

**БЫСТРОЕ УМНОЖЕНИЕ ЭЛЕМЕНТОВ
В КОНЕЧНЫХ ДВУПОРОЖДЁННЫХ ГРУППАХ ПЕРИОДА ПЯТЬ¹**

А. А. Кузнецов, А. С. Кузнецова

*Сибирский государственный аэрокосмический университет, г. Красноярск, Россия***E-mail:** alex_kuznetsov80@mail.ru

Представлен алгоритм, основанный на полиномах Холла, для быстрого умножения элементов в конечных двупорождённых группах периода пять.

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

Введение

Пусть $B_0(2, 5, k)$ — максимальная конечная двупорождённая бернсайдова группа периода 5 степени нильпотентности k . В данном классе групп наибольшей является группа $B_0(2, 5, 12)$, порядок которой равен 5^{34} [1]. Для каждой из $B_0(2, 5, k)$ известны РС-представления (Power Commutator presentation [2, 3]), которые несложно получить, используя систему компьютерной алгебры GAP. Для исследования различных свойств $B_0(2, 5, k)$, например таких, как функция роста или диаметр Кэли группы, часто требуется вычислять произведения её элементов. 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 $B_0(2, 5, k)$, записанных 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 коэффициентов z_i является собирательный процесс [2, 3], который реализован в системах компьютерной алгебры GAP и MAGMA. Однако это не единственный способ для вычисления произведений элементов группы. В работе Ф. Холла [4] показано, что z_i представляют собой полиномиальные функции (в нашем случае над полем $\mathbb{Z}_5$), зависящие от переменных $x_1, \dots, x_i, y_1, \dots, y_i$, которые называют сейчас полиномами Холла. Согласно [4],

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

Ч. Симс в [5] анонсировал, что вычислил указанные полиномиальные функции, однако они так и не были нигде опубликованы. Кроме того, авторам не удалось найти компьютерные программы, в которых реализован метод полиномов Холла для вычисления произведений элементов группы. Для восполнения указанного пробела в настоящей работе приведено подробное описание алгоритма для вычисления полиномов Холла в группах $B_0(2, 5, k)$. Полиномы z_i найдены при помощи машинных вычислений в системе компьютерной алгебры MATLAB, после чего полученные формулы реализованы в виде отдельной программы на языке Си. Сравнение скорости вычисления около 10^4 произведений случайно выбранных элементов в каждой из групп $B_0(2, 5, k)$

¹Работа выполнена при финансовой поддержке гранта РФФИ (код проекта № 10-01-00509-а).

показало, что метод полиномов Холла имеет значительное преимущество перед собирательным процессом. В среднем использование полиномов позволяет получить произведение двух элементов группы на порядок (т. е. в 10 раз) быстрее собирательного процесса.

При описании алгоритма ограничимся случаями $k \leq 4$. Для $k > 4$ полиномы вычисляются аналогично, однако их вывод занимает значительно больше места, что делает невозможным проверить доказательство «вручную». Полиномы для наибольшего случая $k = 12$ содержат также полиномы для всех других k и занимают 42 страницы текста, вследствие чего в работе не приводятся. Их можно легко получить, связавшись с авторами по электронной почте.

Из описания алгоритма, приведённого далее, следует

Теорема 1. 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 $B_0(2, 5, k)$, записанных в коммутаторном виде, где $k \in \mathbb{N}$ и $k \leq 4$. Тогда их произведение равно $a_1^{x_1} \dots a_n^{x_n} \cdot a_1^{y_1} \dots a_n^{y_n} = a_1^{z_1} \dots a_n^{z_n}$, где $z_i \in \mathbb{Z}_5$ — полиномы Холла, задаваемые формулами (1), (2) при $k = 1$, (1)–(3) при $k = 2$, (1)–(5) при $k = 3$ и (1)–(8) при $k = 4$:

