О СЛОЖНОСТИ ПРОИЗВЕДЕНИЙ БУЛЕВЫХ ФУНКЦИЙ В КЛАССЕ ФОРМУЛ

Д. Ю. Черухин*

Работа посвящена изучению сложности булевых функций специального вида при реализации их формулами в произвольном полном конечном базисе. Рассматриваемые функции обладают тем свойством, что они бесповторно выразимы (а следовательно, имеют линейную сложность) в некотором фиксированном конечном базисе. Задача ставится так: для данной последовательности функций $f_1, f_2, \ldots$, бесповторно выразимых в базисе $Б'$, и данного базиса $Б$, $Б \neq Б'$, выяснить, имеет ли она линейную сложность при реализации формулами в базисе $Б$, или нелинейную.

Эта задача возникла после того, как автор решил проблему сравнения полных конечных булевых базисов [2], показав, что базис $Б$ предшествует базису $Б'$ тогда и только тогда, когда все функции из $Б'$ бесповторно выразимы в $Б$. Напомним, что базис $Б$ *не предшествует* [1] базису $Б'$ в том и только в том случае, если существует бесконечная последовательность функций, имеющая в базисе $Б$ сложность, по порядку большую, нежели в $Б'$. Таким образом доказательство в [2] свелось к получению нижних оценок сложности, более того, оказалось, что достаточно ограничиться доказательством нелинейности сложности, а именно, рассматривать только последовательности функций, бесповторно выразимых в базисе $Б'$. Впервые такие последовательности, более точно, последовательности степеней заданной функции, использовала Б. А. Субботовская [1] при решении задачи сравнения базисов в частном случае.

В настоящей работе рассмотрены последовательности степеней функции и их обобщения — последовательности произведений функций. Для них получен критерий линейности сложности при реализации формулами в заданном базисе $Б$.

Пусть $f(x_1, \ldots, x_n)$ и $g(x_1, \ldots, x_m)$ — булевы функции. Их *бесповторным произведением* называется функция

$$(f \otimes g)(x_1, \ldots, x_{nm}) = f(g(x_1, \ldots, x_m), \ldots, g(x_{(n-1)m+1}, \ldots, x_{nm})).$$

Функция

$$f^{(m)} = \underbrace{f \otimes \ldots \otimes f}_{m}$$

называется *m-й степенью* функции f. Функция $f(x_1, \ldots, x_n)$ называется *линейной*, если она представима в виде $a_1x_1 \oplus \ldots \oplus a_nx_n \oplus a_0$, где $a_0, a_1, \ldots, a_n$ — константы. Функция f называется *обобщенно-монотонной*, если она по каждой своей переменной либо возрастает, либо убывает.

Базисом будем называть произвольную полную конечную систему булевых функций. Базис, состоящий только из обобщенно-монотонных функций, называется *обобщенно-монотонным*. Булева функция f называется *бесповторно выразимой* в базисе $Б$, если она представима формулой в базисе $Б$, содержащей ровно одно вхождение каждой существенной переменной функции f. Базис называется *линейным*, если в нём бесповторно выразима функция $x \oplus y$. *Сложностью* формулы называется число вхождений в неё символов переменных. Будем говорить, что последовательность функций $f_1, f_2, \ldots$ имеет *линейную сложность* в базисе $Б$, если существует такая константа C, что для любого n сложность функции f_n в классе формул в базисе $Б$ не более чем в C раз превосходит число существенных переменных функции f_n.

Пусть $f_1, \ldots, f_n$ — булевы функции. Произведение $f_i \otimes \ldots \otimes f_j$, $1 \le i \le j \le n$, называется *линейным блоком* в произведении $f_1 \otimes \ldots \otimes f_n$, если:

1) каждая из функций $f_i, \ldots, f_j$ линейна;

2) хотя бы одна из функций $f_i, \ldots, f_j$ существенно зависит не менее чем от двух переменных;

3) если $i > 1$, то функция f_{i-1} нелинейна; если $j < n$, то функция f_{j+1} нелинейна.

Пусть $Б$ — базис. Введём обозначение $N_Б(f_1 \otimes \ldots \otimes f_n)$ следующим образом:

i) если $Б$ — линейный или обобщенно-монотонный базис, то через $N_Б(f_1 \otimes \ldots \otimes f_n)$ обозначим количество таких номеров i, $1 \le i \le n$, для которых функция f_i не выразима бесповторно в $Б$;

ii) если базис $Б$ нелинеен и не обобщенно-монотонен, то через $N_Б(f_1 \otimes \ldots \otimes f_n)$ обозначим сумму количества таких номеров i, $1 \le i \le n$, для которых функция f_i нелинейна и не выразима бесповторно в $Б$, и числа линейных блоков в произведении $f_1 \otimes \ldots \otimes f_n$.

Автором доказаны следующие теоремы 1 и 2.

Теорема 1 [3] *Пусть f — произвольная булева функция, $Б$ — произвольный базис. Тогда последовательность функций $f^{(1)}, f^{(2)}, \ldots$ имеет в базисе $Б$ линейную сложность в следующих случаях и только в них:*

а) *функция f существенно зависит не более чем от одной переменной;*

б) *функция f линейна, существенно зависит не менее чем от двух переменных и $Б$ — не обобщенно-монотонный базис;*

в) *функция f нелинейна и бесповторно выразима в базисе $Б$.*

Теорема 2 [4] *Пусть $Б$ — базис, $f_1, f_2, \ldots$ — последовательность булевых функций и для каждого n функция f_n представлена в виде $f_n^1 \otimes \ldots \otimes f_n^{k(n)}$. Пусть число существенных переменных каждой из функций f_n^i больше нуля и ограничено сверху некоторой константой, не зависящей ни от n, ни от i. Тогда в базисе $Б$ последовательность $f_1, f_2, \ldots$ имеет линейную сложность в том и только в том случае, когда величина $N_Б(f_n^1 \otimes \ldots \otimes f_n^{k(n)})$ ограничена сверху некоторой константой, не зависящей от n.*

Доказательства теорем 1 и 2 содержатся, соответственно, в [3] и [4].

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект N 99–01–01175), Федеральной целевой программы "Интеграция" (объединённый проект АО–110), Программы "Университеты России" (проект N 992206) и Программы поддержки ведущих научных школ РФФИ (проект N 00–15–96103).

Автор благодарит чл.-корр. РАН О. Б. Лупанова за внимание к работе.

ЛИТЕРАТУРА

[1] Субботовская Б. А. О сравнении базисов при реализации функций алгебры логики формулами // Докл. АН СССР. 1963. Т. 149, N 4. С. 784–787.

[2] Черухин Д. Ю. Алгоритмический критерий сравнения булевых базисов // Математические вопросы кибернетики. Вып. 8. М.: Наука, 1999. С. 77–122.

[3] Черухин Д. Ю. О сложности реализации формулами степеней булевых функций // Дискрет. анализ и исслед. операций. Сер. 1. 2001. Т. 8, N 4. С. 103–111.

[4] Черухин Д. Ю. О сложности реализации формулами произведений булевых функций // Дискрет анализ и исслед. операций. Сер. 1. 2002. Т. 9, N 1. С. 84–94.

* Московский государственный университет им. М. В. Ломоносова