Рефераты

УДК 510.52, 512.622

Оценка сложности абсолютной факторизации параметрических многочленов. Айяд А. — В кн.: Теория сложности вычислений. IX. (Зап. научн. семин. ПОМИ, т. 316), СПб., 2004, с. 5–29.

Построен алгоритм для абсолютной факторизации многочленов с алгебраически независимыми параметрическими коэффициентами. Он разбивает пространство параметров на попарно непересекающиеся конструктивные множества, так что абсолютная факторизация многочленов с коэффициентами в каждом множестве задается равномерно. Именно, для каждого множества имеется некоторое число $l \leq d$, l переменных $C_1, \dots, C_l$, алгебраически независимых над основным полем F, и рациональные функции $b_{J,j}$ от параметров и от переменных $C_1, \dots, C_l$, такие что для всякого параметрического многочлена f с коэффициентами в данном множестве существуют значения $c_1, \dots, c_l \in \overline{F}$, для которых разложение $f = \prod_j G_j$, где $G_j = \sum_{|J|} B_{J,j} Z^J$, абсолютно неприводимо. При этом $Z = (Z_0, \dots, Z_n)$ являются переменными многочлена f, каждое из $B_{J,j}$ является значением функции $b_{J,j}$ от коэффициентов многочлена f и от $c_1, \dots, c_l$. Поле $\overline{F}$ обозначает алгебраическое замыкание поля F.

Количество построенных множеств не превосходит $(2d^2 + 1)^{2n+3d+5}$; кроме того, число арифметических операций в F, выполняемых алгоритмом, является экспоненциальным от числа коэффициентов $r = \binom{n+1+d}{n+1}$ многочлена f и оценивается как $d^{O(ndr^2)}$. Битовая сложность алгоритма в случае основного поля $F = \mathbb{Q}$ не превосходит $d^{O(ndr^2)}$, а в случае $F = \mathbb{F}_p$ не превосходит $\left(pd^{ndr^2}\right)^{O(1)}$, где d — верхняя оценка степени многочлена f.

Алгоритм использует лемму Гензеля и элиминацию кванторов в теории алгебраически замкнутых полей. Библ. – 20 назв.

УДК 519.12, 510.52

Некоторые свойства независимых относительно минимума семейств и групп перестановок. Баргачев В. — В кн.: Теория сложности вычислений. IX. (Зап. научн. семин. ПОМИ, т. 316), СПб., 2004, с. 30–41.

Семейство перестановок $\mathcal{F} \subseteq S_n$ называется независимым по k относительно минимума (сокращенно k-НОМ), если для любого непустого $X \subseteq [n]$, такого что $|X| \leq k$, и для любого $x \in X$ при случайном выборе перестановки $\pi \in \mathcal{F}$ равенство $\pi(x) = \min \pi(X)$ выполняется с вероятностью $1/|X|$. Во втором параграфе исследуется связь между независимостью относительно минимума и независимостью относительно l-го минимума. В третьем параграфе мы приводим конструкцию, позволяющую получить $(k+1)$-НОМ семейства из k-НОМ семейств для любого нечетного k. Как следствие, мы улучшаем известную верхнюю оценку на минимальный размер 4-НОМ семейств. В последнем параграфе исследуются независимые относительно минимума группы перестановок. Библ. – 12 назв.

УДК 510.52, 512.7

Вычисление размерности полуалгебраического множества. Басу С., Поллак Р., Руа М.-Ф. — В кн.: Теория сложности вычислений. IX. (Зап. научн. семин. ПОМИ, т. 316), СПб., 2004, с. 42–54.

Рассматривается задача вычисления вещественной размерности заданного полуалгебраического подмножества R^k, где R – вещественно-замкнутое поле. Доказано, что размерность k' полуалгебраического множества, заданного s многочленами степени d от k переменных, может быть вычислена за время

$$\begin{cases} s^{(k-k')k'} d^{O(k'(k-k'))} & \text{если } k' \geqslant k/2 \\ s^{(k-k'+1)(k'+1)} d^{O(k'(k-k'))} & \text{если } k' < k/2. \end{cases}$$

Этот результат слегка улучшает результат Воробьева (1999), который описал алгоритм сложности $(sd)^{O(k'(k-k'))}$ для той же задачи. Оценка на сложность алгоритма данной статьи улучшает зависимость от количества s многочленов во входе. Библ. – 22 назв.

УДК 519.177.1

О вершинной связности отношения ассоциативной схемы. Евдокимов С. А., Пономаренко И. Н. — В кн.: Теория сложности вычислений. IX. (Зап. научн. семин. ПОМИ, т. 316), СПб., 2004, с. 55–62.

Доказано, что для достаточно замкнутой ассоциативной схемы справедлива гипотеза Брауэра о совпадении вершинной связности и степени любого ее связного базисного отношения. Библ. – 7 назв.

УДК 510.635, 530.1

О применении теории сложности в фундаментальной физике. Крейнович В., Финкельштейн А. М. — В кн.: Теория сложности вычислений. IX. (Зап. научн. семин. ПОМИ, т. 316), СПб., 2004, с. 63–110.

В одной из ранних работ Д.Григорьев исследовал разрешимость и вычислительную сложность различных физических теорий в надежде, что это может быть полезно физикам. В данной статье мы делаем обзор нескольких похожих идей, которые могут быть полезны физикам, в надежде, что дальнейшие исследования могут привести к полезным физическим приложениям. Библ. – 41 назв.

УДК 510.52, 519.16, 510.633

Автоматические доказательства верхних оценок на время работы алгоритмов расщепления. Куликов А. С., Федин С. С. — В кн.: Теория сложности вычислений. IX. (Зап. научн. семин. ПОМИ, т. 316), СПб., 2004, с. 111–128.