$$z_1 = x_1 + y_1; \quad (1)$$

$$z_2 = x_2 + y_2; \quad (2)$$

$$z_3 = x_3 + y_3 + x_2 y_1; \quad (3)$$

$$z_4 = x_4 + y_4 + x_2 \binom{y_1}{2} + x_3 y_1; \quad (4)$$

$$z_5 = x_5 + y_5 + x_2 y_1 y_2 + \binom{x_2}{2} y_1 + x_3 y_2; \quad (5)$$

$$z_6 = x_6 + y_6 + x_2 \binom{y_1}{3} + x_3 \binom{y_1}{2} + x_4 y_1; \quad (6)$$

$$z_7 = x_7 + y_7 + x_2 \binom{y_1}{2} y_2 + \binom{x_2}{2} \binom{y_1}{2} + x_3 y_1 y_2 + x_4 y_2 + x_5 y_1; \quad (7)$$

$$z_8 = x_8 + y_8 + x_2 y_1 \binom{y_2}{2} + \binom{x_2}{2} y_1 y_2 + \binom{x_2}{3} y_1 + x_3 \binom{y_2}{2} + x_5 y_2. \quad (8)$$

Описание алгоритма

Вычислим полиномы Холла для группы $B_0(2, 5, 4)$. Работая с данной группой, автоматически получим полиномы для групп $B_0(2, 5, 1)$, $B_0(2, 5, 2)$ и $B_0(2, 5, 3)$, поэтому нет необходимости отдельно рассматривать эти случаи. При $k < 4$ коммутаторы, вес которых больше k , не рассматриваются, поскольку они равны единице группы по определению.

Запишем РС-представление группы $B_0(2, 5, 4)$ согласно [1].

Коммутаторы веса 1:

a_1, a_2 — образующие группы.

Коммутаторы веса 2:

$a_3 = [a_2, a_1]$.

Коммутаторы веса 3:

$a_4 = [a_3, a_1] = [a_2, a_1, a_1],$
 $a_5 = [a_3, a_2] = [a_2, a_1, a_2].$

Коммутаторы веса 4:

$a_6 = [a_4, a_1] = [a_2, a_1, a_1, a_1],$

$$\begin{aligned} a_7 &= [a_5, a_1] = [a_2, a_1, a_2, a_1], \\ a_8 &= [a_5, a_2] = [a_2, a_1, a_2, a_2]. \end{aligned}$$

Список определяющих соотношений R для базисных коммутаторов:

$$\begin{aligned} a_i^5 &= 1 \quad (1 \leq i \leq 8), \quad [a_2, a_1] = a_3, \quad [a_3, a_1] = a_4, \quad [a_3, a_2] = a_5, \quad [a_4, a_1] = a_6, \\ [a_4, a_2] &= a_7, \quad [a_4, a_3] = 1, \quad [a_5, a_1] = a_7, \quad [a_5, a_2] = a_8, \quad [a_5, a_3] = 1, \quad [a_5, a_4] = 1, \\ [a_6, a_1] &= 1, \quad [a_6, a_2] = 1, \quad [a_6, a_3] = 1, \quad [a_6, a_4] = 1, \quad [a_6, a_5] = 1, \quad [a_7, a_1] = 1, \\ [a_7, a_2] &= 1, \quad [a_7, a_3] = 1, \quad [a_7, a_4] = 1, \quad [a_7, a_5] = 1, \quad [a_7, a_6] = 1, \quad [a_8, a_1] = 1, \\ [a_8, a_2] &= 1, \quad [a_8, a_3] = 1, \quad [a_8, a_4] = 1, \quad [a_8, a_5] = 1, \quad [a_8, a_6] = 1, \quad [a_8, a_7] = 1. \end{aligned}$$

Таким образом,

$$B_0(2, 5, 4) = \langle a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8 \mid R \rangle.$$

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

$$\forall g \in B_0(2, 5, 4) \quad g = a_1^{x_1} a_2^{x_2} a_3^{x_3} a_4^{x_4} a_5^{x_5} a_6^{x_6} a_7^{x_7} a_8^{x_8}, \quad x_i \in \mathbb{Z}_5.$$

Иногда будем писать $g = (x_1, \dots, x_8)$.

