ИЗВЕСТИЯ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ

1998 МАТЕМАТИКА № 1 (428)

КРАТКИЕ СООБЩЕНИЯ

УДК 519.71:95

В.И. ПАНТЕЛЕЕВ

ПОЛИНОМИАЛЬНЫЕ РАЗЛОЖЕНИЯ k-ЗНАЧНЫХ ФУНКЦИЙ ПО ОПЕРАТОРАМ ДИФФЕРЕНЦИРОВАНИЯ И НОРМАЛИЗАЦИИ

Различные представления k-значных функций (функций k-значной логики) представляют интерес в связи с использованием в дискретных вычислительных устройствах [1].

Как известно, произвольную k-значную функцию при простом k можно представить в виде полинома по $\mod k$. Будем называть полиномиальной формой сумму по $\mod k$ конечного числа определенным образом построенных слагаемых.

В последнее время получены различные полиномиальные разложения для булевых функций [2]. В данной работе показывается возможность обобщения этих результатов на случай k-значных функций при простом k.

Будем говорить в дальнейшем функция $f(x_1,\dots,x_n)$, имея в виду, что речь идет о k-значной функции $f(x_1,\dots,x_n)$ при простом k. Используемые в работе операции "+", "$\cdot$" — это сложение и умножение по $\mod k$. Операция "$-$" определяется как противоположная операции "+". Операции $x^{(\alpha)}$ определяются следующим образом:

$$x^{(\alpha)} = k-1-x+\alpha.$$

Функцию $f(x_1,\dots,x_n)$ будем называть невырожденной, если

$$\sum_{\beta_1\dots\beta_n} f(\beta_1,\dots,\beta_n) \neq 0, \quad \beta_i\in\{0,1,\dots,k-1\},$$

и вырожденной в противном случае. При $k=2$ невырожденными будут те и только те функции, у которых вектор значений содержит нечетное число единиц, а в общем случае функция $f(x_1,\dots,x_n)$ является невырожденной тогда и только тогда, когда полином, представляющий эту функцию, имеет степень $n(k-1)$.

Для n-местной функции $f(x_1,\dots,x_n)$ индуктивно определим операторы дифференцирования ($\mathbf{d}$), нормализации ($\mathbf{p}$) и смешанные по ($\mathbf{p}$) и ($\mathbf{d}$):

$$p^{\beta}_{x_j} f(x_1,\dots x_j,\dots,x_n) = f(x_1,\dots x_j^{(\beta)},\dots,x_n), \quad 0\le\beta\le k-1;$$

$$d^{0}_{x_j} f(x_1,\dots x_j,\dots,x_n) = f(x_1,\dots x_j,\dots,x_n);$$

$$d^{\beta}_{x_j} f(x_1,\dots x_j,\dots,x_n) = f(x_1,\dots x_j,\dots,x_n) + f(x_1,\dots x_j-\beta,\dots,x_n), \quad 1\le\beta\le k-1;$$

$$h^{\beta_1,\dots,\beta_m}_{x_1,\dots,x_m} f(x_1,\dots,x_m,\dots x_n) = h^{\beta_1}_{x_1}(h^{\beta_2,\dots,\beta_m}_{x_2,\dots,x_m} f(x_1,\dots,x_m,\dots x_n)), \quad m\le n, \ \ h\in\{p,d,t\}.$$

Зафиксируем набор $t = (t_1, \dots, t_m)$, где $t_i \in \{p, d\}$. Однородно смешанные по p и d операторы t определяются так:

$$t^{\beta}_{x_j} f(x_1, \dots x_j, \dots, x_n) = \begin{cases} d^{\beta}_{x_j} f(x_1, \dots x_j, \dots, x_n), & \text{если } t_j = d; \\ p^{\beta}_{x_j} f(x_1, \dots x_j, \dots, x_n), & \text{если } t_j = p. \end{cases}$$

$$t^{\beta_1, \dots, \beta_m}_{x_1, \dots, x_m} f(x_1, \dots, x_m, \dots, x_n) = t^{\beta_1}_{x_1}(t^{\beta_2, \dots, \beta_m}_{x_2, \dots, x_m} f(x_1, \dots, x_m, \dots, x_n)).$$

