Math-Net.Ru

Общероссийский математический портал

А. С. Зинченко, В. И. Пантелеев, Бинарные термы в полиномиальных представлениях булевых функций, *Матем. заметки*, 2007, том 81, выпуск 2, 217–225

DOI: <https://doi.org/10.4213/mzm3549>

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: 54.80.73.141

26 апреля 2023 г., 14:13:38

Бинарные термы в полиномиальных представлениях булевых функций

А. С. Зинченко, В. И. Пантелеев

Статья посвящена полиномиальным представлениям булевых функций с помощью бинарных термов. В построении термов участвуют переменные и остаточные функции. Частными случаями таких представлений являются разложения функции по переменным, полиномы Жегалкина, представление функций в виде суммы конъюнкций остаточных функций.

Библиография: 4 названия.

Введение. В теории булевых функций, как и в любой функциональной системе, одной из актуальных задач является представление функций термами над функциями меньшей размерности. К проблемам разложения функций тесно примыкают вопросы нахождения специальных форм, т.е. представление функций термами заданного вида. Среди таких представлений традиционно вызывают интерес так называемые полиномиальные. Интерес к полиномиальным представлениям связан с задачами представления функций суперпозицией других функций, нахождения функциональных базисов, исследования сложности представления функций в базисах, а также с использованием в электронике интегральных микросхем, содержащих в своем составе элементы “сложение по модулю 2”.

Пусть $E = \{0, 1\}$. Отображение $f: E^n \rightarrow E$ называют *n-местной булевой функцией*. Булева функция называется *нечетной*, если вектор функции содержит нечетное число единиц. Полиномиальным разложением функции f является представление f в виде $f = S_1 + \dots + S_m$, где сложение рассматривается по mod 2, а S_i построены некоторым специальным образом.

Достаточно часто слагаемые представляют бинарные термы, в построении которых используются только бинарные функции, символы переменных и остаточные разлагаемой функции.

Дадим строгое определение.

Как обычно,

$$x^\sigma = \begin{cases} x, & \text{если } \sigma = 1, \\ \bar{x}, & \text{если } \sigma = 0. \end{cases}$$

Пусть σ_1, σ_2 – константы, x_i, x_j – символы переменных, f_1 и f_2 – некоторые остаточные функции f . Тогда

Работа выполнена при частичной финансовой поддержке Российского фонда фундаментальных исследований (грант № 04-07-90178в).

- 1) если g – бинарная булева функция, то $g(x_i^{\sigma_1}, x_j^{\sigma_2}), g(x_i^{\sigma_1}, f_1), g(f_1, f_2)$ – *бинарные термы*;
- 2) если g – бинарная булева функция, B – бинарный терм, то $g(x_i^{\sigma_1}, B), g(f_1, B)$ – *бинарные термы*.

Среди представлений, в которых слагаемые являются бинарными термами, выделяется два типа: с использованием символов переменных и без использования символов переменных (т.е. слагаемые построены только из остаточных функций).

К представлениям первого типа относятся как хорошо известные: разложение функции по переменной или полином Жегалкина, – так и специальные, например, представление булевых функций в виде суммы по модулю 2 импликаций аргументов [1]. Большое число таких представлений можно найти в [2].

Необходимым условием того, что разложение такого вида можно применить ко всем булевым функциям, является нечетность функций g , используемых в построении бинарных термов. Это требование можно получить из следующего достаточно очевидного утверждения.

ПРЕДЛОЖЕНИЕ 1. *Булева функция $f(x_1, \dots, x_n)$ является нечетной тогда и только тогда, когда степень полинома Жегалкина, представляющего эту функцию, равна n .*

Мы рассматриваем полиномиальные разложения *второго типа* – представления вида

$$f(\tilde{x}_1, \tilde{x}_2, \dots, \tilde{x}_k) = \sum_{\tilde{\sigma}_1 \tilde{\sigma}_2 \dots \tilde{\sigma}_k} \alpha_{\tilde{\sigma}_1 \tilde{\sigma}_2 \dots \tilde{\sigma}_k} [g_1(f_{\tilde{x}_1}^{\tilde{\sigma}_1}, g_2(f_{\tilde{x}_2}^{\tilde{\sigma}_2}, \dots, g_{k-1}(f_{\tilde{x}_{k-1}}^{\tilde{\sigma}_{k-1}}, f_{\tilde{x}_k}^{\tilde{\sigma}_k}) \dots))], \quad (1)$$

