УДК 510.531; 519.174

Системы пар q-удаленных представителей и раскраски графов. Головач П. А. – В кн.: Теория сложности вычислений. VII. (Зап. научн. семин. ПОМИ, т. 293), СПб., 2002, с. 5–25.

В работе доказывается NP-полнота серии задач о раскрасках графов, связанных с задачей назначения радиочастот. Для этого вводятся в рассмотрение задачи о системах q-удаленных представителей (родственные задаче о трансверсали семейства множеств, но, в отличие от нее, NP-полные при $q \geq 2$), оказавшиеся удобными для доказательств NP-полноты задач о раскрасках. Библ. – 11 назв.

УДК 512.510

Криптография с открытым ключом и теория инвариантов. Григорьев Д. Ю. – В кн.: Теория сложности вычислений. VII. (Зап. научн. семин. ПОМИ, т. 293), СПб., 2002, с. 26–38.

Описываются публичные криптосистемы, основанные на теории инвариантов групп. Проводится также обзор известных криптосистем, использующих группы. Библ. – 33 назв.

УДК 512.510

О неабелевых гомоморфных криптосистемах с открытым ключом. Григорьев Д. Ю., Пономаренко И. Н. – В кн.: Теория сложности вычислений. VII. (Зап. научн. семин. ПОМИ, т. 293), СПб., 2002, с. 39–58.

Важной проблемой современной криптографии является возможность реализации секретных вычислений с открытым ключом в алгебраических структурах. Мы строим гомоморфные криптосистемы с открытым ключом, которые представляют собой (секретные) эпиморфизмы $f : G \to H$, где G, H – (публично) известные группы, причём группа H – конечна. Буквой кодируемого сообщения является некоторый элемент $h \in H$, а его кодом является любой элемент $g \in G$, для которого $f(g) = h$. Гомоморфная криптосистема позволяет выполнять вычисления в группе G с закодированной информацией, не зная исходного сообщения в группе H.

В настоящей статье впервые построены гомоморфные криптосистемы над неабелевыми группами H (ранее, гомоморфные криптосистемы были известны лишь для абелевых групп H). Более того, мы строим гомоморфные криптосистемы для всякой неединичной фиксированной разрешимой группы H. Библ. – 23 назв.

УДК 519.177.1; 519.177.3

Блоки в k-связных графах. Карпов Д. В. – В кн.: Теория сложности вычислений. VII. (Зап. научн. семин. ПОМИ, т. 293), СПб., 2002, с. 59–93.

Для k-связного графа через локальную связность вершин определяется понятие блока. Доказывается ряд свойств блоков, обобщающих свойства классических двусвязных блоков связного графа. Кроме того, исследуется структура разбиения графа несколькими разделяющими множествами. Библ. – 9 назв.

УДК 510.662

Метод подъема решений для работы с метапеременными в системе TH∃OREM∀. Конев Б. Ю., Жебелеан Т. – В кн.: Теория сложности вычислений. VII. (Зап. научн. семин. ПОМИ, т. 293), СПб., 2002, с. 94–117.

Данная работа посвящена применению метода метапеременных для поиска доказательств в исчислениях секвенциального вида. Описывается эффективный способ работы с метапеременными и его реализация в системе TH∃OREM∀. В основе метода лежит специальная техника работы с метапеременными для случая, когда алгоритм поиска доказательств представляется в виде AND/OR-дерева. Реализация метода не зависит от стратегии поиска и легко интегрируется с другими специализированными методами поиска доказательств, а также со специальными процедурами унификации и поиска решений. Мы демонстрируем работу метода в контексте специализированной стратегии поиска, применяемой для задач элементарного математического анализа. Библ. – 28 назв.

УДК 510.52

Верхняя оценка $O(2^{0.16254n})$ для X3SAT: более простое доказательство. Куликов А. С. – В кн.: Теория сложности вычислений. VII. (Зап. научн. семин. ПОМИ, т. 293), СПб., 2002, с. 118–128.

Задача точной 3-выполнимости (X3SAT) заключается в нахождении для булевой формулы в 3-КНФ набора истинностных значений, выполняющего ровно по одному литералу в каждом клозе. Хорошо известно, что задача X3SAT является NP-полной. В данной работе мы приводим алгоритм, решающий задачу X3SAT за время $O(2^{0.162536n})$, где n – количество переменных. Приводимое нами доказательство этой оценки несколько проще доказательства Поршена, Рандерата и Шпекенмейера. Эти доказательства независимы (а алгоритмы слегка отличаются), хотя и основаны на одних и тех же идеях из доказательства предыдущей оценки $O(2^{0.186916n})$ тех же авторов. Библ. – 6 назв.

УДК 519.178; 510.52

Решение задачи о максимальном сечении за время $2^{|E|/4}$. Куликов А. С., Федин С. С.– В кн.: Теория сложности вычислений. VII. (Зап. научн. семин. ПОМИ, т. 293), СПб., 2002, с. 129–138.

В данной работе мы приводим детерминированный алгоритм, находящий максимальное сечение в графе за время $\mathrm{poly}(|E|) \cdot 2^{|E|/4}$, где $|E|$ – количество ребер (между двумя вершинами могут быть кратные ребра). Эта оценка улучшает предыдущую известную оценку $\mathrm{poly}(|E|) \cdot 2^{|E|/3}$ Грамма и др. (2000). Библ. – 8 назв.

УДК 510.52; 510.633

Трудные выполнимые формулы для DPLL-подобных алгоритмов. Николенко С. И. – В кн.: Теория сложности вычислений. VII. (Зап. научн. семин. ПОМИ, т. 293), СПб., 2002, с. 139–148.

Данная статья касается нижних оценок времени работы алгоритмов, решающих задачу пропозициональной выполнимости. Рассмотрены два DPLL-подобных алгоритма, использующих эвристики выбора единичного клоза и чистого литерала. Доказаны экспоненциальные нижние оценки на время работы этих алгоритмов на заведомо *выполнимых* формулах. Библ. – 11 назв.

УДК 510.643

Обратимое инфинитарное исчисление без циклических правил для ограниченной FTL. Плюшкявичус Р. – В кн.: Теория сложности вычислений. VII. (Зап. научн. семин. ПОМИ, т. 293), СПб., 2002, с. 149–180.

В статье рассматривается фрагмент линейной временной логики первого порядка с операторами "следующий" и "всегда". Объектами рассмотрения в этом фрагменте являются секвенции специального вида – t-D-секвенции. Для t-D-секвенций построено обратимое секвенциальное исчисление G_ω^+, не содержащее циклических правил, т.е. посылки правил этого исчисления не содержат дублирования главной формулы рассматриваемого правила. Исчисление G_ω^+ содержит только два правила: ω-правило для оператора "всегда" и интегрированное правило отделения (IS). Это правило включает традиционное антецедентное (циклического типа) правило для оператора "всегда", специальное (нециклическое) правило $(\forall \to)$ и традиционное правило для оператора "следующий". Правило $(\to \exists)$ содержится в аксиоме исчисления G_ω^+. Доказана корректность и ω-полнота исчисления G_ω^+. Библ. – 43 назв.