

Министерство образования и науки Российской Федерации
(МИНОБРНАУКИ РОССИИ)
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (ТГУ)
Институт прикладной математики и компьютерных наук
Кафедра защиты информации и криптографии

КУРСОВАЯ РАБОТА

БИБЛИОТЕКА ДЛЯ РАБОТЫ С БУЛЕВЫМИ ФУНКЦИЯМИ ДЛЯ ЯЗЫКА
ПРОГРАММИРОВАНИЯ LYAPAS

Муругов Михаил Алексеевич

Руководитель
канд. физ.-мат. наук, доцент
_____ И.А.Панкратова
« ____ » _____ 201 ____ г.

Студент группы № 1155
_____ М.А.Муругов

Томск 2018

ОГЛАВЛЕНИЕ

Введение.....	2
1 Описание алгоритмов на математическом языке	
1.1 Принадлежность булевой функции к классу T^0	
1.2 Принадлежность булевой функции к классу T^1	
1.3 Преобразование Мёбиуса булевой функции	
1.4 Принадлежность булевой функции к классу линейных булевых функций	
1.5 Принадлежность булевой функции к классу самодвойственных булевых функций	
1.6 ///Определение и алгоритм “реверса” булевого вектора?//	
2 Программные реализации	
2.1 Принадлежность булевой функции к классу T^1	
2.2 Принадлежность булевой функции к классу T^0	
2.3 Преобразование Мёбиуса булевой функции	
2.4 Принадлежность булевой функции к классу линейных булевых функций	
2.5 Принадлежность булевой функции к классу самодвойственных булевых функций	
2.6 ///Алгоритм “реверса” булевого вектора?///	
2.7 ///Нужно ли включать реализации, не описанные в 1.x?///	
3 Экспериментальные данные	
4 Заключение	
Список использованных источников и литературы	
Приложения	

ВВЕДЕНИЕ

Целью этой курсовой работы было написание библиотеки для работы с булевыми функциями для языка программирования LYaPAS. В дальнейшем планируется, что эта библиотека будет использоваться для реализации криптографических алгоритмов и прочих нужд.

///Нужно ли как-то переделать введение?///

ОПИСАНИЕ АЛГОРИТМОВ НА МАТЕМАТИЧЕСКОМ ЯЗЫКЕ

Принадлежность булевой функции к классу T^0

Определение. Булева функция *сохраняет константу 0* (*принадлежит классу T^0*), если на наборе из всех нулей функция принимает значение нуль.

Алгоритм:

Вход: $f(x_1, \dots, x_n)$ – булева функция

Выход: “ f принадлежит классу T^0 ?”

Шаг 1) Если $f(0, 0, \dots, 0) = 0$, то ответ “Да”

Иначе ответ “Нет”

Принадлежность булевой функции к классу T^1

Определение. Булева функция *сохраняет константу 1* (*принадлежит классу T^1*), если на наборе из всех единиц функция принимает значение единица.

Алгоритм:

Вход: $f(x_1, \dots, x_n)$ – булева функция

Выход: “ f принадлежит классу T^1 ?”

Шаг 1) Если $f(1, 1, \dots, 1) = 1$, то ответ “Да”

Иначе ответ “Нет”

Преобразование Мёбиуса булевой функции

Определение. Положительной конъюнкцией называется элементарная конъюнкция, не содержащая инверсий переменных. Договоримся обозначать положительную конъюнкцию через K^+ .

///ОПРЕДЕЛЕНИЕ АНФ ВЗЯТЬ ИЗ “БУЛЕВЫ ФУНКЦИИ В КРИПТОГРАФИИ”!///

Определение. Полиномом Жегалкина, или алгебраической нормальной формой (АНФ), булевой функции $f(x_1, \dots, x_n)$ называется дизъюнкция с исключением различных положительных конъюнкций переменных из множества $X = \{x_1, \dots, x_n\}$, то есть формула вида $P = K_1^+ \oplus \dots \oplus K_p^+$, задающая функцию $f(x_1, \dots, x_n)$.

Определение. Преобразованием Мёбиуса называется функция $\mu: P_2(n) \rightarrow P_2(n)$, где $P_2(n)$ – множество всех булевых функций от n переменных. С помощью преобразования Мёбиуса решается задача построения АНФ булевой функции, и вычислить его значения для функции $f(x)$ можно по формуле $\mu(f(a)) = \bigoplus_{x \leq a} f(x)$. Рассмотрим возможный способ выполнения этого вычисления.

///Убрать способ? Написать сразу рекурсивный алгоритм? Как должна выглядеть в тексте ссылка на литературу? Надо ли приводить подытоживание(краткую суть способа)?///

Построим матрицу отношения предшествования булевых векторов $M_{2^n} = \|m_{ax}\|$, строкам и столбцам которой сопоставлены булевы векторы длины n и $m_{ax} = \begin{cases} 1, & \text{если } x \leq a \\ 0, & \text{иначе} \end{cases}$

$$\text{Например, } M_2 = \begin{matrix} a \backslash x & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{matrix}; \quad M_4 = \begin{matrix} a \backslash x & 00 & 01 & 10 & 11 \\ 00 & 1 & 0 & 0 & 0 \\ 01 & 1 & 1 & 0 & 0 \\ 10 & 1 & 0 & 1 & 0 \\ 11 & 1 & 1 & 1 & 1 \end{matrix}$$