где $g_1(y_1, y_2), \dots, g_{k-1}(y_1, y_2)$ – бинарные булевы функции, $\tilde{x}_1, \tilde{x}_2, \dots, \tilde{x}_k$ – некоторое разбиение множества переменных $\{x_1, \dots, x_n\}$ булевой функции f , $\tilde{\sigma}_1, \tilde{\sigma}_2, \dots, \tilde{\sigma}_k$ – наборы констант, причем $|\tilde{\sigma}_1| = |\tilde{x}_1|, |\tilde{\sigma}_2| = |\tilde{x}_2|, \dots, |\tilde{\sigma}_k| = |\tilde{x}_k|, f_{\tilde{x}_i}^{\tilde{\sigma}_i}$ – функция, полученная из f подстановкой констант набора $\tilde{\sigma}_i$ вместо переменных множества $\tilde{x}_i$ соответственно, $i = 1, 2, \dots, k$. Суммирование ведется по всевозможным значениям $\tilde{\sigma}_1, \dots, \tilde{\sigma}_k, \alpha_{\tilde{\sigma}_1 \dots \tilde{\sigma}_k}$ – константа из E .

В [3], [4] рассмотрены такие разложения при разбиении множества переменных на две части и показано, что любую булеву функцию можно представить суммой произведений или суммой дизъюнкций собственных подфункций.

Естественным является вопрос, а какие еще функции, сохраняющие возможность применения разложения к произвольной функции, могут быть использованы в построении слагаемых при любом разбиении множества переменных на k частей?

Как и для представлений первого типа, для разложений вида (1) справедливо

ПРЕДЛОЖЕНИЕ 2. *Если разложение (1) имеет место для любой булевой функции f , то функции $g_1, \dots, g_{k-1}$ являются нечетными.*

В предлагаемой работе показывается, что при разбиении переменных на две части в разложении (1) кроме конъюнкции или дизъюнкции можно использовать только импликации ($x \rightarrow y = (1101)$ или $x \leftarrow y = (1011)$), а для любого $k > 2$ найдется функция $f(x_1, \dots, x_n)$ и разбиение множества переменных на k частей, при которых такое разложение невозможно.

Основной результат. Вначале покажем, что при $k = 2$ в разложении (1) могут участвовать функции $g_1 = y_1 \rightarrow y_2$ и $g_1 = y_1 \leftarrow y_2$.

ТЕОРЕМА 1. Для любой булевой функции $f(\tilde{x}, \tilde{y})$ имеют место разложения

$$f(\tilde{x}, \tilde{y}) = \sum_{\tilde{\sigma}_1 \tilde{\sigma}_2} \alpha_{\tilde{\sigma}_1 \tilde{\sigma}_2} (f_{\tilde{x}}^{\tilde{\sigma}_1} \rightarrow f_{\tilde{y}}^{\tilde{\sigma}_2}) \quad u \quad f(\tilde{x}, \tilde{y}) = \sum_{\tilde{\sigma}_1 \tilde{\sigma}_2} \alpha_{\tilde{\sigma}_1 \tilde{\sigma}_2} (f_{\tilde{x}}^{\tilde{\sigma}_1} \leftarrow f_{\tilde{y}}^{\tilde{\sigma}_2}). \quad (2)$$

ДОКАЗАТЕЛЬСТВО проведем только для второго разложения. Для первого случая оно аналогично. Используем метод неопределенных коэффициентов. Из (2) имеем

$$\begin{aligned} f(\tilde{x}, \tilde{y}) &= \alpha_{\tilde{0}\tilde{0}}(f_{\tilde{x}}^{\tilde{0}} \cdot f_{\tilde{y}}^{\tilde{0}} + f_{\tilde{y}}^{\tilde{0}} + 1) + \dots + \alpha_{\tilde{0}\tilde{1}}(f_{\tilde{x}}^{\tilde{0}} \cdot f_{\tilde{y}}^{\tilde{1}} + f_{\tilde{y}}^{\tilde{1}} + 1) + \dots \\ &+ \alpha_{\tilde{1}\tilde{0}}(f_{\tilde{x}}^{\tilde{1}} \cdot f_{\tilde{y}}^{\tilde{0}} + f_{\tilde{y}}^{\tilde{0}} + 1) + \dots + \alpha_{\tilde{1}\tilde{1}}(f_{\tilde{x}}^{\tilde{1}} \cdot f_{\tilde{y}}^{\tilde{1}} + f_{\tilde{y}}^{\tilde{1}} + 1). \end{aligned}$$