Метод расщепления является одним из наиболее хорошо изученных подходов к решению различных NP-трудных задач. Основная идея данного метода заключается в расщеплении входного примера задачи на несколько более простых примеров (упрощаемых в дальнейшем некоторыми правилами упрощения), таких что, построив решение для каждого из них, возможно за полиномиальное время построить решение для исходного примера. Написано большое количество статей, описывающих алгоритмы этого типа, и, как правило, большая часть такой статьи посвящена разбору случаев. В данной статье мы представляем программу, которая, получив на вход множество правил упрощения, автоматически порождает доказательство верхней оценки на время работы алгоритма расщепления, использующего эти правила. В качестве примера мы приводим результаты экспериментов такой программы на задачах SAT, MAXSAT и $(n, 3)$-MAXSAT (задача MAXSAT для случая, когда каждая переменная появляется во входной формуле не более трех раз.) Библ. – 13 назв.

УДК 510.531, 510.642

Интуиционистские системы Фреге полиномиально эквивалентны. Минц Г., Кожевников А. — В кн.: Теория сложности вычислений. IX. (Зап. научн. семин. ПОМИ, т. 316), СПб., 2004, с. 129–146.

В работе (Cook, Reckhow, 1979) было доказано, что две произвольные классические системы Фреге полиномиально моделируют друг друга. Аналогичное доказательство не проходит в случае интуиционистских систем Фреге, так как последние могут содержать невыводимые допустимые правила вывода. Правило вывода A/B называется *выводимым* в некоторой системе доказательств S, если формула $A \to B$ выводима в S. Правило A/B называется *допустимым* в S, если для всех подстановок σ из выводимости формулы $\sigma(A)$ следует выводимость формулы $\sigma(B)$. В данной работе мы показываем, как устранить все применения допустимых правил, увеличивая сложность исходного доказательства не более чем полиномиально. Следовательно, две произвольные интуиционистские системы Фреге полиномиально эквивалентны. Библ. – 20 назв.

УДК 510.635, 510.57

Новый разрешимый хорновский фрагмент исчисления предикатов. Оревков В. П. — В кн.: Теория сложности вычислений. IX. (Зап. научн. семин. ПОМИ, т. 316), СПб., 2004, с. 147–162.

В работе описано расширение хорновского варианта класса формул $\forall\exists$. Для секвенций из этого класса доказана разрешимость проблемы выводимости в исчислении предикатов. Найдены сложностные характеристики, фиксация которых разбивает это расширение на полиномиально разрешимые подклассы. Фиксация максимальной размерности предикатов разбивает рассматриваемое расширение на подклассы, принадлежащие NP. Библ. – 11 назв.

УДК 510.52, 512.643.2

О теоретическом и практическом ускорении вероятностного вычисления определителя целочисленной матрицы. Пан В. Я. — В кн.: Теория сложности вычислений. IX. (Зап. научн. семин. ПОМИ, т. 316), СПб., 2004, с. 163–187.

Рассматривается алгоритм Видеманна–Копперсмита–Калтофена–Вилларда для вероятностного вычисления определителя целочисленной матрицы. Существенно упрощена и ускорена его критическая по времени компонента, где вычисляется минимальный многочлен, порождающий матрицу. Таким образом, алгоритм становится более подходящим для практики, оставаясь асимптотически быстрым. Библ. – 58 назв.

УДК 510.52

Нижние оценки для схем и линейные коды. Р. Патури, П. Пудлак — В кн.: Теория сложности вычислений. IX. (Зап. научн. семин. ПОМИ, т. 316), СПб., 2004, с. 188–204.

В 1977 году Вэлиант предложил использующий теорию графов метод доказательства нижних оценок для алгебраических схем с гейтами, вычисляющими линейные функции. Он использовал этот метод лоя сведения задачи доказательства нижних оценок для таких схем к доказательству нижних оценок на жесткость матрицы, понятие о которой он ввел в своей статье. Наилучшая нижняя оценка для матрицы, заданной в явном виде, принадлежит Дж. Фридману (1993), который доказал нижнюю оценку для матриц, порождающих коды, исправляющие ошибки, над конечным полем. Он показал, что это доказательство может быть интерпретировано как оценка некоторого параметра, определенного для всех конечномерных линейных пространств. В этой заметке мы определяем другой параметр, который может быть использован для доказательства нижних оценок на схемы с линейными гейтами. Наш параметр может быть больше параметра Фридмана и, по-видимому, несравним с жесткостью. Таким образом, доказать нижние оценки при помощи этого понятия может оказаться проще. Библ. – 14 назв.

УДК 510.52, 519.16

О рациональных языках бесконечных вещественных трасс максимальной топологической сложности. Финкель О., Рессейр Ж.-П., Симоне П. — В кн.: Теория сложности вычислений. IX. (Зап. научн. семин. ПОМИ, т. 316), СПб., 2004, с. 205–223.

Рассматривается множество $\mathbb{R}^\omega(\Gamma, D)$ бесконечных вещественных трасс над алфавитом зависимостей (Γ, D) без изолированного символа, снабженное топологией, индуцированной префиксной метрикой. Доказывается, что все рациональные языки бесконечных вещественных трасс являются аналитическими множествами. Приводится новое доказательство того, что существуют рациональные языки бесконечных вещественных трасс, являющиеся аналитическими, но не борелевскими множествами, причем $\mathbf{\Sigma}^1_1$-полными, т.е. максимальной возможной топологической сложности. Для этого приводится $\mathbf{\Sigma}^1_1$-полный язык, фундаментально отличающийся от известного примера $\mathbf{\Sigma}^1_1$-полного бесконечного вещественного рационального отношения, данного в (Finkel, 2003). Библ. – 35 назв.