Предисловие

В настоящем сборнике представлены статьи, посвященные разработке математических методов и алгоритмов для различных задач дискретной математики и теоретического программирования. Первые девять статей посвящены разработке и анализу алгоритмов в некоторых задачах дискретной математики, а последние четыре работы связаны с анализом и преобразованиями программ в целях обеспечения компьютерной безопасности.

В статье А. И. Поспелова рассмотрена задача упаковки прямоугольников в заданное число полос, тесно связанная с построением расписаний для группы кластеров. В статье предложен приближенный алгоритм и показано, что он гарантированно дает размещение, не более чем в 3 раза худшее по сравнению с оптимальным.

Статья С. Н. Жука также посвящена анализу некоторых эвристик в задаче упаковки прямоугольников в несколько полос. Предложен эффективный алгоритм, который размещает прямоугольники по полосам в онлайновом режиме и гарантирует константную мультипликативную точность. Это достигнуто за счёт правильной формализации понятии «допустимая полоса для прямоугольника». Показано, также, что полученная оценка точности достижима на некоторых исходных данных.

В статье С. А. Фомина описан новый приближенный алгоритм для задачи положительного линейного программирования, имеющий наилучшую из известных оценок быстродействия.

В статье Н. Н. Кузюрина и О.А. Прокопьева доказана алгоритмическая трудность распознавания возможности аппроксимации заданной булевой функции другой (более простой) булевой функцией.

В статье М. Н. Вялого рассматривается алгоритмическая сложность основных задач комбинаторики слов при задании слова сжатым описанием. А именно, в качестве слов, в которых ищутся вхождения подслов, рассматриваются таблицы значений булевых полиномов. Построены эффективные алгоритмы проверки вхождения слова фиксированной длины в таблицу значений полинома фиксированной степени, последовательного порождения вхождений при тех же условиях.

В статье Т. В. Андреевой доказана унимодальность частично упорядоченного множества, диаграмма Хассе которого является декартовой степенью k–звезды, т.е. дерева с $k+1$ вершинами, одна из которых имеет степень k.

В статье Н. Н. Кузюрина «Обобщенные покрытия и их аппроксимации» получены верхние и нижние оценки размеров обобщенных покрытий матриц, состоящих из 0, 1 и -1. Полученные оценки свидетельствуют о

точности по порядку метода вероятностного округления в задачах ЦЛП с $(0, \pm 1)$–матрицами ограничений.

В статье Н. Н. Кузюрина «Probabilistic analysis of the greedy algorithm» доказана асимптотическая точность жадного алгоритма в задаче о покрытии при анализе в среднем (на случайных исходных данных).

В статье Н. Н. Кузюрина, С. А. Мартишина и В. М. Храпченко рассматривается задача поиска часто встречающихся комбинаций, связанная с анализом данных (data mining). Рассмотрены некоторые теоретические аспекты, связанные с алгоритмической сложностью задачи и существованием эффективных приближенных алгоритмов. Предложен генетический алгоритм для решения этой задачи и проведено исследование его эффективности на случайных данных.

В статье Н. П. Варновского исследуется проблема определения стойкости обфускирующих преобразований программ. В статье обсуждаются требования к стойкости обфускации и устанавливается невозможность построения универсального обфускатора, удовлетворяющего требованиям стойкости, основанным на парадигме «серого ящика».

В статье К. С. Иванова и В. А. Захарова предложен новый подход к оценке качества обфускирующих преобразований, используемых на практике: обфускация считается относительно стойкой, если она способна противодействовать прикладным алгоритмам верификации и анализа программ. Построены примеры обфускирующих преобразований, соответствующих введенному критерию, и оценена их сложность.

В статье А. В. Шокурова изучается задача построения гомоморфных систем шифрования данных, позволяющих проводить вычисления над зашифрованными данными. Показано, что для одного класса алгебраических схем вычислений существует такое эффективное гомоморфное шифрование, при котором размер схемы изменяется незначительно, но извлечение исходных данных на основе наблюдаемых вычислений становится практически невозможным.

В статье И. М. Захарьящева и В. А. Захарова предложена новая модель программ, предназначенная для решения задач проверки эквивалентности программ и проведения эквивалентных преобразований. Отличительная особенность этой модели состоит в том, что построение трассы вычисления и формирование результатов вычисления проводятся на основе разных операционных семантик. Это позволяет описывать в рамках единой модели поведение программ различных типов, включая реагирующие программы. Предложен новый метод построения алгоритмов проверки эквивалентности программ в предложенной модели.

Член-корреспондент РАН В. П. Иванников