Так как это равенство должно выполняться при всех значениях $\tilde{x}, \tilde{y}$, то его можно записать в матричном виде

$$\begin{pmatrix} f(\tilde{0}, \tilde{0}) \\ \vdots \\ f(\tilde{0}, \tilde{1}) \\ \vdots \\ f(\tilde{1}, \tilde{0}) \\ \vdots \\ f(\tilde{1}, \tilde{1}) \end{pmatrix} = G \cdot \begin{pmatrix} \alpha_{\tilde{0}, \tilde{0}} \\ \vdots \\ \alpha_{\tilde{0}, \tilde{1}} \\ \vdots \\ \alpha_{\tilde{1}, \tilde{0}} \\ \vdots \\ \alpha_{\tilde{1}, \tilde{1}} \end{pmatrix}, \quad (3)$$

где

$$G = \begin{pmatrix} f(\tilde{0}, \tilde{0}) \cdot f(\tilde{0}, \tilde{0}) + f(\tilde{0}, \tilde{0}) + 1 & \dots & f(\tilde{1}, \tilde{0}) \cdot f(\tilde{0}, \tilde{1}) + f(\tilde{0}, \tilde{1}) + 1 \\ \vdots & \ddots & \vdots \\ f(\tilde{0}, \tilde{1}) \cdot f(\tilde{0}, \tilde{0}) + f(\tilde{0}, \tilde{0}) + 1 & \dots & f(\tilde{1}, \tilde{1}) \cdot f(\tilde{0}, \tilde{1}) + f(\tilde{0}, \tilde{1}) + 1 \\ \vdots & \ddots & \vdots \\ f(\tilde{0}, \tilde{0}) \cdot f(\tilde{1}, \tilde{0}) + f(\tilde{1}, \tilde{0}) + 1 & \dots & f(\tilde{1}, \tilde{0}) \cdot f(\tilde{1}, \tilde{1}) + f(\tilde{1}, \tilde{1}) + 1 \\ \vdots & \ddots & \vdots \\ f(\tilde{0}, \tilde{1}) \cdot f(\tilde{1}, \tilde{0}) + f(\tilde{1}, \tilde{0}) + 1 & \dots & f(\tilde{1}, \tilde{1}) \cdot f(\tilde{1}, \tilde{1}) + f(\tilde{1}, \tilde{1}) + 1 \end{pmatrix}.$$

Матрица G имеет размерность $2^{|\tilde{\sigma}_1|+|\tilde{\sigma}_2|} \times 2^{|\tilde{\sigma}_1|+|\tilde{\sigma}_2|}$, $|\tilde{\sigma}_1| + |\tilde{\sigma}_2| = n$. Строки матрицы G занумеруем парами $(\tilde{i}, \tilde{j})$, которые являются всевозможными значениями переменных наборов $\tilde{x}$ и $\tilde{y}$ соответственно, столбцы – всевозможными значениями наборов $\tilde{\sigma}_1$ и $\tilde{\sigma}_2$. Элемент, стоящий на пересечении строки $(\tilde{i}_1, \tilde{j}_1)$ и столбца $(\tilde{\sigma}_1, \tilde{\sigma}_2)$, имеет вид $f(\tilde{\sigma}_1, \tilde{j}_1) \cdot f(\tilde{i}_1, \tilde{\sigma}_2) + f(\tilde{i}_1, \tilde{\sigma}_2) + 1$.

Покажем, что если элементарными преобразованиями в G получена нулевая строка, то в левой части (3) мы тоже получим нуль. Доказательство разобьем на две части. Сначала мы рассмотрим случай, когда в линейной комбинации участвует нечетное число строк, а затем четное количество строк.

Пусть в матрице G сумма строк с номерами $(\tilde{i}_1, \tilde{j}_1), \dots, (\tilde{i}_{2k+1}, \tilde{j}_{2k+1})$ дает нулевую строку. Нужно показать, что $f(\tilde{i}_1, \tilde{j}_1) + \dots + f(\tilde{i}_{2k+1}, \tilde{j}_{2k+1}) = 0$.

Далее мы будем рассматривать только элементы матрицы G , стоящие в строках с номерами $(\tilde{i}_1, \tilde{j}_1), \dots, (\tilde{i}_{2k+1}, \tilde{j}_{2k+1})$.

По предположению сумма элементов, взятых из произвольного столбца, равна нулю.