Для функции $g(x_1, \dots, x_n)$ и оператора $h \in \{p, d, t\}$ определим матрицу $G[h(g)]$:

$$G = \begin{pmatrix} h^{0,\dots,0}_{x_1,\dots,x_n} g(0, \dots, 0) & \dots & h^{k-1,\dots,k-1}_{x_1,\dots,x_n} g(0, \dots, 0) \\ h^{0,\dots,0}_{x_1,\dots,x_n} g(0, \dots, 1) & \dots & h^{k-1,\dots,k-1}_{x_1,\dots,x_n} g(0, \dots, 1) \\ \dots & \dots & \dots \\ h^{0,\dots,0}_{x_1,\dots,x_n} g(k-1, \dots, k-1) & \dots & h^{k-1,\dots,k-1}_{x_1,\dots,x_n} g(k-1, \dots, k-1) \end{pmatrix}.$$

Сформулируем основной результат.

Теорема. *Пусть $g(x_1, \dots, x_n)$ — фиксированная функция, тогда любую функцию $f(x_1, \dots, x_n)$ можно представить полиномиальной формой вида:*

$$f(x_1, \dots, x_n) = \sum_{\beta_1, \dots, \beta_n} a_{\beta_1, \dots, \beta_n} h^{\beta_1, \dots, \beta_n}_{x_1, \dots, x_n} g(x_1, \dots, x_n), \tag{1}$$

где $h \in \{p, d, t\}$, $a_{\beta_1, \dots, \beta_n} \in \{0, 1, \dots, k-1\}$, $\beta_i \in \{0, 1, \dots, k-1\}$ тогда и только тогда, когда функция $g(x_1, \dots, x_n)$ невырожденная. Если $h = p$, то матрица коэффициентов

$$A = [G[p(g)]]^{k-1} \cdot F \cdot \left(\sum_{\beta_1, \dots, \beta_n} g(\beta_1, \dots, \beta_n) \right)^{-1},$$

где F — вектор-столбец значений функции $f(x_1, \dots, x_n)$.

Перед доказательством теоремы введем некоторые понятия и докажем лемму. Назовем систему чисел $\{a_1, \dots, a_m\}$ невырожденной, если

$$a_1 + \dots + a_m \neq 0.$$

Введем матрицы порядка k^n, которые будем называть циркулянт циркулянтов n-го порядка, индуктивно определяемые следующим образом: при $n = 1$ это циркулянт вида

$$\begin{pmatrix} a_0 & a_1 & a_2 & a_3 & \dots & a_{k-1} \\ a_{k-1} & a_0 & a_1 & a_2 & \dots & a_{k-2} \\ a_{k-2} & a_{k-1} & a_0 & a_1 & \dots & a_{k-3} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_1 & a_2 & a_3 & a_4 & \dots & a_0 \end{pmatrix}, \qquad a_i \in \{0, 1, \dots, k-1\}.$$

Пусть $A_0, \dots, A_{k-1}$ — циркулянты циркулянтов $(l-1)$-го порядка. Тогда циркулянт циркулянтов (l)-го порядка имеет следующий вид:

$$\begin{pmatrix} A_0 & A_1 & A_2 & A_3 & \dots & A_{k-1} \\ A_{k-1} & A_0 & A_1 & A_2 & \dots & A_{k-2} \\ A_{k-2} & A_{k-1} & A_0 & A_1 & \dots & A_{k-3} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ A_1 & A_2 & A_3 & A_4 & \dots & A_0 \end{pmatrix}$$

Лемма 1. *Определитель циркулянта циркулянтов n-го порядка отличен от нуля тогда и только тогда, когда система чисел, образованная элементами первой строки, является невырожденной.*

Доказательство. Пусть $E_{\tau_0\ldots\tau_{n-2}\tau_{n-1}}$ — циркулянт циркулянтов n-го порядка, элементами которого являются нули и единицы. Индекс τ_{n-1} показывает, что среди $A_0,\ldots,A_{k-1}$ ненулевой будет матрица $A_{\tau_{n-1}}$, где A_i — циркулянты циркулянтов $n-1$-го порядка и так далее до матриц размерности k. Несложно показать, что такие матрицы обладают свойствами:

1. $E_{i_1\ldots i_n}\cdot E_{j_1\ldots j_n}=E_{j_1\ldots j_n}\cdot E_{i_1\ldots i_n}$;
2. $E^k_{i\ldots j}=E_{0\ldots 0}=E$.

