Следствие 2 означает, что свойство ВРП-функции задавать подстановку или n-квазигруппу зависит лишь от разрядных многочленов, а не от выбора разрядного множества $\mathcal{B}$, относительно которого рассматривается такая функция. Это позволяет строить различные подстановки и ВРП n-квазигруппы, используя одни и те же разрядные многочлены, но разные разрядные множества.

ЛИТЕРАТУРА

1. *Елизаров В. П.* Конечные кольца. М.: Гелиос-АРВ, 2006.
2. *Заец М. В.* О классе вариационно-координатно полиномиальных функций над примарным кольцом вычетов // Прикладная дискретная математика. 2014. № 3. С. 12–28.
3. *Заец М. В., Никонов В. Г., Шишков А. Б.* Класс функций с вариационно-координатной полиномиальностью над кольцом $\mathbb{Z}_{2^m}$ и его обобщение // Матем. вопросы криптографии. 2013. Т. 4. № 3. С. 19–45.
4. *Заец М. В.* Классы полиномиальных и вариационно-координатно полиномиальных функций над кольцом Галуа // Прикладная дискретная математика. Приложение. 2013. № 6. С. 13–15.
5. *Lausch H. and Nobauer W.* Algebra of polynomials. Amsterdam: North-Holl. Publ. Co, 1973.
6. *Заец М. В.* Построение подстановок с использованием вариационно-координатно полиномиальных функций над примарным кольцом вычетов // Матем. вопросы криптографии. 2015. Т. 6. № 1. С. 5–32.
7. *Нечаев А. А.* Полиномиальные преобразования конечных коммутативных локальных колец главных идеалов // Матем. заметки. 1980. Т. 27. Вып. 6. С. 885–899.
8. *Белоусов В. Д.* n-Арные квазигруппы. Кишинев: Штиинца, 1972.

УДК 519.688 DOI 10.17223/2226308X/10/6

О ГРАФЕ КЭЛИ ОДНОЙ ПОДГРУППЫ БЕРНСАЙДОВОЙ ГРУППЫ $B_0(2,5)$[1]

А. А. Кузнецов, А. С. Кузнецова

Пусть $B_0(2,5)$ — максимальная конечная двупорожденная бернсайдова группа периода 5, порядок которой равен 5^{34}. Определим автоморфизм φ, при котором каждый порождающий элемент отображается в другой порождающий. Пусть $C_{B_0(2,5)}(\varphi)$ — централизатор φ в $B_0(2,5)$. Известно, что $|C_{B_0(2,5)}(\varphi)| = 5^{17}$. В работе вычислена функция роста данного централизатора для минимального порождающего множества. В результате получены диаметр и средний диаметр соответствующего графа Кэли $C_{B_0(2,5)}(\varphi)$.

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

Одним из важных инструментов для определения строения группы является изучение её роста относительно фиксированного порождающего множества. Пусть $G = \langle X \rangle$. Шаром K_s радиуса s группы G будем называть множество всех её элементов, которые могут быть представлены в виде групповых слов в алфавите X длиною, не превышающей s. Для каждого целого неотрицательного s можно определить функцию роста группы $F(s)$, которая равна числу элементов группы G относительно X, представимых в виде несократимых групповых слов длиною s. Таким образом,

$$F(0) = |K_0| = 1,\ F(s) = |K_s| - |K_{s-1}| \text{ при } s \in \mathbb{N}.$$

[1]Работа поддержана РФФИ и Правительством Красноярского края (проект № 17-47-240318).

Как правило, функцию роста конечной группы представляют в виде таблицы, в которую записывают ненулевые значения $F(s)$.

Отметим, что при вычислении функции роста группы мы параллельно выясняем характеристики соответствующего графа Кэли, например такие, как диаметр и средний диаметр [1]. 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 $D_X(G)$. Соответственно средний диаметр $\overline{D}_X(G)$ равен $\dfrac{1}{|G|}\sum\limits_{s=0}^{s_0} s \cdot F(s)$.

К сожалению, вычисление функции роста большой конечной группы является хотя и разрешимой, но весьма сложной проблемой. Это связано с тем, что в общем случае задача по определению минимального слова элемента группы, как показали С. Ивен и О. Голдрейх [2], является NP-трудной. Таким образом, в наихудшем случае количество элементарных операций, которые необходимо выполнить для решения указанной задачи, представляет собой экспоненциальную функцию от $|X|$.

Отметим, что подобные задачи естественным образом возникают в теории кодирования и криптографии. Сюда можно отнести задачу эффективного восстановления вершин в графе, например в графе Хэмминга, который является графом Кэли. Многие вопросы в рамках этой задачи остаются открытыми [3].

Пусть $B(2,5) = \langle a_1, a_2 \rangle$ — свободная двупорождённая бернсайдова группа периода 5. На сегодняшний день неизвестно, конечна или бесконечна данная группа. Далее, пусть $B_0(2,5) = \langle a_1, a_2 \rangle$ — максимальная конечная группа, порядок которой равен 5^{34} [4]. Если $B(2,5)$ конечна, то $B_0(2,5) = B(2,5)$.

