

ЛИТЕРАТУРА

1. Заикин О. С., Семенов А. А. Технология крупноблочного параллелизма в SAT-задачах // Проблемы управления. 2008. № 1. С. 43–50.
2. Заикин О. С. Реализация процедур прогнозирования трудоемкости параллельного решения SAT-задач // Вестник УГАТУ. 2010. Т. 14. № 4(39). С. 210–220.
3. Посыпкин М. А., Заикин О. С., Беспалов Д. В., Семенов А. А. Решение задач криптоанализа поточных шифров в распределенных вычислительных средах // Труды ИСА РАН. 2009. Т. 46. С. 119–137.
4. <http://boinc.berkeley.edu> — Berkeley Open Infrastructure for Network Computing.
5. <http://www.desktopgrid.hu> — SZTAKI desktop grig.

УДК 519.7

**BOOLEAN FUNCTIONS — СИСТЕМА ДЛЯ РАБОТЫ
С БУЛЕВЫМИ ФУНКЦИЯМИ¹**

Н. А. Коломеец, А. В. Павлов

Предлагается новая система для работы с булевыми функциями *Boolean Functions*. Эта система ориентирована на пользователей-программистов и представляет собой библиотеку классов и функций на языке C++; она может быть полезна для проведения компьютерных экспериментов и тестов, связанных с булевыми функциями. В отличие от других систем, таких, как MAGMA, система является узконаправленной на работу с булевыми функциями специального вида. Кроме того, *Boolean Functions* бесплатна и свободно распространяема.

Для решения многих математических задач требуется подготовка экспериментальной базы и проведение компьютерных тестов. Каждый раз для новой подобной задачи приходится заново создавать все вспомогательные функции, такие, как проверка принадлежности функции какому-либо классу или перевод функции в различные представления (АНФ, таблица истинности, трейс-форма). Предлагаемая система предназначена для сокращения этих действий. На данный момент *Boolean Functions* является весьма неполной системой, хотя и содержит некоторые готовые алгоритмы; предполагается дальнейшее её развитие и выпуск новых версий.

Система позволяет работать с двоичными векторами и совершать стандартные операции над ними, такие, как определение веса Хэмминга, сложение двух векторов, вычисление их скалярного произведения, сравнение двух векторов и др.

Библиотека работает с представлениями булевой функции в виде АНФ, таблицы истинности и представлением с помощью следа (трейс-форма), а также умеет переводить одно представление в другое.

Boolean Functions позволяет проверять, являются ли две булевы функции аффинно эквивалентными (используется алгоритм [1]), а также генерировать функции, аффинно эквивалентные заданной.

Основное предназначение данной системы — работа с булевыми функциями специального вида, в частности с бент-функциями. Система позволяет проверять, является ли булева функция бент-функцией. *Boolean Functions* содержит алгоритмы генерации бент-функций от 4, 6 и 8 переменных степени не больше 3, алгоритм генерации

¹Работа выполнена при финансовой поддержке РФФИ (проект № 11-01-00997) и ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт № 02.740.11.0362).

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 ЗАДАЧ¹

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.

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