Math-Net.Ru

Общероссийский математический портал

С. Н. Селезнева, Мультипликативная сложность некоторых функций алгебры логики, *Дискрет. матем.*, 2014, том 26, выпуск 4, 100–109

DOI: <https://doi.org/10.4213/dm1308>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением <http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.205.225.156

26 апреля 2023 г., 16:08:06

Мультипликативная сложность некоторых функций алгебры логики

© 2014 г. С. Н. Селезнева*

Мультипликативной (или конъюнктивной) сложностью функции алгебры логики $f(x_1, \dots, x_n)$ (соответственно, системы функций алгебры логики $F = \{f_1, \dots, f_m\}$) называется минимальное число элементов конъюнкции в схемах из функциональных элементов в базисе $\{x \& y, x \oplus y, 1\}$, каждая из которых реализует функцию f (соответственно, все функции из системы F). Мультипликативную сложность функции f (системы функций F) будем обозначать через $\mu(f)$ (через $\mu(F)$). В работе доказано, что $\mu(f) = n - 1$, если функция $f(x_1, \dots, x_n)$ представима в виде $x_1 x_2 \dots x_n \oplus q(x_1, \dots, x_n)$, где q – функция степени два ($n \geq 3$). В работе также доказано, что $\mu(f) \leq n - 1$, если функция $f(x_1, \dots, x_n)$ представима в виде суммы по модулю 2 двух мультиаффинных функций. Кроме того, в работе показано, что $\mu(F) = n - 1$, если $F = \{x_1 x_2 \dots x_n, f(x_1, \dots, x_n)\}$, где f – или функция степени два, или мультиаффинная функция.

Работа поддержана РФФИ, гранты 13-01-00684-а и 13-01-00958-а.

Ключевые слова: функция алгебры логики, схема из функциональных элементов (СФЭ), сложность, мультипликативная (конъюнктивная) сложность, верхняя оценка.

1. Введение

Мультипликативной (или конъюнктивной) сложностью функции алгебры логики $f(x_1, \dots, x_n)$ (соответственно, системы функций алгебры логики $F = \{f_1, \dots, f_m\}$) называется минимальное число элементов конъюнкции в схемах из функциональных элементов в базисе $\{x \& y, x \oplus y, 1\}$, каждая из которых реализует функцию f (соответственно, все функции из системы F). Мультипликативную сложность функции f (системы функций F) будем обозначать через $\mu(f)$ (через $\mu(F)$). В [1–7] изучалась мультипликативная сложность функций алгебры логики. В [3, 4] было найдено точное значение функции Шеннона мультипликативной сложности $\mu(n, 2)$ функций второй степени $\mu(n, 2) = \lfloor n/2 \rfloor$, где $\lfloor a \rfloor$ обозначает наибольшее целое число, не превосходящее число a . В [3] доказано, что мультипликативная сложность произвольной мультиаффинной функции, зависящей от n переменных, не превосходит $(n - 1)$. В [2] доказано, что мультипликативная сложность произвольной симметрической функции, зависящей от n переменных, не превосходит $n + O(\sqrt{n})$. В [7] найдено точное значение мультипликативной сложности для последовательности функций $f_n(x_1, \dots, x_n) = \bigvee_{1 \leq i < j \leq n} x_i x_j$. В [8] изучалась зависимость между

*Место работы: МГУ имени М.В. Ломоносова, e-mail: selezn@cs.msu.ru

мультипликативной сложностью функций и сложностью их реализации схемами из функциональных элементов в базисе из всех функций алгебры логики, зависящих от двух переменных. В названной работе показано, как найти нижнюю оценку сложности реализации функции схемами из функциональных элементов в этом базисе, если известна мультипликативная сложность этой функции. В [9] рассматривалось соотношение между мультипликативной и аддитивной сложностями функций.

2. Основные определения

Пусть $B = \{0, 1\}$. На множестве B^n введем частичный порядок $\leq$. Если $\alpha = (a_1, \dots, a_n) \in B^n$ и $\beta = (b_1, \dots, b_n) \in B^n$, то $\alpha \leq \beta$, если $a_1 \leq b_1, \dots, a_n \leq b_n$ ($n \geq 1$). Весом $|\alpha|$ набора $\alpha = (a_1, \dots, a_n) \in B^n$ назовем величину $\sum_{i=1}^n a_i$ (здесь рассматривается сумма целых чисел). Монотонную элементарную конъюнкцию (моном) $\prod_{i: a_i=1} x_i$ обозначим K_α и назовем соответствующей набору $\alpha = (a_1, \dots, a_n) \in B^n$. По определению будем считать, что $K_{(0, \dots, 0)} = 1$.

