Сравнительный анализ конечных абелевых групп в связи с их криптографическими приложениями

А. В. ГАЛАТЕНКО
Московский государственный университет им. М. В. Ломоносова
e-mail: agalat@msu.ru

А. А. НЕЧАЕВ

А. Е. ПАНКРАТЬЕВ
Московский государственный университет им. М. В. Ломоносова
e-mail: anton.pankratiev@gmail.com

УДК 512.542

Ключевые слова: конечная абелева группа, биграмма, матрица переходных вероятностей.

Аннотация

В работе представлены результаты экспериментального анализа свойств конечных абелевых групп небольших порядков с точки зрения применимости исследуемых групп в криптографических приложениях.

Abstract

A. V. Galatenko, A. A. Nechaev, A. E. Pankrat'ev, Comparing finite Abelian groups from the standpoint of their cryptographic applications, Fundamentalnaya i prikladnaya matematika, vol. 20 (2015), no. 1, pp. 9—16.

This work presents the results of an experimental study of some properties of low-order finite Abelian groups from the standpoint of the applicability of such groups in cryptographic applications.

1. Введение. Постановка задачи

Рассматриваются две группы $G_1, G_2 < S(\Omega)$ подстановок на алфавите $\Omega = \overline{0, p^n - 1}$, где p — простое число:

G_1 — регулярное представление циклической группы $(\mathbb{Z}_{p^n}, +)$ подстановками

$$\hat{g} = \begin{pmatrix} x \\ x + g \end{pmatrix}; \tag{1}$$

G_2 — регулярное представление элементарной абелевой p-группы $(\mathbb{Z}_p^n, \oplus)$ подстановками
$$\hat{g} = \begin{pmatrix} x \\ x \oplus g \end{pmatrix} \tag{2}$$
при естественном представлении чисел из Ω двоичными векторами, соответствующими двоичной записи.

В качестве усложняющих преобразований рассматриваются и сравниваются между собой случайно порождённые подстановки из множеств $(G_1h)^k$ и $(G_2h)^k$, где $h \in S(\Omega)$. Имеется в виду, что элементы каждой из групп перенумерованы каким-либо образом,
$$G_i = \{g_0^{(i)}, \ldots, g_{p^n-1}^{(i)}\}, \quad i \in \overline{1,2},$$
и случайное порождение подстановки $\xi \in (G_ih)^k$ сводится к порождению управляющей комбинации, т. е. последовательности значений
$$s_1, \ldots, s_k \in \overline{0, p^n - 1} \tag{3}$$
случайных равномерно распределённых на множестве $\overline{0, p^n - 1}$ независимых величин, и вычислению суммарного шифра: произведения
$$\xi = g_{s_1}^{(i)} h \cdot \ldots \cdot g_{s_k}^{(i)} h \in (G_ih)^k. \tag{4}$$
Назовём множество
$$\Omega^{\langle 2\rangle} = \{(a,b)\colon a, b \in \Omega,\ a \neq b\}$$
множеством ненулевых биграмм множества Ω.

Матрицей переходных вероятностей ненулевых биграмм множества суммарных шифров $(G_ih)^k$ называют матрицу $\mathcal{P}_2\big((G_ih)^k\big)$ размера $m \times m$, $m = (q^2 - q)$, $q = p^n$, строки и столбцы которой занумерованы в одинаковом порядке биграммами из $\Omega^{\langle 2\rangle}$, такую что на пересечении её строки с номером (a,b) и столбца с номером (c,d) стоит число
$$\mathcal{P}\begin{pmatrix} ab \\ cd \end{pmatrix} = \frac{1}{q^k}\, \nu_k \begin{pmatrix} ab \\ cd \end{pmatrix}, \tag{5}$$
где $\nu\binom{ab}{cd}$ — число управляющих комбинаций (3), таких что подстановка (4) удовлетворяет условию
$$\xi(a) = c, \quad \xi(b) = d.$$

Назовём множество G_ih *основанием шифра* $(G_ih)^k$ и определим *показатель* $\partial_2(G_ih)$ *2-транзитивности основания* G_ih как наименьшее натуральное k, такое что множество $(G_ih)^k$ 2-транзитивно, т. е. матрица $\mathcal{P}_2\big((G_ih)^k\big)$ положительна. Если такого k не существует, будем писать $\partial_2(G_ih) = \infty$.

Мы изучаем здесь показатель $\partial_2(G_ih)$ в качестве основной характеристики криптографических качеств шифров вида $(G_ih)^k$.

Заметим, что при условии $\partial_2(G_ih) < \infty$ последовательность дважды стохастических матриц $\mathcal{P}_2\big((G_ih)^k\big)$, $k = 1, 2, \ldots$, сходится к равновероятной матрице.

