всех бент-функций, находящихся на минимальном расстоянии от заданной (подробнее см. [2]), а также алгоритм построения кодов, состоящих из векторов значений бент-функций, сдвиги которых на заданную бент-функцию являются линейными кодами (подробнее см. [3]).

Работа с достаточно сложными объектами (представления булевых функций и т. д.) базируется на более простых элементах, таких, как векторы, матрицы и подпространства. Реализованы также различные итераторы, позволяющие строить переборные схемы для векторов, матриц и подпространств.

Первая версия системы *Boolean Functions* будет доступна на странице Института математики им. С. Л. Соболева СО РАН `http://math.nsc.ru/~bf` .

ЛИТЕРАТУРА

1. *Meng Q., Yang M., Zhang H., and Liu Y.* Analysis of Affinely Equivalent Boolean Functions // Cryptology ePrint Archive, Report 2005/025.
2. *Коломеец Н. А., Павлов А. В.* Свойства бент-функций, находящихся на минимальном расстоянии друг от друга // Прикладная дискретная математика. 2009. № 4. С. 5–20.
3. *Павлов А. В.* Бент-функции и линейные коды в CDMA // Прикладная дискретная математика. Приложение. 2010. № 3. С. 95–97.

УДК 519.7

ПРИМЕНЕНИЕ SAT-ПОДХОДА В РЕШЕНИИ КОМБИНАТОРНЫХ ЗАДАЧ[1]

А. А. Семенов, И. В. Отпущенников, С. Е. Кочемазов

Рассмотрим использование SAT-подхода в решении различных дискретных задач «переборной» природы. Для многих относительно простых по постановкам дискретных задач не известно алгоритмов, эффективных хотя бы на некоторых практически значимых подклассах рассматриваемых задач.

Простейший пример такого рода — анализ свойств недетерминированного автомата $\tilde{A}$, распознающего некоторый регулярный язык. Может оказаться так, что диагностируемое свойство (либо его отсутствие) может быть установлено эффективно для детерминированного автомата A, который эквивалентен $\tilde{A}$. Однако процедура преобразования $\tilde{A}$ в A обычно крайне трудоемка [1]. Более того, реализация этой процедуры требует работы со структурами данных, представляющими автоматы. Другой подход к этой проблеме состоит в переходе от автомата $\tilde{A}$ к кодирующей его системе булевых уравнений $S(\tilde{A})$. Такой переход осуществляется эффективно [2]. Диагностируемое свойство автомата $\tilde{A}$ либо его отсутствие может быть установлено на основе решения системы $S(\tilde{A})$. Решение системы $S(\tilde{A})$ может быть найдено с применением современных быстрых булевых решателей (SAT-решателей, [3]).

Следующий пример такого рода — автоматные модели в современной вычислительной биологии [4]. На первый взгляд совершенно непонятно, какие вычислительные методы следует использовать для их изучения. Однако с этими моделями естественным образом связываются некоторые дискретные функции (см., например, [5]), и для выявления тех или иных свойств моделей приходится решать задачи обращения таких функций, которые также допускают эффективную сводимость к булевым уравнениям.

[1]Работа поддержана грантом РФФИ, проект № 11-07-00377-а.

Еще одна область применения SAT-подхода связана с задачами комбинаторной оптимизации. Имеются мощные коммерческие пакеты решения оптимизационных задач из семейства 0—1-целочисленного линейного программирования (ЦЛП). Соответствующие алгоритмы комбинируют технику ветвей, границ и отсечений с методами решения задач линейного программирования над полем рациональных чисел. Однако данные методы подходят далеко не ко всем задачам комбинаторной оптимизации. Современные решатели ЦЛП-задач, как правило, не работают с нелинейными и невыпуклыми целевыми функциями. Между тем и такие задачи допускают эффективную сводимость к булевым уравнениям и, в конечном счете, к SAT-задачам.

В работе приведены результаты решения задачи поиска неподвижных точек и циклов автоматных отображений в генных сетях дискретно-автоматной природы со сложными многофакторными механизмами внутреннего взаимодействия и результаты параллельного решения SAT-задач, кодирующих квадратичную задачу о назначениях, в отношении которой коммерческие решатели, основанные на методе ветвей и границ, оказываются низкоэффективными.

ЛИТЕРАТУРА

1. *Хопкрофт Дж., Мотвани Р., Ульман Дж.* Введение в теорию автоматов, языков и вычислений. М.: Вильямс, 2002.
2. *Семенов А. А., Отпущенников И. В., Кочемазов С. Е.* Пропозициональный подход в задачах тестирования дискретных автоматов // Современные технологии. Системный анализ. Моделирование. 2009. № 4. С. 48–56.
3. `http://www.satlive.org` — Up-to-date links for the SATisfability Problem.
4. Системная компьютерная биология / под ред. Н. А. Колчанова, С. С. Гончарова, В. А. Лихошвая, В. А. Иванисенко. Новосибирск: Изд-во СО РАН, 2008.
5. *Евдокимов А. А., Кочемазов С. Е., Семенов А. А.* Применение символьных вычислений к исследованию дискретных моделей некоторых классов генных сетей // Вычислительные технологии. 2011. Т. 16. № 1. С. 30–47.

УДК 519.6

О ПАРАЛЛЕЛЬНЫХ ВЫЧИСЛЕНИЯХ ПРИ РЕАЛИЗАЦИИ МЕТОДА СОГЛАСОВАНИЯ В КРИПТОАНАЛИЗЕ

В. М. Фомичев

Метод согласования [1 – 4] применяется для определения ключа криптосистемы, как правило, по известным открытому и шифрованному тексту. Он менее трудоемок по сравнению с полным опробованием ключей, если функция шифрования $E(q, x)$ открытого текста x по ключу $q \in V_n = \{0, 1\}^n$ допускает декомпозицию на две функции как $E(q, x) = g(q, g'(q, x))$, где для множеств существенных ключевых переменных K и K' соответственно функций g и g' выполнено $K \setminus K' \neq \varnothing$ и $K' \setminus K \neq \varnothing$. Наибольший эффект от применения метода достигается, если множества K и K' равномощны и $K \cap K' = \varnothing$. При этом опробование ключа выполняется как независимое опробование переменных из множеств K и K' и ключ q определяется с вычислительной сложностью порядка $\mathrm{O}(2^{n/2})$ операций типа зашифрования-расшифрования при использовании памяти, достаточной для хранения порядка $\mathrm{O}(2^{n/2})$ ключей.

Оценим среднее время параллельных вычислений и размер памяти для реализации метода согласования применительно к некоторым итеративным симметричным блоч-