Math-Net.Ru

Общероссийский математический портал

В. И. Пантелеев, Н. А. Перязев, О представлении функций k -значной логики суммой произведений остаточных подфункций, *Дискрет. матем.*, 2007, том 19, выпуск 2, 94–100

DOI: <https://doi.org/10.4213/dm24>

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: 54.164.48.24

26 апреля 2023 г., 06:13:05

О представлении функций k -значной логики суммой произведений остаточных подфункций

© 2007 г. В. И. Пантелеев, Н. А. Перязев

Множество переменных функции k -значной логики $f(x_1, \dots, x_n)$ разбивается на t частей, $t > 1$, и рассматривается полиномиальное представление функции f , в котором слагаемые являются произведением всех возможных остаточных подфункций, соответствующих взятому разбиению. Исследуются условия при которых любую функцию можно представить такой полиномиальной формой.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, грант 04-07-90178.

В теории функций k -значной логики, 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, то есть представления функций термами заданного вида. Среди таких представлений традиционно вызывают интерес так называемые полиномиальные представления.

Под полиномиальным, как правило, понимается представление функций k -значной логики в виде суммы по модулю k специальным образом построенных слагаемых. Среди известных таких представлений можно отметить полином Жегалкина для функций алгебры логики, в котором слагаемые представляют собой произведения некоторых переменных [1].

В данной работе рассматриваются полиномиальные представления, в которых слагаемые являются произведениями остаточных функций.

Как обычно под n -местной функцией k -значной логики будем понимать отображение из E_k^n в E_k , где $E_k = \{0, 1, \dots, k-1\}$.

Для функции $f(x_1, \dots, x_n)$ разобьем множество переменных $\{x_1, \dots, x_n\}$ на t частей $\tilde{u}_1, \dots, \tilde{u}_t$, $t > 1$. Функция $f(\tilde{u}_1, \dots, \tilde{u}_{i-1}, \tilde{\sigma}_i, \tilde{u}_{i+1}, \dots, \tilde{u}_t)$, полученная заменой переменных множества $\tilde{u}_i$ на константы из набора $\tilde{\sigma}_i$, называется остаточной по переменным $\tilde{u}_i$, $i \in \{1, \dots, t\}$, и $|\tilde{\sigma}_i| = |\tilde{u}_i|$ для всех i .

Найдем условия на k и t , при которых любую функцию k -значной логики $f(x_1, \dots, x_n)$ можно представить полиномиальной формой вида

$$\sum_{\tilde{\sigma}_1 \in E_k^{|\tilde{u}_1|}, \dots, \tilde{\sigma}_t \in E_k^{|\tilde{u}_t|}} \beta_{\tilde{\sigma}_1 \dots \tilde{\sigma}_t} f(\tilde{u}_1, \tilde{\sigma}_2, \dots, \tilde{\sigma}_t) f(\tilde{\sigma}_1, \tilde{u}_2, \dots, \tilde{\sigma}_t) \dots f(\tilde{\sigma}_1, \dots, \tilde{\sigma}_{t-1}, \tilde{u}_t) \quad (1)$$

или

$$\sum_{\tilde{\sigma}_1 \in E_k^{|\tilde{u}_1|}, \dots, \tilde{\sigma}_t \in E_k^{|\tilde{u}_t|}} \alpha_{\tilde{\sigma}_1 \dots \tilde{\sigma}_t} f(\tilde{\sigma}_1, \tilde{u}_2, \dots, \tilde{u}_t) f(\tilde{u}_1, \tilde{\sigma}_2, \dots, \tilde{u}_t) \dots f(\tilde{u}_1, \dots, \tilde{u}_{t-1}, \tilde{\sigma}_t) \quad (2)$$

где суммирование берется по всем возможным наборам $\tilde{\sigma}_1, \dots, \tilde{\sigma}_t$, коэффициенты $\alpha_{\tilde{\sigma}_1 \dots \tilde{\sigma}_t}$ и $\beta_{\tilde{\sigma}_1 \dots \tilde{\sigma}_t}$ принадлежат E_k , операции сложения и умножения выполняются по модулю k .