Для того чтобы определить функции z_i , сначала необходимо вычислить произведения вида $a_j^y a_i^x$ для всех $1 \leq i < j \leq 8$, $x, y = 1, 2, 3, 4$. Для пары (j, i) требуется по 16 значениям произведений (y, x) найти интерполяционный полином для каждого из 8 коммутаторов.

Начнем с первого случая $a_2^y a_1^x$:

$$\begin{aligned} a_2^1 a_1^1 &= (1, 1, 1, 0, 0, 0, 0, 0), & a_2^1 a_1^2 &= (2, 1, 2, 1, 0, 0, 0, 0), \\ a_2^1 a_1^3 &= (3, 1, 3, 3, 0, 1, 0, 0), & a_2^1 a_1^4 &= (4, 1, 4, 1, 0, 4, 0, 0), \\ a_2^2 a_1^1 &= (1, 2, 2, 0, 1, 0, 0, 0), & a_2^2 a_1^2 &= (2, 2, 4, 2, 2, 0, 1, 0), \\ a_2^2 a_1^3 &= (3, 2, 1, 1, 3, 2, 3, 0), & a_2^2 a_1^4 &= (4, 2, 3, 2, 4, 3, 1, 0), \\ a_2^3 a_1^1 &= (1, 3, 3, 0, 3, 0, 0, 1), & a_2^3 a_1^2 &= (2, 3, 1, 3, 1, 0, 3, 2), \\ a_2^3 a_1^3 &= (3, 3, 4, 4, 4, 3, 4, 3), & a_2^3 a_1^4 &= (4, 3, 2, 3, 2, 2, 3, 4), \\ a_2^4 a_1^1 &= (1, 4, 4, 0, 1, 0, 0, 4), & a_2^4 a_1^2 &= (2, 4, 3, 4, 2, 0, 1, 3), \\ a_2^4 a_1^3 &= (3, 4, 2, 2, 3, 4, 3, 2), & a_2^4 a_1^4 &= (4, 4, 1, 4, 4, 1, 1, 1). \end{aligned}$$

Запишем

$$a_2^y a_1^x = a_1^x a_2^y a_3^{f_3^{(1,2)}(x,y)} a_4^{f_4^{(1,2)}(x,y)} \dots a_8^{f_8^{(1,2)}(x,y)},$$

где $f_r^{(1,2)}(x, y) = \sum_{p=1}^4 \sum_{q=1}^4 \beta_{pq}^r x^p y^q$ — некоторые полиномы над полем $\mathbb{Z}_5$. Для их определения выполним интерполяцию для каждого коммутатора $r = 3, 4, \dots, 8$.

Для нахождения $f_r^{(1,2)}(x, y)$ требуется решить систему линейных уравнений над указанным полем:

$$\sum_{p=1}^4 \sum_{q=1}^4 \beta_{pq}^r x^p y^q = z_r^{yx}, \quad x, y = 1, 2, 3, 4, \quad (9)$$

где z_r^{yx} — значение r -го коммутатора для пары (y, x) . Данная система имеет 16 переменных и состоит из 16 уравнений.

Покажем на примере 8-го коммутатора нахождение $f_8^{(1,2)}(x, y)$. Для краткости вместо β_{pq}^8 будем писать β_{pq} . Подставив в систему (9) все значения z_8^{yx} , получим

