстановочного остова $[t_1, \dots, t_r]$ следует равенство

$$\begin{aligned} \chi_W(g) &= |X| - \max \left\{ \sum_{i=1}^r c_{iifh}(g) \mid h \in S_r \right\} = \\ &= |X| - \sum_{i=1}^r \max \{ c_{ij}(g) \mid j = 1, \dots, r \} = |X| - v(\mathbf{c}(g)). \square \end{aligned}$$

Рассмотрим подстановки, максимально далекие от группы IG_W . Их можно считать аналогом бент-функций. Прежде всего, оценим максимальное расстояние между произвольной фиксированной подстановкой и группой IG_W . Пусть $C_{w,r}^{(\max)}$ — множество всех "максимально равномерных" матриц, т.е. матриц $\mathbf{c}_W = \|c_{ij}\| \in C_{w,r}$, удовлетворяющих одному из следующих трёх условий:

- (1) $\mathbf{c}_W$ — $(0, 1)$ -матрица и если $w < r$, то в каждой её строке и в каждом столбце имеется ровно w элементов, равных единице.
- (2) Если $w \equiv 0 \pmod{r}$, то в каждой строке все элементы равны wr^{-1} .
- (3) Если $w > r$, $w \not\equiv 0 \pmod{r}$, то $c_{ij} \leq \lceil wr^{-1} \rceil$ для $i, j = 1, \dots, r$.

Утверждение 3. Если $W \in W_{w,r}$ и $g \in S(X)$, то

$$\chi_W(g) \leq |X| - \lceil wr^{-1} \rceil r. \quad (4)$$

Равенство имеет место тогда и только тогда, когда $\mathbf{c}_W(g) \in C_{w,r}^{(\max)}$.

Доказательство. Обозначим через $\mathbf{c}_W((i_1, j_1), \dots, (i_{t-1}, j_{t-1}))$ матрицу, полученную из матрицы $\mathbf{c}_W$ удалением строк $i_1, \dots, i_{t-1}$ и столбцов $j_1, \dots, j_{t-1}$.

Для произвольной матрицы $\mathbf{c}_W(g) \in C_{w,r}$ выполняется неравенство

$$\lceil wr^{-1} \rceil r \leq \max \left\{ \sum_{i=1}^r c_{ii^h}(g) \mid h \in S_r \right\}.$$

Действительно, пусть наибольший элемент b_1 матрицы $\mathbf{c}_W(g)$ находится на пересечении i_1 -й строки и j_1 -го столбца, а наибольший элемент b_t матрицы $\mathbf{c}_W((i_1, j_1), \dots, (i_{t-1}, j_{t-1}))$ находится на пересечении i_t -й строки и j_t -го столбца матрицы $\mathbf{c}_W(g)$, $t = 1, \dots, r$. Тогда

$$\begin{aligned} b_1 &\geq w/r, \quad b_2 \geq (w - b_1)/(r - 1) \geq w/r, \\ b_3 &\geq (w - b_1 - b_2)/(r - 2) \geq w/r, \dots, b_r \geq \\ &\geq (w - b_1 - \dots - b_{r-1})/(r - (r - 1)) \geq w/r. \end{aligned}$$

Так как b_i — целые числа, то $b_i \geq \lceil w/r \rceil$ для $i = 1, \dots, r$. Значит,

$$\lceil wr^{-1} \rceil r \leq b_1 + \dots + b_r.$$

Отсюда и из неравенства

$$b_1 + \dots + b_r \leq \max \left\{ \sum_{i=1}^r c_{ii^h}(g) \mid h \in S_r \right\}$$

получаем, что

$$\lceil wr^{-1} \rceil r \leq b_1 + \dots + b_r \leq \max \left\{ \sum_{i=1}^r c_{ii^h}(g) \mid h \in S_r \right\}.$$

Согласно равенству (3) всегда

$$\chi_W(g) \leq |X| - \lceil wr^{-1} \rceil r.$$

Найдём условия выполнения равенства.

- (1) Если $w \leq r$, то $\lceil wr^{-1} \rceil r = r$ и $\chi_W(g) \leq |X| - r$. Пусть матрица $\mathbf{c}_W(g)$ такова, что $\chi_W(g) = |X| - r$. Так как $b_i \geq \lceil w/r \rceil$ для $i = 1, \dots, r$, то $b_1 + \dots + b_r = r$ тогда и только тогда, когда $b_i = 1$ для $i = 1, \dots, r$. Значит, $c_{ij}(g) \in \{0, 1\}$, где $i, j = 1, \dots, r$, и в каждой строке и в каждом столбце матрицы $\mathbf{c}_W(g)$ ровно w элементов равны единице, остальные элементы нули.

Таким образом, при $w \leq r$ равенство $\chi_W(g) = |X| - r$ достигается тогда и только тогда, когда $\mathbf{c}_W(g) \in C_{w,r}^{(\max)}$.

- (2) Если $w > r$, $w \equiv 0 \pmod{r}$, то из неравенства (4) имеем

$$\chi_W(g) \leq |X| - w.$$

Пусть $\mathbf{c}_W(g)$ — такая матрица, что $\chi_W(g) = |X| - w$. Так как $b_i \geq w/r$ для $i = 1, \dots, r$, то $b_1 + \dots + b_r = w$ тогда и только тогда, когда $b_i = w/r$ для $i = 1, \dots, r$. Значит, $c_{ij}(g) \leq wr^{-1}$ для $i, j = 1, \dots, r$.

Из того, что элементы матрицы $\mathbf{c}_W(g)$ должны удовлетворять соотношениям

$$\sum_{i=1}^r c_{ij}(g) = w, \quad \sum_{i=1}^r c_{ji}(g) = w, \quad c_{ij}(g) \in \{0, \dots, wr^{-1}\}$$

для $i, j = 1, \dots, r$, следует, что все элементы матрицы $\mathbf{c}_W(g)$ равны w/r .

