Предисловие

В настоящем сборнике представлены статьи, посвященные разработке методов синтеза и анализа алгоритмов для различных задач дискретной математики и теоретического программирования.

Статья С.Н. Жука посвящена задаче упаковки произвольного множества прямоугольников в несколько полубесконечных полос. Эта задача является обобщением нескольких известных NP-трудных задач: задачи об m-процессорном расписании, задачи об упаковке в контейнеры, задачи об упаковке прямоугольников в одну полосу. Основным результатом работы является доказательство существования алгоритма для рассматриваемой задачи, работающего в режиме on-line и гарантирующего нахождение решения, отличающегося от оптимального не более, чем в константу раз.

В статье Н.Н. Кузюрина и А.И. Поспелова рассматривается задача упаковки множества прямоугольников в вертикальную полубесконечную полосу единичной ширины. Изучен важный подкласс онлайновых алгоритмов для этой задачи – так называемые шельфовые алгоритмы. Предложен общий метод вероятностного анализа шельфовых алгоритмов, позволяющий для многих шельфовых алгоритмов оценивать математическое ожидание незаполненной площади. Получены верхние и нижние оценки математического ожидания незаполненной площади для шельфовых алгоритмов, использующих различные вспомогательные эвристики для упаковки в контейнеры.

Учебно-методическая статья Н.П. Варновского и А.В. Шокурова знакомит читателя (не претендуя на полноту обзора результатов) с важным криптографическим примитивом — гомоморфным шифрованием, представляющим интерес как с прикладной, так и с чисто математической точек зрения. В статье затронуты также и некоторые смежные вопросы. Отмечено, что несмотря на многолетние исследования в области гомоморфного шифрования, основные проблемы остаются нерешенными.

Статья В.А. Захарова и И.В. Коннова посвящена униформной проблеме верификации параметризованных систем взаимодействующих процессов. Для верификации параметризованных систем применяется метод поиска инвариантов с использованием специальных отношений порядка на множестве конечных систем переходов. Введен новый тип предпорядка — так называемая квази-блочная симуляция. В статье доказано, что квази-блочная симуляция сохраняет выполнимость формул из $ACTL^*_{-X}$, и асинхронная композиция процессов монотонна по отношению квази-блочной симуляции. Показано, каким образом можно использовать квази-блочную симуляцию для верификации параметризованных асинхронных систем процессов с синхронным обменом сообщениями.

В статье П.Е. Булычева, В.А. Захарова и И.В. Коннова исследован один из новейших методов проверки различных отношений симуляции и бисимуляции между конечными размеченными системами переходов, которые используются для моделирования и верификации систем распределенных взаимодействующих процессов. Этот метод позволяет сводить задачу проверки указанных отношений к проблеме существования выигрышных стратегий в паритетных играх, порожденных проверяемыми системами переходов. Метод паритетных игр был применен авторами для построения эффективных алгоритмов проверки простых и справедливых отношений симуляции и бисимуляции по прореживанию (stuttering simulation/bisimulation). В результате были впервые разработаны алгоритмы проверки отношения симуляции по прореживанию, которые имеют такую же сложность по времени и объему памяти, как и наилучшие алгоритмы проверки обычной симуляции конечных размеченных систем переходов. Предложенные в этой статье алгоритмы проверки симуляции могут быть использованы для верификации систем распределенных программ.

Статья В.А. Захарова, Н.Н. Кузюрина, Р.И Подловченко и В.С. Щербины посвящена проблемам обнаружения сложных компьютерных вирусов — так называемых полиморфных и метаморфных вирусов, обладающих способностью модифицировать (обфускировать) свою подпись. Показано, что задача обнаружения таких вирусов может быть сведена к проблеме проверки эквивалентности программ. Предложен подход к анализу стойкости обфускирующих преобразований на основе анализа сложности проблемы эквивалентности в алгебраических моделях программ, используемых для построения обфускирующих преобразований. Дан обзор основных результатов по сложности проблемы эквивалентности в различных алгебраических моделях программ.

В статье И.А Лаврова освещены важные аспекты классической теории алгоритмов и теории сложности вычислений. Показано, что ряд подходов к формализации понятия сложности вычислений неадекватно отражает данное понятие. Более последовательным представляется построение различных иерархий классов сложности. С помощью подобных классов удается локализовать уровни сложности ряда классических математических задач.

Чл.-корр. РАН В.П.Иванников