Рассмотрим столбцы с теми же номерами, что и взятые нами строки. Найдем сумму всех элементов, стоящих в выбранных столбцах.

Заметим, что если на пересечении строки $(\tilde{i}_l, \tilde{j}_l)$ и столбца $(\tilde{i}_s, \tilde{j}_s)$ стоит элемент $f(\tilde{i}_s, \tilde{j}_l) \cdot f(\tilde{i}_l, \tilde{j}_s) + 1$, то на пересечении строки $(\tilde{i}_s, \tilde{j}_s)$ и столбца $(\tilde{i}_l, \tilde{j}_l)$ стоит элемент $f(\tilde{i}_l, \tilde{j}_s) \cdot f(\tilde{i}_s, \tilde{j}_l) + 1$, при сложении этих элементов получим $f(\tilde{i}_s, \tilde{j}_l) + f(\tilde{i}_l, \tilde{j}_s)$.

В результате получим

$$\sum_{1 \leq s, l \leq 2k+1, s \neq l} f(\tilde{i}_l, \tilde{j}_s) + 1,$$

где 1 – сумма элементов, стоящих в строках и столбцах с одинаковыми номерами (таких элементов нечетное количество и все они равны 1, так как $f(i_s, j_s) \cdot f(i_s, j_s) + f(i_s, j_s) + 1 = 1$). По условию сумма в каждом столбце равна 0, следовательно,

$$\sum_{1 \leq s, l \leq 2k+1, s \neq l} f(\tilde{i}_l, \tilde{j}_s) = 1.$$

Рассмотрим столбцы с номерами $(\tilde{i}_1, \tilde{j}_1), (\tilde{i}_1, \tilde{j}_2), \dots, (\tilde{i}_1, \tilde{j}_{2k+1})$. Сумма всех элементов, стоящих в этих столбцах, тоже должна быть равна нулю. Имеем $2k+1$ строк и $2k+1$ столбцов, всего $4k^2 + 4k + 1$ – нечетное число элементов. На каждом месте стоит сумма трех слагаемых: $f(\tilde{i}_1, \tilde{j}_s) \cdot f(\tilde{i}_s, \tilde{j}_l) + f(\tilde{i}_s, \tilde{j}_l) + 1$, где $1 \leq s, l \leq 2k+1$.

Имеем

$$\sum_{1 \leq s, l \leq 2k+1} (f(\tilde{i}_1, \tilde{j}_s) \cdot f(\tilde{i}_s, \tilde{j}_l) + f(\tilde{i}_s, \tilde{j}_l) + 1) = 0,$$

следовательно,

$$\sum_{1 \leq s, l \leq 2k+1} f(\tilde{i}_1, \tilde{j}_s) \cdot f(\tilde{i}_s, \tilde{j}_l) = \sum_{1 \leq s, l \leq 2k+1} f(\tilde{i}_s, \tilde{j}_l) + 1.$$

Перепишем это равенство в виде

$$\begin{aligned} & f(\tilde{i}_1, \tilde{j}_1) \cdot \sum_{1 \leq l \leq 2k+1} f(\tilde{i}_1, \tilde{j}_l) + f(\tilde{i}_1, \tilde{j}_2) \cdot \sum_{1 \leq l \leq 2k+1} f(\tilde{i}_2, \tilde{j}_l) + \dots \\ & + f(\tilde{i}_1, \tilde{j}_{2k+1}) \cdot \sum_{1 \leq l \leq 2k+1} f(\tilde{i}_{2k+1}, \tilde{j}_l) = \sum_{1 \leq s, l \leq 2k+1} f(\tilde{i}_s, \tilde{j}_l) + 1. \end{aligned}$$

Рассмотрев столбцы с номерами $(\tilde{i}_2, \tilde{j}_1), \dots, (\tilde{i}_2, \tilde{j}_{2k+1})$, получим

$$\begin{aligned} & f(\tilde{i}_2, \tilde{j}_1) \cdot \sum_{1 \leq l \leq 2k+1} f(\tilde{i}_1, \tilde{j}_l) + f(\tilde{i}_2, \tilde{j}_2) \cdot \sum_{1 \leq l \leq 2k+1} f(\tilde{i}_2, \tilde{j}_l) + \dots \\ & + f(\tilde{i}_2, \tilde{j}_{2k+1}) \cdot \sum_{1 \leq l \leq 2k+1} f(\tilde{i}_{2k+1}, \tilde{j}_l) = \sum_{1 \leq s, l \leq 2k+1} f(\tilde{i}_s, \tilde{j}_l) + 1 \end{aligned}$$