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 4 & 2 & 3 & 4 & 2 & 1 & 3 & 4 & 2 & 1 & 3 & 4 & 1 & 3 & 1 \\ 3 & 4 & 3 & 2 & 4 & 3 & 1 & 2 & 4 & 3 & 1 & 2 & 4 & 1 & 2 & 1 \\ 4 & 1 & 4 & 4 & 1 & 4 & 1 & 4 & 1 & 4 & 1 & 4 & 1 & 1 & 4 & 1 \\ 2 & 2 & 4 & 2 & 4 & 3 & 2 & 4 & 3 & 1 & 4 & 3 & 1 & 3 & 1 & 1 \\ 4 & 3 & 3 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 4 & 4 & 4 & 3 & 3 & 1 \\ 1 & 3 & 2 & 4 & 1 & 4 & 2 & 3 & 2 & 3 & 4 & 1 & 4 & 3 & 2 & 1 \\ 3 & 2 & 1 & 3 & 4 & 2 & 2 & 1 & 3 & 4 & 4 & 2 & 1 & 3 & 4 & 1 \\ 3 & 3 & 4 & 3 & 4 & 2 & 3 & 4 & 2 & 1 & 4 & 2 & 1 & 2 & 1 & 1 \\ 1 & 2 & 3 & 4 & 1 & 4 & 3 & 2 & 3 & 2 & 4 & 1 & 4 & 2 & 3 & 1 \\ 4 & 2 & 2 & 1 & 1 & 1 & 3 & 3 & 3 & 3 & 4 & 4 & 4 & 2 & 2 & 1 \\ 2 & 3 & 1 & 2 & 4 & 3 & 3 & 1 & 2 & 4 & 4 & 3 & 1 & 2 & 4 & 1 \\ 4 & 4 & 1 & 4 & 1 & 4 & 4 & 1 & 4 & 1 & 1 & 4 & 1 & 4 & 1 & 1 \\ 3 & 1 & 2 & 2 & 4 & 3 & 4 & 3 & 1 & 2 & 1 & 2 & 4 & 4 & 3 & 1 \\ 2 & 1 & 3 & 3 & 4 & 2 & 4 & 2 & 1 & 3 & 1 & 3 & 4 & 4 & 2 & 1 \\ 1 & 4 & 4 & 1 & 1 & 1 & 4 & 4 & 4 & 4 & 1 & 1 & 1 & 4 & 4 & 1 \end{bmatrix} \cdot \begin{pmatrix} \beta_{11} \\ \beta_{21} \\ \beta_{12} \\ \beta_{31} \\ \beta_{22} \\ \beta_{13} \\ \beta_{41} \\ \beta_{32} \\ \beta_{23} \\ \beta_{14} \\ \beta_{42} \\ \beta_{33} \\ \beta_{24} \\ \beta_{43} \\ \beta_{34} \\ \beta_{44} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 4 \\ 3 \\ 2 \\ 1 \end{pmatrix}.$$

Ранг матрицы системы равен 16, поэтому она имеет единственное решение $\beta_{11} = 2$, $\beta_{12} = 2$, $\beta_{13} = 1$, все остальные коэффициенты равны нулю. Следовательно,

$$f_8^{(1,2)}(x, y) = 2xy + 2xy^2 + xy^3.$$

Аналогичным образом вычисляются все полиномы $f_r^{(1,2)}(x, y)$. Перечислим их:

$$f_1^{(1,2)}(x, y) = x,$$

$$f_2^{(1,2)}(x, y) = y,$$

$$f_3^{(1,2)}(x, y) = xy,$$

$$f_4^{(1,2)}(x, y) = 2xy + 3x^2y = \binom{x}{2}y,$$

$$f_5^{(1,2)}(x, y) = 2xy + 3xy^2 = x\binom{y}{2},$$

$$f_6^{(1,2)}(x, y) = 2xy + 2x^2y + x^3y = \binom{x}{3}y,$$

$$f_7^{(1,2)}(x, y) = 4xy + xy^2 + x^2y + 4x^2y^2 = \binom{x}{2}\binom{y}{2},$$

$$f_8^{(1,2)}(x, y) = 2xy + 2xy^2 + xy^3 = x\binom{y}{3}.$$

Таким образом,

$$a_2^y a_1^x = \left(x, y, xy, \binom{x}{2}y, x\binom{y}{2}, \binom{x}{3}y, \binom{x}{2}\binom{y}{2}, x\binom{y}{3} \right).$$