Таким образом, равенство $\chi_W(g) = |X| - w$ достигается тогда и только тогда, когда в каждой строке матрицы $\mathbf{c}_W(g)$ все элементы равны w/r , т.е. $\left\{g \in S(X) \mid \mathbf{c}_W(g) \in C_{w,r}^{(\max)}\right\}$.

- (3) Если $w > r$, $w \not\equiv 0 \pmod{r}$, то для произвольной матрицы $\mathbf{c}_W(g) \in C_{w,r}$ выполняется неравенство

$$\chi_W(g) \leq |X| - r \cdot \lceil wr^{-1} \rceil.$$

Так как $b_i \geq \lceil w/r \rceil$ для $i = 1, \dots, r$, то

$$b_1 + \dots + b_r = r \cdot \lceil wr^{-1} \rceil$$

тогда и только тогда, когда $b_i = \lceil w/r \rceil$. Значит, $c_{ij}(g) \leq \lceil wr^{-1} \rceil$ для $i, j = 1, \dots, r$. Тогда из утверждения 1 и неравенства $c_{ij}(g) \leq \lceil wr^{-1} \rceil$ имеем

$$|X| - \sum_{i=1}^r \max \{c_{ij}(g) \mid j \in \{1, \dots, r\}\} \leq |X| - r \cdot \lceil wr^{-1} \rceil \leq \chi_W(g).$$

Неравенство (4) даёт оценку

$$\chi_W(g) \leq |X| - r \cdot \lceil wr^{-1} \rceil.$$

Значит, равенство

$$\chi_W(g) = |X| - r \cdot \lceil wr^{-1} \rceil$$

достигается тогда и только тогда, когда в каждой строке матрицы $\mathbf{c}_W(g)$ наибольший элемент равен $\lceil wr^{-1} \rceil$, т.е. для множества подстановок $\left\{g \in S(X) \mid \mathbf{c}_W(g) \in C_{w,r}^{(\max)}\right\}$. $\square$

Утверждение 4. Пусть $l : \{1, \dots, r^m\} \times \{1, \dots, m\} \rightarrow \{1, \dots, r\}$, $W = \{W_1, \dots, W_{r^m}\}$ — система импримитивности группы $\text{IG}_W \leq S(X^m)$, $W_i = W_{l(i,1)}^{(1)} \times \dots \times W_{l(i,m)}^{(m)}$ и $W^{(j)} = \{W_1^{(j)}, \dots, W_r^{(j)}\}$ — система импримитивности группы $\text{IG}_{W^{(j)}} \leq S(X)$, $j = 1, \dots, m$, $s = (s_1, \dots, s_m)$ — произвольный элемент из группы $S(X)^m$. Тогда:

- (1) $c_{ij}(s) = \prod_{t=1}^m c_{l(i,t)l(j,t)}(s_t)$ для $i, j = 1, \dots, r^m$.
- (2) $\chi_W(s) = |X|^m - \max \left\{ \sum_{i=1}^{r^m} \prod_{t=1}^m c_{l(i,t)l(i^h,t)}(s_t) \mid h \in S_{r^m} \right\}$.
- (3) $\chi_W(s) \leq |X|^m - \prod_{i=1}^m (|X| - \chi_{W^{(i)}}(s_i))$.

Доказательство. Для любых $i, j = 1, \dots, r^m$ справедливы равенства

$$\begin{aligned} c_{ij}(s) &= \left| \left(W_{l(i,1)}^{(1)} \times \dots \times W_{l(i,m)}^{(m)} \right)^s \cap \left(W_{l(j,1)}^{(1)} \times \dots \times W_{l(j,m)}^{(m)} \right) \right| = \\ &= \prod_{t=1}^m \left| \left(W_{l(i,t)}^{(t)} \right)^{s_i} \cap W_{l(j,t)}^{(t)} \right| = \prod_{t=1}^m c_{l(i,t)l(j,t)}(s_t). \end{aligned}$$

Значит,

$$\mathbf{c}_W(s) = \left(\prod_{t=1}^m c_{l(i,t)l(j,t)}(s_t) \right).$$

Из теоремы 1 следует, что

$$\chi_W(s) = |X|^m - \max \left\{ \sum_{i=1}^{r^m} \prod_{t=1}^m c_{l(i,t)l(i^h,t)}(s_t) \mid h \in S_{r^m} \right\}.$$

Приведём оценку сверху расстояния $\chi_W(s)$. Обозначим

$$\bar{\chi}(s_i, g_i) = |\{\alpha \in X \mid \alpha^{s_i} = \alpha^{g_i}\}| = |X| - \chi(s_i, g_i).$$

Так как

$$\bar{\chi}((s_1, \dots, s_m), (g_1, \dots, g_m)) = \prod_{i=1}^m \bar{\chi}(s_i, g_i) = \prod_{i=1}^m (|X| - \chi(s_i, g_i)),$$

то

$$\begin{aligned} \chi((s_1, \dots, s_m), (g_1, \dots, g_m)) &= |X|^m - \bar{\chi}((s_1, \dots, s_m), (g_1, \dots, g_m)) = \\ &= |X|^m - \prod_{i=1}^m (|X| - \chi(s_i, g_i)). \end{aligned}$$

Кроме того, из включения

$$\text{IG}_{W^{(1)}} \times \dots \times \text{IG}_{W^{(m)}} \leq \text{IG}_W,$$

следует, что

$$\chi_W(s) \leq \min \{ \chi(s, (g_1, \dots, g_m)) \mid (g_1, \dots, g_m) \in \text{IG}_{W^{(1)}} \times \dots \times \text{IG}_{W^{(m)}} \}.$$

Значит,

$$\begin{aligned} &\chi_W(s) \leq \\ &\leq \min \left\{ |X|^m - \prod_{i=1}^m (|X| - \chi(s_i, g_i)) \mid (g_1, \dots, g_m) \in \text{IG}_{W^{(1)}} \times \dots \times \text{IG}_{W^{(m)}} \right\} \leq \\ &\leq |X|^m - \prod_{i=1}^m (|X| - \chi_{W^{(i)}}(s_i)). \square \end{aligned}$$

Отметим, что для любой подстановки $b \in S_r$ выполняется неравенство

$$|X| - \sum_{i=1}^r \max \{ c_{ij}(g) \mid j = 1, \dots, r \} \leq \chi_W(g) \leq |X| - \sum_{i=1}^r c_{ii^b}(g). \quad (5)$$

Неравенство (5) позволяет оценить величину $\chi_W(g)$, когда её трудно найти по формуле (3).