Функцией алгебры логики (ФАЛ) f , зависящей от n переменных, назовем отображение $f: B^n \rightarrow B$, $n = 0, 1, \dots$. Каждая функция алгебры логики $f(x_1, \dots, x_n)$ может быть представлена формулой вида

$$\bigoplus_{\alpha \in B^n: c_f(\alpha)=1} K_\alpha,$$

где $c_f(\alpha) = \bigoplus_{\beta \leq \alpha} f(\beta) \in B$ – коэффициенты, $\alpha \in B^n$, и $\bigoplus$ обозначает сложение по модулю 2. Это представление функций алгебры логики называется полиномом Жегалкина, или алгебраической нормальной формой (АНФ). Каждая функция алгебры логики представляется полиномом Жегалкина однозначно [10]. Степенью $\deg(f)$ функции $f(x_1, \dots, x_n)$ называется величина $\max_{\alpha \in B^n: c_f(\alpha)=1} |\alpha|$.

Схемой из функциональных элементов (СФЭ, или просто схемой) в базисе $\{x \& y, x \oplus y, 1\}$ называется ориентированный ациклический граф, полустепень захода каждой вершины которого равна или нулю, или двум. Вершины, полустепень захода которых равна нулю, называются входными. Каждой из них приписывается или некоторая переменная x_i , или константа 1. Все остальные вершины называются внутренними вершинами схемы. Каждой внутренней вершине приписывается или $\&$ (элемент конъюнкции), или $\oplus$ (элемент сложения по модулю 2). Некоторые из вершин, как внутренние, так и входные, называются выходными. Им приписываются попарно различные выходные переменные y_j . В каждой вершине v СФЭ S реализуется некоторая функция алгебры логики f_v , зависящая от переменных, приписанных входным вершинам этой схемы. Если v – это входная вершина, то $f_v = x_i$ (если вершине v приписана переменная x_i) и $f_v = 1$ (если вершине v приписана константа 1). Если в вершину v входят дуги из вершин v_1 и v_2 , причем в вершинах v_1 и v_2 реализуются соответственно функции f_{v_1} и f_{v_2} , а самой вершине v приписан элемент $\&$ (соответственно, элемент $\oplus$), то $f_v = f_{v_1} \& f_{v_2}$ (соответственно, $f_v = f_{v_1} \oplus f_{v_2}$). Говорят, что схема S реализует систему функций $F = \{f_1, \dots, f_m\}$, если для каждого $j = 1, \dots, m$ в схеме S найдется вершина v_j , в которой реализуется функция f_j .

Мультипликативной (или конъюнктивной) сложностью $\mu(S)$ схемы S называется число вершин в этой схеме, которым приписаны элементы конъюнкции $\&$. Мультипликативной (или конъюнктивной) сложностью $\mu(F)$ системы функций F называется минимальная мультипликативная сложность среди всех схем, реализующих систему F . Мультипликативной (или конъюнктивной) сложностью $\mu(f)$ функции $f(x_1, \dots, x_n)$ называется минимальная мультипликативная сложность среди всех схем, реализующих функцию f .

3. Основные леммы

В этом разделе мы рассмотрим леммы, которые будут применяться в следующих разделах при доказательстве оценок мультипликативной сложности функций. Сначала сформулируем лемму 1 из [3], на которую будем ссылаться при получении нижних оценок.

Лемма 1 ([3]). Для произвольной функции f алгебры логики $\mu(f) \geq \deg(f) - 1$.

Теперь докажем леммы, которые будем применять при нахождении верхних оценок мультипликативной сложности функций.

Функция f называется аффинной, если $\deg(f) \leq 1$. Множество всех аффинных функций, зависящих от переменных $x_1, \dots, x_n$, обозначим A^n . Аффинная функция f называется линейной, если $c_f(0, \dots, 0) = 0$. Множество всех линейных функций, зависящих от переменных $x_1, \dots, x_n$, обозначим L^n . Линейные функции $g_1, \dots, g_m$ называются линейно независимыми, если из равенства

$$c_1 g_1 \oplus \dots \oplus c_m g_m = 0,$$

где $c_1, \dots, c_m \in B$, следует, что $c_1 = \dots = c_m = 0$. В противном случае линейные функции $g_1, \dots, g_m$ называются линейно зависимыми. Известно, что множество L^n является линейным пространством размерности n [11].