Вторая пара $a_3^y a_1^x$:

$$\begin{aligned}
 a_3^1 a_1^1 &= (1, 0, 1, 1, 0, 0, 0, 0), & a_3^1 a_1^2 &= (2, 0, 1, 2, 0, 1, 0, 0), \\
 a_3^1 a_1^3 &= (3, 0, 1, 3, 0, 3, 0, 0), & a_3^1 a_1^4 &= (4, 0, 1, 4, 0, 1, 0, 0), \\
 a_3^2 a_1^1 &= (1, 0, 2, 2, 0, 0, 0, 0), & a_3^2 a_1^2 &= (2, 0, 2, 4, 0, 2, 0, 0), \\
 a_3^2 a_1^3 &= (3, 0, 2, 1, 0, 1, 0, 0), & a_3^2 a_1^4 &= (4, 0, 2, 3, 0, 2, 0, 0), \\
 a_3^3 a_1^1 &= (1, 0, 3, 3, 0, 0, 0, 0), & a_3^3 a_1^2 &= (2, 0, 3, 1, 0, 3, 0, 0), \\
 a_3^3 a_1^3 &= (3, 0, 3, 4, 0, 4, 0, 0), & a_3^3 a_1^4 &= (4, 0, 3, 2, 0, 3, 0, 0), \\
 a_3^4 a_1^1 &= (1, 0, 4, 4, 0, 0, 0, 0), & a_3^4 a_1^2 &= (2, 0, 4, 3, 0, 4, 0, 0), \\
 a_3^4 a_1^3 &= (3, 0, 4, 2, 0, 2, 0, 0), & a_3^4 a_1^4 &= (4, 0, 4, 1, 0, 4, 0, 0); \\
 a_3^y a_1^x &= (x, 0, y, xy, 0, 2xy + 3x^2y, 0, 0).
 \end{aligned}$$

Третья пара $a_3^y a_2^x$:

$$\begin{aligned}
 a_3^1 a_2^1 &= (0, 1, 1, 0, 1, 0, 0, 0), & a_3^1 a_2^2 &= (0, 2, 1, 0, 2, 0, 0, 1), \\
 a_3^1 a_2^3 &= (0, 3, 1, 0, 3, 0, 0, 3), & a_3^1 a_2^4 &= (0, 4, 1, 0, 4, 0, 0, 1), \\
 a_3^2 a_2^1 &= (0, 1, 2, 0, 2, 0, 0, 0), & a_3^2 a_2^2 &= (0, 2, 2, 0, 4, 0, 0, 2), \\
 a_3^2 a_2^3 &= (0, 3, 2, 0, 1, 0, 0, 1), & a_3^2 a_2^4 &= (0, 4, 2, 0, 3, 0, 0, 2), \\
 a_3^3 a_2^1 &= (0, 1, 3, 0, 3, 0, 0, 0), & a_3^3 a_2^2 &= (0, 2, 3, 0, 1, 0, 0, 3), \\
 a_3^3 a_2^3 &= (0, 3, 3, 0, 4, 0, 0, 4), & a_3^3 a_2^4 &= (0, 4, 3, 0, 2, 0, 0, 3), \\
 a_3^4 a_2^1 &= (0, 1, 4, 0, 4, 0, 0, 0), & a_3^4 a_2^2 &= (0, 2, 4, 0, 3, 0, 0, 4), \\
 a_3^4 a_2^3 &= (0, 3, 4, 0, 2, 0, 0, 2), & a_3^4 a_2^4 &= (0, 4, 4, 0, 1, 0, 0, 4); \\
 a_3^y a_2^x &= (0, x, y, 0, xy, 0, 0, 2xy + 3x^2y).
 \end{aligned}$$

Четвёртая пара $a_4^y a_1^x$:

$$\begin{aligned}
 a_4^1 a_1^1 &= (1, 0, 0, 1, 0, 1, 0, 0), & a_4^1 a_1^2 &= (2, 0, 0, 1, 0, 2, 0, 0), \\
 a_4^1 a_1^3 &= (3, 0, 0, 1, 0, 3, 0, 0), & a_4^1 a_1^4 &= (4, 0, 0, 1, 0, 4, 0, 0), \\
 a_4^2 a_1^1 &= (1, 0, 0, 2, 0, 2, 0, 0), & a_4^2 a_1^2 &= (2, 0, 0, 2, 0, 4, 0, 0), \\
 a_4^2 a_1^3 &= (3, 0, 0, 2, 0, 1, 0, 0), & a_4^2 a_1^4 &= (4, 0, 0, 2, 0, 3, 0, 0), \\
 a_4^3 a_1^1 &= (1, 0, 0, 3, 0, 3, 0, 0), & a_4^3 a_1^2 &= (2, 0, 0, 3, 0, 1, 0, 0), \\
 a_4^3 a_1^3 &= (3, 0, 0, 3, 0, 4, 0, 0), & a_4^3 a_1^4 &= (4, 0, 0, 3, 0, 2, 0, 0), \\
 a_4^4 a_1^1 &= (1, 0, 0, 4, 0, 4, 0, 0), & a_4^4 a_1^2 &= (2, 0, 0, 4, 0, 3, 0, 0), \\
 a_4^4 a_1^3 &= (3, 0, 0, 4, 0, 2, 0, 0), & a_4^4 a_1^4 &= (4, 0, 0, 4, 0, 1, 0, 0); \\
 a_4^y a_1^x &= (x, 0, 0, y, 0, xy, 0, 0).
 \end{aligned}$$

Пятая пара $a_4^y a_2^x$:

$$\begin{aligned} a_4^1 a_2^1 &= (0, 1, 0, 1, 0, 0, 1, 0), & a_4^1 a_2^2 &= (0, 2, 0, 1, 0, 0, 2, 0), \\ a_4^1 a_2^3 &= (0, 3, 0, 1, 0, 0, 3, 0), & a_4^1 a_2^4 &= (0, 4, 0, 1, 0, 0, 4, 0), \\ a_4^2 a_2^1 &= (0, 1, 0, 2, 0, 0, 2, 0), & a_4^2 a_2^2 &= (0, 2, 0, 2, 0, 0, 4, 0), \\ a_4^2 a_2^3 &= (0, 3, 0, 2, 0, 0, 1, 0), & a_4^2 a_2^4 &= (0, 4, 0, 2, 0, 0, 3, 0), \\ a_4^3 a_2^1 &= (0, 1, 0, 3, 0, 0, 3, 0), & a_4^3 a_2^2 &= (0, 2, 0, 3, 0, 0, 1, 0), \\ a_4^3 a_2^3 &= (0, 3, 0, 3, 0, 0, 4, 0), & a_4^3 a_2^4 &= (0, 4, 0, 3, 0, 0, 2, 0), \\ a_4^4 a_2^1 &= (0, 1, 0, 4, 0, 0, 4, 0), & a_4^4 a_2^2 &= (0, 2, 0, 4, 0, 0, 3, 0), \\ a_4^4 a_2^3 &= (0, 3, 0, 4, 0, 0, 2, 0), & a_4^4 a_2^4 &= (0, 4, 0, 4, 0, 0, 1, 0); \\ a_4^y a_2^x &= (0, x, 0, y, 0, 0, xy, 0). \end{aligned}$$

Шестая пара $a_4^y a_3^x$. Коммутаторы a_4 и a_3 перестановочны, поэтому $a_4^y a_3^x = a_3^x a_4^y$. Теперь рассмотрим $a_5^y a_1^x$:

$$\begin{aligned} a_5^1 a_1^1 &= (1, 0, 0, 0, 1, 0, 1, 0), & a_5^1 a_1^2 &= (2, 0, 0, 0, 1, 0, 2, 0), \\ a_5^1 a_1^3 &= (3, 0, 0, 0, 1, 0, 3, 0), & a_5^1 a_1^4 &= (4, 0, 0, 0, 1, 0, 4, 0), \\ a_5^2 a_1^1 &= (1, 0, 0, 0, 2, 0, 2, 0), & a_5^2 a_1^2 &= (2, 0, 0, 0, 2, 0, 4, 0), \\ a_5^2 a_1^3 &= (3, 0, 0, 0, 2, 0, 1, 0), & a_5^2 a_1^4 &= (4, 0, 0, 0, 2, 0, 3, 0), \\ a_5^3 a_1^1 &= (1, 0, 0, 0, 3, 0, 3, 0), & a_5^3 a_1^2 &= (2, 0, 0, 0, 3, 0, 1, 0), \\ a_5^3 a_1^3 &= (3, 0, 0, 0, 3, 0, 4, 0), & a_5^3 a_1^4 &= (4, 0, 0, 0, 3, 0, 2, 0), \\ a_5^4 a_1^1 &= (1, 0, 0, 0, 4, 0, 4, 0), & a_5^4 a_1^2 &= (2, 0, 0, 0, 4, 0, 3, 0), \\ a_5^4 a_1^3 &= (3, 0, 0, 0, 4, 0, 2, 0), & a_5^4 a_1^4 &= (4, 0, 0, 0, 4, 0, 1, 0); \\ a_5^y a_1^x &= (x, 0, 0, 0, y, 0, xy, 0). \end{aligned}$$

И наконец, последняя неперестановочная пара $a_5^y a_2^x$:

$$\begin{aligned} a_5^1 a_2^1 &= (0, 1, 0, 0, 1, 0, 0, 1), & a_5^1 a_2^2 &= (0, 2, 0, 0, 1, 0, 0, 2), \\ a_5^1 a_2^3 &= (0, 3, 0, 0, 1, 0, 0, 3), & a_5^1 a_2^4 &= (0, 4, 0, 0, 1, 0, 0, 4), \\ a_5^2 a_2^1 &= (0, 1, 0, 0, 2, 0, 0, 2), & a_5^2 a_2^2 &= (0, 2, 0, 0, 2, 0, 0, 4), \\ a_5^2 a_2^3 &= (0, 3, 0, 0, 2, 0, 0, 1), & a_5^2 a_2^4 &= (0, 4, 0, 0, 2, 0, 0, 3), \\ a_5^3 a_2^1 &= (0, 1, 0, 0, 3, 0, 0, 3), & a_5^3 a_2^2 &= (0, 2, 0, 0, 3, 0, 0, 1), \\ a_5^3 a_2^3 &= (0, 3, 0, 0, 3, 0, 0, 4), & a_5^3 a_2^4 &= (0, 4, 0, 0, 3, 0, 0, 2), \\ a_5^4 a_2^1 &= (0, 1, 0, 0, 4, 0, 0, 4), & a_5^4 a_2^2 &= (0, 2, 0, 0, 4, 0, 0, 3), \\ a_5^4 a_2^3 &= (0, 3, 0, 0, 4, 0, 0, 2), & a_5^4 a_2^4 &= (0, 4, 0, 0, 4, 0, 0, 1); \\ a_5^y a_2^x &= (0, x, 0, 0, y, 0, 0, xy). \end{aligned}$$

Все оставшиеся пары $a_j^y a_i^x$ перестановочны, т. е. $a_j^y a_i^x = a_i^x a_j^y$.

Таким образом, имеем полный набор соотношений для осуществления собирательного процесса в аналитическом виде:

$$a_j^y a_i^x = a_i^x a_j^y a_{j+1}^{f_{j+1}^{(i,j)}(x,y)} a_{j+2}^{f_{j+2}^{(i,j)}(x,y)} \dots a_8^{f_8^{(i,j)}(x,y)}, \quad 1 \leq i < j \leq 8. \quad (10)$$

Пользуясь (10), можем вычислить произведение $a_1^{x_1} \dots a_8^{x_8} \cdot a_1^{y_1} \dots a_8^{y_8} = a_1^{z_1} \dots a_8^{z_8}$. После выполнения данной процедуры найдём все z_i (1)–(8).

Теорема доказана.

ЛИТЕРАТУРА

1. *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.
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 summer seminar, University of Alberta, 12–30 August, 1957. London: Queen Mary College, 1969.
5. *Sims C.* Fast multiplication and growth in groups // Proc. Intern. Symp. Symbolic and Algebraic Computation. New York, NY, USA, 1998. P. 165–170.