УДК 519.7;658.512

Представление булевых многочленов в виде ZDD-диаграмм

П. В. Фокин[*], **Ю. А. Блинков**[†]

[*] *ЗАО «РОСА», Москва, Россия, 123557*

[†] *Механико-математический факультет*
Саратовский государственный университет им. Н.Г. Чернышевского
ул. Астраханская, д. 83, корп. 9, Саратов, Россия, 410012

Булевы базисы Грёбнера проявили свою практическую применимость для ряда задач, таких как HFE (Hidden Field Equations) в криптографии, моделирование квантовых вычислений и к задаче «Выполнимость» для конъюнктивной нормальной формы. Алгоритмы построения базисов Грёбнера имеют экспоненциальную сложность построения как по времени выполнения, так и по требуемой памяти. Для более компактного хранения булевых многочленов было предложено использовать ZDD-диаграммы. Показана связь ZDD-диаграмм с специальным видом рекурсивным представлением многочленов, которое отождествляет ZDD-диаграмму с некоторым набором равенств. Доказана лемма дающая число вершин в ZDD-диаграмме для представления булевого многочлена, состоящего из всех мономов до степени d включительно. Представлен пакет на языке C++11 для работы с ZDD-диаграммами. В состав пакета входят собственная реализация красно-чёрных деревьев, списков и менеджера памяти. Пакет разрабатывался для использования как внутреннее представление булевых многочленов, в ней реализованы операции сложения и умножение двух многочленов, а также умножение на переменную, которое используются при построении инволютивных базисов Грёбнера.

Ключевые слова: булевы многочлены, бинарная диаграмма решений, базис Грёбнера, задача «Выполнимость».

1. Введение

Двоичные диаграммы решений (Binary Decision Diagram, BDD) [1] являются удобным инструментом представления и оперирования булевыми функциями и широко используются в различных областях, например для формальной верификации программных и аппаратных систем.

Определение 1. Двоичные диаграммы решений — это направленный ациклический граф с двумя терминальными узлами $\{0, 1\}$, которые соответствуют значениям представляемой булевой функции. Выходная степень терминальных вершин равна 0. Все остальные вершины имеют выходную степень 2 и называются узлами решений. Одна вершина имеет входную степень, равную 0, эта вершина является корнем. Рёбра, выходящие из узлов решений, соответствуют значению 0 (0-ребро, else-ребро) или 1 (1-ребро, then-ребро) для соответствующей переменной.

BDD диаграммы можно использовать для представления булевых многочленов, при этом сплошные ребра соответствуют умножению, назовём их *мультипликативными*, а пунктирные — сложению, *аддитивные* рёбра. Для примера представим в виде BDD диаграммы моном (рис. 1) и сумму переменных (рис. 2).

Последовательность узлов, начинающихся с вершины и заканчивающаяся терминальным узлом, называется путём. В случае когда порядок переменных для всех путей остаётся постоянным, такую диаграмму будем называть *упорядоченной* (Ordered BDD, OBDD).

Статья поступила в редакцию 30 декабря 2013 г.

Работа поддержана грантами РФФИ (12-07-00294-а алгебро-логический подход к исследованию задач «Выполнимость», ассоциированных с криптоанализом асимметричных шифров; 13-01-00668-а развитие методов компьютерной алгебры для моделирования перепутанности многочастичных систем, дискретных квантовых систем, а также систем со связями).

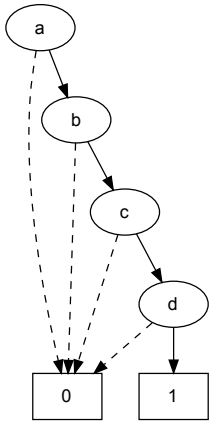

Рис. 1. $a \cdot b \cdot c \cdot d$

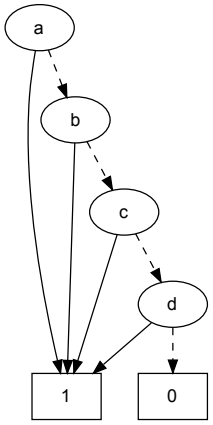

Рис. 2. $a + b + c + d$

Определение 2 (см. [2]). OBDD будет называться *двоичной диаграммой с отбрасыванием незначащих нулей* (Zero-suppressed Decision Diagram, ZDD) если она удовлетворяет следующим требованиям:

1) она не содержит одинаковых поддиаграмм,
2) из неё исключены те вершины, мультипликативные ребра которых заканчиваются в терминальной вершине соответствующей 0.

Наиболее характерные различия представленных диаграмм, на примере булевого многочлена p

$$p = abc + ab + bc + b + c + 1 \tag{1}$$

и порядком переменных $a \succ b \succ c$, показаны на рис. 3–5.

