КРАСНОЯРСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ

КУЗНЕЦОВ А.А., КУЗЬМИН Д.А., ЛЫТКИНА Д.В,
ТУХВАТУЛЛИНА Л.Р., ФИЛИППОВ К.А.

КОМПЬЮТЕРНЫЕ АЛГОРИТМЫ ТЕОРЕТИКО–МНОЖЕСТВЕННОГО АНАЛИЗА СЛОЖНЫХ АЛГЕБРАИЧЕСКИХ СИСТЕМ

Красноярск-2009

УДК 519.712.2
ББК 22.19

Кузнецов А.А., Кузьмин Д.А. Лыткина Д.В, Тухватуллина Л.Р., Филиппов К.А. Компьютерные алгоритмы теоретико-множественного анализа сложных алгебраических систем. Красноярск: КрасГАУ, 2009. 186 с.

В монографии изучаются компьютерные алгоритмы для моделирования сложных алгебраических систем. Книга будет полезна научным работникам, студентам и аспирантам, специализирующимся в области компьютерной алгебры.

Рецензенты:
доктор физико-математических наук К.В. Сафонов
доктор физико-математических наук С.И. Сенашов

Утвержено к печати ученым советом
Красноярского государственного аграрного университета

Содержание

Введение

Современные научные данные и современные системные представления позволяют говорить о мире как о бесконечной иерархической системе систем [72]. Выдающийся советский ученый Н.Н. Моисеев определяет *системный анализ*, как совокупность методов, основанных на использовании ЭВМ и ориентированных на исследование сложных систем — технических, экономических, экологических и т. д. [62].

Однако методология системного анализа в приведенных выше областях может быть спроецирована на изучение объектов из других разделов естествознания (математика, физика и т. д.). Например, в математике за последние десятилетия появилось новое направление — *компьютерное доказательство теорем*. Первым примером крупной математической теоремы, для доказательства которой был применен компьютер, стала теорема о четырех красках, доказанная в 1976 г. К. Аппелом и У. Хакеном [98, 99]. Конечно, указанное направление существенно использует методы информатики и вычислительной техники, что делает его междисциплинарным.

В настоящей работе предлагается методология работы со сложными дискретными объектами, характеризующимися большим числом элементов и требующих применения высокопроизводительных ЭВМ. Для формального описания указанных объектов на компьютере необходимы теоретико-множественные представления — дискретные *алгебраические* *системы*. Алгебраической системой принято называть множество с заданным на нем набором операций, удовлетворяющим некоторой системе аксиом [7, 59, 79]. Представление алгебраических систем в виде объектов, поддающихся вычислительной обработке, и ответ на три главных вопроса:

- Что такое вычисление математического объекта?
- Как его вычислить наиболее эффективно?
- Каким образом обеспечить достоверность вычислений?

определяют основные задачи *компьютерной алгебры* [15,52,71,77].

Одним из важных и интересных направлений компьютерной алгебры является *вычислительная теория групп* (computational group theory), далее ВТГ. Объектом исследования данного направления являются алгебраические системы с одной бинарной операцией (группоиды, полугруппы, моноиды, группы и т. д.) [53]. Как самостоятельное научное направление со своей проблематикой ВТГ оформилась после того как в 1911 г. М. Дэн сформулировал основные алгоритмические проблемы теории групп: проблему распознавания равенства, известную в литературе также под названием "проблема тождества слов", проблему сопряженности и проблему изоморфизма [106]. ВТГ находит многочисленные приложения как в самой математике (в геометрии, теории функций, теории дифференциальных уравнений и др.), так и за ее пределами (в кристаллографии, в классической и квантовой механике, в теории элементарных частиц, в химии, в биологии и т. д.) [8]. В связи с всеобщей информатизацией период доминирования непрерывной математики в значительной мере сменился периодом преобладания дискретной математики. В результате расширились и приложения теории групп:

комбинаторика, теория конечных геометрий, теория графов, теория кодирования, теория сложности вычислений, криптография и т. д. [13]. Первые компьютерные программы для работы с группами были реализованы в начале 50-х годов XX века [112]. С тех пор эта сфера научной деятельности получила широкое распространение, исследования по соответствующей тематике ведутся во многих научных центрах по всему миру [9]. Помимо отдельных программ, разработано несколько мощных систем компьютерной алгебры, специализированных на вычислениях в группах (GAP [107], Magma [116]), накоплен также богатый опыт использования систем компьютерной алгебры общего назначения (Maple, Mathematica, Matlab и др. [16]) для теоретико-групповых вычислений. Привлечение фактического материала, получаемого при помощи символьных вычислений в различных классах групп, стало характерной чертой развития теории групп. В подтверждении этого факта уместно напомнить, что первоначальное построение многих простых спорадических групп существенно использовало вычисления на компьютере. Так в 1982 году Р. Грисс-младший построил группу, названную "монстром" за то, что число её элементов равно

$$808017424794512875886459904961710757005754368000000000,$$

или приближенно $8 \cdot 10^{53}$ [14].

