ЛИТЕРАТУРА

1. *Семенов А. Д., Артамонов Д. В., Брюхачев А. В.* Идентификация систем управления. Учеб. пособие. Пенза: Изд-во Пенз. ун-та, 2003. 211 с.
2. Материалы компании AlterTrader Research [Электронный ресурс]. `http://www.altertrader.com/` — 21.04.2015.
3. *Загоруйко Н. Г., Кутненко О. А.* Методы распознавания, основанные на алгоритме AdDel // Сиб. журн. индустр. матем. 2004. Т. 7. № 1. С. 39–47.
4. *Воронцов К. В.* Методы обучения ранжированию (Learning to rank). Курс лекций. [Электронный ресурс]. 2013. `http://www.machinelearning.ru/wiki/images/8/89/Voron-ML-Ranking-slides.pdf`
5. *Кожушко О. А., Тарков М. С.* Использование иерархической временной памяти для идентификации системы ранжирования документов // Проблемы информатики. 2015. №1(26). С. 47–54.

УДК 519.688 DOI 10.17223/2226308X/8/57

ПОЛИНОМЫ ХОЛЛА БЕРНСАЙДОВЫХ ГРУПП ПЕРИОДА 3[1]

А. А. Кузнецов, К. В. Сафонов

Пусть $B_k = (k, 3)$ — бернсайдова k-порождённая группа периода 3. В работе вычислены полиномы Холла для B_k при $k \leqslant 4$.

Ключевые слова: *периодическая группа, собирательный процесс, полиномы Холла.*

Пусть $B_k = (k, 3)$ — бернсайдова k-порождённая группа периода 3. Ф. Леви и ван дер Варден доказали [1], что $|B_k| = 3^{k+\binom{k}{2}+\binom{k}{3}}$ и ступень нильпотентности B_k не превышает 3.

Для каждой B_k несложно получить pc-представление (*power commutator presentation*), используя систему компьютерной алгебры GAP или MAGMA.

Пусть $a_1^{x_1} \dots a_n^{x_n}$ и $a_1^{y_1} \dots a_n^{y_n}$ — два произвольных элемента в группе B_k, записанные в коммутаторном виде. Тогда их произведение равно

$$a_1^{x_1} \dots a_n^{x_n} \cdot a_1^{y_1} \dots a_n^{y_n} = a_1^{z_1} \dots a_n^{z_n}.$$

Основой для нахождения степеней z_i является собирательный процесс [2, 3], который реализован в указанных системах компьютерной алгебры. Кроме того, существует альтернативный способ для вычисления произведений элементов группы, предложенный Ф. Холлом [4]. Холл показал, что z_i представляют собой полиномиальные функции (в нашем случае над полем $\mathbb{Z}_3$), зависящие от переменных $x_1, \dots, x_i, y_1, \dots, y_i$, которые принято сейчас называть *полиномами Холла*. Согласно [4],

$$z_i = x_i + y_i + p_i(x_1, \dots, x_{i-1}, y_1, \dots, y_{i-1}).$$

Необходимость применения полиномов Холла возникает при решении задач, требующих многократного умножения элементов группы. Исследование структуры графа Кэли некоторой группы является одной из таких задач. Вычислительные эксперименты на ЭВМ в группах периода пять и семь [5, 6] выявили, что метод полиномов Холла

[1]Работа выполнена при поддержке Министерства образования и науки РФ (проект Б 112/14) и гранта Президента РФ (проект МД-3952.2015.9).

имеет преимущество перед традиционным собирательным процессом. Следует также отметить, что данный метод легко программно реализуем, в том числе на многопроцессорных вычислительных системах.

В настоящей работе вычислены ранее неизвестные полиномы Холла для групп B_k при $k \leqslant 4$. Для $k > 4$ полиномы вычисляются аналогично, однако их вывод занимает значительно больше места. Заметим, что, вычислив полиномы для некоторого k, нетрудно получить полиномы Холла для меньших значений k.

Получим в GAP pc-представление группы B_4.

Коммутаторы веса 1:

$$a_1, a_2, a_3, a_4 \text{ — образующие группы.}$$

Коммутаторы веса 2:

$$a_5 = [a_2, a_1],\ a_6 = [a_3, a_1],\ a_7 = [a_3, a_2],\ a_8 = [a_4, a_1],\ a_9 = [a_4, a_2],\ a_{10} = [a_4, a_3].$$

Коммутаторы веса 3:

$$a_{11} = [a_5, a_3] = [a_2, a_1, a_3],\ a_{12} = [a_5, a_4] = [a_2, a_1, a_4],$$
$$a_{13} = [a_6, a_4] = [a_3, a_1, a_4],\ a_{14} = [a_7, a_4] = [a_3, a_2, a_4].$$

Список определяющих соотношений R для базисных коммутаторов (тривиальные соотношения вида $a_i^3 = 1$ и $[a_j, a_i] = 1$ для краткости не приводятся):

$$[a_2, a_1] = a_5,\ [a_3, a_1] = a_6, [a_3, a_2] = a_7, [a_4, a_1] = a_8,\ [a_4, a_2] = a_9,\ [a_4, a_3] = a_{10},$$
$$[a_5, a_3] = a_{11},\ [a_5, a_4] = a_{12},\ [a_6, a_2] = a_{11}^2,\ [a_6, a_4] = a_{13},\ [a_7, a_1] = a_{11},\ [a_7, a_4] = a_{14},$$
$$[a_8, a_2] = a_{12}^2,\ [a_8, a_3] = a_{13}^2,\ [a_9, a_1] = a_{12},\ [a_9, a_3] = a_{14}^2,\ [a_{10}, a_1] = a_{13},\ [a_{10}, a_2] = a_{14}.$$

Таким образом, $B_4 = \langle\, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14} \mid R \,\rangle$.