3. Расстояние от подстановки до группы IG_W в терминах коэффициента изометричности

Рассмотрим ещё одну меру близости между произвольной подстановкой и группой IG_W . Несложно показать, что любая группа IG_W является не только группой изометрий метрики Хемминга на словах длины r над алфавитом W , но и группой изометрий метрики графа орбиталов [6]

$$\mu_W(\alpha, \beta) = \begin{cases} 1, & \text{если } \alpha \in W_i, \beta \in W_j, i \neq j, \\ 2, & \text{если } \alpha, \beta \in W_i, i \in \{1, \dots, r\}. \end{cases}$$

Величиной, характеризующей для данной метрики $\mu = \mu_W$ удалённость подстановки g от группы IG_W , является коэффициент изометричности

$$\eta_W(g) = \sum_{\alpha, \beta \in X} I(\mu(\alpha^g, \beta^g) = \mu(\alpha, \beta)),$$

здесь $I(A)$ — индикатор выполнения условия A .

Очевидно, чем меньше значение коэффициента изометричности, тем хуже подстановка $g \in S(X)$ сохраняет метрику μ . В этом смысле можно говорить, что при меньшем значении коэффициента изометричности подстановка $g \in S(X)$ лежит дальше от группы IG_W в метрике

$$\rho_W(g) = |X|^2 - \eta_W(g) = 2w|X| - 2 \sum_{i=1}^r \sum_{t=1}^r c_{it}(g)^2,$$

чем подстановка при большем значении коэффициента изометричности.

В частности, $0 \leq \rho_W(g) \leq |X|^2$ и $\rho_W(g) = 0$, если $g \in IG_W$. Рассмотрим коэффициент изометричности более подробно.

Утверждение 5. Пусть $W \in W_{w,r}$ и $g \in S(X)$. Тогда

$$\eta_W(g) = |X|^2 - 2 \left(w|X| - \sum_{i=1}^r \sum_{t=1}^r c_{it}(g)^2 \right) \leq |X|^2.$$

Доказательство. Из определения следует, что

$$\begin{aligned} \eta_W(g) &= \sum_{\alpha, \beta \in X} I(\mu_W(\alpha^g, \beta^g) = \mu_W(\alpha, \beta)) = \\ &= \sum_{\alpha, \beta \in X: \mu_W(\alpha, \beta) = 0} I(\mu_W(\alpha^g, \beta^g) = 0) + \sum_{\alpha, \beta \in X: \mu_W(\alpha, \beta) = 2} I(\mu_W(\alpha^g, \beta^g) = 2) + \\ &+ \sum_{\alpha, \beta \in X: \mu_W(\alpha, \beta) = 1} I(\mu_W(\alpha^g, \beta^g) = 1) = |X| + \sum_{\alpha, \beta \in X: \mu_W(\alpha, \beta) = 2} I(\mu_W(\alpha^g, \beta^g) = 2) + \\ &+ \sum_{\alpha, \beta \in X: \mu_W(\alpha, \beta) = 1} I(\mu_W(\alpha^g, \beta^g) = 1). \end{aligned}$$

Имеют место равенства

$$\begin{aligned}
 & \sum_{\alpha, \beta \in X: \mu_W(\alpha, \beta) = 2} I(\mu_W(\alpha^g, \beta^g) = 2) = \\
 &= \sum_{i=1}^r \sum_{j=1}^r \sum_{\alpha, \beta \in W_i, \alpha \neq \beta} I((\alpha^g, \beta^g) \in W_j^2) = \\
 &= \sum_{i=1}^r \sum_{j=1}^r \sum_{\alpha, \beta \in W_i} I((\alpha^g, \beta^g) \in W_j^2) - \sum_{i=1}^r \sum_{j=1}^r \sum_{\alpha, \beta \in W_i, \alpha = \beta} I((\alpha^g, \beta^g) \in W_j^2) = \\
 &= \sum_{i=1}^r \sum_{j=1}^r c_{ij}(g)^2 - \sum_{i=1}^r \sum_{j=1}^r c_{ij}(g) = \sum_{i=1}^r \sum_{j=1}^r c_{ij}(g)^2 - |X|. \tag{6}
 \end{aligned}$$

Пусть $j, t \in \{1, \dots, r\}$. Воспользовавшись равенством (1), получаем:

$$\sum_{\beta \in W_j} I(\beta^g \notin W_t) = |W_t| - |W_j^g \cap W_t| = w - c_{jt}(g). \tag{7}$$

Применяя равенство (7), имеем

$$\begin{aligned}
 & \sum_{\alpha, \beta \in X: \mu_W(\alpha, \beta) = 1} I(\mu_W(\alpha^g, \beta^g) = 1) = \\
 &= \sum_{j, i \in \{1, \dots, r\}, j \neq i} \sum_{\alpha \in W_i} \sum_{\beta \in W_j} \sum_{t=1}^r I(\alpha^g \in W_t) I(\beta^g \notin W_t) = \\
 &= \sum_{j, i \in \{1, \dots, r\}, j \neq i} \sum_{t=1}^r c_{it}(g) \cdot (w - c_{jt}(g)) = \\
 &= \sum_{j, i \in \{1, \dots, r\}, j \neq i} \sum_{t=1}^r c_{it}(g) \cdot w - \sum_{j, i \in \{1, \dots, r\}, j \neq i} \sum_{t=1}^r c_{it}(g) \cdot c_{jt}(g). \tag{8}
 \end{aligned}$$

