УДК 519.713.4+519.172.3

Примитивные орграфы с большими экспонентами и медленно синхронизируемые автоматы. Ананичев Д. С., Волков М. В., Гусев В. В. — В кн.: Комбинаторика и теория графов. IV. (Зап. научн. семин. ПОМИ, т. 402) СПб., 2012, с. 9–39.

Мы приводим несколько бесконечных серий синхронизируемых автоматов, для каждого из которых длина кратчайшего синхронизирующего слова близка к квадрату числа состояний. Все эти автоматы тесно связаны с примитивными ориентированными графами с большими экспонентами. Библ. – 28 назв.

УДК 519.175.3

Нижние оценки количества ключей шифра Закревского. Ананичев Д. С., Дубленных Д. Д. — В кн.: Комбинаторика и теория графов. IV. (Зап. научн. семин. ПОМИ, т. 402) СПб., 2012, с. 40–44.

Рассматриваются автоматы Мили как криптографические преобразователи. Формализуется определение шифра Закревского как некоторого множества таких автоматов. Строятся нижние оценки размера ключевого пространства такого шифра. Библ. – 2 назв.

УДК 519.256

Эффективное сжатие данных с помощью прямолинейных программ. Бурмистров И. С., Козлова А. В., Курпилянский Е. Б., Хворост А. А. — В кн.: Комбинаторика и теория графов. IV. (Зап. научн. семин. ПОМИ, т. 402) СПб., 2012, с. 45–68.

Изучаются два алгоритма построения контекстно свободных грамматик, выводящих заданный текст. Первый алгоритм является модификацией известного алгоритма Риттера и строит грамматику на основе AVL-деревьев, второй алгоритм использует декартовы деревья. Описываются результаты экспериментов по сравнению эффективности этих двух алгоритмов и алгоритма Риттера на различных наборах данных и по сравнению алгоритмы построения грамматик с алгоритмами из семейства алгоритмов Лемпеля-Зива по степени сжатия. Библ. – 15 назв.

УДК 519.612

Оценки сложности алгоритма Григорьева для решения тропических линейных систем. Давыдов А. П. — В кн.: Комбинаторика и теория графов. IV. (Зап. научн. семин. ПОМИ, т. 402) СПб., 2012, с. 69–82.

Исследуется алгоритм решения целочисленных тропических линейных систем, предложенный Д. Ю. Григорьевым в 2010 году. В работе впервые получена неполиномиальная нижняя оценка на время работы этого алгоритма, а также улучшена известная верхняя оценка. Библ. – 6 назв.

УДК 519.713.4

Синхронизируемые случайные автоматы над 4-буквенным алфавитом. Закс Ю. И., Скворцов Е. С. — В кн.: Комбинаторика и теория графов. IV. (Зап. научн. семин. ПОМИ, т. 402) СПб., 2012, с. 83–90.

Изучается синхронизация случайного автомата, распределенного равномерно на множестве всех детерминированных конечных автоматов с n состояниями и m буквами. Мы показываем, что для $m = 4$ вероятность того, что случайный автомат синхронизируем, больше положительной константы. Библ. – 9 назв.

УДК 510.53

Полная односторонняя функция, основанная на свободном $\mathbb{Z}\times\mathbb{Z}$-модуле конечного ранга. Николенко С. И., Тугарёв Д. С. — В кн.: Комбинаторика и теория графов. IV. (Зап. научн. семин. ПОМИ, т. 402) СПб., 2012, с. 91–107.

Известно, что задача принадлежности подполумодулю для свободного $\mathbb{Z} \times \mathbb{Z}$-модуля конечного ранга неразрешима. Модифицируя конструкцию неразрешимости, мы строим комбинаторную полную одностороннюю функцию, основанную на свободном $\mathbb{Z} \times \mathbb{Z}$-модуле конечного ранга. Библ. – 23 назв.

УДК 512.542.7, 519.14, 510.52

Базы шуровых антисимметрических когерентных конфигураций и проверка изоморфизма шуровых турниров. Пономаренко И. Н. — В кн.: Комбинаторика и теория графов. IV. (Зап. научн. семин. ПОМИ, т. 402) СПб., 2012, с. 108–147.

Хорошо известно, что для каждой группы перестановок G нечетного порядка найдется множество точек, стабилизатор которого в G тривиален, а если эта группа примитивна, то найдется и база размера

не более 3. Эти результаты обобщаются на когерентную конфигурацию группы G (в этом случае конфигурация шурова и антисимметрическая). Это позволяет построить алгоритм полиномиальной сложности для распознавания и проверки изоморфизма шуровых турниров (т.е. раскрашенных по дугам турниров, когерентные конфигурации которых шуровы). Библ. – 24 назв.

УДК 510.58

Преобразования функций с помощью автоматов. Саллинен Т. — В кн.: Комбинаторика и теория графов. IV. (Зап. научн. семин. ПОМИ, т. 402) СПб., 2012, с. 148–169.

Используются традиционные модели вычислений для определения довольно нетрадиционных вычислительных процессов. Конкретнее, автоматы с одной лентой используются для вычисления вещественнозначных функций, а автоматы с двумя лентами – для описания преобразований этих функций. В роли таких преобразований рассматриваются интегрирование и дифференцирование функций. Библ. – 8 назв.

УДК 519.11.14

О k-абелевой избегаемости. Хуова М., Кархюмяки Ю. — В кн.: Комбинаторика и теория графов. IV. (Зап. научн. семин. ПОМИ, т. 402) СПб., 2012, с. 170–182.

Мы изучаем недавно введенное понятие *k-абелевой эквивалентности* слов, приводим его некоторые основные свойства, и концентрирумся на проблеме избегаемости. Это отношение эквивалентности считает количество подслов длины k для фиксированного натурального числа k. Мы интересуемся размером наименьшего алфавита, в котором можно избежать k-абелевых квадратов и кубов соответственно. Для 2-абелевых квадратов этот размер равен четырём – аналогично случаю *абелевых слов*, в то время как для 2-абелевых кубов мы имеем только сильное свидетельство в пользу того, что этот размер равен двум – аналогично случаю *слов*. Кроме того, мы указываем несколько свойств морфизмов, которые показывают, что было бы трудно найти ответы на наши вопросы путем простого итерирования морфизмов. Библ. – 17 назв.

УДК 519.68

Использование запросов существенности для расшифровки бесповторных функций. Чистиков Д. В. — В кн.: Комбинаторика и теория графов. IV. (Зап. научн. семин. ПОМИ, т. 402) СПб., 2012, с. 183–217.

Булева функция называется бесповторной, если ее можно выразить формулой над базисом $\{\wedge, \vee, \neg\}$, в которой каждая переменная встречается не более одного раза. Рассматривается задача расшифровки, или идентификации, неизвестной бесповторной функции f, зависящей от известного множества переменных $x_1, \ldots, x_n$, с помощью запросов. Алгоритмы могут выполнять стандартные запросы принадлежности, а также запросы двух специальных типов, выявляющие существенность переменных у подфункций f. Строятся два алгоритма точной идентификации: первый выполняет $O(n^2)$ запросов типа да/нет, второй — $O(n \log^2 n)$ запросов с ответами логарифмической длины. Мощностная нижняя оценка числа бит, передаваемых от оракулов к алгоритмам в худшем случае, составляет $\Omega(n \log n)$. Библ. – 14 назв.