Тогда циркулянт циркулянтов

$$G=\sum_{\tau_1\ldots\tau_n}a_{\tau_1\ldots\tau_n}\cdot E_{\tau_1\ldots\tau_n},$$

где $a_{\tau_1\ldots\tau_n}$ — элементы первой строки матрицы G;

$$G^k=\sum_{\tau_1\ldots\tau_n}a^k_{\tau_1\ldots\tau_n}\cdot E^k_{\tau_1\ldots\tau_n}=\sum_{\tau_1\ldots\tau_n}a_{\tau_1\ldots\tau_n}\cdot E=\Bigl(\sum_{\tau_1\ldots\tau_n}a_{\tau_1\ldots\tau_n}\Bigr)\cdot E.$$

И так как $|G|^k=|G|$, то $|G|\neq 0$ тогда и только тогда, когда

$$\sum_{\tau_1\ldots\tau_n}a_{\tau_1\ldots\tau_n}\neq 0,$$

т.е. система чисел, образованная элементами первой строки, должна быть невырожденной. □

При доказательстве теоремы рассмотрим три случая, соответствующие различным операторам.

a) $h=p$. Доказательство проведем методом неопределенных коэффициентов.

Разложение (1) перепишем в матричном виде:

$$F=G\cdot A,$$

где F — вектор-столбец значений функции $f(x_1,\ldots,x_n)$, A — матрица коэффициентов разложения (1), $G=G[p(g)]$.

Так как $i^{(j)}=(i+1)^{(j+1)}$, то матрица G является циркулянтом циркулянтов n-го порядка.

По лемме, учитывая, что $|G|\neq 0$ тогда и только тогда, когда функция $g(x_1,\ldots,x_n)$ невырожденная, получаем справедливость первого утверждения теоремы.

Кроме того, для невырожденных функций выполняется и следующее утверждение, справедливость которого установили при доказательстве леммы: *k-я степень циркулянта циркулянтов, полученного из невырожденной функции, равна единичной матрице, умноженной на число, равное сумме всех значений этой функции.*

Умножим равенство $G\cdot A=F$ слева на G^{k-1}, получим

$$\sum_{\beta_1,\ldots,\beta_n}g(\beta_1,\ldots,\beta_n)\cdot A=G^{k-1}\cdot F.$$

И, следовательно,

$$A=G^{k-1}\cdot F\cdot\Bigl(\sum_{\beta_1,\ldots,\beta_n}g(\beta_1,\ldots,\beta_n)\Bigr)^{-1}.$$

b) Перейдем к доказательству случая $h=d$.

Матричная запись равенства (1) будет следующей:

$$F=G\cdot A,\quad \text{где } G=G[d(g)].$$

Можно показать, что G получена из циркулянта циркулянтов элементарными преобразованиями, и определитель ее будет отличен от нуля тогда и только тогда, когда функция $g(x_1,\ldots,x_n)$ является невырожденной.

Матрицу коэффициентов можно найти с помощью обратной матрицы.

c) Доказательство этого случая сводится к случаям a) и b).

Автор выражает признательность Перязеву Н.А. за полезные замечания.

Литература

1. Поспелов Д.А. *Логические методы анализа и синтеза схем.* – М.: Энергия, 1974. – 368 с.
2. Винокуров С.Ф., Перязев Н.А. *Полиномиальная декомпозиция булевых функций по образам однородных операторов от невырожденных функций* // Изв. вузов. Математика. – 1996. – № 1. – С. 17–21.

Иркутский государственный университет

Поступили
полный текст 29.04.1993
краткое сообщение 26.05.1997