3. *Sarkar S. and Sim S. M.* A deeper understanding of the XOR count distribution in the context of lightweight cryptography // LNCS. 2016. V. 9646. P. 167–182.
4. *Toh D., Teo J., Khoo K., and Sim S. M.* Lightweight MDS serial-type matrices with minimal fixed XOR count // LNCS. 2018. V. 10831. P. 51–71.
5. *Gupta K. C. and Ray I. G.* On constructions of MDS matrices from companion matrices for lightweight cryptography // LNCS. 2013. V. 8128. P. 29–43.

УДК 519.688 DOI 10.17223/2226308X/12/60

ВЫЧИСЛИТЕЛЬНЫЕ ЭКСПЕРИМЕНТЫ В КОНЕЧНЫХ ДВУПОРОЖДЁННЫХ БЕРНСАЙДОВЫХ ГРУППАХ ПЕРИОДА 5

А. А. Кузнецов

Пусть $B_0(2,5) = \langle a_1, a_2 \rangle$ — наибольшая конечная двупорождённая бернсайдова группа периода 5, порядок которой равен 5^{34}. Для каждого элемента данной группы существует единственное представление вида $a_1^{\alpha_1} \cdot a_2^{\alpha_2} \cdot \ldots \cdot a_{34}^{\alpha_{34}}$, где $\alpha_i \in \mathbb{Z}_5$, $i = 1, 2, \ldots, 34$. Здесь a_1 и a_2 — порождающие элементы $B_0(2,5)$, $a_3, \ldots, a_{34}$ — коммутаторы, которые вычисляются рекурсивно через a_1 и a_2. Определим факторгруппу группы $B_0(2,5)$ следующего вида: $B_k = B_0(2,5)/\langle a_{k+1}, \ldots, a_{34} \rangle$. Очевидно, что $|B_k| = 5^k$. На основе проведённых вычислительных экспериментов сформулирована гипотеза о диаметре группы B_k для симметричного порождающего множества $\{a_1, a_1^{-1}, a_2, a_2^{-1}\}$.

Ключевые слова: *функция роста группы, группа Бернсайда.*

Настоящая работа продолжает исследования, начатые в [1, 2], которые посвящены разработке алгоритмов для исследования роста в конечных двупорождённых группах периода 5. В [1] основной упор сделан на создании алгоритмов минимальной вычислительной сложности, а в [2] разработан ресурсно-эффективный алгоритм, который имеет низкую пространственную сложность и сохраняет вычислительную сложность на приемлемом уровне.

Напомним основные определения [1]. Пусть $G = \langle X \rangle$. *Шаром* K_s радиуса s группы G будем называть множество всех её элементов, которые могут быть представлены в алфавите X в виде несократимых групповых слов длины не больше s. Все элементы одинаковой длины i образуют *сферу* P_i радиуса i. Единица группы e является пустым словом, длина которого равна нулю. Согласно данным определениям, $K_s = \bigcup\limits_{i=0}^{s} P_i$.

Для каждого целого неотрицательного i можно определить (сферическую) функцию роста группы $F(G)$, которую будем записывать в виде вектора $F(G) = (F_0, F_1, \ldots, F_i, \ldots)$, где $F_i = |P_i|$. Пусть $F_{s_0} > 0$, но $F_{s_0+1} = 0$, тогда s_0 является диаметром графа Кэли группы G в алфавите порождающих X, который будем обозначать $D_X(G)$. Средний диаметр $\overline{D}_X(G)$ равен $\dfrac{1}{|G|} \sum\limits_{s=0}^{s_0} sF_s$.

Заметим, что решение некоторых задач теории кодирования и криптографии сводится к исследованию соответствующих графов Кэли. Например, открытая проблема эффективного восстановления вершин в графе Хэмминга является одной из таких задач [3].

Кратко опишем алгоритмы из [1, 2].