Вычислить функцию роста $B_0(2,5)$ относительно минимального порождающего множества в настоящее время едва ли возможно, поскольку количество её элементов очень велико:

$$5^{34} = 5820766091346740722656 25 \approx 5 \cdot 10^{23}.$$

Отметим, что на сегодняшний день при помощи компьютерных вычислений удалось получить функции роста фактор-групп группы $B_0(2,5)$, порядок которых не превышает 5^{17} [5].

Рассмотрим отображение φ следующего вида:

$$\varphi : \begin{cases} a_1 \to a_2, \\ a_2 \to a_1. \end{cases}$$

Нетрудно увидеть [6], что φ является инволютивным автоморфизмом в группах $B(2,5)$ и $B_0(2,5)$.

Пусть $C_{B(2,5)}(\varphi)$ и $C_{B_0(2,5)}(\varphi)$ — централизаторы автоморфизма φ в $B(2,5)$ и $B_0(2,5)$ соответственно. Согласно теореме В. П. Шункова [7], если $C_{B(2,5)}(\varphi)$ окажется конечной группой, то группа $B(2,5)$ также будет конечна. Другими словами, если $C_{B(2,5)}(\varphi) = C_{B_0(2,5)}(\varphi)$, то $B(2,5) = B_0(2,5)$. По этой причине исследование функций роста $C_{B_0(2,5)}(\varphi)$ представляет большой интерес. Далее для краткости вместо $C_{B_0(2,5)}(\varphi)$ будем писать C.

В [6] исследовано строение группы C и получены следующие результаты:

1) $|C| = 5^{17}$;
2) ступени разрешимости и нильпотентности равны 3 и 6 соответственно;
3) 3 — минимальное число порождающих C.

Целью настоящей работы является исследование функции роста группы C относительно минимального порождающего множества $X = \{x_1, x_2, x_3\}$.

Результаты компьютерных вычислений

Вычисление функции роста группы C относительно X проведено по алгоритму из [5]. Для эффективного умножения элементов были задействованы полиномы Холла [8]. Алгоритм реализован на языке C++. В качестве инструмента распараллеливания использована библиотека OpenMP. Вычисления проводились на компьютере, имеющем 8-ядерный процессор и 64 Гб оперативной памяти под ОС Linux. Трансляция программы осуществлялась встроенным в систему компилятором gcc. Время вычисления функции роста составило примерно 36 ч.

Функция роста группы содержит в себе информацию о характеристиках соответствующего графа Кэли:

Следствие. $D_X(C) = 33$, $\overline{D}_X(C) \approx 26{,}1$.

ЛИТЕРАТУРА

1. *Кузнецов А. А., Кузнецова А. С.* Параллельный алгоритм для исследования графов Кэли групп подстановок // Вестник СибГАУ. 2014. № 1. С. 34–39.
2. *Even S. and Goldreich O.* The Minimum Length Generator Sequence is NP-Hard // J. Algorithms. 1981. No. 2. P. 311–313.
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. *Кузнецов А. А.* Об одном алгоритме вычисления функций роста в конечных двупорождённых группах периода пять // Прикладная дискретная математика. 2016. № 3. С. 116–125.
6. *Кузнецов А. А., Филиппов К. А.* Об одном автоморфизме порядка 2 бернсайдовой группы $B_0(2, 5)$ // Владикавказский математический журнал. 2010. № 4. С. 44–48.
7. *Шунков В. П.* О периодических группах с почти регулярной инволюцией // Алгебра и логика. 1972. № 4. С. 470–494.
8. *Кузнецов А. А., Кузнецова А. С.* Быстрое умножение элементов в конечных двупорождённых группах периода пять // Прикладная дискретная математика. 2013. № 1. С. 110–116.

УДК 519.151, 519.725, 519.165 DOI 10.17223/2226308X/10/7

ОБ ОДНОРОДНЫХ МАТРОИДАХ И БЛОК-СХЕМАХ

Н. В. Медведев, С. С. Титов

Работа посвящена вопросам, связанным с разграничением доступа посредством идеальных совершенных схем разделения секрета и матроидов. Рассматриваются однородные матроиды, т. е. такие, все циклы которых имеют одинаковую мощность, при этом, возможно, не все подмножества этой мощности являются циклами. Установлена их связь с блок-схемами, в том числе с семейством троек Штейнера, а именно доказано, что матроид, у которого когиперплоскости — тройки Штейнера, является однородным связным и разделяющим, если его мощность не меньше семи. Доказано, что блок-схема, в которой каждая пара различных элементов появляется в единственном блоке, задаёт когиперплоскости однородного связного разделяющего матроида. Выдвинуты гипотезы для дальнейшего исследования.

Ключевые слова: *схемы разделения секрета, однородные матроиды, блок-схемы, циклы.*

Разграничение доступа на основе схем разделения секрета (СРС) состоит в том, чтобы заранее заданные (разрешённые) коалиции участников могли однозначно вос-