и так далее до столбцов с номерами $(\tilde{i}_{2k+1}, \tilde{j}_1), \dots, (\tilde{i}_{2k+1}, \tilde{j}_{2k+1})$. В результате будем иметь систему из $2k+1$ равенств:

$$\begin{aligned} & f(\tilde{i}_t, \tilde{j}_1) \cdot \sum_{1 \leq l \leq 2k+1} f(\tilde{i}_1, \tilde{j}_l) + f(\tilde{i}_t, \tilde{j}_2) \cdot \sum_{1 \leq l \leq 2k+1} f(\tilde{i}_2, \tilde{j}_l) + \dots \\ & + f(\tilde{i}_t, \tilde{j}_{2k+1}) \cdot \sum_{1 \leq l \leq 2k+1} f(\tilde{i}_{2k+1}, \tilde{j}_l) = \sum_{1 \leq s, l \leq 2k+1} f(\tilde{i}_s, \tilde{j}_l) + 1, \quad t = 1, \dots, 2k+1. \end{aligned}$$

Если

$$\sum_{1 \leq s, l \leq 2k+1} f(\tilde{i}_s, \tilde{j}_l) = 1,$$

то учитывая, что

$$\sum_{1 \leq s, l \leq 2k+1, s \neq l} f(\tilde{i}_s, \tilde{j}_l) = 1,$$

получаем

$$\sum_{1 \leq s, l \leq 2k+1, s=l} f(\tilde{i}_s, \tilde{j}_l) = 0,$$

т.е.

$$f(\tilde{i}_1, \tilde{j}_1) + f(\tilde{i}_2, \tilde{j}_2) + \dots + f(\tilde{i}_{2k+1}, \tilde{j}_{2k+1}) = 0,$$

что и требовалось доказать.

Покажем, что предположение

$$\sum_{1 \leq s, l \leq 2k+1} f(\tilde{i}_s, \tilde{j}_l) = 0$$

приведет к противоречию. Обозначим

$$\sum_{1 \leq l \leq 2k+1} f(\tilde{i}_p, \tilde{j}_l) = x_p, \quad p = 1, \dots, 2k+1.$$

Очевидно,

$$\sum_{1 \leq s, l \leq 2k+1} f(\tilde{i}_s, \tilde{j}_l) = x_1 + x_2 + \dots + x_{2k+1}.$$

По предположению $x_1 + x_2 + \dots + x_{2k+1} = 0$, и, кроме того, имеем систему

$$f(\tilde{i}_t, \tilde{j}_1) \cdot x_1 + f(\tilde{i}_t, \tilde{j}_2) \cdot x_2 + \dots + f(\tilde{i}_t, \tilde{j}_{2k+1}) \cdot x_{2k+1} = 1, \quad t = 1, \dots, 2k+1, \quad (4)$$

откуда следует, что не все x_i , $i = 1, \dots, 2k+1$, равны 0.

Таким образом, среди x_i , $i = 1, \dots, 2k+1$, есть четное (не равное 0) число единиц. Не ограничивая общности, считаем, что это $x_1, \dots, x_{2r}$, $r \leq k$. Тогда из (4) получаем

$$f(\tilde{i}_t, \tilde{j}_1) + f(\tilde{i}_t, \tilde{j}_2) + \dots + f(\tilde{i}_t, \tilde{j}_{2r}) = 1, \quad t = 1, \dots, 2k+1.$$

Отсюда, учитывая то, какие значения принимают x_i , следует

$$\begin{aligned} \sum_{2r+1 \leq m \leq 2k+1} f(\tilde{i}_t, \tilde{j}_m) &= 0, & 1 \leq t \leq 2r, \\ \sum_{2r+1 \leq m \leq 2k+1} f(\tilde{i}_t, \tilde{j}_m) &= 1, & 2r+1 \leq t \leq 2k+1. \end{aligned} \quad (5)$$

Рассмотрим столбцы с номерами $(\tilde{i}_{2r+1}, \tilde{j}_{2r+1}), \dots, (\tilde{i}_{2r+1}, \tilde{j}_{2k+1})$. Сумма всех элементов, стоящих в этих столбцах, должна равняться нулю. Имеем

$$\sum_{1 \leq s \leq 2k+1} (f(\tilde{i}_{2r+1}, \tilde{j}_s) \cdot f(\tilde{i}_s, \tilde{j}_{2r+1}) + f(\tilde{i}_s, \tilde{j}_{2r+1}) + 1) = 0,$$