Второй важной характеристикой шифров указанного вида является скорость сходимости соответствующей матрицы биграмм к равновероятной.

В связи с этим мы выделяем следующие параметры:

$N_k(G_i)$ — количество подстановок $h \in S(\Omega)$, для которых $\partial_2(G_i h) = k$;

$N_k(G_i/\mathcal{H})$ — количество подстановок h из данного подмножества $\mathcal{H} \subset S(\Omega)$, для которых $\partial_2(G_i h) = k$;

$N_l(G_i;\varepsilon)$ — количество подстановок $h \in S(\Omega)$, для которых все элементы $(m \times m)$-матрицы $\mathcal{P}_2\big((G_i h)^l\big)$ лежат в интервале $[\frac{1}{m}(1-\varepsilon), \frac{1}{m}(1+\varepsilon)]$;

$\bar{N}_l(G_i;\varepsilon)$ — количество подстановок $h \in S(\Omega)$, для которых все элементы $(m \times m)$-матрицы $\mathcal{P}_2\big((G_i h)^l\big)$ лежат в интервале $[\frac{1}{m}(1-\varepsilon), \frac{1}{m}(1+\varepsilon)]$, но не все элементы матрицы $\mathcal{P}_2\big((G_i h)^{l-1}\big)$ попадают в данный интервал. Нетрудно убедиться, что при этом $\bar{N}_l(G_i;\varepsilon) = N_l(G_i;\varepsilon) - N_{l-1}(G_i;\varepsilon)$, т. е. величины $N_l(G_i;\varepsilon)$ являются накопленными суммами величин $\bar{N}_l(G_i;\varepsilon)$.

Заметим, что всегда $\partial_2(G_i h) \geqslant 3$ (М. М. Глухов [1]).

2. Упрощения вычислений

Имеют место соотношения

$$\mathcal{P}_2\big((Gh)^k\big) = \big(\mathcal{P}_2(Gh)\big)^k = \mathcal{P}_2(GhG)^{k-1} \cdot \mathcal{P}_2(h), \tag{6}$$

из которых следует, что матрица $\mathcal{P}_2\big((Gh)^k\big)$ отличается лишь перестановкой столбцов от матрицы $\mathcal{P}_2(GhG)^{k-1}$, а для вычисления последней удобно использовать представление

$$\mathcal{P}_2(G_i h G_i)^l = I \otimes Q_i(h)^l, \quad l \in \mathbb{N}, \tag{7}$$

где I — равновероятная $(q \times q)$-матрица, а $Q_i(h)$ — $\big((q-1)\times(q-1)\big)$-матрица переходных вероятностей разностей ненулевых биграмм, т. е. матрица, у которой строки и столбцы занумерованы ненулевыми элементами из Ω и на пересечении строки с номером u и столбца с номером v стоит число

$$\frac{1}{q}\mu\binom{u}{v},$$

где $\mu\binom{u}{v}$ — число решений уравнения

$$h(x+u) - h(x) = v, \quad \text{если} \quad i = 1; \quad h(x \oplus u) \oplus h(x) = v, \quad \text{если} \quad i = 2. \tag{8}$$

3. Результаты эксперимента для случая $p = 2$, $n = 3$

Отметим, что $8! = 40\,320 = 38\,912 + 1\,280 + 128$. Результаты эксперимента для случая $p = 2$, $n = 3$ представлены в табл. 1—3.

Таблица 1. Значения параметров $N_k(G_i)$

k	$G_1 \cong \mathbb{Z}_8$	$G_2 \cong \mathbb{Z}_2^3$
$<\infty$	38 912	32 256
3	32 384	10 752
4	6 528	16 128
5	—	5 376

Таблица 2. Значения параметров $\bar{N}_l(G_i; 0{,}5)$

l	$G_1 \cong \mathbb{Z}_8$	$G_2 \cong \mathbb{Z}_2^3$
3	6 144	0
4	25 216	10 752
5	3 584	16 128
6	1 536	5 376
7	1 536	0
8	512	0
9	128	0
10	256	0
всего	38 912	32 256

Таблица 3. Значения параметров $\bar{N}_l(G_i; 0{,}25)$

l	$G_1 \cong \mathbb{Z}_8$	$G_2 \cong \mathbb{Z}_2^3$
3	1 024	0
4	17 152	10 752
5	13 056	10 752
6	2 688	5 376
7	1 792	5 376
8	2 048	0
9	256	0
10	0	0
11	512	0
12	0	0
13	128	0
14	256	0
всего	38 912	32 256

Проведён анализ перестановок $h \in S(\Omega)$ с точки зрения сравнения структуры соответствующих матриц $Q_1(h)$ и $Q_2(h)$.