Учитывая, что $\sum_{t=1}^r c_{it}(g) = w$, $|X| = r \cdot w$ согласно равенству (1), получаем

$$\begin{aligned}
 \sum_{j, i \in \{1, \dots, r\}, j \neq i} \sum_{t=1}^r c_{it}(g) w &= \sum_{j, i \in \{1, \dots, r\}, j \neq i} w^2 = r(r-1)w^2 = \\
 &= |X|^2 - |X| \cdot w. \tag{9}
 \end{aligned}$$

Далее,

$$\begin{aligned}
 \sum_{j, i \in \{1, \dots, r\}, j \neq i} \sum_{t=1}^r c_{it}(g) c_{jt}(g) &= \sum_{i=1}^r \sum_{t=1}^r c_{it}(g) \left(\sum_{j \in \{1, \dots, r\} \setminus \{i\}} c_{jt}(g) \right) = \\
 &= \sum_{i=1}^r \sum_{t=1}^r c_{it}(g) (w - c_{it}(g)) = \sum_{i=1}^r w^2 - \sum_{i=1}^r \sum_{t=1}^r c_{it}(g)^2 =
 \end{aligned}$$

$$= |X| w - \sum_{i=1}^r \sum_{t=1}^r c_{it}(g)^2. \quad (10)$$

Подставляя равенства (9) и (10) в (8), имеем

$$\begin{aligned} & \sum_{\alpha, \beta \in X: \mu_W(\alpha, \beta)=1} I(\mu_W(\alpha^g, \beta^g) = 1) = \\ & = |X|^2 + \sum_{i=1}^r \sum_{t=1}^r c_{it}(g)^2 - 2|X|w. \end{aligned} \quad (11)$$

Подставляя равенства (11) и (6) в выражение для η_W , получаем

$$\eta_W(g) = |X|^2 + 2 \sum_{i=1}^r \sum_{t=1}^r c_{it}(g)^2 - 2w|X|. \quad (12)$$

Из равенства (1) следует, что

$$\sum_{t=1}^r c_{it}(g)^2 \leq \left(\sum_{t=1}^r c_{it}(g) \right)^2 = w^2$$

для произвольного $i \in \{1, \dots, r\}$. Значит,

$$\sum_{i=1}^r \sum_{t=1}^r c_{it}(g)^2 \leq w^2 r, \text{ и } \eta_W(g) \leq |X|^2. \quad \square$$

Укажем нижнюю оценку коэффициента изометричности $\eta_W(g)$.

Следствие 2. Пусть выполнены условия утверждения 5. Тогда:

(1) Если $w \leq r$, то

$$\begin{aligned} |X|^2 - 2|X|(w-1) & \leq \eta_W(g), \\ 0 & \leq \rho_W(g) \leq 2|X|(w-1). \end{aligned}$$

(2) Если $w > r$, то $w = \lfloor r^{-1}w \rfloor x_1 + \lceil r^{-1}w \rceil x_2$ при некоторых $x_1, x_2 \geq 0, x_1 + x_2 = r$

$$\begin{aligned} |X|^2 - 2w|X| + 2r \left(\lfloor r^{-1}w \rfloor^2 x_1 + \lceil r^{-1}w \rceil^2 x_2 \right) & \leq \eta_W(g), \\ 0 & \leq \rho_W(g) \leq 2w|X| - 2r \left(\lfloor r^{-1}w \rfloor^2 x_1 + \lceil r^{-1}w \rceil^2 x_2 \right). \end{aligned}$$

(3) Если $w > r, w \not\equiv 0 \pmod{r}$, то

$$|X|^2 + 2w^2(1-r) \leq \eta_W(g), \quad 0 \leq \rho_W(g) \leq 2w^2(r-1).$$

Доказательство. Справедливы равенства

$$\min \left\{ \sum_{j=1}^r c_j^2 \mid c_1, \dots, c_r \in \mathbb{N}_0, c_1 + \dots + c_r = w \right\} =$$

$$= \begin{cases} \lfloor wr^{-1} \rfloor^2 x_1 + \lceil wr^{-1} \rceil^2 x_2, & \text{если } w > r, \\ w, & \text{если } w \leq r. \end{cases} \quad (13)$$

Отсюда и из утверждения 5 при $w < r$ получаем соотношение

$$\begin{aligned} \eta_W(g) &= |X|^2 + 2 \sum_{i=1}^r \sum_{t=1}^r c_{it}(g)^2 - 2w|X| \geq \\ &\geq |X|^2 + 2wr - 2w|X| = |X|^2 + 2|X|(1-w). \end{aligned}$$

Если $w > r$, то из равенств (12) и (13) имеем

$$\begin{aligned} 2 \sum_{i=1}^r \sum_{t=1}^r c_{it}(g)^2 &\geq 2r \left(\lfloor r^{-1}w \rfloor^2 x_1 + \lceil r^{-1}w \rceil^2 x_2 \right), \\ \eta_W(g) &\geq |X|^2 + 2r \left(\lfloor r^{-1}w \rfloor^2 x_1 + \lceil r^{-1}w \rceil^2 x_2 \right) - 2w|X|. \end{aligned}$$

Если $w \equiv 0 \pmod{r}$, то из равенств (12) и (13) следует, что

$$\begin{aligned} \sum_{i=1}^r \sum_{t=1}^r c_{it}(g)^2 &= (wr^{-1})^2 \cdot r^2 = w^2, \\ \eta_W(g) &\geq |X|^2 + 2w^2 - 2w|X| = |X|^2 + 2w^2(1-r). \end{aligned}$$

Значит,

$$|X|^2 - 2w(|X| - w) \leq \eta_W(g). \square$$

По следствию 2 максимально ρ_W -удалёнными от группы IG_W являются подстановки с минимальным коэффициентом изометричности. Приведём примеры значений коэффициента изометричности для групп сплетений IG_W для $W \in W_{2,2^{n-1}}$ и $W \in W_{2^{n-1},2}$, являющихся группами изометрий групповых подметрик метрики Хемминга [4].