Рассматриваемые в рамках ВТГ алгебраические системы следует отнести к разряду сложных [61]. Дело в том, что проблема тождества слов в группах, как показал П.С. Новиков [69], в общем случае алгоритмически неразрешима. Аналогичный результат для полугрупп получен независимо А.А. Марковым [60] и Э. Постом [122]. Алгоритмическая неразрешимость проблемы изоморфизма в группах была доказана С.И. Адяном [1] и М. Рабином [123]. И, наконец, алгоритмическая неразрешимость проблемы сопряженности в группах была получена У. Буном [102].

В то же время, для частных случаев групп такие алгоритмы существуют. Главным образом, их применение связано с решением задач о конечности группы, определении ее структуры и изоморфизма с другими группами. Прежде всего, современные системы компьютерной алгебры, ориентированные на группы, способны производить вычисления с несколькими разновидностями последних. В первую очередь это группы подстановок, матричные группы и конечноопределенные группы (заданные конечным числом образующих и соотношений). Для первых двух классов имеется множество эффективных алгоритмов, ориентированных на разные типы задач. Так, например, некоторые виды вычислений могут быть проведены с использованием полиномиальных, или даже почти линейных по времени алгоритмов [124].

Ситуация с конечноопределенными группами значительно сложнее. Здесь есть принципиальная трудность, состоящая в неразрешимости проблемы тождества слов в общем случае. Имеется весьма ограниченный набор базисных алгоритмов: метод Тодда-Коксеттера перечисления смежных классов и процедура Кнута-Бендикса по переписыванию слов в некоторой нормальной форме путем сбора всех существующих пар эквивалентных слов [112, 126]. В частных подклассах конечноопределенных групп, в которых проблема тождества слов разрешима, опять имеется большое число методов и алгоритмов. Упомянем здесь подклас конечных групп, а также полициклических групп (имеющих конечный субнормальный ряд с циклическими факторами). Особенно эффективные алгоритмы разработаны для пересечения этих классов, т. е. для конечных разрешимых групп. Некоторые из внедренных здесь методов превосходят по быстродействию своих аналогов в группах подстановок [112, 126]. В последнее время помимо детерминированных алгоритмов для нужд ВТГ пытаются также применять и вероятностные методы [103, 119], основанные на генетических алгоритмах [11, 76].

В связи с интенсивным развитием высокопроизводительных вычислительных систем — суперкомпьютеров[1], а также соответствующего программного обеспечения для реализации параллельных алгоритмов ([6, 10, 54, 97]), появилась возможность существенно повысить скорость расчетов в задачах ВТГ.

Несмотря на то, что квантовые компьютеры ([68, 74]) еще находятся в стадии разработки, в работе [100] уже предложены квантовые алгоритмы для вычислений в группах.

К важнейшему классу задач ВТГ относят бернсайдову проблематику. Проблема Бернсайда о периодических группах фиксированного периода была поставлена известным английским математиком У. Бернсайдом в 1902 году в следующей форме [105].

Пусть $x_1, x_2, \ldots, x_m$ — конечное число независимых элементов, порождающих группу G, в которой для любого элемента g выполнено соотношение $g^n = 1$, где n — данное целое число. Будет ли определенная таким образом группа конечной, и если да, то каков ее порядок?

Впоследствии эти группы получили название *свободных бернсайдовых групп* и обозначение $B(m,n)$. Перечислим известные к настоящему времени результаты по данным группам. $B(m,n)$ конечна для $n = 2$ (тривиальный случай), $n = 3$ (У. Бернсайд, 1902 [105]), $n = 4$ ($m = 2$ —

[1]28 июля 2009 г. президент РФ Д.А. Медведев на заседании Совета безопасности заявил, что разработка суперкомпьютеров является приоритетной задачей России. "... У нас считанные единицы моделей обсчитываются на суперкомпьютерах, а остальные делаются на ватмане с применением известных прежних подходов. При этом только цифровой подход может дать необходимый эффект, повысить уровень прогнозирования и управления самыми сложными процессами", — отметил он [75].