Вначале рассмотрим случай, когда $t = 2$, то есть множество переменных разбивается на 2 части. В этом случае разложения (1) и (2) совпадают.

Справедливо следующее утверждение.

Теорема 1. Для любой функции k -значной логики $f(\tilde{u}, \tilde{v})$ имеет место разложение

$$f(\tilde{u}, \tilde{v}) = \sum_{\tilde{\sigma} \in E_k^{|\tilde{u}|}, \tilde{\tau} \in E_k^{|\tilde{v}|}} \alpha_{\tilde{\sigma}\tilde{\tau}} f(\tilde{\sigma}, \tilde{v}) f(\tilde{u}, \tilde{\tau}), \quad \alpha_{\tilde{\sigma}\tilde{\tau}} \in E_k, \quad (3)$$

тогда и только тогда, когда

$$k = p_1 p_2 \dots p_s,$$

где $p_1, p_2, \dots, p_s$ — попарно различные простые числа, $s \geq 1$.

Справедливость данного разложения при $k = 2$ доказана в [2].

Для доказательства оставшейся части мы воспользуемся некоторыми результатами из теории колец [3, 4] и рассмотрим специальное полиномиальное представление матриц.

Ассоциативное кольцо R с единицей называется регулярным, если уравнение $axa = a$ разрешимо для всех $a \in R$. Регулярными кольцами являются тела и прямые суммы тел.

Предложение 1 ([3]). Конечные регулярные кольца исчерпываются прямыми суммами матричных колец над конечными полями.

Предложение 2 ([4]). Коммутативное кольцо является регулярным тогда и только тогда, когда оно не содержит ненулевых нильпотентных элементов.

Отсюда следует, что кольцо вычетов по модулю k является регулярным тогда и только тогда, когда k — простое число или произведение простых чисел.

Если R — произвольное ассоциативное кольцо с единицей, то через R_n обозначим кольцо матриц порядка n над кольцом R , а через $R_{m \times n}$ — множество всех матриц размерности $m \times n$ с элементами из кольца R .

Предложение 3 ([3]). Кольцо R_n регулярно тогда и только тогда, когда регулярно кольцо R .

На $R_{m \times n}$ определим операцию $\odot$ следующим образом: если $A = (a_{i,j})$, $B = (b_{i,j})$, то $A \odot B = C = (c_{i,j})$ и $c_{i,j} = a_{i,j} b_{i,j}$.

Выделим одно свойство введенной операции:

$$\begin{pmatrix} 0 & \dots & 0 & a_{1i} & 0 & \dots & 0 \\ 0 & \dots & 0 & a_{2i} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & a_{ni} & 0 & \dots & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \\ b_{i1} & b_{i2} & \dots & b_{in} \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{pmatrix} = \begin{pmatrix} a_{1i} & a_{1i} & \dots & a_{1i} \\ a_{2i} & a_{2i} & \dots & a_{2i} \\ \dots & \dots & \dots & \dots \\ a_{ni} & a_{ni} & \dots & a_{ni} \end{pmatrix} \odot \begin{pmatrix} b_{i1} & b_{i2} & \dots & b_{in} \\ b_{i1} & b_{i2} & \dots & b_{in} \\ \dots & \dots & \dots & \dots \\ b_{i1} & b_{i2} & \dots & b_{in} \end{pmatrix}.$$

Для $A \in R_{m \times n}$ через A_i (A^j) обозначим матрицу размерности $m \times n$, полученную из A заменой всех строк (столбцов) на строку (столбец) матрицы A с номером i (с номером j).

Доказательство теоремы будет основано на следующей лемме.