- (1) Группа IG_W с системой импримитивности $W = \{W_0, W_1\} \in W_{2^{n-1},2}$, где W_0 — множество всех векторов чётного веса, является группой изометрий метрики

$$\mu_W(\alpha, \beta) = \begin{cases} 1, & \text{если } \|\beta \oplus \alpha\| \equiv 1 \pmod{2}, \\ 2, & \text{если } \|\beta \oplus \alpha\| \equiv 0 \pmod{2}. \end{cases}$$

Для произвольной подстановки $g \in S(V_{2^n})$ имеет место равенство

$$c_{11}(g) + c_{12}(g) = c_{21}(g) + c_{22}(g) = 2^{n-1}.$$

Из утверждения 5 и следствия 2 имеем

$$\eta_W(g) = 2 \left((2^n - c_{11}(g))^2 + c_{11}(g)^2 + (2^n - c_{22}(g))^2 + c_{22}(g)^2 \right).$$

- (2) Группа IG_W с системой импримитивности $W = \{W_1, \dots, W_{2^{n-1}}\} \in W_{2,2^{n-1}}$, где $W_i = \{\alpha_i, \alpha_i \oplus \vec{1}\}$, является группой изометрий метрики

$$\mu_W(\alpha, \beta) = \begin{cases} 1, & \text{если } \|\alpha \oplus \beta\| \in \{1, \dots, n-1\}, \\ 2, & \text{если } \|\alpha \oplus \beta\| = n. \end{cases}$$

Так как

$$\sum_{t=1}^{2^{n-1}} c_{it}(g) = \sum_{t=1}^{2^{n-1}} c_{tj}(g) = 2, \quad i, j \in \{1, \dots, 2^{n-1}\},$$

то из следствия 2 имеем

$$\left(1 - \frac{1}{2^{n-1}}\right) |X|^2 \leq \eta_W(g) \leq |X|^2.$$

Следствие 2 позволяет оценить число подстановок $g \in S(X)$, максимально далеких от группы IG_W в метрике ρ_W . Для этого обозначим через $C_{w,r}^{(\max)}(\rho)$ множество всех матриц $\mathbf{c}_W = \|c_{ij}\| \in C_{w,r}$ со следующими свойствами.

- (1) Если $\lceil wr^{-1} \rceil \leq 1$, то $C_{w,r}^{(\max)}(\rho) = C_{w,r}^{(\max)}$.
- (2) Если $\lceil wr^{-1} \rceil \geq 2$, то в каждой строке матрицы $\mathbf{c}_W(g)$ ровно x_1 элементов равны $\lceil wr^{-1} \rceil$ и ровно x_2 элементов равны $\lceil wr^{-1} \rceil$, где

$$w = \lceil wr^{-1} \rceil x_1 + \lceil wr^{-1} \rceil x_2, \quad x_1, x_2 \geq 0, \quad x_1 + x_2 = r.$$

Утверждение 6. Пусть $W \in W_{w,r}$, $\mathbf{c}$ — произвольная матрица из $C_{w,r}^{(\max)}(\rho)$. Тогда число $n_{w,r}^{(2)}$ подстановок, максимально далёких от группы IG_W в метрике $\rho_W(g)$, удовлетворяет соотношениям:

- (1) $n_{w,r}^{(2)} = \left| C_{w,r}^{(\max)}(\rho) \right| \cdot |\{g \in S(X) | \mathbf{c} = \mathbf{c}_W(g)\}|$.
- (2) $n_{w,r}^{(2)} \leq \binom{r}{w} (w!)^{2r}$, если $w \leq r$.
- (3) $n_{w,r}^{(2)} = ((w/r)!)^{-r^2} (w!)^{2r}$, если $w > r$, $w \equiv 0 \pmod{r}$.
- (4) $n_{w,r}^{(2)} \leq \binom{r}{x_1} \lceil r^{-1}w \rceil^{-r \cdot x_1} \lceil r^{-1}w \rceil^{-r \cdot x_2} (w!)^{2r}$, если

$$w > r, \quad w \not\equiv 0 \pmod{r}, \quad w = \lceil r^{-1}w \rceil x_1 + \lceil r^{-1}w \rceil x_2,$$

$$x_1, x_2 \geq 0, \quad x_1 + x_2 = r.$$

Доказательство. 1, 2. Пусть $w \leq r$. Из доказательства следствия 2 получаем, что подстановка $g \in S(X)$ максимально удалена от группы IG_W в метрике $\rho_W(g)$, если в каждой строке матрицы $\mathbf{c}_W(g)$ имеется ровно w элементов, равных единице, т.е. $C_{w,r}^{(\max)}(\rho) = C_{w,r}^{(\max)}$. Очевидно, что

$$n_{w,r}^{(2)} = \left| C_{w,r}^{(\max)}(\rho) \right| \cdot |\{g \in S(X) | \mathbf{c} = \mathbf{c}_W(g)\}|, \quad \left| C_{w,r}^{(\max)}(\rho) \right| \leq \binom{r}{w}.$$

Пусть $\mathbf{c}$ — произвольная матрица из множества $C_{w,r}^{(\max)}(\rho)$. Из следствия 1 и включения $c_{ij} \in \{0, 1\}$ получаем, что

$$|\{g \in S(X) | \mathbf{c} = \mathbf{c}_W(g)\}| = (w!)^{2r}.$$

Отсюда следует справедливость пункта 2.