У. Бернсайд [105], $m > 2$ — И.Н. Санов, 1940 [78]), $n = 6$ (М. Холл, 1958 [108]). $B(m,n)$ бесконечна для нечётных $n \geq 665$ (С.И. Адян, П.С. Новиков, 1968 для $n \geq 4381$ [70], 1975 для $n \geq 665$ [2]); для четных: $n \geq 2^{48}$ и n делится на 2^9 (С.В. Иванов, 1994 [114]), $n = 16k \geq 8000$ (И.Г. Лысёнок, 1996 [56]). Отметим, что перечисленные результаты были получены без привлечения компьютерных вычислений. Для других же показателей, наименьший из которых $n = 5$, вопрос о конечности $B(m,n)$ остается открытым.

Приведем порядки конечных бернсайдовых групп. Группа $B(m,2)$ явлется элементарной абелевой и имеет порядок 2^m. Ф. Леви и Б. Л. Ван дер Варден показали, что $|B(m,3)| = 3^a$, где $a = m + C_m^2 + C_m^3$ (1933 [115]), здесь C_m^k — биномиальный коэффициент. Для показателя $n = 4$ известны порядки следующих бернсайдовых групп: $|B(2,4)| = 2^{12}$ (Дж. Тобин, 1954 [128]), $|B(3,4)| = 2^{69}$ (А. Байес, Дж. Кауцкий, Дж. Уэмсли, 1974 [101]), $|B(4,4)| = 2^{422}$ (Дж. Хавас, М. Ньюмен, 1980 [110]), $|B(5,4)| = 2^{2728}$ (Е. О'Брайн, М. Ньюмен, 1996 [120]). Для последних трех случаев порядки групп были вычислены при помощи компьютера. И, наконец, $|B(m,6)| = 2^a 3^b$, где $a = 1 + (m-1)3^c$, $b = 1 + (m-1)2^m$ и $c = m + C_m^2 + C_m^3$ (М. Холл, 1958 [108]).

Более общий вопрос о локальной конечности периодических групп без ограничения на порядки элементов имеет название *"общая проблема Бернсайда"*, отрицательное решение которой было получено Е.С. Голодом [12] в 1964 году. После чего была построена целая серия примеров бесконечных групп из которых отметим результат С.В. Алешина, полученный на основе автоматных преобразований [4].

В 1950 году в работе В. Магнуса [37] была сформулирована еще одна проблема, известная как *"ослабленная проблема Бернсайда"*. В ней требовалось выяснить, существует ли максимальная конечная периодическая группа $B_0(m,n)$ с данным числом порождающих m и фиксированным периодом n. Связь ослабленной проблемы с основной проблемой Бернсайда сводится к тому, что если бы не существовало бесконечных периодических групп, то группа $B(m,n)$ и была бы максимальной конечной периодической группой при этих m и n [3]. Первый результат по этой проблеме был получен в 1955 г. А.И. Кострикиным было установлено существование группы $B_0(2,5)$ [20]. Затем $B_0(m,5)$ — в 1956 г. [21,111], и $B_0(m,p)$ — в 1958 г. [22]. Окончательное положительное решение ослабленной проблемы Бернсайда для любых m и n было получено Е.И. Зельмановым [17].

Компьютерный эксперимент в рамках бернсайдовой проблематике внушителен. Большинство работ в этом направлении используют комбинаторно-перечислительные методы в коммутаторном исчислении, базирующиеся на конструкциях алгебры Ли [80]. Исчерпывающий библиографический список можно найти в монографиях [112, 126, 129]. Выделим некоторые результаты. Например, в [109], используя результат А.И. Кострикина из [20] о том, что $5^{31} \leq |B_0(2,5)| \leq 5^{34}$, было получено $|B_0(2,5)| = 5^{34}$. В [121] было показно, что $|B_0(2,7)| = 7^{20416}$. Доказательство этого результата заняло около одного года непрерывного машинного счета. Среди отечественных исследователей особо стоит отметить работы А.И. Скопина и его учеников [18, 55, 63–66, 81–93], внесшие значительный вклад в развитие ВТГ.