.....

$$\sum_{1 \leq s \leq 2k+1} (f(\tilde{i}_{2r+1}, \tilde{j}_s) \cdot f(\tilde{i}_s, \tilde{j}_{2k+1}) + f(\tilde{i}_s, \tilde{j}_{2k+1}) + 1) = 0.$$

Сложив эти равенства, получим

$$\begin{aligned}
& f(\tilde{i}_{2r+1}, \tilde{j}_1) \cdot \sum_{2r+1 \leq m \leq 2k+1} f(\tilde{i}_1, \tilde{j}_m) + \dots + f(\tilde{i}_{2r+1}, \tilde{j}_{2r}) \cdot \sum_{2r+1 \leq m \leq 2k+1} f(\tilde{i}_{2r}, \tilde{j}_m) \\
& + f(\tilde{i}_{2r+1}, \tilde{j}_{2r+1}) \cdot \sum_{2r+1 \leq m \leq 2k+1} f(\tilde{i}_{2r+1}, \tilde{j}_m) + \dots \\
& + f(\tilde{i}_{2r+1}, \tilde{j}_{2k+1}) \cdot \sum_{2r+1 \leq m \leq 2k+1} f(\tilde{i}_{2k+1}, \tilde{j}_m) \\
& + \sum_{2r+1 \leq m \leq 2k+1} f(\tilde{i}_1, \tilde{j}_m) + \dots + \sum_{2r+1 \leq m \leq 2k+1} f(\tilde{i}_{2r}, \tilde{j}_m) + \dots \\
& + \sum_{2r+1 \leq m \leq 2k+1} f(\tilde{i}_{2r+1}, \tilde{j}_m) + \dots + \sum_{2r+1 \leq m \leq 2k+1} f(\tilde{i}_{2k+1}, \tilde{j}_m) + 1 = 0.
\end{aligned}$$

Заменим в левой части суммы на соответствующие нули и единицы по (5), получим

$$\sum_{2r+1 \leq m \leq 2k+1} f(\tilde{i}_{2r+1}, \tilde{j}_m) = 0,$$

противоречие с (5) при $t = 2r + 1$.

Пусть в матрице G сумма строк с номерами $(\tilde{i}_1, \tilde{j}_1), \dots, (\tilde{i}_{2k}, \tilde{j}_{2k})$ дает нулевую строку. Нужно показать, что

$$f(\tilde{i}_1, \tilde{j}_1) + \dots + f(\tilde{i}_{2k}, \tilde{j}_{2k}) = 0.$$

Сложим элементы, стоящие в строках и столбцах с номерами $(\tilde{i}_1, \tilde{j}_1), \dots, (\tilde{i}_{2k}, \tilde{j}_{2k})$. Получим

$$\sum_{1 \leq l, t \leq 2k, l \neq t} f(\tilde{i}_l, \tilde{j}_t) = 0.$$

Далее для столбцов с номерами $(\tilde{i}_1, \tilde{j}_1), \dots, (\tilde{i}_1, \tilde{j}_{2k})$ получаем

$$\sum_{1 \leq s, l \leq 2k} (f(\tilde{i}_1, \tilde{j}_s) \cdot f(\tilde{i}_s, \tilde{j}_l) + f(\tilde{i}_s, \tilde{j}_l) + 1) = 0,$$

отсюда

$$\begin{aligned}
& f(\tilde{i}_1, \tilde{j}_1) \cdot \sum_{1 \leq l \leq 2k} f(\tilde{i}_1, \tilde{j}_l) + f(\tilde{i}_1, \tilde{j}_2) \cdot \sum_{1 \leq l \leq 2k} f(\tilde{i}_2, \tilde{j}_l) + \dots \\
& + f(\tilde{i}_1, \tilde{j}_{2k}) \cdot \sum_{1 \leq l \leq 2k} f(\tilde{i}_{2k}, \tilde{j}_l) = \sum_{1 \leq s, l \leq 2k} f(\tilde{i}_s, \tilde{j}_l).
\end{aligned}$$