Лемма 1. Пусть R — регулярное кольцо. Для любой матрицы $A \in R_{m \times n}$ найдутся такие $\sigma_{ij} \in R$, что

$$A = \sum_{i=1}^m \sum_{j=1}^n \sigma_{ij} A_i \odot A^j. \quad (4)$$

Доказательство. Взяв нулевой столбец или строку и, приписывая справа или снизу A нужное число раз, мы получим квадратную матрицу C . Пусть для определенности порядок этой матрицы равен m , то есть $C \in R_m$.

Так как кольцо R_m регулярно, найдется такая матрица $B \in R_m$, что $C = CBC$. Простой подсчет показывает, что столбцы (строки) матрицы CB (BC) являются линейными комбинациями (с коэффициентами из R) столбцов (строк) матрицы C .

Если $C = (c_{i,j})$, $CB = D = (d_{i,j})$, то

$$\begin{aligned} CBC &= \sum_{i=1}^m \begin{pmatrix} 0 & \dots & 0 & d_{1i} & 0 & \dots & 0 \\ 0 & \dots & 0 & d_{2i} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & d_{mi} & 0 & \dots & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \\ c_{i1} & c_{i2} & \dots & c_{im} \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{pmatrix} \\ &= \sum_{i=1}^m \begin{pmatrix} d_{1i} & d_{1i} & \dots & d_{1i} \\ d_{2i} & d_{2i} & \dots & d_{2i} \\ \dots & \dots & \dots & \dots \\ d_{mi} & d_{mi} & \dots & d_{mi} \end{pmatrix} \begin{pmatrix} c_{i1} & c_{i2} & \dots & c_{im} \\ c_{i1} & c_{i2} & \dots & c_{im} \\ \dots & \dots & \dots & \dots \\ c_{i1} & c_{i2} & \dots & c_{im} \end{pmatrix} \end{aligned}$$

Для любого i столбец $(d_{1i} d_{2i} \dots d_{mi})^T$ является линейной комбинацией столбцов матрицы C с коэффициентами из R . Заменяя столбцы линейными комбинациями и раскрыв скобки, получим, что

$$C = CBC = \sum_{i=1}^m \sum_{j=1}^m \sigma_{ij} C^i \odot C_j, \quad \sigma_{ij} \in R.$$

После этого, удалив из матриц C , C^i , C_j лишние столбцы, получим нужный результат. Лемма доказана.

Укажем один способ нахождения коэффициентов разложения (4) в случае, если кольцо R является полем.

Зафиксируем в матрице A размерности $m \times n$ матрицу M , соответствующую базисному минору, стоящему на пересечении строк с номерами $i_1, \dots, i_s$ и столбцов с номерами $j_1, \dots, j_s$. Вычислим M^{-1} . Построим матрицу B размерности $n \times m$, у которой на пересечении столбцов с номерами $i_1, \dots, i_s$ и строк с номерами $j_1, \dots, j_s$ стоит блок M^{-1} , а остальные элементы равны 0. Тогда в произведении AB столбец с номером p является линейной комбинацией базисных столбцов матрицы A , коэффициенты которой являются элементами столбца p матрицы B . Значит, элемент $b_{i,j}$ из матрицы B является коэффициентом перед $A^i \odot A_j$ в разложении (4).

Вернемся к доказательству теоремы.

Докажем достаточность. Представим функцию f матрицей F размерности $|\tilde{u}| \times |\tilde{v}|$. Тогда $f(\tilde{\sigma}, \tilde{v})$ при фиксированном наборе $\tilde{\sigma}$ — это строка матрицы F , а $f(\tilde{u}, \tilde{\tau})$ при фиксированном наборе $\tilde{\tau}$ — это столбец матрицы F . Возможность разложения следует из возможности представления матрицы полиномиальной формой (4).