Однако, как было сказано, вопрос о конечности бернсайдовых групп для показателей 5, 7, 8 и т. д. до сих пор не решен. Наибольший интерес представляет двупорожденная группа периода 5 (группа $B(2,5)$), поскольку это группа имеет наименьший показатель и наименьшее число порождающих в сравнении с другими бернсайдовыми группами, конечность которых не определена. Кроме этого, достаточно хорошо изучена структура группы $B_0(2,5)$, и если $B(2,5)$ конечна, то $B(2,5) \simeq B_0(2,5)$. Особую интригу придает тот факт, что при показателях $n = 4$ и $n = 6$ бернсайдовы группы конечны. В связи с чем, представляется актуальным создание новых методов, алгоритмов и программ для решения проблем бернсайдового типа.

При неоспоримых преимуществах применения ЭВМ для исследования сложных систем у этого метода имеются и свои недостатки [73,104]. Как было сказано, совершенствование вычислительной техники привело к тому, что она начала использоваться при доказательстве теорем.

Правомерно ли систематическое проведение доказательств, осуществляемых с помощью компьютера? С точки зрения математической традиции подобные доказательства неправомерны, поскольку процедура проверки корректности доказательства в данном случае весьма затруднительна.

Поэтому, одной из актуальных задач системного анализа, становится разработка инструментария для обеспечения надежности и достоверности компьютерных доказательств.

Монография состоит из введения, пяти глав основного текста, заключения, списка литературы и приложений. Материалы исследования опубликованы в [24–51].

В **первой главе** определены новые методологические концепции моделирования дискретных алгебраических систем на основе которых в последующих главах конструируется комплекс алгоритмов для исследования систем указанного вида.

Во **второй главе** настоящей работы строится комплекс алгоритмов для вычисления элементов и соотношений в бернсайдовых группах, а также определения структуры указанных групп.

В **третьей главе** конструируется комплекс алгоритмов для вычисления элементов и соотношений в произвольных конечнопорожденных периодических группах, заданных порождающими элементами и определяющими соотношениями, а также определения структуры указанных групп.

В **главе 4** приведены результаты компьютерного моделирования группы $B(2,5)$. Затем сделан сравнительный анализ указанной группы с универсальной конечной бернсайдовой группой $B_0(2,5)$.

В **пятой главе** на основе компьютерного моделирования решается вопрос 16.57 из "Коуровской тетради" [67] о распознаваемости по спектру проективной специальной линейной группы размерности 2 над полем $GF(7)$ — группы $L_2(7)$.

В **заключении** монографиии приведены основные результаты и выводы, полученные по результатам компьютерного моделирования дискретных алгебраических систем.

В **приложениях** приводятся результаты компьютерных расчетов в бернсайдовых групп $B(2,4)$ и $B(3,3)$, частичный список соотношений группы $B(2,5)$, а также список элементов специального вида группы $B_0(2,5)$.

Авторы сердечно благодарят А.К. Шлёпкина за всестороннюю поддержку, полученную во время написания работы. Также авторы благодарны всем студентам, аспирантам и профессиональным программистам, в частности, С.А. Тарасову, Ю.С. Тарасову и Е.В. Грачеву, которые провели экспертизу результатов, полученных при помощи ЭВМ.

Глава 1

Методологические концепции моделирования дискретных алгебраических систем

В настоящей главе определены новые методологические концепции моделирования дискретных алгебраических систем на основе которых в последующих главах конструируется комплекс алгоритмов для исследования систем указанного вида.

1.1. Представление дискретной алгебраической системы в виде динамической системы специальных объектов

Пусть задано конечное множество $X = \{x_1, x_2, \ldots, x_m\}$, которое назовем *алфавитом*. Определим

$$G = \langle X, \cdot \rangle \tag{1.1}$$

— некоторая дискретная алгебраическая система, состоящая из множества элементов, порожденных $\{x_1, x_2, \ldots, x_m\}$, с одной бинарной операцией "$\cdot$". Системы такого вида называют *группоидами*.

Будем представлять систему вида (1.1) следующим образом:

$$G = \lim_{s \to \infty} K_s,$$

где $K_s = (P_s, T_s, A_s, C_s)$ — динамическая система специальных объектов, состоящая из последовательности слов (минимальных или независимых - см. ниже) P_s, не превышающих по длине s; таблицы умножения T_s, построенной из последовательности слов P_s; алгоритма поиска соотношений A_s в таблице T_s, основанного на групповой аксиоматике; списка соотношений C_s, получаемого при помощи A_s. Понятие "предела" в данном случае специфично, однако хорошо согласуется с классическим определением предела последовательности (см. главу 2). Указанное представление явилось базисом для построения комплекса алгоритмов моделирования дискретных алгебраических систем (главы 2, 3).