3. Пусть $w > r$, $w \equiv 0 \pmod{r}$. Из доказательства следствия 2 получаем, что подстановка $g \in S(X)$ максимально удалена от группы IG_W в метрике $\rho_W(g)$, если в каждой строке матрицы $\mathbf{c}_W(g)$ все элементы равны w/r , т.е.

$$c_{i1}(g) = c_{i2}(g) = \dots = c_{ir}(g) = wr^{-1}$$

для $i = 1, \dots, r$. Такая матрица $\mathbf{c} \in C_{w,r}$ единственна. Из равенства (2) получаем требуемое.

4. Пусть $w > r$, $w \not\equiv 0 \pmod{r}$. Из доказательства следствия 2 получаем, что подстановка $g \in S(X)$ максимально удалена от группы IG_W в метрике $\rho_W(g)$, если в каждой строке матрицы $\mathbf{c}_W(g)$ точно x_1 элементов равны $\lceil wr^{-1} \rceil$ и точно x_2 элементов равны $\lfloor wr^{-1} \rfloor$. Число всех таких матриц не превосходит $\binom{r}{x_1}^r$. Из равенства (2) получаем, что

$$|\{g \in S(X) | \mathbf{c} = \mathbf{c}_W(g)\}| = \lfloor r^{-1}w \rfloor^{-r \cdot x_1} \lceil r^{-1}w \rceil^{-r \cdot x_2} (w!)^{2r}.$$

Отсюда получаем требуемое. $\square$

Отметим, что в доказательстве утверждения 6 помимо оценки числа подстановок, максимально далёких от группы IG_W в метрике $\rho_W(g)$, содержится их полное описание.

Из утверждения 3 и следствия 2 следует, что множество подстановок, максимально далёких от группы IG_W в метрике $\rho_W(g)$, и множество подстановок, максимально далёких от группы IG_W в метрике Хемминга, задаются одним и тем же множеством матриц $C_{w,r}^{(\max)}$, если $\lceil wr^{-1} \rceil \leq 1$ или $w \equiv 0 \pmod{r}$. Если же $\lceil wr^{-1} \rceil \geq 2$ и $w \not\equiv 0 \pmod{r}$, то имеет место включение $C_{w,r}^{(\max)}(\rho) \subseteq C_{w,r}^{(\max)}$.

4. Примеры расстояний χ_W

4.1. Расстояния χ_W в случае $W \in W_{w,2}$

Пусть $r = 2$, $n = 2w$, $W \in W_{w,2}$. Тогда для произвольной подстановки $g \in S(X)$ матрица $\mathbf{c}_W(g)$ имеет вид

$$\mathbf{c}_W(g) = \begin{pmatrix} a & w-a \\ w-a & a \end{pmatrix}$$

для некоторого элемента $a \in \{0, \dots, w\}$. Следовательно,

$$\begin{aligned} \chi_W(g) &= 2w - \max\{2a, 2(w-a)\} = \\ &= 2w - 2 \max\{a, w-a\} = 2 \min\{a, w-a\}. \end{aligned}$$

В частности, расстояние всегда чётно.

Из утверждения 2 следует, что

$$|\{g \in S(X) | \mathbf{c} = \mathbf{c}_W(g)\}| = (w!)^2 \binom{w}{a}^2.$$

Значит, число подстановок, удалённых от множества IG_W на величину $\chi_W(g)$, равно:

$$\begin{aligned}
& - (w!)^2 \binom{w}{a}^2 + (w!)^2 \binom{w}{w-a}^2 = 2(w!)^2 \binom{w}{a}^2, \text{ если } a \neq w/2; \\
& - (w!)^2 \binom{w}{w/2}^2, \text{ если } a = w/2.
\end{aligned}$$

Наибольшее расстояние подстановок $g \in S(X)$ до группы IG_W равно $2 \lfloor w/2 \rfloor$. Значит, число подстановок, находящихся от множества IG_W на максимальном расстоянии, равно $(w!)^2 \binom{w}{w/2}^2$ при $w \equiv 0 \pmod{2}$ и равно $2(w!)^2 \binom{w}{\lfloor w/2 \rfloor}^2$ при $w \not\equiv 0 \pmod{2}$.

4.2. Алгоритм блочного шифрования SMS4

Приведём оценку расстояния χ_W для преобразований алгоритма блочного шифрования SMS4 [2] до группы IG_W при некоторых системах импримитивности W .

Пусть функция $f : V_{32} \rightarrow V_{32}$ задаётся равенством

$$f(\alpha) = \alpha \oplus (\alpha \lll 2) \oplus (\alpha \lll 10) \oplus (\alpha \lll 18) \oplus (\alpha \lll 24),$$

где $\alpha \lll j$ — циклический сдвиг вектора $\alpha \in V_{32}$ на j координат влево, $s = (s_1, s_2, s_3, s_4)$ — слой s -боксов алгоритма SMS4, где $s_1 = s_2 = s_3 = s_4$, $s_i \in S(V_8)$.

Раундовая функция $g_k : V_{32}^4 \rightarrow V_{32}^4$ алгоритма SMS4 задаётся равенством

$$g_k : (\delta_3, \delta_2, \delta_1, \delta_0) \mapsto (\delta_3, \delta_2, \delta_1, \delta_3 \oplus (\delta_2 \oplus \delta_1 \oplus \delta_0 \oplus k)^h),$$

где $h = sf$, $h_k : V_{32} \rightarrow V_{32}$, $h_k : \beta \mapsto \beta \oplus k$, $k \in V_{32}$ — раундовый ключ.