Лемма 2. Если $g_i \in L^n$, $i = 1, \dots, l$, $l \geq 2$, и функции $g_1, \dots, g_l$ являются линейно независимыми, то найдутся такие константы $a_1, \dots, a_n \in B$ и такие функции $h_{l+1}, \dots, h_n \in A^n$, что

$$\left(\prod_{i=1}^l (g_i \oplus a_i) \right) \cdot \left(\prod_{i=l+1}^n h_i \right) = x_1 \dots x_n.$$

Доказательство. Добавим к линейным функциям $g_1, \dots, g_l$ линейные функции $g_{l+1}, \dots, g_n \in L^n$ так, чтобы линейные функции $g_1, \dots, g_n$ оказались линейно независимыми. Мы всегда можем это сделать, так как размерность линейного пространства L^n равна n .

Рассмотрим систему линейных уравнений

$$\begin{cases} g_1(x_1, \dots, x_n) & = & g_1(1, \dots, 1), \\ & \dots, \\ g_n(x_1, \dots, x_n) & = & g_n(1, \dots, 1). \end{cases} \quad (1)$$

Заметим, что по построению единичный набор $(1, \dots, 1) \in B^n$ является решением системы (1). Линейные функции $g_1, \dots, g_n$ линейно независимы, поэтому (см., например, [11]) система (1) имеет единственное решение. Заметим, что множество

решений системы (1) является множеством наборов из B^n , на которых функция $\prod_{i=1}^n (g_i \oplus g_i(1, \dots, 1) \oplus 1)$ принимает значение 1. Так как единственное решение системы (1) – это единичный набор $(1, \dots, 1) \in B^n$, получаем, что

$$\prod_{i=1}^n (g_i \oplus g_i(1, \dots, 1) \oplus 1) = x_1 \dots x_n.$$

Отсюда находим, что $a_i = g_i(1, \dots, 1) \oplus 1$ при $i = 1, \dots, l$, $h_i(x_1, \dots, x_n) = g_i(x_1, \dots, x_n) \oplus g_i(1, \dots, 1) \oplus 1$ при $i = l+1, \dots, n$.

Лемма 3. Если $g_i \in L^n$, $a_i \in B$, $i = 1, \dots, l$, $l \geq 2$, функции $g_1, \dots, g_l$ являются линейно независимыми и k – такое число, что $n - k \leq l$, то найдутся такие функции $h_1, \dots, h_{n-k} \in A^n$ и $h_{n-k+1}, \dots, h_l \in A^k$, что

$$\prod_{i=1}^l (g_i \oplus a_i) = \prod_{i=1}^l h_i.$$

Доказательство. Рассмотрим систему линейных уравнений

$$\begin{cases} g_1(x_1, \dots, x_n) &= a_1 \oplus 1, \\ &\dots, \\ g_l(x_1, \dots, x_n) &= a_l \oplus 1. \end{cases} \quad (2)$$

Так как функции $g_1, \dots, g_l$ линейно независимы, мы можем (см., например, [11]) преобразовать систему (2) к такому виду

$$\begin{cases} h_1(x_1, \dots, x_k, x_{k+1}, \dots, x_{n-1}, x_n) = 1, \\ h_2(x_1, \dots, x_k, x_{k+1}, \dots, x_{n-1}) = 1, \\ \dots, \\ h_{n-k}(x_1, \dots, x_k, x_{k+1}) = 1, \\ h_{n-k+1}(x_1, \dots, x_k) = 1, \\ \dots, \\ h_l(x_1, \dots, x_k) = 1, \end{cases} \quad (3)$$

где $h_1, \dots, h_{n-k} \in A^n$, $h_{n-k+1}, \dots, h_l \in A^n$, что множества решений систем (2) и (3) совпадают. Следовательно,

$$\prod_{i=1}^l h_i = \prod_{i=1}^l (g_i \oplus a_i).$$

Лемма 4. Пусть $f_n(x_1, \dots, x_n) = x_1 \dots x_n \oplus \bar{x}_1 \dots \bar{x}_n$, где $n \geq 2$. Тогда $\mu(f_n) = n - 2$.