Докажем необходимость. Если

$$k = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_l^{\alpha_l},$$

где $p_1, \dots, p_l$ — попарно различные простые числа и по крайней мере один из показателей больше единицы, то кольцо $\langle E_k; +, \cdot \rangle$ не является регулярным. Тогда такое кольцо содержит нильпотентный элемент $a \in E_k$, степень нильпотентности которого равна 2 и функция

$$f(x, y) = x \cdot y + a$$

не представима в виде

$$f(x, y) = \sum_{\sigma \in E_k, \tau \in E_k} \alpha_{\sigma\tau} f(\sigma, y) \cdot f(x, \tau).$$

Теорема доказана.

Приведем один пример такого разложения.

Пример 1. Двухместная функция 5-значной логики $f(x, y)$ задана таблицей

$x \backslash y$	0	1	2	3	4
0	4	0	0	3	0
1	1	2	0	0	2
2	4	0	1	3	0
3	4	0	3	3	0
4	2	3	1	1	3

Разобьем переменные на две части, x и y .

Для определения коэффициентов разложения (3) воспользуемся методом предложенным после доказательства леммы.

Выберем базисный минор, образованный строками и столбцами с номерами 1, 2, 3. Ему соответствует матрица

$$M = \begin{pmatrix} 4 & 0 & 0 \\ 1 & 2 & 0 \\ 4 & 0 & 1 \end{pmatrix}.$$

Тогда матрица M^{-1} имеет вид

$$\begin{pmatrix} 4 & 0 & 0 \\ 3 & 3 & 0 \\ 4 & 0 & 1 \end{pmatrix}.$$

Этот блок будет стоять на пересечении строк и столбцов с номерами 1, 2, 3. Значит ненулевые коэффициенты являются элементами с индексами (1, 1), (2, 1), (2, 2), (3, 1), (3, 3) и в разложении (3) останутся слагаемые: $f(x, 0)f(0, y)$ (первый столбец, первая строка); $f(x, 1)f(0, y)$ (второй столбец, первая строка); $f(x, 2)f(0, y)$ (третий столбец, первая строка); $f(x, 1)f(1, y)$ (второй столбец, вторая строка); $f(x, 2)f(2, y)$ (третий столбец, третья строка).

Функцию можно представить полиномиальной формой

$$\begin{aligned} f(x, y) = & 4f(x, 0)f(0, y) + 3f(x, 1)f(0, y) + 4f(x, 2)f(0, y) \\ & + 3f(x, 1)f(1, y) + f(x, 2)f(2, y) \end{aligned}$$

Теорема 2. Для любой функции $f(x_1, \dots, x_n)$ для любого разбиения

$$\{x_1, \dots, x_n\} = \tilde{u}_1 \cup \dots \cup \tilde{u}_t, \quad t > 1,$$

равенство

$$\begin{aligned} & f(\tilde{u}_1, \dots, \tilde{u}_t) \\ = & \sum_{\tilde{\sigma}_1 \in E_k^{|\tilde{u}_1|}, \dots, \tilde{\sigma}_t \in E_k^{|\tilde{u}_t|}} \beta_{\tilde{\sigma}_1 \dots \tilde{\sigma}_t} f(\tilde{u}_1, \tilde{\sigma}_2, \dots, \tilde{\sigma}_t) f(\tilde{\sigma}_1, \tilde{u}_2, \dots, \tilde{\sigma}_t) \dots f(\tilde{\sigma}_1, \dots, \tilde{\sigma}_{t-1}, \tilde{u}_t) \end{aligned}$$

имеет место тогда и только тогда, когда $k = p_1 p_2 \dots p_s$, где $p_1, p_2, \dots, p_s$ — попарно различные простые числа, $s \geq 1$.

Доказательство. Докажем достаточность. Разбиение $\{x_1, \dots, x_n\} = \tilde{u}_1 \cup \dots \cup \tilde{u}_t$ и соответствующее ему полиномиальное представление можно получить следующим образом: сначала выполняем разбиение $\{x_1, \dots, x_n\} = \tilde{u}_1 \cup \tilde{v}_1$ и рассматриваем представление (3) для этого разбиения, затем переменные из $\tilde{v}_1$ разбиваем на $\tilde{u}_2 \cup \tilde{v}_2$ и для функций, зависящих от $\tilde{v}_1$ и полученных при первом разбиении, используем представление (3). Этот процесс продолжаем до тех пор, пока не получим нужного разбиения и (с использованием дистрибутивности умножения относительно сложения) соответствующего полиномиального представления.

