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

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.

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: $f(x_1, x_2, \dots, x_n)$ – 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: $f(x_1, x_2, \dots, x_n)$ – 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. *Полиномом Жегалкина*, или *алгебраической нормальной формой (АНФ)*, булевой функции $f(x_1, x_2, \dots, x_n)$ 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 $f(x_1, x_2, \dots, x_n)$.

Определение. Преобразованием Мёбиуса называется функция $\mu: P_2(n) \to P_2(n)$, 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 $\mu\big(f(a)\big) = \bigoplus\limits_{x \le a} f(x)$. Рассмотрим возможный способ выполнения этого вычисления.

///Убрать способ? Написать сразу рекурсивный алгоритм?///

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

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

Нетрудно убедиться, что $M_{2^n} = \begin{Vmatrix} M_{2^{n-1}} & 0 \\ M_{2^{n-1}} & M_{2^{n-1}} \end{Vmatrix}^{(*)}$ 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:

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

На «дне» рекурсии для функции от одной переменной

$$\mu(f) = \begin{Vmatrix} 1 & 0 \\ 1 & 1 \end{Vmatrix} \cdot \begin{Vmatrix} f(0) \\ f(1) \end{Vmatrix} = \begin{Vmatrix} f(0) \\ f(1) \oplus f(1) \end{Vmatrix}$$

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 линеен.

Алгоритм:

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

Выход: "f – линейна?"

Шаг 1) $g \coloneqq \mu(f)$

Шаг 2) $g(0, \dots, 0) := 0$

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

Шаг 3.1) $g(a) \coloneqq 0$

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 $f(x_1, \dots, x_n) = \bar{g}(\overline{x_1}, \dots, \overline{x_n})$.

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

////Нужно ли вводить определение для reverseBits?///

Алгоритм:

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

Выход: "f – самодвойственна?"

Шаг 1) f_0 – младшая половина вектора значений f

f_1 – старшая половина вектора значений f