Группа $G = \langle f, h_k | k \in V_{32} \rangle$ имеет системы импримитивности $W^{(i)} = \left\{ \left(\left(W_1^{(i)} \right)^4 \right)^g | g \in G \right\}$, $i = 1, \dots, 5$, каждая из которых задаётся блоком импримитивности $\left(W_1^{(i)} \right)^4$, являющимся декартовой степенью.

$$W_1^{(1)} = \{(\alpha_7, 0, \alpha_5, 0, \alpha_3, 0, \alpha_1, 0) | (\alpha_7, \alpha_5, \alpha_3, \alpha_1) \in V_4\},$$

$$W_1^{(2)} = \{(0, \alpha_6, 0, \alpha_4, 0, \alpha_2, 0, \alpha_0) | (\alpha_6, \alpha_4, \alpha_2, \alpha_0) \in V_4\},$$

$$W_1^{(3)} = \{(0, 1, 0, 1, 0, 1, 0, 1), \vec{0}\}, W_1^{(4)} = \{(1, 0, 1, 0, 1, 0, 1, 0), \vec{0}\},$$

$$W_1^{(5)} = \{(1, 1, 1, 1, 1, 1, 1, 1), \vec{0}\}.$$

Положим

$$\widetilde{W}^{(i)} = \left\{ W_1^{(i)} \oplus \beta | \beta \in V_8 \right\}, \quad i = 1, \dots, 5.$$

Для каждой из систем импримитивности найдём оценку расстояния $\chi_{W^{(i)}}(h)$, $i = 1, \dots, 5$. Так как $W^{(i)}$ — блок импримитивности группы G , то $\chi_{W^{(i)}}(s) = \chi_{W^{(i)}}(sf)$, и достаточно найти только расстояние от слоя s -боксов $s = (s_1, s_2, s_3, s_4)$ до группы $\text{IG}_{W^{(i)}}$.

I. Система импримитивности $W^{(1)}$. Матрица $\mathbf{c}_{\widetilde{W}^{(1)}}(s_1)$ находится прямыми вычислениями:

$$\mathbf{c}_{\widetilde{W}^{(1)}}(s_1) = \begin{pmatrix} 1 & 3 & 0 & 0 & 0 & 1 & 3 & 1 & 3 & 1 & 0 & 0 & 2 & 0 & 1 & 0 \\ 0 & 2 & 1 & 0 & 1 & 0 & 1 & 1 & 2 & 1 & 1 & 0 & 0 & 0 & 5 & 1 \\ 2 & 0 & 2 & 1 & 2 & 1 & 0 & 2 & 2 & 0 & 2 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 2 & 2 & 2 & 1 & 4 & 1 & 2 & 0 & 0 \\ 2 & 2 & 0 & 1 & 2 & 1 & 2 & 1 & 2 & 0 & 1 & 0 & 0 & 0 & 0 & 2 \\ 0 & 1 & 3 & 0 & 1 & 2 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 1 & 1 & 2 \\ 1 & 0 & 3 & 0 & 1 & 2 & 0 & 1 & 1 & 2 & 0 & 1 & 0 & 1 & 1 & 2 \\ 1 & 0 & 3 & 2 & 0 & 1 & 2 & 1 & 0 & 2 & 1 & 0 & 0 & 1 & 0 & 2 \\ 2 & 2 & 1 & 3 & 0 & 1 & 1 & 2 & 0 & 0 & 0 & 2 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 2 & 1 & 3 & 1 & 0 & 1 & 2 & 0 & 0 & 0 & 2 & 2 & 0 \\ 0 & 1 & 1 & 0 & 0 & 2 & 1 & 2 & 0 & 0 & 2 & 2 & 2 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 2 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 2 & 2 & 1 & 2 \\ 2 & 1 & 0 & 3 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 3 & 1 & 0 & 2 \\ 2 & 0 & 0 & 0 & 2 & 0 & 1 & 0 & 0 & 4 & 4 & 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 2 & 1 & 1 & 1 & 0 & 0 & 1 & 2 & 2 & 3 & 0 & 2 \\ 2 & 1 & 0 & 1 & 1 & 0 & 1 & 3 & 1 & 1 & 1 & 2 & 0 & 0 & 2 & 0 \end{pmatrix}.$$

Тогда $\sum_{i=1}^{16} c_{ii^b}(s_1) = 44$ для

$$b = (1, 2, 15, 14, 10, 6, 3)(7, 9, 4, 12, 16, 8)(5)(11)(13).$$

Нетрудно убедиться, что

$$\sum_{i=1}^r \max \{c_{ij}(g) | j = 1, \dots, r\} = \sum_{i=1}^r c_{ii^b}(g).$$

Таким образом, из неравенства (5) следует, что $\chi_{\widetilde{W}^{(1)}}(s_1) = 212$. Из утверждения 3 получаем, что наибольшее расстояние между подстановкой из $S(V_8)$ и группой $\text{IG}_{\widetilde{W}^{(1)}}$ равно $2^8 - 2^4 = 240$. Значит, s_1 не лежит на наибольшем расстоянии от $\text{IG}_{\widetilde{W}^{(1)}}$, но находится относительно не далеко от подстановок, лежащих на наибольшем расстоянии от $\text{IG}_{\widetilde{W}^{(1)}}$.

Из утверждения 4 имеем $\chi_{W^{(1)}}(s) \leq 2^{32} - 44^4$. Из утверждения 3 следует, что наибольшее расстояние между подстановкой из $S(V_{32})$ и группой $\text{IG}_{W^{(1)}}$ равно $2^{32} - 2^{16}$. Так как $44^4 \approx 2^{21.838}$, то расстояние между раундовой функцией алгоритма SMS4 и $\text{IG}_{W^{(1)}}$ не является максимальным.