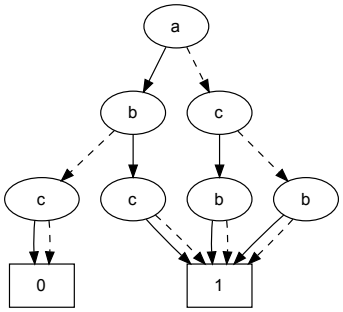

Рис. 3. BDD

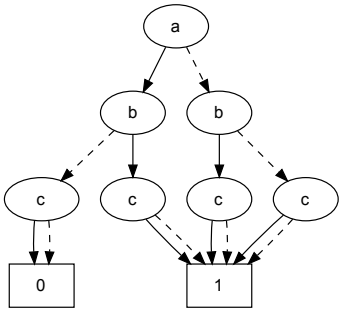

Рис. 4. OBDD

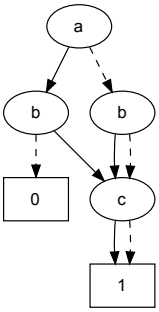

Рис. 5. ZDD

Проведём аналогию между рекурсивной записью многочленов и их графическим изображением в виде ZDD-диаграмм.

2. ZDD-диаграммы и рекурсивная форма многочленов

Представим многочлен p из (1) в полной рекурсивной форме с порядком переменных $a \succ b \succ c$

$$p = a \cdot (b \cdot (c \cdot 1 + 1) + c \cdot 0 + 0) + b \cdot (c \cdot 1 + 1) + c \cdot 1 + 1\,. \tag{2}$$

Можно заметить, что между полной рекурсивной записью (2) многочлена p и OBDD диаграммой на рис. 4 имеется взаимно однозначное соответствие, при котором вершины соответствуют операндам, а операции рёбрам. Уберём в рекурсивной форме (2) многочлена p тривиальное умножение на 0 и отождествим повторяющиеся элементы:

$$\begin{gathered} r_0 = c \cdot 1 + 1, \\ r_1 = b \cdot r_0, \\ p = a \cdot (r_1 + 0) + r_1 + r_0. \end{gathered} \tag{3}$$

Назовём форму (3) *сжатой рекурсивной формой* булевого многочлена p. Между сжатой рекурсивной формой (3) многочлена p и ZDD-диаграммой на рис. 5, также имеется взаимно однозначное соответствие, при котором вершины соответствуют операндам, а операции рёбрам. В дальнейшем для упрощения записи операцию умножения будем опускать.

3. Некоторые свойства ZDD-диаграмм

Рассмотрим следующую лемму, дающую число вершин для представления булевого многочлена, состоящего из всех мономов до степени d включительно.

Лемма 1. *Пусть $0 < d \leqslant n$, тогда ZDD-диаграмма представляющая все мономы до степени d включительно от n переменных содержит в точности $(n + 1 - d)d$ нетерминальных вершин.*

Для леммы 1, используя введённое выше понятие сжатой рекурсивной формы, можно дать следующее доказательство.

Доказательство. При $n = 1$ доказательство тривиально. Предположим выполнение леммы для $n = k$. В линейном случае при $d = 1$ доказательство также тривиально, и мы будем рассматривать случай $2 \leqslant d \leqslant k + 1$. Запишем многочлен $p^d_{x_1 \succ \ldots \succ x_{k+1}}$, состоящий из всех мономов до степени d включительно в сжатой рекурсивной форме с порядком переменных $x_1 \succ \ldots \succ x_{k+1}$

$$\ldots$$

$$p^{d-1}_{x_2 \succ \ldots \succ x_{k+1}} = x_2 p^{d-2}_{x_3 \succ \ldots \succ x_{k+1}} + p^{d-1}_{x_3 \succ \ldots \succ x_{k+1}}, \tag{4}$$

$$p^{d}_{x_2 \succ \ldots \succ x_{k+1}} = x_2 p^{d-1}_{x_3 \succ \ldots \succ x_{k+1}} + p^{d}_{x_3 \succ \ldots \succ x_{k+1}}, \tag{5}$$

$$p^{d}_{x_1 \succ \ldots \succ x_{k+1}} = x_1 p^{d-1}_{x_2 \succ \ldots \succ x_{k+1}} + p^{d}_{x_2 \succ \ldots \succ x_{k+1}}. \tag{6}$$

Первое слагаемое в правой части равенства (6) даёт число вершин $1 + (k + 1 - (d - 1))(d - 1)$, второе слагаемое $(k + 1 - d)d$, но из него нужно вычесть число повторяющихся вершин многочлена $p^{d-1}_{x_3 \succ \ldots \succ x_{k+1}}$ в правых частях равенств (4), (5). В результате имеем $1 + (k+1-(d-1))(d-1) + (k+1-d)d - (k-(d-1))(d-1) = ((k+1)+1-d)d$. □

Лемма 2 (см. [3]). *Пусть $0 < d \leqslant n$, тогда ZDD-диаграмма представляющая все d–элементные подмножества, n–элементного множества содержит в точности $(n + 1 - d)d$ нетерминальных вершин.*

Доказательство леммы 2, используя понятие сжатой рекурсивной формы, можно провести аналогично доказательству леммы 1.

На рис. 6, 7 показано различие ZDD-диаграмм для случаев лемм 1 и 2.