Докажем необходимость. Если элемент $a \in E_k$ является нильпотентным, степень нильпотентности которого равна 2, то, очевидно, $a^t = 0$ для всех $t > 2$. Тогда функция $f(x_1, x_2, \dots, x_t) = x_1 x_2 \dots x_t + a$ не представима нужной полиномиальной формой при разбиении $\{x_1, \dots, x_t\} = \{x_1\} \cup \dots \cup \{x_t\}$. Теорема доказана.

Теорема 3. Для любого k и любого $t, t > 2$, найдется функция $f(x_1, \dots, x_n)$ и разбиение $\{x_1, \dots, x_n\} = \tilde{u}_1 \cup \dots \cup \tilde{u}_t$, при котором f нельзя представить в виде

$$\begin{aligned} & f(\tilde{u}_1, \dots, \tilde{u}_t) \\ = & \sum_{\tilde{\sigma}_1 \in E_k^{|\tilde{u}_1|}, \dots, \tilde{\sigma}_t \in E_k^{|\tilde{u}_t|}} \alpha_{\tilde{\sigma}_1 \dots \tilde{\sigma}_t} f(\tilde{\sigma}_1, \tilde{u}_2, \dots, \tilde{u}_t) f(\tilde{u}_1, \tilde{\sigma}_2, \dots, \tilde{u}_t) \dots f(\tilde{u}_1, \dots, \tilde{u}_{t-1}, \tilde{\sigma}_t). \end{aligned}$$

Доказательство. Надо рассмотреть случай, когда $k = p_1 \dots p_s$, $s > 0$ и $p_1, \dots, p_s$ — различные простые числа. Для булевых функций это показано в [5]. Для остальных значений k рассмотрим функцию

$$f(x_1, x_2, \dots, x_t) = x_1 x_2 \dots x_t$$

и разбиение $\{x_1, x_2, \dots, x_t\} = \{x_1\} \cup \dots \cup \{x_t\}$.

Предположим, что эту функцию можно представить необходимой полиномиальной формой.

При нечетном t получим, что

$$\begin{aligned} f(1, 1, \dots, 1) &= 1, \\ f(1, \dots, 1, \sigma_i, 1, \dots, 1) &= \sigma_i, \\ f(k-1, k-1, \dots, k-1) &= (k-1)^t = k-1 \neq 1, \\ f(k-1, \dots, k-1, \sigma_i, k-1, \dots, k-1) &= \sigma_i \end{aligned}$$

и

$$\begin{aligned} 1 &= f(1, 1, \dots, 1) \\ &= \sum_{\sigma_1 \in E_k, \dots, \sigma_t \in E_k} \alpha_{\sigma_1 \dots \sigma_t} f(\sigma_1, 1, \dots, 1) f(1, \sigma_2, \dots, 1) \dots f(1, \dots, 1, \sigma_t) \\ &= \sum_{\sigma_1 \in E_k, \dots, \sigma_t \in E_k} \alpha_{\sigma_1 \dots \sigma_t} \sigma_1 \sigma_2 \dots \sigma_t \\ &= \sum_{\sigma_1 \in E_k, \dots, \sigma_t \in E_k} \alpha_{\sigma_1 \dots \sigma_t} f(\sigma_1, k-1, \dots, k-1) f(k-1, \sigma_2, \dots, k-1) \dots f(k-1, \dots, k-1, \sigma_t) \\ &= f(k-1, k-1, \dots, k-1) = k-1. \end{aligned}$$

Получаем противоречие.