Аналогичное равенство можно получить для столбцов с номерами $(\tilde{i}_t, \tilde{j}_1), \dots, (\tilde{i}_t, \tilde{j}_{2k})$ для $t = 2, \dots, 2k$. В результате снова имеем систему равенств

$$\begin{aligned}
& f(\tilde{i}_t, \tilde{j}_1) \cdot \sum_{1 \leq l \leq 2k} f(\tilde{i}_1, \tilde{j}_l) + f(\tilde{i}_t, \tilde{j}_2) \cdot \sum_{1 \leq l \leq 2k} f(\tilde{i}_2, \tilde{j}_l) + \dots \\
& + f(\tilde{i}_t, \tilde{j}_{2k}) \cdot \sum_{1 \leq l \leq 2k} f(\tilde{i}_{2k}, \tilde{j}_l) = \sum_{1 \leq s, l \leq 2k} f(\tilde{i}_s, \tilde{j}_l), \quad t = 1, \dots, 2k.
\end{aligned}$$

Если

$$\sum_{1 \leq s, l \leq 2k} f(\tilde{i}_s, \tilde{j}_l) = 0,$$

то доказывать нечего. Случай

$$\sum_{1 \leq s, l \leq 2k} f(\tilde{i}_s, \tilde{j}_l) = 1$$

опять приводит к противоречию.

Пусть

$$\sum_{1 \leq l \leq 2k} f(\tilde{i}_p, \tilde{j}_l) = x_p, \quad p = 1, \dots, 2k.$$

Тогда

$$f(\tilde{i}_t, \tilde{j}_1) \cdot x_1 + f(\tilde{i}_t, \tilde{j}_2) \cdot x_2 + \dots + f(\tilde{i}_t, \tilde{j}_{2k}) \cdot x_{2k} = 1, \quad t = 1, \dots, 2k. \quad (6)$$

Снова имеем

$$\sum_{1 \leq s, l \leq 2k} f(\tilde{i}_s, \tilde{j}_l) = x_1 + x_2 + \dots + x_{2k}.$$

По предположению $x_1 + \dots + x_{2k} = 1$, следовательно, имеем нечетное число нулей и нечетное число единиц. Не ограничивая общности, считаем, что $x_1 = \dots = x_{2l+1} = 1$, а $x_{2l+2} = \dots = x_{2k} = 0$. Из (6) имеем

$$\sum_{1 \leq m \leq 2l+1} f(\tilde{i}_t, \tilde{j}_m) = 1 \quad \text{для всех } t.$$

Рассмотрим столбцы с номерами $(\tilde{i}_1, \tilde{j}_{2r+2}), \dots, (\tilde{i}_1, \tilde{j}_{2k})$. Сумма всех элементов, стоящих в этих столбцах, должна равняться нулю. Имеем

$$\begin{aligned} & \sum_{1 \leq s \leq 2k} (f(\tilde{i}_1, \tilde{j}_s) \cdot f(\tilde{i}_s, \tilde{j}_{2r+2}) + f(\tilde{i}_s, \tilde{j}_{2r+2}) + 1) + \dots \\ & + \sum_{1 \leq s \leq 2k} (f(\tilde{i}_1, \tilde{j}_s) \cdot f(\tilde{i}_s, \tilde{j}_{2k}) + f(\tilde{i}_s, \tilde{j}_{2k}) + 1) = 0. \end{aligned}$$

Тогда

$$\begin{aligned} & f(\tilde{i}_1, \tilde{j}_1) \cdot \sum_{2r+2 \leq m \leq 2k} f(\tilde{i}_1, \tilde{j}_m) + f(\tilde{i}_1, \tilde{j}_2) \cdot \sum_{2r+2 \leq m \leq 2k} f(\tilde{i}_2, \tilde{j}_m) + \dots \\ & + f(\tilde{i}_1, \tilde{j}_{2k}) \cdot \sum_{2r+2 \leq m \leq 2k} f(\tilde{i}_{2k}, \tilde{j}_m) \\ & + \sum_{2r+2 \leq m \leq 2k} f(\tilde{i}_1, \tilde{j}_m) + \dots + \sum_{2r+2 \leq m \leq 2k} f(\tilde{i}_{2k}, \tilde{j}_m) \\ & = f(\tilde{i}_1, \tilde{j}_{2r+2}) + \dots + f(\tilde{i}_1, \tilde{j}_{2k}) + 1 = \sum_{2r+2 \leq m \leq 2k} f(\tilde{i}_1, \tilde{j}_m) + 1 = 0, \end{aligned}$$

следовательно,

$$\sum_{2r+2 \leq m \leq 2k} f(\tilde{i}_1, \tilde{j}_m) = 1,$$

но

$$\sum_{2r+2 \leq m \leq 2k} f(\tilde{i}_1, \tilde{j}_m) = 0,$$

получили $1 = 0$ – противоречие. Следовательно, предположение о том, что

$$\sum_{1 \leq s, l \leq 2k} f(\tilde{i}_l, \tilde{j}_s) = 1,$$

неверно. Теорема доказана.