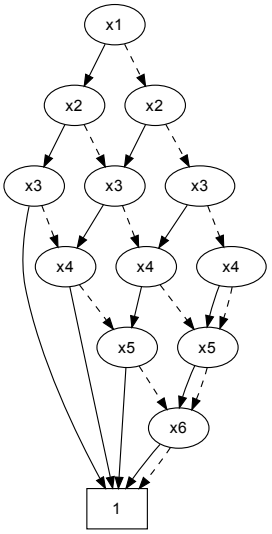

Рис. 6. ZDD-диаграмма для случая леммы 1

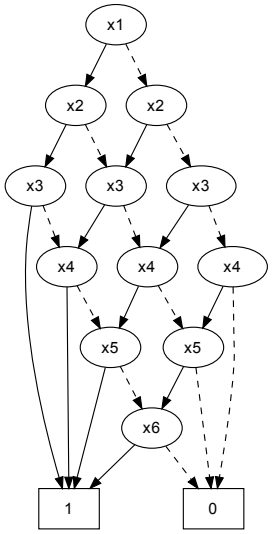

Рис. 7. ZDD-диаграмма для случая леммы 2

4. Описание пакета

Для использования ZDD-диаграмм как внутреннего представления булевых многочленов при вычисление инволютивного базиса Грёбнера, а также для исследования свойств диаграмм был реализован C++11 пакет (`https://bitbucket.org/fokinpv/ginv/wiki/Home`), с обёрткой на Cython для использования в языке программирования Python.

В состав пакета входят собственная реализации красно-чёрных деревьев, списков и менеджера памяти. Основной структурой управляющей узлами ZDD-диаграммы является кэш. В представленном пакете кэш запрограммирован в виде красно-чёрного дерева, узлами которого являются списки узлов ZDD-диаграммы с одинаковым номером переменной. Кэш может быть как общим для нескольких ZDD-диаграмм, так и локальным, с узлами из одной диаграммы.

Библиотека разрабатывалась для использования как внутреннее представление булевых многочленов, в ней реализованы операции сложения и умножение двух многочленов, а также умножение на переменную, которое используются при построении инволютивных базисов Грёбнера [4]. Также реализованы операции над множествами «объединение», «пересечение» и «разность».

Для удобства записи и исследования свойств ZDD-диаграммы реализована возможность вывода многочлена в сжатой рекурсивной форме.

5. Заключение

Введено понятие сжатой рекурсивной формы, которое отождествляет ZDD-диаграмму с некоторым набором равенств. Используя понятие сжатой рекурсивной формы, доказана лемма, дающая число вершин для представления булевого

многочлена, состоящего из всех мономов до степени d включительно. Представлен пакет на языке C++ для работы с ZDD-диаграммами.

Литература

1. *Lee C. Y.* Representation of Switching Circuits by Binary-Decision Programs // Bell Systems Technical Journal. — 1959. — Vol. 38. — Pp. 985–999.
2. *Minato S.-i.* Zero-Suppressed bdds for Set Manipulation in Combinatorial Problems // Design Automation, 1993. 30th Conference on. — 1993. — Pp. 272–277.
3. *Motter D. B., Roy J. A., Markov I. L.* Resolution Cannot Polynomially Simulate Compressed-BFS // Annals of Mathematics and Artificial Intelligence. — 2005. — Vol. 44, No 1–2. — Pp. 121–156.
4. *Gerdt V. P., Zinin M. V., Blinkov Y. A.* On Computation of Boolean Involutive Bases // Programming and Computing Software. — 2010. — Vol. 36, No 2. — Pp. 117–123.

UDC 519.7;658.512

Presentation of Boolean Polynomials as ZDD-Diagrams

P. V. Fokin[*], **Yu. A. Blinkov**[†]

[*] *ROSA Company, Moscow, Russia, 123557*

[†] *Mechanics and Mathematics Department*
Saratov State University named after N.G. Chernyshevsky
83, Astrakhanskaya str., building 9, Saratov, Russia, 410012

Boolean Gröbner basis have shown their practical efficiency for different problems. Among them are algebraic cryptanalysis HFE (Hidden Field Equations), modeling of quantum computing and boolean satisfiability problem (SAT). Algorithms for computing Gröbner basis have exponential complexity for execution time as well as for memory usage. The more appropriate data structure was introduced, which is based on zero-suppressed binary decision diagrams (ZDD). Also we show the relation between ZDD and special recursive notation of polynomials. The recursive notation is the collection of equalities which have had one-to-one correspondence with graphical presentation of ZDDs. We prove lemma which gives the number of nodes estimation for ZDD which represent boolean polynomial with all monoms up to d degree of n variables. Furthermore, we present C++11 ZDD package providing possibility for addition and multiplication of boolean polynomials, multiplication by variable, presentation in compressed recursive form and graphical presentation. The package includes its own implementation of red-black trees, lists, and memory manager. ZDD package was developed for using as internal data structure of the boolean polynomials for computation of involutive Gröbner basis.

Key words and phrases: boolean polynomials, binary decision diagram, Gröbner basis, SAT.