

УДК 518.5+513.6

О сложности решения параметрических полиномиальных систем уравнений. А. Аяд. — В кн.: Теория представлений, динамические системы, комбинаторные методы. XIX. (Зап. научн. семин. ПОМИ, т. 387), СПб., 2011, с. 5–52.

В работе представлены три алгоритма: первый алгоритм находит решения нульмерных параметрических однородных систем за экспоненциальное время от количества неизвестных  $n$ . Второй алгоритм факторизует параметрические полиномы от нескольких переменных за экспоненциальное время от  $n$  и верхней оценки степеней факторизуемых полиномов  $d$ . Третий алгоритм разлагает алгебраическое многообразие положительной размерности, определенное параметрической системой полиномиальных уравнений, на неприводимые для всех значений параметров компоненты. Оценка сложности этого алгоритма двойная экспонента от  $n$ . С другой стороны, теоретической нижней оценкой задачи разрешения параметрической полиномиальной системы уравнений также является двойная экспонента от  $n$ . Библ. — 71 назв.

УДК 512.54

Йога коммутаторов. Вавилов Н. А., Степанов А. В., Хазрат Р., Чжанг Дзунхонг. — В кн.: Теория представлений, динамические системы, комбинаторные методы. XIX. (Зап. научн. семин. ПОМИ, т. 387), СПб., 2011, с. 53–82.

В настоящей статье мы обсуждаем несколько новых вариантов локализационных методов для вычислений в группах точек алгебраических и близких к ним групп. В первую очередь, это относительная локализация, универсальная локализация и метод локализации-пополнения. Кроме описания общей стратегии, мы формулируем некоторые типичные результаты conjugation calculus и commutator calculus. Кроме того, мы формулируем несколько недавних результатов, относительные коммутационные формулы, ограниченность длины коммутаторов в элементарных образующих, нильпотентная фильтрация конгруэнц-подгрупп, полученных с помощью этих методов. В целом это показывает, что локализационные методы могут быть значительно эффективнее, чем раньше считалось. Библ. — 74 назв.

## УДК 512.62

Перестановочные двучлены и группы, порожденные ими. Васильев Н. Н., Рыбалкин М. А. — В кн.: Теория представлений, динамические системы, комбинаторные методы. XIX. (Зап. научн. семин. ПОМИ, т. 387), СПб., 2011, с. 83–101.

Работа посвящена изучению свойств перестановочных двучленов над конечными полями и исследованию возможности применения двучленов в качестве функции шифрования. Для экспериментального исследования перестановочных двучленов в работе представлен алгоритм перечисления таких двучленов. Данный алгоритм позволил перечислить все перестановочные двучлены для порядков конечных полей до 15000. На основе полученных данных были исследованы порядки групп, порожденные перестановочными двучленами, и было обнаружено, что в некоторых конечных полях  $\mathbb{F}_q$  любая биекция на отрезке  $[1..q - 1]$  может быть представлена в виде композиции перестановочных двучленов. В работе также был исследован вопрос о возможности построения перестановочных двучленов для произвольных больших конечных полей, и была продемонстрирована ненадежность прямого обобщения криптографического протокола RSA, используя в качестве функции шифрования не одночлены, а двучлены. Библ. — 9 назв.

## УДК 517.986

Инварианты Казимира и скаляры группы  $SU(2) \otimes SU(3)$  для смешанного состояния системы кубит-кутрит. Гердт В., Младенов Д., Палий Ю., Хведелидзе А. — В кн.: Теория представлений, динамические системы, комбинаторные методы. XIX. (Зап. научн. семин. ПОМИ, т. 387), СПб., 2011, с. 102–121.

В данной работе предприняты первые шаги на пути описания квантовой двухчастичной системы, состоящей из двух- и трехуровневой подсистем — пары кубит-кутрит. Для систем кубит-кубит и кубит-кутрит приведены вычисления функции Молина и коэффициентов ряда Пуанкаре кольца локальных унитарных инвариантов, дано их сравнение с известными результатами. Требование положительной определенности матрицы плотности системы кубит-кутрит сформулировано в виде системы полиномиальных неравенств, содержащих пять элементов Казимира обертывающей алгебры  $\mathfrak{su}(6)$ . Библ. — 26 назв.

УДК 514.84+517.987

Конечные квантовые модели: конструктивный подход к описанию квантового поведения. Корняк В. В. — В кн.: Теория представлений, динамические системы, комбинаторные методы. XIX. (Зап. научн. семин. ПОМИ, т. 387), СПб., 2011, с. 122–144.

Универсальность квантовой механики – её применимость к физическим системам совершенно различной природы и масштабов – указывает на то, что квантовое поведение может быть проявлением общематематических свойств систем, содержащих неразличимые, т. е. лежащие на одной и той же орбите некоторой группы симметрий, элементы. В этой статье мы показываем, что квантовое поведение возникает естественным образом в системах с конечным числом элементов связанных нетривиальными группами симметрий. “Конечный” подход позволяет увидеть особенности квантового описания более отчетливо и без необходимости в концепциях типа “коллапс волновой функции”, “параллельные вселенные Эверетта” и т. п. В частности, в предположении конечности любая квантовая динамика сводится к простой перестановочной динамике. Преимуществом конечных квантовых моделей является возможность их конструктивного изучения методами компьютерной алгебры и вычислительной теории групп. Библ. – 12 назв.

УДК 519.63+517.951

Корректные и самоспряженные задачи для биквадратичных операторов. Парасидис И. Н., Цекрекос П. С., Локкас Т. Г. — В кн.: Теория представлений, динамические системы, комбинаторные методы. XIX. (Зап. научн. семин. ПОМИ, т. 387), СПб., 2011, с. 145–162.

В работе представлен простой метод проверки корректности и самопряженности операторов, представленных в виде  $B^4$ , соответствующих некоторым краевым задачам. Дается представление для единственных решений таких задач. Алгоритм легко реализуется в системах компьютерной алгебры. В примерах использовались системы Derive и Mathematica. Библ. – 13 назв.

УДК 511.3

Вычисления значений  $L$ -функций и полиномы Чебышева. Проскурин Н. В. — В кн.: Теория представлений, динамические системы, комбинаторные методы. XIX. (Зап. научн. семин. ПОМИ, т. 387), СПб., 2011, с. 163–166.

В работе предложен метод вычисления значений  $L$ -функций с использованием полиномов Чебышева и чебышевского метода экономизации. Библ. – 3 назв.

УДК 518.5+513.6

Эффективная конструкция неособого в коразмерности один алгебраического многообразия над полем нулевой характеристики. Чистов А. Л. — В кн.: Теория представлений, динамические системы, комбинаторные методы. XIX. (Зап. научн. семина. ПОМИ, т. 387), СПб., 2011, с. 167–188.

Пусть  $k$  – поле нулевой характеристики, конечно порождённое над полем рациональных чисел. Пусть  $f$  – полином степени самое большее  $d$  от  $n$  переменных с коэффициентами из поля  $k$  и неприводимый над алгебраическим замыканием  $\bar{k}$ . Тогда мы строим неособое в коразмерности один алгебраическое многообразие  $V$  и конечный бирациональный изоморфизм  $V \rightarrow \mathcal{Z}(f)$ , где  $\mathcal{Z}(f)$  является гиперповерхностью всех общих нулей многочлена  $f$  в аффинном пространстве. Время работы алгоритма для построения  $V$  полиномиально от длины записи входных данных. Библ. – 8 назв.