Каждый элемент группы выражается единственным образом в виде нормального коммутаторного слова:

$$\forall g \in B_4 \quad (g = a_1^{x_1} a_2^{x_2} a_3^{x_3} a_4^{x_4} a_5^{x_5} a_6^{x_6} a_7^{x_7} a_8^{x_8} a_9^{x_9} a_{10}^{x_{10}}, a_{11}^{x_{11}}, a_{12}^{x_{12}}, a_{13}^{x_{13}}, a_{14}^{x_{14}}), \quad x_i \in \mathbb{Z}_3.$$

Основным результатом настоящей работы является

Теорема 1. Пусть $a_1^{x_1} \dots a_{14}^{x_{14}}$ и $a_1^{y_1} \dots a_{14}^{y_{14}}$ — два произвольных элемента в группе B_4, записанные в коммутаторном виде. Тогда их произведение равно $a_1^{x_1} \dots a_{14}^{x_{14}} \times$ $\times\, a_1^{y_1} \dots a_{14}^{y_{14}} = a_1^{z_1} \dots a_{14}^{z_{14}}$, где $z_i \in \mathbb{Z}_3$ — полиномы Холла, задаваемые следующими формулами:

$$z_1 = x_1 + y_1,$$
$$z_2 = x_2 + y_2,$$
$$z_3 = x_3 + y_3,$$
$$z_4 = x_4 + y_4,$$
$$z_5 = x_5 + y_5 + x_2 y_1,$$
$$z_6 = x_6 + y_6 + x_3 y_1,$$
$$z_7 = x_7 + y_7 + x_3 y_2,$$
$$z_8 = x_8 + y_8 + x_4 y_1,$$
$$z_9 = x_9 + y_9 + x_4 y_2,$$
$$z_{10} = x_{10} + y_{10} + x_4 y_3,$$

$$z_{11} = x_{11} + y_{11} + x_5y_3 + 2x_6y_2 + x_7y_1 + x_2x_3y_1 + x_2y_1y_3 + 2x_3y_1y_2,$$
$$z_{12} = x_{12} + y_{12} + x_5y_4 + 2x_8y_2 + x_9y_1 + x_2x_4y_1 + x_2y_1y_4 + 2x_4y_1y_2,$$
$$z_{13} = x_{13} + y_{13} + x_{10}y_1 + x_6y_4 + 2x_8y_3 + x_3x_4y_1 + x_3y_1y_4 + 2x_4y_1y_3,$$
$$z_{14} = x_{14} + y_{14} + x_{10}y_2 + x_7y_4 + 2x_9y_3 + x_3x_4y_2 + x_3y_2y_4 + 2x_4y_2y_3.$$

ЛИТЕРАТУРА

1. *Levi F. and van der Waerden B.* Uber eine besondere Klasse von Gruppen // Abh. Math. Sem. Univ. Hamburg. 1933. No. 9. S. 154–158.
2. *Sims C.* Computation with Finitely Presented Groups. Cambridge: Cambridge University Press, 1994. 628 p.
3. *Holt D., Eick B., and O'Brien E.* Handbook of computational group theory. Boca Raton: Chapman & Hall/CRC Press, 2005. 514 p.
4. *Hall P.* Nilpotent groups, Notes of lectures given at the Canadian Mathematical Congress 1957 Summer Seminar, in The collected works of Philip Hall. Oxford: Clarendon Press, 1988. P. 415–462.
5. *Кузнецов А. А., Кузнецова А. С.* Быстрое умножение элементов в конечных двупорождённых группах периода пять // Прикладная дискретная математика. 2013. №1. С. 110–116.
6. *Кузнецов А. А. Сафонов К. В.* Hall's polynomials of finite two-generator groups of exponent seven // Журнал СФУ. Сер. математика и физика. 2014. №2. С. 186–190.

УДК 512.54.05+519.712.4 DOI 10.17223/2226308X/8/58

О СЛОЖНОСТИ ЗАДАЧИ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ В ИНТЕРВАЛЕ В ГРУППЕ С ЭФФЕКТИВНЫМ ИНВЕРТИРОВАНИЕМ

М. В. Николаев

Задача дискретного логарифмирования в интервале заключается в поиске для заданной конечной группы G (с аддитивной записью операции), заданных $P, Q \in G$, $N < |G| - 1$ такого значения n, что $Q = nP$, $0 \leqslant n \leqslant N$. Одним из наиболее эффективных методов решения данной задачи является алгоритм Годри — Шоста. В 2010 г. С. Гэлбрейт и К. Руправи представили усовершенствованную версию алгоритма для групп с эффективным инвертированием. Оценка средней трудоёмкости решения задачи составила $(1{,}36 + o(1))\sqrt{N}$ групповых операций в G при $N \to \infty$. В настоящей работе приводится новая модификация алгоритма Годри — Шоста для решения задачи дискретного логарифмирования в интервале в группе с эффективным инвертированием и получена оценка средней трудоёмкости, составляющая $(1 + \varepsilon)\sqrt{\pi N/2}$ групповых операций в G.

Ключевые слова: *задача дискретного логарифмирования в интервале, алгоритм Годри — Шоста.*

Приведём постановки задач.

Определение 1. Задача дискретного логарифмирования.
Дано: группа $G = \langle P \rangle$, $Q \in G$.
Найти: $n \in \{0, \ldots, |G| - 1\}$, такое, что $Q = nP$.

Определение 2. Задача дискретного логарифмирования в интервале.
Дано: группа $G = \langle P \rangle$, $Q \in G$, $N \in \mathbb{N}$, $2|N$, $N < |G| - 1$, $Q = nP$ для некоторого (неизвестного) $n \in \{-N/2, \ldots, N/2\}$.
Найти: n.