Ниже через $\bar{\partial}_2(G_i h)$ будем обозначать такое натуральное k, что матрица $\mathcal{P}_2\big((G_i h)^k\big)$ положительна и при этом все элементы $(m\times m)$-матрицы $\mathcal{P}_2\big((G_i h)^k\big)$ лежат в интервале $[\frac{1}{2m}, \frac{3}{2m}]$ (т. е. в интервале $[\frac{1}{m}(1-\varepsilon), \frac{1}{m}(1+\varepsilon)]$ при $\varepsilon = 0{,}5$), но не все элементы матрицы $\mathcal{P}_2\big((G_i h)^{k-1}\big)$ попадают в данный интервал. Если такого k не существует, то полагаем $\bar{\partial}_2(G_i h) = \infty$.

Получены следующие результаты: среди всех подстановок $h \in S(\Omega)$

— для 1408 перестановок $\bar{\partial}_2(G_1 h) = \infty$ и $\bar{\partial}_2(G_2 h) = \infty$;
— для 576 перестановок $\bar{\partial}_2(G_1 h) = 3$ и $\bar{\partial}_2(G_2 h) = \infty$;
— для 3584 перестановок $\bar{\partial}_2(G_1 h) = 4$ и $\bar{\partial}_2(G_2 h) = \infty$;
— для 2432 перестановок $\bar{\partial}_2(G_1 h) = 3$ и $\bar{\partial}_2(G_2 h) = 4$;
— нет перестановок, для которых $\bar{\partial}_2(G_1 h) = 3$ и $\bar{\partial}_2(G_2 h) = 3$;
— нет перестановок, для которых $\bar{\partial}_2(G_1 h) = 4$ и $\bar{\partial}_2(G_2 h) = 3$.

3.1. Случай группы G_1

Для группы $G_1\mathbb{Z}_8$ получены также следующие результаты.

— Для 1 280 перестановок $h \in S(\Omega)$ матрицы $Q_1(h)$ соответствуют цепям Маркова, разбивающимся на два эргодических класса без циклических подклассов; из них в 960 случаях матрицы симметричны, а оставшиеся 320 симметричны относительно центра, причём 256 из них равны предельной матрице

1/4	0	1/4	0	1/4	0	1/4
0	1/3	0	1/3	0	1/3	0
1/4	0	1/4	0	1/4	0	1/4
0	1/3	0	1/3	0	1/3	0
1/4	0	1/4	0	1/4	0	1/4
0	1/3	0	1/3	0	1/3	0
1/4	0	1/4	0	1/4	0	1/4

и 64 матрицы равны предельной матрице

1/6	1/6	1/6	0	1/6	1/6	1/6
1/6	1/6	1/6	0	1/6	1/6	1/6
1/6	1/6	1/6	0	1/6	1/6	1/6
0	0	0	1	0	0	0
1/6	1/6	1/6	0	1/6	1/6	1/6
1/6	1/6	1/6	0	1/6	1/6	1/6
1/6	1/6	1/6	0	1/6	1/6	1/6

.

— 40 перестановкам (включая тождественную) соответствуют идемпотентные матрицы.
— Для 88 перестановок матрицы $Q_1(h)$ соответствуют цепи Маркова, состоящей из одного эргодического класса, разбивающегося на циклические подклассы. Эти подстановки имеют вид

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ x & a & x \pm 2 & a \pm 2 & x+4 & a+4 & x \mp 2 & a \mp 2 \end{pmatrix}.$$

Здесь x, a — элементы разной чётности и все элементы рассматриваются по модулю 8.

3.2. Случай группы G_2

Для группы $G_2 \cong \mathbb{Z}_2^3$ получены также следующие результаты.

— Для 5608 перестановок $h \in S(\Omega)$ матрицы $Q_2(h)$ соответствуют цепям Маркова, разбивающимся на два эргодических класса без циклических подклассов.
— 232 перестановкам (включая тождественную) соответствуют идемпотентные матрицы; все матрицы являются симметричными.

3.3. Связь между случаями групп $G_1 \cong \mathbb{Z}_8$ и $G_2 \cong \mathbb{Z}_2^3$

Если для некоторой перестановки $h \in S(\Omega)$ соответствующая матрица $Q_2(h)$ (для случая группы $\mathbb{Z}_2^3$) в некоторой конечной степени становится положительной, то соответствующая той же перестановке матрица $Q_1(h)$ (для случая группы $\mathbb{Z}_8$) также становится положительной. Однако при этом нельзя утверждать, что для фиксированной подстановки показатель транзитивности в случае группы $\mathbb{Z}_8$ не превосходит показателя транзитивности в случае группы $\mathbb{Z}_2^3$: такого рода «монотонность» нарушается для 640 перестановок (см., например, перестановку 2147), для которых матрицы имеют показатель 3 и 4 в группах $G = \mathbb{Z}_2^3$ и $\mathbb{Z}_8$ соответственно.