При четных t

$$\begin{aligned} x_1 \dots x_t &= \sum_{\sigma_1 \in E_k, \dots, \sigma_t \in E_k} \alpha_{\sigma_1 \dots \sigma_t} f(\sigma_1, x_2, \dots, x_t) f(x_1, \sigma_2, x_3, \dots, x_t) \dots f(x_1, \dots, x_{t-1}, \sigma_t) \\ &= (x_1 \dots x_t)^{t-1} \sum_{\sigma_1 \in E_k, \dots, \sigma_t \in E_k} \alpha_{\sigma_1 \dots \sigma_t} \sigma_1 \sigma_2 \dots \sigma_t. \end{aligned}$$

При $x_1 = \dots = x_t = 1$ получим равенство

$$\sum_{\sigma_1 \in E_k, \dots, \sigma_t \in E_k} \alpha_{\sigma_1 \dots \sigma_t} \sigma_1 \sigma_2 \dots \sigma_t = 1,$$

и значит, равенство

$$x_1 \dots x_t = (x_1 \dots x_t)^{t-1}$$

должно быть справедливо для всех $x_1, \dots, x_t$ (или $a^{t-1} = a$ для всех $a \in E_k$).

Пусть $p_1 = \max\{p_1, p_2, \dots, p_s\}$. С учетом того, что $p_1, p_2, \dots, p_s$ — простые числа и

$$a^{t-1} = a \pmod{p_1 \dots p_s} \iff a^{t-1} = a \pmod{p_i},$$

получаем, что $t > p_1$.

Рассмотрим функцию $h(x_1, \dots, x_t) = x_1 + x_2 + \dots + x_{p_1+1}$. Для нее остаточная функция $h_{x_i}^{\sigma_i}$ по i -му аргументу, $1 \leq i \leq p_1 + 1$, равна

$$x_1 + \dots + x_{i-1} + \sigma_i + x_{i+1} + \dots + x_{p_1+1},$$

для остальных значений i остаточная функция равна $x_1 + x_2 + \dots + x_{p_1+1}$.

Если $s > 1$, то при $x_1 = x_2 = \dots = x_{p_1+1} = p_2 \dots p_s$ получим равенство

$$p_2 \dots p_s = \sum_{\sigma_1 \dots \sigma_t} \alpha_{\sigma_1 \dots \sigma_t} \sigma_1 \dots \sigma_{p_1+1} (p_2 \dots p_s)^{t-(p_1+1)}.$$

При $x_1 = x_2 = \dots = x_{p_1+1} = (k-1)p_2 \dots p_s$ получим равенство

$$(k-1)p_2 \dots p_s = \sum_{\sigma_1 \dots \sigma_t} \alpha_{\sigma_1 \dots \sigma_t} \sigma_1 \dots \sigma_{p_1+1} ((k-1)p_2 \dots p_s)^{t-(p_1+1)}.$$

С учетом четностей и того, что $p_1 = \max\{p_1, p_2, \dots, p_s\}$, имеем противоречие $1 = k - 1$.

Если $s = 1$, то также получаем противоречие, так как $x_1 = x_2 = \dots = x_{p_1+1} = 1$ и $x_1 = x_2 = \dots = x_{p_1+1} = k - 1$. Теорема доказана.

Список литературы

1. Жегалкин И. И., Арифметизация символической логики. *Матем. сб.* (1929) **36**, 305–338.
2. Винокуров С. Ф., Перязев Н. А., Разложение булевых функций в сумму произведений собственных подфункций. *Дискретная математика* (1993) **5**, №3, 121–123.
3. Скорняков Л. А., *Дедекиндовы структуры с дополнениями и регулярные кольца*. Физматгиз, Москва, 1961.
4. Goodearl K. R., *Von Neumann regular rings*. Pitman, London, 1979.
5. Винокуров С. Ф., Пантелеев В. И., Полиномиальное представление булевых функций с использованием только остаточных функций. В сб.: *Труды XII Байкальской международной конф.*, т. 5. Иркутск, 2001, с. 27–31.

Статья поступила 30.01.2006.