Алгоритм 1 вычисляет шар K_s фиксированного радиуса s произвольной конечной группы G, заданной порождающим множеством X. Данный алгоритм имеет низкую

вычислительную сложность, однако при его реализации каждый элемент группы необходимо хранить в памяти компьютера, и если группа имеет большой порядок, то применение алгоритма 1 становится невозможным.

Пусть φ — гомоморфизм G на группу Q и N — ядро φ, т. е. $Q = G/N$. По аналогии с группой, для каждого смежного класса qN определим сферу $P_i(q)$, шар $K_s(q)$ и функцию роста $F_i(q)$:

$$P_i(q) = \{g : g \in P_i \text{ и } \varphi(g) = q\}, \quad K_s(q) = \bigcup_{i=0}^{s} P_i(q), \quad F_i(q) = |P_i(q)|.$$

Пусть $F_d(q) > 0$, но $F_{d+1}(q) = 0$, тогда d будем называть диаметром смежного класса qN и обозначать $D_X(qN)$.

Если Q — сравнительно большая группа, то множество $K_{2s}(q)$ будет значительно меньше, чем $K_{2s}(G)$. Данный факт взят за основу построения алгоритма 2, который, получив на входе шар K_s группы G радиуса s, фактор-группу $Q = G/N$ и некоторый элемент $q \in Q$, возвращает функцию роста $F(q) = (F_0(q), \ldots, F_{2s}(q))$ для шара $K_{2s}(q)$ смежного класса qN радиуса $2s$.

Объединив алгоритмы 1 и 2, получим алгоритм 3, который вычисляет функцию роста $F(G) = \sum\limits_{q \in Q} F(q)$ шара K_{2s} фиксированного радиуса $2s$ произвольной конечной группы G, заданной порождающим множеством X.

Пусть $B_0(2,5) = \langle a_1, a_2 \rangle$ — максимальная конечная двупорождённая бернсайдова группа периода 5, порядок которой равен 5^{34} [4]. При помощи системы компьютерной алгебры GAP легко получить коммутаторное представление данной группы [5]. В этом случае каждый элемент $g \in B_0(2,5)$ может быть однозначно записан в виде $a_1^{\alpha_1} \cdot a_2^{\alpha_2} \cdot \cdot \ldots \cdot a_{34}^{\alpha_{34}}$, где $\alpha_i \in \mathbb{Z}_5$ и $i = 1, 2, \ldots, 34$. Здесь a_1 и a_2 — порождающие элементы $B_0(2,5)$; $a_3, \ldots, a_{34}$ — коммутаторы, которые вычисляются рекурсивно через a_1 и a_2 [4].

Определим фактор-группу $B_k = B_0(2,5)/\langle a_{k+1}, \ldots, a_{34} \rangle$. Очевидно, что $|B_k| = 5^k$ и $g = a_1^{\alpha_1} \cdot a_2^{\alpha_2} \cdot \ldots \cdot a_k^{\alpha_k}$ для всех $g \in B_k$.

Пусть $A_4 = \{a_1, a_1^{-1}, a_2, a_2^{-1}\}$ — симметричное порождающее множество групп B_k.

Отметим, что на сегодняшний день при помощи компьютерных вычислений удалось получить функции роста групп B_k при $k \leqslant 19$ [1, 2]. В настоящее время ведутся расчёты функции роста группы $B_{20} = \langle A_4 \rangle$ по алгоритму 3, при этом $s = 20$, $Q = B_{10}$ и $N = \langle a_{11}, \ldots, a_{20} \rangle$.

При суммировании получаемых функций роста $F(q)$ смежных классов qN отмечено, что, начиная с некоторого шага (не более 10 % от порядка группы), промежуточные функции роста группы $F(B_{20})$ сохраняют области возрастания и убывания. Рис. 1 наглядно отражает данный факт. Вычислительные эксперименты в группах B_k при $k \leqslant 19$ показали, что и в них промежуточные функции роста ведут себя аналогично. Кроме того, выяснилось, что при $k \leqslant 19$ смежный класс eN_k всегда включает слова максимальной длины группы, на основании чего можно сформулировать гипотезу для всех $2 \leqslant k \leqslant 34$:

Гипотеза 1. $D_{A_4}(eN_k) = D_{A_4}(B_k)$, где $|N_k| \sim |Q_k| \sim |B_k|^{1/2}$.