Доказательство. 1. Верхняя оценка. Заметим, что

$$f_n(x_1, \dots, x_n) = (x_1 \sim x_2)(x_2 \sim x_3) \dots (x_{n-2} \sim x_{n-1})(x_{n-1} \sim x_n),$$

где $x \sim y = x \oplus y \oplus 1$. Отсюда $\mu(f_n) \leq n - 2$.

2. Нижняя оценка. Заметим, что $\deg(f_n) = n - 1$. Согласно лемме 1 для произвольной функции f верно, что $\mu(f) \geq \deg(f) - 1$. Поэтому $\mu(f_n) \geq n - 2$.

Получаем, что $\mu(f_n) = n - 2$.

Лемма 5. Пусть $F_n = \{x_1 \dots x_n, \bar{x}_1 \dots \bar{x}_n\}$. Тогда $\mu(F_n) = n - 1$.

Доказательство. 1. Верхняя оценка. Заметим, что

$$\begin{aligned}x_1 \dots x_n &= x_1 \cdot f_n(x_1, \dots, x_n), \\ \bar{x}_1 \dots \bar{x}_n &= x_1 \dots x_n \oplus f_n(x_1, \dots, x_n),\end{aligned}$$

где

$$f_n(x_1, \dots, x_n) = x_1 \dots x_n \oplus \bar{x}_1 \dots \bar{x}_n.$$

По лемме 4 $\mu(f_n) \leq n - 2$. Поэтому $\mu(F_n) \leq n - 1$.

2. Нижняя оценка. Заметим, что степень каждой из функций системы F_n равна n . Поэтому $\mu(F_n) \geq n - 1$ [3].

Получаем, что $\mu(F_n) = n - 1$.

4. Мультипликативная сложность функций, являющихся суммой произведения n переменных и квадратичной функции

Функция алгебры логики f называется квадратичной, если $\deg(f) = 2$. В [4] доказано, что для произвольной квадратичной функции f , зависящей от n переменных, $\mu(f) \leq \lfloor n/2 \rfloor$. Кроме того, в [4] описаны квадратичные функции, зависящие от n переменных, мультипликативная сложность которых равна $\lfloor n/2 \rfloor$.

Теорема 1. Если $n \geq 3$, и ФАЛ $f(x_1, \dots, x_n)$ может быть представлена в виде $x_1 \dots x_n \oplus q(x_1, \dots, x_n)$, где $\deg(q) = 2$, то $\mu(f) = n - 1$.

Доказательство. 1. Верхняя оценка. В [4, 3] показано, что каждую ФАЛ степени 2 можно представить в виде $g_0 \oplus \bigoplus_{i=1}^l g_{2i-1} g_{2i}$, где $g_i \in L^n$, $i = 1, \dots, 2l$, $g_0 \in A^n$, и линейные функции $g_1, \dots, g_{2l}$ линейно независимы. Представим функцию $q(x_1, \dots, x_n)$ в таком виде. Заметим, что $2l \leq n$, так как размерность линейного пространства L^n равна n .

По лемме 2 найдем такие константы $a_1, \dots, a_{2l} \in B$ и такие функции $h_{2l+1}, \dots, h_n \in A^n$, что

$$\left(\prod_{i=1}^l (g_{2i-1} \oplus a_{2i-1}) \cdot (g_{2i} \oplus a_{2i}) \right) \cdot \left(\prod_{i=2l+1}^n h_i \right) = x_1 \cdot \dots \cdot x_n.$$

Заметим, что

$$g_{2i-1} \cdot g_{2i} = (g_{2i-1} \oplus a_{2i-1}) \cdot (g_{2i} \oplus a_{2i}) \oplus h_i$$

для некоторых $h_i \in A^n$, $i = 1, \dots, l$. Отсюда получаем, что

$$q(x_1, \dots, x_n) = h_0 \oplus \bigoplus_{i=1}^l (g_{2i-1} \oplus a_{2i-1}) \cdot (g_{2i} \oplus a_{2i}),$$