1.2. Концепция минимальных слов

На множестве порождающих системы вида (1.1) введем отношение порядка "$\prec$" (меньше): $\{x_1 \prec x_2 \prec \ldots \prec x_m\}$. Пусть g элемент из G. Тогда его можно представить в виде конечного произведения из свободных порождающих, т. е. $g = \alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_s$, где $\alpha_i \in X$, правую часть данного равенства мы будем называть словом и записывать $v = \alpha_1\alpha_2 \ldots \alpha_s$. В некоторых случаях, если необходимо подчеркнуть связь между элементом g и представляющим его словом v (т. е. записью элемента g через образующие), мы будем писать $g_v = \alpha_1 \cdot \alpha_2 \ldots \cdot \alpha_s$. Натуральное число s будем называть длиной слова v. Функция $L(v)$ определена на множестве всех слов и равна длине слова v, т.е. $L(v) = s$ для слова v, указанного выше. Единица группоида (если таковая в нем имеется) — e будет представлена пустым словом, которое мы также будем обозначать e. По определению длина пустого слова равна 0. Говорят, что слово x входит в слово w, если можно указать такие слова p и q, что $w = pxq$. Если при этом слово p (слово q) пусто, то говорят, что x есть начало (конец) слова w. Слово вида $w = \underbrace{xx...x}_{n}$ будем называть n-периодическим. Слово w будем называть n-апериодическим, если в него не входит никакое непустое слово вида x^n, т.е. $w \neq p\underbrace{xx...x}_{n}q$.

Определение отношения порядка на множестве слов. Будем говорить, что слово w меньше слова v и записывать это как $w \prec v$, если имеет место одно из следующих утверждений:

1. $L(w) < L(v)$.
2. Если $L(w) = L(v)$, тогда пусть $w = \alpha_1\alpha_2\ldots\alpha_s$ и $v = \beta_1\beta_2\ldots\beta_s$, $\alpha_1 = \beta_1$, $\alpha_2 = \beta_2$, ..., $\alpha_{k-1} = \beta_{k-1}$, $\alpha_k \prec \beta_k$ для некоторого $1 \leq k \leq s$.

Определение соотношения в группоиде. Пусть $v = \alpha_1\alpha_2\ldots\alpha_s$ и $w = \beta_1\beta_2\ldots\beta_r$ — два слова, представляющих один элемент $g \in G$, т. е. $g_v = \alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_s = g_w = \beta_1 \cdot \beta_2 \cdot \ldots \cdot \beta_r$. Тогда равенство

$$\alpha_1\alpha_2\ldots\alpha_s = \beta_1\beta_2\ldots\beta_r$$

мы будет называть соотношением в G.

Определение минимального слова. Слово v будем называть минимальным в G относительно введенного порядка, если для любого другого слова w, удовлетворяющего условию $g_v = g_w$, будет выполняться $v \prec w$.

Необходимость использования минимальных слов возникает в задачах сравнения двух и более объектов в тех случаях, когда применение традиционных форматов представления по ряду причин не эффективно (см. главу 4). Предложенная концепция минимальных слов позволяет создать единообразное представление рассматриваемых систем, что делает возможным их сравнение по способу вхождения минимальных слов в данные объекты.

1.3. Концепция независимых слов

Определение независимого слова. Рассмотрим некоторое подмножество слов V в алфавите X. Слово v называется независимым относительно V, если для любого $w \in V$, невозможна ситуация $w = pvq$, где p и q некоторые слова. Другими словами, v не является подсловом никакого слова w из V. Если, к тому же само слово $v \in V$, то говорят, что v независимо в V.

Представление элементов дискретных алгебраических систем в виде независимых слов позволяет существенно снизить вычислительную сложность алгоритмов при компьютерном моделировании систем указанного вида, а также значительно уменьшить объем используемой оперативной памяти ЭВМ. Это связано с тем, что число независимых слов в рассматриваемом математическом объекте на несколько порядков меньше общего числа элементов, в то же время множество независимых слов содержит в себе полную информацию о всех элементах системы.