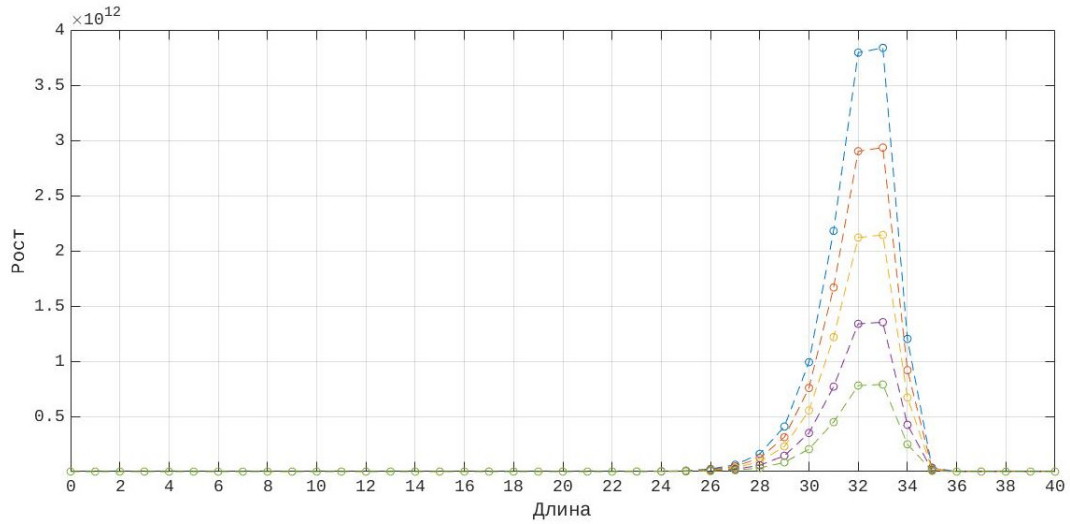

Рис. 1. Промежуточные функции роста $F(B_{20})$

Результаты вычислительных экспериментов в группах B_k при $20 \leqslant k \leqslant 25$ представлены в таблице.

k	20	21	22	23	24	25
$D_{A_4}(eN_k)$	38	39	41	44	44	46

Если гипотеза верна, то значения диаметров смежных классов eN_k в таблице равны диаметрам соответствующих групп B_k относительно порождающего множества A_4.

ЛИТЕРАТУРА

1. *Кузнецов А. А.* Об одном алгоритме вычисления функций роста в конечных двупорождённых группах периода 5 // Прикладная дискретная математика. 2016. № 3(33). С. 116–125.
2. *Кузнецов А. А., Кузнецова А. С.* Ресурсно-эффективный алгоритм для исследования роста в конечных двупорождённых группах периода 5 // Прикладная дискретная математика. 2018. № 42. С. 94–103.
3. *Константинова Е. В.* Комбинаторные задачи на графах Кэли. Новосибирск: НГУ, 2010. 110 с.
4. *Havas G., Wall G., and Wamsley J.* The two generator restricted Burnside group of exponent five // Bull. Austral. Math. Soc. 1974. No. 10. P. 459–470.
5. *Sims C.* Computation with Finitely Presented Groups. Cambridge: Cambridge University Press, 1994. 628 p.

УДК 512.55 DOI 10.17223/2226308X/12/61

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЭФФЕКТИВНОСТИ РЕШЕНИЯ ПСЕВДОБУЛЕВЫХ СИСТЕМ ЛИНЕЙНЫХ НЕРАВЕНСТВ АЛГОРИТМАМИ ИМИТАЦИИ ОТЖИГА, БАЛАША И ВНУТРЕННЕЙ ТОЧКИ

Г. О. Маняев, А. Н. Шурупов

Целью работы является разработка и исследование надёжности релаксационного алгоритма решения псевдобулевых систем линейных неравенств, построенного