где $h_0 = g_0 \oplus \bigoplus_{i=1}^l h_i \in A^n$. Следовательно,

$$\begin{aligned}f(x_1, \dots, x_n) &= \left(\prod_{i=1}^l (g_{2i-1} \oplus a_{2i-1}) \cdot (g_{2i} \oplus a_{2i}) \right) \cdot \left(\prod_{i=2l+1}^n h_i \right) \oplus \\ &\quad \oplus h_0 \oplus \bigoplus_{i=1}^l (g_{2i-1} \oplus a_{2i-1}) \cdot (g_{2i} \oplus a_{2i}).\end{aligned}\tag{4}$$

Схему, реализующую функцию f , будем строить по полученной формуле (4). Сначала реализуем функции $(g_{2i-1} \oplus a_{2i-1}) \cdot (g_{2i} \oplus a_{2i})$, $i = 1, \dots, l$. Для этого понадобится l элементов конъюнкции. Затем реализуем функцию

$$\left(\prod_{i=1}^l (g_{2i-1} \oplus a_{2i-1}) \cdot (g_{2i} \oplus a_{2i}) \right) \cdot \left(\prod_{i=2l+1}^n h_i \right).$$

При этом добавим еще $(n-l-1)$ элементов конъюнкции. Затем реализуем функцию f по формуле (4) без дополнительных элементов конъюнкции.

Получаем, что $\mu(f) \leq n-1$.

2. Нижняя оценка. По лемме 1 получаем, что $\mu(f) \geq n-1$.

Следовательно, $\mu(f) = n-1$.

Следствие 1. Если $F = \{x_1 \dots x_n, q(x_1, \dots, x_n)\}$, где $\deg(q) = 2$, то $\mu(F) = n-1$.

Доказательство. Верхняя оценка $\mu(F) \leq n-1$ следует из доказательства теоремы 1, так как по этому доказательству видно, как построить схему с $(n-1)$ элементами конъюнкции, в которой реализуются функции $x_1 \dots x_n$ и $q(x_1, \dots, x_n)$.

Нижняя оценка $\mu(F) \geq n-1$ следует из того, что в системе F содержится функция $x_1 \dots x_n$ степени n .

5. Мультипликативная сложность функций, являющихся суммой двух мультиаффинных функций

Функция алгебры логики $f(x_1, \dots, x_n)$ называется мультиаффинной, если найдутся такие аффинные функции $h_1, \dots, h_s$, что $f = \prod_{i=1}^s h_i$. Мультиаффинные функции рассматривались в [12] в связи с задачей выполнимости конъюнктивных нормальных форм. Сформулируем лемму 6 из [3], которую будем применять в доказательствах.

Лемма 6 ([3]). Если функция $f(x_1, \dots, x_n)$ является мультиаффинной, то найдутся такие линейно независимые функции $g_1, \dots, g_l \in L^n$, и такие константы $a_1, \dots, a_l \in B$, где $l = \deg(f)$, что

$$f(x_1, \dots, x_n) = \prod_{i=1}^l (g_i \oplus a_i).$$

Рассмотрим мультиаффинную функцию $f(x_1, \dots, x_n)$, и пусть $\deg(f) = l$, $l \leq n$. По лемме 6 функцию f можно представить в виде $f(x_1, \dots, x_n) = \prod_{i=1}^l (g_i \oplus a_i)$, где $g_1, \dots, g_l$ — линейно независимые линейные функции, и $a_1, \dots, a_l \in B$. Добавим к линейным функциям $g_1, \dots, g_l$ такие линейные функции $g_{l+1}, \dots, g_n$, что линейные функции $g_1, \dots, g_n$ являются линейно независимыми. Мы всегда можем так сделать.

Рассмотрим аффинные замены переменных:

$$\begin{aligned} y_1 &= g_1 \oplus a_1, \\ &\dots, \\ y_l &= g_l \oplus a_l, \\ y_{l+1} &= g_{l+1}, \\ &\dots, \\ y_n &= g_n. \end{aligned}$$

Это преобразование переменных переводит мультиаффинную функцию f в функцию $y_1 \dots y_l$. Кроме того, это преобразование невырожденно (обратимо), так как линейные функции $g_1, \dots, g_n$ линейно независимы. Поэтому найдутся такие линейно независимые линейные функции $h_1, \dots, h_n$, зависящие от переменных $y_1, \dots, y_n$, и такие $b_1, \dots, b_n \in B$, что

$$\begin{aligned} x_1 &= h_1 \oplus b_1, \\ &\dots, \\ x_n &= h_n \oplus b_n. \end{aligned}$$

Эти рассуждения мы будем применять далее в доказательствах теорем.

