Секция «Вычислительная математика и кибернетика»

О сложности распознавания периодичности булевых функций, заданных полиномами

Бухман Антон Владимирович
Аспирант
Московский государственный университет имени М.В. Ломоносова, Факультет вычислительной математики и кибернетики, Москва, Россия
E-mail: antfb@rambler.ru

Пусть $E_2 = \{0, 1\}$. *Булевой функцией*, зависящей от n переменных, будем называть любое отображение вида $f : E_2^n \to E_2$. *Мономом* над переменными $x_1, \ldots, x_n$ называется любое выражение вида $x_{i_i} \ldots x_{i_l}$, где $l \geq 1, 1 \leq i_1, \ldots, i_l \leq n$, все переменные различны; либо просто 1. Равенство мономов рассматривается с точностью до перестановки сомножителей. *Полиномом* называется сумма по модулю 2 конечного числа различных мономов или 0 (можно понимать как сумму нулевого числа мономов). *Длиной* полинома называется число его слагаемых. Длину нулевого полинома будем считать равной 0. Рассматривается задание функций в виде полиномов Жегалкина. Известно, что любая булева функция может быть представлена единственным полиномом Жегалкина. Пусть $f(x_1, \ldots, x_n)$ – булева функция, и $\tau \in E_2^n, \tau = (\tau_1, \ldots, \tau_n)$, где $\tau_i \in E_2$. Функцию $f(x_1 + \tau_1, \ldots, x_n + \tau_n)$ для краткости далее в статье будет обозначать $f(x + \tau)$. Булева функция f называется *периодической с периодом* $\tau \neq (0, \ldots, 0)$, если $f(x+\tau) = f(x)$. В данной заметке рассматривается тема, относящаяся к сложности распознавания свойств булевых функций, заданных полиномами. Исследования в этой теме были начаты в работах [1,2]. Рассматривается следующая задача распознавания: на вход подаётся полином булевой функции и булев вектор. Требуется определить является ли этот вектор периодом функции. Решение данной задачи непосредственно проверкой по определению имеет экспоненциальную временную сложность. Возникает вопрос о построении более быстрого алгоритма. Получены следующие результаты.

Теорема 1. Существует RAM машина, которая получив на вход полином функции и булев вектор, определяет является ли данный вектор периодом этой функции. Причём время работы алгоритма на входе длины N будет составлять $O(N^3)$ тактов машины.

Теорема 1 даёт полиномиальный алгоритм проверки того, является ли заданный вектор периодом функции. Однако, остаётся нерешённым вопрос в случае, когда вектор неизвестен заранее. То есть задача ставится таким образом: на вход подан полином функции надо определить, имеет ли функция какой-либо период. Получен следующий результат.

Теорема 2. По полиному функции Π_f можно построить систему булевых уравнений такую, что любое решение этой системы кроме $(0, \ldots, 0)$ будет периодом функции и обратно, любой период функции f будет решением системы, причём эта система будет содержать не более $(l^2 + l)(n + 1)$ уравнений, где l – длина полинома Π_f.

Терема 2 даёт полиномиальное сведение задачи о поиске всех периодов функции к поиску всех решений системы булевых уравнений.

Литература

1. Горшков С.П. О сложности распознавания мультиаффинности, биюнктивности, слабой положительности и слабой отрицательности булевой функции // Обозрение прикл. и промышленной матем. Сер. Дискр. матем. 1997. No. 4. С. 216-237.

2. Селезнева С.Н. О сложности распознавания полноты множества булевых функций, реализованных полиномами Жегалкина // Дискретная математика. 1997. No. 4. С. 34-41.