Алгоритмы реализованы на языке программирования C++ с использованием библиотеки NTL [3]. В таблице проводятся результаты экспериментов на компьютере с процессором Intel core i7 с тактовой частой 3,33 ГГц при значении параметра $k = 100$.

Время работы алгоритмов варьируется в пределах, отличающихся на порядок. В связи с этим в таблице указано худшее время в трёх случайных экспериментах.

Результаты экспериментов с 1024-битовым модулем

p и q, биты	g, биты	Время алг. 1, с	Время алг. 2, с
512	256	46	24
	320	51	31
	384	58	19
1024	512	1082	213
	640	908	660
	768	794	98

Из таблицы видно, что, несмотря на предложенное ускорение метода построения специальных простых, выработка модуля криптосистемы Common Prime RSA занимает неприемлемо большое время. Отметим, что выработка пары случайных простых чисел без дополнительных свойств занимает десятые доли секунды.

ЛИТЕРАТУРА

1. *Hinek M. J.* Another look at small RSA exponents // LNCS. 2006. V. 3860. P. 82–98.
2. *Hinek M. J.* Cryptanalysis of RSA and Its Variants. CRC Press, 2009.
3. *Shoup V.* NTL — a library for doing number theory // http://www.shoup.net

УДК 519.688

ПОЛИНОМЫ ХОЛЛА ДЛЯ КОНЕЧНЫХ ДВУПОРОЖДЁННЫХ ГРУПП ПЕРИОДА СЕМЬ[1]

А. А. Кузнецов, К. В. Сафонов

Пусть $B_k = B_0(2, 7, k)$ — максимальная конечная двупорождённая группа периода 7 ступени нильпотентности k. В работе вычислены полиномы Холла для B_k при $k \leqslant 4$.

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

Пусть $B_k = B_0(2, 7, k)$ — максимальная конечная двупорождённая группа периода 7 ступени нильпотентности k. В данном классе групп наибольшей является группа B_{28}, порядок которой равен 7^{20416} [1]. Для каждой из B_k получены pc-представления (power commutator presentation) [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_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 системах компьютерной алгебры GAP и MAGMA. Кроме того, существует альтернативный способ для вычисления произведений элементов группы, предложенный Ф. Холлом [4]. Холл показал, что z_i представляют собой полиномиальные

[1]Работа выполнена при поддержке Министерства образования и науки Российской Федерации, проект Б 112/14.

функции (в нашем случае над полем $\mathbb{Z}_7$), зависящие от переменных $x_1, \ldots, x_i, y_1, \ldots, y_i$, которые принято сейчас называть *полиномами Холла*. Согласно [4],

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

Необходимость применения полиномов Холла возникает при решении задач, требующих многократного умножения элементов группы. Исследование структуры графа Кэли некоторой группы является одной из таких задач [5, 6]. Проведённые вычислительные эксперименты на ЭВМ в двупорождённых группах периода пять [7] выявили, что метод полиномов Холла имеет преимущество перед традиционным собирательным процессом. Поэтому имеются основания полагать, что при изучении графов Кэли групп B_k применение полиномов окажется предпочтительнее собирательного процесса. Следует также отметить, что данный метод легко программно реализуем, в том числе на многопроцессорных вычислительных системах.

В 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, что делает невозможным проверить доказательство без применения ЭВМ.

Основным результатом настоящей работы является

Теорема 1. Пусть $a_1^{x_1} \ldots a_n^{x_n}$ и $a_1^{y_1} \ldots a_n^{y_n}$ — два произвольных элемента в группе B_k, записанные в коммутаторном виде, где $k \in \mathbb{N}$ и $k \leqslant 4$. Тогда их произведение равно $a_1^{x_1} \ldots a_n^{x_n} \cdot a_1^{y_1} \ldots a_n^{y_n} = a_1^{z_1} \ldots a_n^{z_n}$, где $z_i \in \mathbb{Z}_7$ — полиномы Холла, задаваемые формулами (1), (2) при $k = 1$; (1)–(3) при $k = 2$; (1)–(5) при $k = 3$; (1)–(8) при $k = 4$:

$$z_1 = x_1 + y_1, \tag{1}$$

$$z_2 = x_2 + y_2, \tag{2}$$

$$z_3 = x_3 + y_3 + x_2y_1, \tag{3}$$

$$z_4 = x_4 + y_4 + 3x_2y_1 + x_3y_1 + 4x_2y_1^2, \tag{4}$$

$$z_5 = x_5 + y_5 + 3x_2y_1 + x_3y_2 + 4x_2^2y_1 + x_2y_1y_2, \tag{5}$$

$$z_6 = x_6 + y_6 + 5x_2y_1 + 3x_3y_1 + x_4y_1 + 3x_2y_1^2 + 6x_2y_1^3 + 4x_3y_1^2, \tag{6}$$