По лемме 6 мультипликативная сложность каждой мультиаффинной функции, зависящей от n переменных, не превосходит $(n - 1)$. Мы получаем (теоремы 2, 3, 4) оценки мультипликативной сложности функций алгебры логики, которые представимы в виде суммы по модулю 2 двух мультиаффинных функций.

Теорема 2. Если ФАЛ $f(x_1, \dots, x_n)$ может быть представлена в виде $f_1(x_1, \dots, x_n) \oplus f_2(x_1, \dots, x_n)$, где f_1, f_2 – мультиаффинные функции, и $\deg(f) = n$, то $\mu(f) = n - 1$ ($n \geq 2$).

Доказательство. 1. Верхняя оценка. Так как $\deg(f) = n$, то обратимыми аффинными заменами переменных функцию $f(x_1, \dots, x_n)$ можно преобразовать к виду $x_1 \dots x_n \oplus h(x_1, \dots, x_n)$, где h – мультиаффинная функция, и $\deg(h) < n$. По лемме 6 представим функцию $h(x_1, \dots, x_n)$ в виде $\prod_{i=1}^l g_i$, где $g_1, \dots, g_l \in A^n$, линейные функции $g_1 \oplus g_1(0, \dots, 0), \dots, g_l \oplus g_l(0, \dots, 0)$ линейно независимы, и $l = \deg(h)$. Не ограничивая общности рассуждений, пусть $g_i(1, \dots, 1) = 1$ при $i = 1, \dots, k$, и $g_i(1, \dots, 1) = 0$ при $i = k + 1, \dots, l$.

Воспользуемся леммой 2. Найдем такие функции $g_{l+1}, \dots, g_n \in A^n$, что

$$\prod_{i=1}^k g_i \cdot \prod_{i=k+1}^l \bar{g}_i \cdot \prod_{i=l+1}^n g_i = x_1 \dots x_n.$$

Тогда

$$\begin{aligned} f(x_1, \dots, x_n) &= x_1 \dots x_n \oplus h(x_1, \dots, x_n) = x_1 \dots x_n \oplus \prod_{i=1}^l g_i = \\ &= \prod_{i=1}^k g_i \cdot \prod_{i=k+1}^l \bar{g}_i \cdot \prod_{i=l+1}^n g_i \oplus \prod_{i=1}^k g_i \cdot \prod_{i=k+1}^l g_i = \\ &= \prod_{i=1}^k g_i \cdot \left(\prod_{i=k+1}^l \bar{g}_i \cdot \prod_{i=l+1}^n g_i \oplus \prod_{i=k+1}^l g_i \right). \end{aligned} \quad (5)$$

Схему с $(n - 1)$ элементами конъюнкции для функции $x_1 \dots x_n \oplus h(x_1, \dots, x_n)$ будем строить по формуле (5).

Сначала строим произведение $\prod_{i=1}^k g_i$ при помощи $(k-1)$ элементов конъюнкции.

Затем воспользуемся леммой 4. Рассмотрим схему S_{l-k} , реализующую функцию $f_{l-k} = y_1 \dots y_{l-k} \oplus \bar{y}_1 \dots \bar{y}_{l-k}$ с $(l-k-2)$ элементами конъюнкции. На входы $y_1, \dots, y_{l-k}$ подадим аффинные функции $g_{k+1}, \dots, g_l$ соответственно. Полученная новая схема S'_{l-k} реализует функцию $\prod_{i=k+1}^l g_i \oplus \prod_{i=k+1}^l \bar{g}_i$ с $(l-k-2)$ элементами конъюнкции. Добавляя один элемент конъюнкции, строим функцию $\left(\prod_{i=1}^k g_i\right) \cdot \left(\prod_{i=k+1}^l g_i \oplus \prod_{i=k+1}^l \bar{g}_i\right)$. Домножая эту функцию на функцию g_{k+1} , можно построить функции $\left(\prod_{i=1}^k g_i\right) \cdot \left(\prod_{i=k+1}^l g_i\right)$ и $\left(\prod_{i=1}^k g_i\right) \cdot \left(\prod_{i=k+1}^l \bar{g}_i\right)$.

Добавляя $(n-l-1)$ элементов конъюнкции, строим произведение $\prod_{i=l+1}^n g_i$.