II. Система импримитивности $W^{(2)}$. Матрица $\mathbf{c}_{\widetilde{W}^{(1)}}(s_1)$ находится прямыми

вычислениями:

$$\mathbf{c}_{\widetilde{W}^{(1)}}(s_1) = \begin{pmatrix} 1 & 3 & 0 & 0 & 0 & 1 & 3 & 1 & 3 & 1 & 0 & 0 & 2 & 0 & 1 & 0 \\ 0 & 2 & 1 & 0 & 1 & 0 & 1 & 1 & 2 & 1 & 1 & 0 & 0 & 0 & 5 & 1 \\ 2 & 0 & 2 & 1 & 2 & 1 & 0 & 2 & 2 & 0 & 2 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 2 & 2 & 2 & 1 & 4 & 1 & 2 & 0 & 0 \\ 2 & 2 & 0 & 1 & 2 & 1 & 2 & 1 & 2 & 0 & 1 & 0 & 0 & 0 & 0 & 2 \\ 0 & 1 & 3 & 0 & 1 & 2 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 1 & 1 & 2 \\ 1 & 0 & 3 & 0 & 1 & 2 & 0 & 1 & 1 & 2 & 0 & 1 & 0 & 1 & 1 & 2 \\ 1 & 0 & 3 & 2 & 0 & 1 & 2 & 1 & 0 & 2 & 1 & 0 & 0 & 1 & 0 & 2 \\ 2 & 2 & 1 & 3 & 0 & 1 & 1 & 2 & 0 & 0 & 0 & 2 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 2 & 1 & 3 & 1 & 0 & 1 & 2 & 0 & 0 & 0 & 2 & 2 & 0 \\ 0 & 1 & 1 & 0 & 0 & 2 & 1 & 2 & 0 & 0 & 2 & 2 & 2 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 2 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 2 & 2 & 1 & 2 \\ 2 & 1 & 0 & 3 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 3 & 1 & 0 & 2 \\ 2 & 0 & 0 & 0 & 2 & 0 & 1 & 0 & 0 & 4 & 4 & 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 2 & 1 & 1 & 1 & 0 & 0 & 1 & 2 & 2 & 3 & 0 & 2 \\ 2 & 1 & 0 & 1 & 1 & 0 & 1 & 3 & 1 & 1 & 1 & 2 & 0 & 0 & 2 & 0 \end{pmatrix}.$$

Тогда $\sum_{i=1}^{16} c_{ii^b}(s_1) = 44$ для

$$b = (1, 2, 15, 14, 10, 6, 3)(7, 9, 4, 12, 16, 8)(5)(11)(13).$$

Нетрудно убедиться, что

$$\sum_{i=1}^r \max \{c_{ij}(g) | j = 1, \dots, r\} = \sum_{i=1}^r c_{ii^b}(g).$$

Таким образом, из неравенства (5) следует, что $\chi_{\widetilde{W}^{(1)}}(s_1) = 212$.

Из утверждения 3 следует, что наибольшее расстояние между подстановками из $S(V_8)$ и группой $\text{IG}_{\widetilde{W}^{(2)}}$ равно 240. Значит, подстановка s_1 не лежит на максимальном расстоянии от группы $\text{IG}_{\widetilde{W}^{(2)}}$. Расстояния $\chi_{\widetilde{W}^{(2)}}(s_1)$, $\chi_{\widetilde{W}^{(1)}}(s_1)$, хотя и близки, но различны, и $\chi_{\widetilde{W}^{(2)}}(s_1) < \chi_{\widetilde{W}^{(1)}}(s_1)$. Система $\widetilde{W}^{(2)}$ менее "тривиальна", в отличие от системы $\widetilde{W}^{(1)}$. Кроме того, для системы $\widetilde{W}^{(2)}$ подстановка s_1 находится на меньшем расстоянии от группы $\text{IG}_{\widetilde{W}^{(2)}}$, чем от группы $\text{IG}_{\widetilde{W}^{(1)}}$.

Согласно утверждению 4, $\chi_{W^{(2)}}(s) \leq 2^{32} - (45)^4$. Из утверждения 4 следует, что наибольшее расстояние между подстановкой из $S(V_{32})$ и группой $\text{IG}_{W^{(2)}}$ равно $2^{32} - 2^{16}$. Так как $45^4 \approx 2^{21.967}$, то расстояние между раундовой функцией алгоритма SMS4 и $\text{IG}_{W^{(2)}}$ заведомо не является максимальным.

III. Системы импримитивности $W^{(3)}, W^{(4)}, W^{(5)}$. Во всех матрицах $\mathbf{c}_{W^{(3)}}(s)$, $\mathbf{c}_{W^{(4)}}(s)$, $\mathbf{c}_{W^{(5)}}(s)$ каждая строка имеет два элемента, равных 1, остальные элементы нулевые. Справедливы равенства $\chi_{\widetilde{W}^{(i)}}(s_1) = 128$, $i = 3, 4, 5$. Следовательно, из утверждения 4 имеем $\chi_{W^{(i)}}(s) = 2^{32} - 2^{28}$, $i = 3, 4, 5$. Отметим, что наибольшее расстояние между подстановкой из $S(V_{32})$ и группой $\text{IG}_{W^{(i)}}$ равно $2^{32} - 2^{28}$, $i = 3, 4, 5$. Таким образом, раундовая функция алгоритма SMS4 находится на максимальном расстоянии от группы $\text{IG}_{W^{(i)}}$, $i = 3, 4, 5$.

Список литературы

1. Bailey R. F., *Permutation groups, error-correcting codes and uncovering*, PhD thesis, Queen Mary, Univ. London, 2005.
2. Zhang L., Zhang W., Wu W., Cryptanalysis of reduced-round SMS4 Block cipher. In: *Proc. of ACISP'08*, 2008, pp. 216–229.
3. Погорелов Б. А., Пудовкина М. А., Линейные структуры групп подстановок векторных пространств. В сб.: *Математика и безопасность информационных технологий*. МЦНМО, Москва, 2007, с. 142–147.
4. Глухов М. М., Елизаров В. П., Нечаев А. А., *Алгебра*. Гелиос АРВ, Москва, 2003.
5. Погорелов Б. А., Пудовкина М. А., Факторструктуры преобразований. *Математические вопросы криптографии* (2012) **3**, №3, 81–104.
6. Погорелов Б. А., Пудовкина М. А., Натуральные метрики и их свойства. Ч.2. Случай метрик Хемминга. *Математические вопросы криптографии* (2012) **3**, №1, 71–95.

Статья поступила 25.07.2013.