$$\begin{aligned} z_7 = x_7 + y_7 + 2x_2^2y_1^2 + 2x_2y_1 + x_4y_2 + x_5y_1 + 5x_2y_1^2 + 5x_2^2y_1 + 4x_2y_1^2y_2 + \\ +3x_2y_1y_2 + x_3y_1y_2, \end{aligned} \tag{7}$$

$$\begin{aligned} z_8 = x_8 + y_8 + 5x_2y_1 + 3x_3y_2 + x_5y_2 + 3x_2^2y_1 + 6x_2^3y_1 + 4x_3y_2^2 + 4x_2y_1y_2^2 + \\ +4x_2^2y_1y_2 + 6x_2y_1y_2. \end{aligned} \tag{8}$$

ЛИТЕРАТУРА

1. *O'Brien E. A. and Vaughan-Lee M. R.* The 2-generator restricted Burnside group of exponent 7 // Int. J. Algebra Comput. 2002. No. 12. 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. *Кузнецов А. А., Кузнецова А. С.* Компьютерное моделирование конечных двупорожденных групп периода 5 // Вестник Сибирского государственного аэрокосмического университета. 2012. № 5. С. 59–62.

6. *Кузнецов А. А., Кузнецова А. С.* О взаимосвязи функций роста в симметрических группах с задачами комбинаторной оптимизации // Вестник Сибирского государственного аэрокосмического университета. 2012. № 6. С. 57–62.
7. *Кузнецов А. А., Кузнецова А. С.* Быстрое умножение элементов в конечных двупорождённых группах периода пять // Прикладная дискретная математика. 2013. № 1. С. 110–116.

УДК 519.85

ЭВРИСТИКИ ПОСТРОЕНИЯ НАДЕЖНОЙ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ[1]

Р. Э. Шангин

Рассматривается известная NP-трудная задача нахождения минимального остовного k-дерева в простом взвешенном графе. Данную задачу необходимо решать при проектировании надежной телекоммуникационной сети наименьшей стоимости. Предлагается серия эвристических алгоритмов. Определены оценки трудоёмкости алгоритмов, доказана их корректность. Проведён вычислительный эксперимент по сравнению эффективности предложенных алгоритмов, как между собой, так и с известными приближёнными и точными алгоритмами.

Ключевые слова: *остовное k-дерево, надёжная сеть, IFI-сеть, NP-трудность, эвристики.*

Эффективное решение проблемы надежности информационных сетей, в первую очередь, заключается в проектировании сети, устойчивой как к сбоям отдельных каналов, так и к полным отказам некоторых звеньев системы. В начале 1980-х годов А. Фарлеем введена концепция IFI-сетей (Isolated Failure Immune networks) [1]. Такие IFI-сети являются устойчивыми к сбоям трех типов:

1) удаление рёбер, не имеющих общую вершину;
2) удаление несмежных вершин;
3) удаление рёбер и вершин, если рёбра не инцидентны ни одной удалённой вершине или не инцидентны вершине, смежной с удалённой.

В работе [1] А. Фарлей доказал, что 2-дерево [2] есть минимальная (по включению рёбер) IFI-сеть. Отсюда задача проектирования IFI-сети может быть представлена как задача построения остовного k-дерева минимального веса, известная в зарубежной литературе как *Minimum Spanning k-tree Problem* (MSkT) и являющаяся обобщением классической задачи нахождения минимального остовного дерева (MST) [3].

Определение 1. Связный неориентированный граф T называется k-деревом, если его построение возможно осуществить рекурсивно по правилам: полный граф из $k+1$ вершин есть k-дерево; k-дерево с $i+1$ вершинами получается из k-дерева с i вершинами добавлением в него новой вершины j и k рёбер таким образом, чтобы новая вершина j стала смежной со всеми вершинами некоторой клики размера k.

Формулировка задачи MSkT следующая. Пусть $G = (V, E)$ — полный взвешенный граф с множествами вершин V (телекоммуникационные терминалы) и рёбер E (возможные связи между терминалами), причём для каждого ребра $[i, j] \in E$ задан его вес $w(i, j) \geqslant 0$, равный стоимости прокладки кабеля или трансляции сигналов между терминалами i и j. Обозначим $T(G)$ множество всех остовных k-деревьев в гра-

[1]Исследование выполнено при поддержке Министерства образования и науки Российской Федерации, соглашение № 14.B37.21.0395.