Добавляя еще 1 элемент конъюнкции и элементы сложения по модулю 2, строим искомую функцию.

Всего мы затратили $(k-1) + (l-k-2) + 2 + (n-l-1) + 1 = n-1$ элементов конъюнкции.

2. Нижняя оценка. По лемме 1 получаем: $\mu(f) \geq n-1$.

Следовательно, $\mu(f) = n-1$.

Теорема 3. Если ФАЛ $f(x_1, \dots, x_n)$ может быть представлена в виде $f_1(x_1, \dots, x_n) \oplus f_2(x_1, \dots, x_n)$, где f_1, f_2 – мультиаффинные функции, $f_1 \neq f_2$, и $\deg(f_1) = \deg(f_2) = n$, то $\mu(f) = n-2$ ($n \geq 2$).

Доказательство. 1. Верхняя оценка. Не ограничивая общности рассуждений, обратимыми аффинными заменами переменных функцию $f(x_1, \dots, x_n)$ можно преобразовать к виду $x_1 \dots x_n \oplus x_1 \dots x_k \bar{x}_{k+1} \dots \bar{x}_n$. Так как $f_1 \neq f_2$, то $k < n$. Тогда

$$x_1 \dots x_n \oplus x_1 \dots x_k \bar{x}_{k+1} \dots \bar{x}_n = x_1 \dots x_k \cdot (x_{k+1} \dots x_n \oplus \bar{x}_{k+1} \dots \bar{x}_n). \quad (6)$$

Схему, реализующую функцию $x_1 \dots x_m \oplus x_1 \dots x_k \bar{x}_{k+1} \dots \bar{x}_n$ с $(n-2)$ элементами конъюнкции, будем строить по формуле (6). По лемме 4 функцию $x_{k+1} \dots x_n \oplus \bar{x}_{k+1} \dots \bar{x}_n$ можно реализовать схемой с $(n-k-2)$ элементами конъюнкции. Добавляя еще k элементов конъюнкции, получаем схему для искомой функции.

2. Нижняя оценка $\mu(f) \geq n-2$ следует из леммы 1, так как $\deg(f) = n-1$.

Следствие 2. Если $F = \{x_1 \dots x_n, f(x_1, \dots, x_n)\}$, где f – мультиаффинная функция, то $\mu(F) = n-1$.

Доказательство. Если $\deg(f) < n$, то верхняя оценка $\mu(F) \leq n-1$ следует из доказательства теоремы 2, так как из этого доказательства видно, как построить схему с $(n-1)$ элементами конъюнкции, в которой реализуются функции $x_1 \dots x_n$ и $f(x_1, \dots, x_n)$.

Если $\deg(f) = n$, то, не ограничивая общности рассуждений, можно считать, что функция $f(x_1, \dots, x_n)$ имеет вид $x_1 \dots x_k \bar{x}_{k+1} \dots \bar{x}_n$, где $k < n$. По теореме 4 для функции $x_1 \dots x_n \oplus f(x_1, \dots, x_n)$ можно построить схему с $(n-2)$ элементами конъюнкции. Тогда

$$\begin{aligned} x_1 \dots x_n &= x_{k+1} \cdot (x_1 \dots x_n \oplus f(x_1, \dots, x_n)), \\ f(x_1, \dots, x_n) &= x_1 \dots x_n \oplus (x_1 \dots x_n \oplus f(x_1, \dots, x_n)). \end{aligned}$$

Отсюда $\mu(F) \leq n - 1$.

Нижняя оценка $\mu(F) \geq n - 1$ следует из того, что в системе F содержится функция $x_1 \dots x_n$ степени n .

Теорема 4. Если ФАЛ $f(x_1, \dots, x_n)$ может быть представлена в виде $f_1(x_1, \dots, x_n) \oplus f_2(x_1, \dots, x_n)$, где f_1, f_2 – мультиаффинные функции, и $\deg(f_1) < n$, $\deg(f_2) < n$, то $\mu(f) \leq n - 1$ ($n \geq 2$).