Нетрудно убедиться, что $M_{2^n} = \left\| \begin{matrix} M_{2^{n-1}} & 0 \\ M_{2^{n-1}} & M_{2^{n-1}} \end{matrix} \right\|^{(*)}$ и $\mu(f) = M_{2^n} \cdot f$, где f – вектор-столбец значений функции f . Если f_0 и f_1 – соответственно младшая и старшая половины вектора значений f , то по формуле (*) получим следующую рекурсивную формулу:

$$M_{2^n} \cdot f = \left\| \begin{matrix} M_{2^{n-1}} & 0 \\ M_{2^{n-1}} & M_{2^{n-1}} \end{matrix} \right\| \cdot \left\| \begin{matrix} f_0 \\ f_1 \end{matrix} \right\| = \left\| \begin{matrix} M_{2^{n-1}} \cdot f_0 \\ M_{2^{n-1}} \cdot (f_0 \oplus f_1) \end{matrix} \right\|.$$

На «дне» рекурсии для функции от одной переменной

$$\mu(f) = \left\| \begin{matrix} 1 & 0 \\ 1 & 1 \end{matrix} \right\| \cdot \left\| \begin{matrix} f(0) \\ f(1) \end{matrix} \right\| = \left\| \begin{matrix} f(0) \\ f(1) \oplus f(0) \end{matrix} \right\|$$

На основании этого способа преобразование Мёбиуса реализовано программно.

Принадлежность булевой функции к классу линейных булевых функций

Определение. *Длиной* булева вектора назовем количество его компонент, а *весом* вектора – количество компонент, равных единице

Длину булева вектора a в дальнейшем будем обозначать $l(a)$. Запись $l(f)$, где f – булева функция, будет обозначать длину вектора её значений.

Вес булева вектора a в дальнейшем будем обозначать $w(a)$. Запись $w(f)$, где f – булева функция, будет обозначать вес вектора её значений.

Определение. *Длиной полинома Жегалкина* назовем количество конъюнкций в полиноме, а его *степенью* – наибольший из рангов конъюнкций, входящих в полином.

Определение. Полином Жегалкина называется *линейным*, если его степень не превышает единицы.

Определение. Булева функция называется *линейной* (*принадлежит классу L*), если ее полином Жегалкина линейен.

Алгоритм:

Вход: $f(x_1, \dots, x_n)$ – булева функция

Выход: “ f – линейна?”

Шаг 1) $g := \mu(f)$

Шаг 2) $g(0, 0, \dots, 0) := 0$

Шаг 3) Для всех векторов a таких, что $l(a) = n$ и $w(a) = 1$:

Шаг 3.1) $g(a) := 0$

Шаг 4) Если $w(g) = 0$, то ответ “Да”

Иначе ответ “Нет”

Принадлежность булевой функции к классу самодвойственных булевых функций

Определение. Булева функция $f(x_1, \dots, x_n)$ называется *двойственной булевой функции* $g(x_1, \dots, x_n)$, если она получена из $g(x_1, \dots, x_n)$ инверсией всех аргументов и самой функции, то есть $f(x_1, \dots, x_n) = \overline{g(\overline{x_1}, \dots, \overline{x_n})}$.

Определение. Булева функция $f(x_1, \dots, x_n)$ *самодвойственна* (принадлежит классу S), если она равна двойственной себе функции, то есть $f(x_1, \dots, x_n) = \overline{f(\overline{x_1}, \dots, \overline{x_n})}$.

Алгоритм:

Вход: $f(x_1, \dots, x_n)$ – булева функция

Выход: “ f – самодвойственна?”

Шаг 1) Для всех векторов a таких, что $l(a) = n$:

Шаг 1.1) Если $f(a) \neq \overline{f(\overline{a})}$, то ответ “Нет”

Шаг 2) Ответ “Да”

ПРОГРАММНЫЕ РЕАЛИЗАЦИИ

Перед изложением дальнейшего материала необходимо кое-что обозначить:

Во-первых, булевы функции в языке LYaPAS представляются векторами их значений.

Во-вторых, вектора значений булевых функций хранятся в логических комплексах L , каждый элемент которого занимает в памяти 4 байта (32 бита). Таким образом, т.к. $l(f(x_1, \dots, x_n)) = 2^n$, то функция до 5 аргументов включительно помещается в один элемент комплекса. От 6 в 2 элемента, от 7 в 4 и т.д. Количество элементов комплекса, необходимых для хранения функции от n аргументов можно вычислить по формуле $Q = \left\lceil \frac{2^n + 31}{32} \right\rceil$.

Принадлежность к классу T^0

Проверка булевой функции на принадлежность к классу T^0 тривиальна. Необходимо просто посмотреть на самый первый бит вектора её значений. Если этот бит равен нулю, то функция сохраняет константу 0.

Принадлежность к классу T^1

Проверка булевой функции на принадлежность к классу T^1 немного сложнее, чем к классу T^0 , т.к. у функций, зависящих от $n \leq 5$ аргументов старший бит вектора значений находится в нулевом элементе комплекса и его сначала необходимо найти. В общем же случае найти старший бит вектора значений функции можно по следующим правилам:

$i = \left\lceil \frac{2^n + 31}{32} \right\rceil - 1$, $j = 2^n \pmod{32}$, где i – индекс элемента комплекса, а j – номер бита в элементе с индексом i .

Преобразование Мёбиуса булевой функции

///TODO///

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Быкова С.В. Учебно-методический комплекс «Булевы функции». Томск 2006.
2. Панкратова И.А. Учебное пособие «Булевы функции в криптографии». Томск 2014.