4. Вычислительный эксперимент для $p = 2$, $n = 4$

В случае $n = 4$ порядок симметрической группы S_{16} равен

$$16! = 20\,922\,789\,888\,000.$$

Для этого случая проведён вычислительный эксперимент. Случайным образом были построены 100 000 000 перестановок из группы S_{16}, и для каждой перестановки вычислялись две матрицы переходных вероятностей разностей биграмм:

для групп $\mathbb{Z}_{16}$ и $\mathbb{Z}_2^4$. Затем вычислялось транзитивное замыкание полученных матриц.

Для случайного порождения перестановок использовался метод Фишера—Йетса (тасование Фишера—Йетса [2]), который иногда называется методом Кнута (тасованием Кнута [3]). Был построен массив $\mathcal{H}$ из 100 000 000 перестановок $h \in \mathrm{S}_{16}$, среди которых нашлось лишь 240 повторяющихся. Таким образом $|\mathcal{H}| = 99\,999\,760$.

Результаты эксперимента приведены в табл. 4.

Таблица 4. Вычислительный эксперимент для $p = 2$, $n = 4$

	$G \cong \mathbb{Z}_{16}$	$G \cong \mathbb{Z}_2^4$
количество $h \in \mathcal{H}$, для которых $\partial_2(Gh) < \infty$	99 984 167	99 766 042
количество $h \in \mathcal{H}$, для которых $\partial_2(Gh) = \infty$	15 833	233 958
$\max\limits_{h\in\mathcal{H}}\{\partial_2(Gh)\colon \partial_2(Gh) < \infty\}$	7	9
$N_3(G_i/\mathcal{H})$	99 559 867	6 036 375
$N_4(G_i/\mathcal{H})$	<1 %	93 080 529

Отметим, что для вычисления всех возможных значений $\partial_2(Gh)$ для подстановок h степени 16 нет необходимости осуществлять полный перебор 16! перестановок, поскольку они разбиваются на классы по 16 штук, имеющие одинаковые матрицы. Вместе с тем по предварительным оценкам временны́е затраты на перебор $15! = 1\,307\,674\,368\,000$ перестановок на суперкомпьютере не должны превысить несколько десятков часов.

5. Результаты экспериментов для случая $p = 3$, $n = 2$

Проведён сравнительный анализ групп $\mathbb{Z}_9$ и $\mathbb{Z}_3^2$. Полученные результаты представлены в табл. 5 (отметим, что $9! = 362\,880$).

Таблица 5. Значения параметров $N_k(G_i)$

k	$G_1 \cong \mathbb{Z}_9$	$G_2 \cong \mathbb{Z}_3^2$
$<\infty$	361 584	357 696
3	332 424	314 928
4	28 674	40 176
5	486	2 592

Установлены следующие факты:

— для всех 1 296 перестановок $h \in S(\Omega)$, для которых $\partial_2(G_1h) = \infty$, также имеет место $\partial_2(G_2h) = \infty$;

— имеется всего 295 812 перестановок $h \in S(\Omega)$, для которых $\partial_2(G_1h) = \partial_2(G_2h) = 3$;

— имеется всего 19 116 перестановок $h \in S(\Omega)$, для которых $3 < \partial_2(G_1h) < \infty$ и $\partial_2(G_2h) = 3$;

— имеется всего 34 344 перестановок $h \in S(\Omega)$, для которых $\partial_2(G_1h) = 3$ и $3 < \partial_2(G_2h) < \infty$.

6. Заключение

Проведённые эксперименты позволяют выдвинуть гипотезу о том, что

$$N_3(G_1) \gg N_3(G_2), \tag{9}$$

причём при условии $\partial_2(G_1h) = \partial_2(G_2h) = 3$ последовательность матриц $\mathcal{P}(G_1h)^i$ сходится к равномерной матрице быстрее, чем последовательность $\mathcal{P}(G_2h)^i$ (см. табл. 2, 3).

С этой точки зрения использование группы $G_1 \cong \mathbb{Z}_{2^n}$ при построении криптографических примитивов может оказаться более эффективным, чем использование группы $G_2 \cong \mathbb{Z}_2^n$.

Литература

[1] Глухов М. М. О 2-транзитивных произведениях регулярных групп подстановок // Тр. по дискр. матем. — 2000. — Т. 3. — С. 37—52.

[2] Fisher R. A., Yates F. Statistical Tables for Biological, Agricultural and Medical Research. — London: Oliver & Boyd, 1948. — P. 26—27.

[3] Knuth D. E. The Art of Computer Programming. Vol. 2: Seminumerical Algorithms. — Reading, MA: Addison-Wesley, 1969. — P. 124—125.