Доказательство. Пусть $\deg(f_1) = m$, $\deg(f_2) = l$, и $m \leq l < n$. Обратимыми аффинными заменами переменных функцию $f(x_1, \dots, x_n)$ преобразуем к виду $x_1 \dots x_m \oplus t(x_1, \dots, x_n)$, где t – мультиаффинная функция и $\deg(t) = l$. Представим мультиаффинную функцию $t(x_1, \dots, x_n)$ в виде $\prod_{i=1}^l g_i$, где $g_1, \dots, g_l \in A^n$ и линейные функции $g_1 \oplus g_1(0, \dots, 0), \dots, g_l \oplus g_l(0, \dots, 0)$ линейно независимы.

Пользуясь леммой 3, найдем такие функции $h_1, \dots, h_{n-m} \in A^n$ и $h_{n-m+1}, \dots, h_l \in A^m$, что

$$\prod_{i=1}^n g_i = \prod_{i=1}^l h_i.$$

Тогда

$$x_1 \dots x_m \oplus t(x_1, \dots, x_n) = x_1 \dots x_m \oplus \left(\prod_{i=1}^{n-m} h_i \right) \cdot \left(\prod_{i=1}^{l-(n-m)} h_{n-m+i} \right). \quad (7)$$

Схему для функции $x_1 \dots x_m \oplus t(x_1, \dots, x_n)$ будем строить по формуле (7). По следствию 2 систему из двух функций $x_1 \dots x_m$ и $\prod_{i=1}^{l-(n-m)} h_{n-m+i}$ можно реализовать схемой с $(m - 1)$ элементами конъюнкции. Для построения схемы для функции $\prod_{i=1}^{n-m} h_i$ понадобится $((n - m) - 1)$ элементов конъюнкции. Добавляя еще один элемент конъюнкции и элементы сложения по модулю 2, получаем схему с $(n - 1)$ элементами конъюнкции для искомой функции.

Следствие 3. Если $F = \{f_1(x_1, \dots, x_n), f_2(x_1, \dots, x_n)\}$, где f_1, f_2 – мультиаффинные функции, то $\mu(F) \leq n - 1$.

Доказательство. Если степень хотя бы одной из функций f_1, f_2 равна n , то утверждение доказано в следствии 2. Если $\deg(f_1) < n$, $\deg(f_2) < n$, то оценка $\mu(F) \leq n - 1$ следует из доказательства теоремы 3, так как из этого доказательства видно, как построить схему с $(n - 1)$ элементами конъюнкции, в которой реализуются функции f_1 и f_2 .

Список литературы

1. Нечипорук Э.И., “О сложности схем в некоторых базисах, содержащих нетривиальные элементы с нулевыми весами”, *Проблемы кибернетики*, **8** (1962), 123–160.
2. Boyar J., Peralta R., Pochuev D., “On the multiplicative complexity of Boolean functions over the basis $\{\wedge, \oplus, 1\}$ ”, *Theor. Comput. Sci.*, **235** (2000), 43–57.
3. Schnorr C.P., “The multiplicative complexity of Boolean functions”, Proc. of 6th Int. Conf. AAECC-6, *Lect. Notes Comput. Sci.*, **357** (1989), 45–58.

4. Mirwald R., Schnorr C.P., “The multiplicative complexity of quadratic Boolean forms”, *Theor. Comput. Sci.*, **102** (1992), 307–328.
5. Boyar J., Peralta R., Pochuev D., “Concrete multiplicative complexity of symmetric functions”, Tech. Rep. YALEU/DCS/TR1219. Comput. Sci. Dep. Yale Univ., 2001.
6. Boyar J., Peralta R., “The exact multiplicative complexity of the Hamming weight function”.
7. Краснова Т.И., “О конъюнктивной сложности схем в базисе Жегалкина для одной последовательности булевых функций”, Материалы XI Междунар. сем. “Дискретная математика и ее приложения”, 2012, 138–141.
8. Kojevnikov A., Kulikov A.S., “Circuit complexity and multiplicative complexity of Boolean functions”, Proc. of 6th Conf. on Computability (CiE 2010), *Lect. Notes Comput. Sci.*, **6158** (2010), 239–245.
9. Sergeev I.S., “A relation between additive and multiplicative complexity of Boolean functions”, arXiv:1303.4177. 2013..
10. Яблонский С.В., *Введение в дискретную математику*, М.: Высшая школа, 2001.
11. Курош А.Г., *Курс высшей алгебры*, М.: Наука, 1971.
12. Schaefer T.J., “The complexity of satisfiability problems”, Proc. of the 10th ACM Symp. on Theory of Computing, 1978, 216–226.

Статья поступила 23.05.2014.