Функции g_1 , которые допускают разложения для всех булевых функций, при $k = 2$ являются нечетными, и, кроме того, выполняется условие $g_1(1, 1) \neq 0$. Это условие можно получить из (1) непосредственно, взяв в качестве функции f константу 1.

Но, кроме того, справедлив следующий результат.

ПРЕДЛОЖЕНИЕ 3. *Для любой нечетной булевой функции $g_1(y_1, y_2)$ такой, что $g_1(1, 1) = 0$, существует не равная тождественной константе функция, которая не допускает представления в виде (1) при $k = 2$.*

ДОКАЗАТЕЛЬСТВО. Пусть $g_1(1, 1) = 0$. Тогда если вектор функции g_1 содержит одну 1, то можно взять, например, соответствующую селекторную функцию, а если три 1, то функцию $xy + 1$.

Таким образом, в случае, когда множество переменных разбивается на две части, можно сформулировать окончательный результат.

ТЕОРЕМА 2. *Разложение (1) при $k = 2$ имеет место для любой булевой функции тогда и только тогда, когда $g_1 \in \{\vee, \cdot, \leftarrow, \rightarrow\}$.*

Следующее утверждение показывает, что случаям $k = 2$ описываются все разложения, применимые к любой булевой функции.

ТЕОРЕМА 3. *Для любого $k > 2$, для любых нечетных бинарных булевых функций $g_1, \dots, g_{k-1}$ существует функция f и разбиение множества переменных на k частей, при котором не имеет место разложение (1).*

ДОКАЗАТЕЛЬСТВО. Такой функцией является, в частности, функция f , обладающая следующими свойствами:

- а) она симметрична;
- б) ее полином Жегалкина содержит нечетное количество слагаемых;
- в) каждая переменная входит в нечетное число слагаемых;
- г) для каждой переменной x_i в полиноме Жегалкина есть слагаемое x_i .

Если $k = 2m + 1$, то функцией, обладающей такими свойствами, является линейная функция $f = x_1 + x_2 + \dots + x_{2m+1}$. А при $k = 2m$ таковой является, в частности, функция, полученная из полинома Жегалкина, у которого свободный член равен нулю, коэффициенты при произведении $2m - 1$ переменных тоже равны 0, а коэффициенты при всех остальных возможных произведениях равны 1.

Очевидно, для таких функций выполняется $f_{x_i}^{\sigma_i}(0, \dots, 0) = \sigma_i$ и $f_{x_i}^{\sigma_i}(1, \dots, 1) = \sigma_i$. И тогда

$$\begin{aligned} 0 = f(0, \dots, 0) &= \sum_{\sigma_1 \dots \sigma_{2m+1}} a_{\sigma_1 \dots \sigma_{2m+1}} g_1(\sigma_1, g_2(\sigma_2, \dots, g_{2m}(\sigma_{2m}, \sigma_{2m+1}) \dots)) \\ &= f(1, \dots, 1) = 1. \end{aligned}$$

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] Г. С. Авсаркисян, “Представление булевых функций суммой по модулю 2 импликацией аргументов”, *Автоматика и вычислительная техника*, 1977, № 1, 8–11.
- [2] *Избранные вопросы булевых функций*, ред. С. Ф. Винокуров, Н. А. Перязев, Физматлит, М., 2001.
- [3] С. Ф. Винокуров, Н. А. Перязев, “Разложение булевых функций в сумму произведений собственных подфункций”, *Дискрет. матем.*, **5**:3 (1993), 102–104.
- [4] С. Ф. Винокуров, В. И. Пантелеев, “Полиномиальное представление булевых функций с использованием только остаточных функций”, *Труды XII Байкальской международной конференции*, **5**, Иркутск, 2001, 27–31.

А. С. Зинченко

Иркутский государственный педагогический университет

E-mail: azinchenko@gmail.com

Поступило

12.03.2005

Исправленный вариант

01.08.2006

В. И. Пантелеев

Иркутский государственный университет

E-mail: vp@math.isu.ru