ЛОГИЧЕСКИЕ МЕТОДЫ В ИНФОРМАТИКЕ
(Вычислительные системы)
1993 год Выпуск 148

УДК 519.71:95

ПОЛИНОМИАЛЬНАЯ ДЕКОМПОЗИЦИЯ БУЛЕВЫХ ФУНКЦИЙ ПО ОБРАЗАМ ОДНОРОДНЫХ ОПЕРАТОРОВ ОТ НЕВЫРОЖДЕННЫХ ФУНКЦИЙ

С.Ф.Винокуров, Н.А.Перязев

В работе рассматриваются полиномиальная декомпозиция и полиномиальные канонические формы булевых функций. Для этих целей плодотворным оказался операторный подход. Многие из разложений, рассмотренные в [1-4], являются частными случаями разложений, вводимых ниже.

Индуктивно определим операторы, используемые в дальнейшем изложении:

$$b^0_{x_1} f(x) = f(0, x_2, \ldots, x_n),\quad b^1_{x_1} f(x) = f(1, x_2, \ldots, x_n),$$

$$p^0_{x_1} f(x) = f(\overline{x}_1, x_2, \ldots, x_n),$$

$$d^0_{x_1} f(x) = f(x) \oplus f(x_1, x_2, \ldots, x_n),$$

$$h^1_{x_1} f(x) = f(x) \quad \text{для} \quad h \in \{p, d\},$$

$$h^{\tau_1, \ldots, \tau_m}_{x_1, \ldots, x_m} f(x_1, \ldots, x_n) =$$

$$= h^{\tau_m}_{x_m} \left[h^{\tau_1, \ldots, \tau_{m-1}}_{x_1, \ldots, x_{m-1}} f(x_1, \ldots, x_n) \right]$$

где $m \le n$, для всех $h \in \{b, d, p\}$.

Операторы b, p, d называются соответственно операторами подстановки, нормализации, дифференцирования.

Введем также однородно смешанные из p и d операторы t, которые определяются по набору $(t_1,\dots,t_n)$, где $t_i \in \{p,d\}$, следующим образом:

$$t^1_{x_i} f(x) = f(x)\,,\quad t^0_{x_i} f(x) = \begin{cases} p^0_{x_i} f(x)\,, & \text{если} \quad t_i = p; \\ d^0_{x_i} f(x)\,, & \text{если} \quad t_i = d; \end{cases}$$

$$t^{\tau_1,\dots,\tau_m}_{x_1,\dots,x_m} f(x) = t^{\tau_m}_{x_m} \left[t^{\tau_1,\dots,\tau_{m-1}}_{x_1,\dots,x_{m-1}} f(x) \right], \quad \text{где} \quad m \le n.$$

Другими словами, при однородно смешанном операторе по каждой переменной действует либо оператор p, либо d в зависимости от набора $(t_1,\dots, t_n)$. В дальнейшем такие операторы будем называть просто однородными.

Договоримся о том, что если у оператора нет верхнего индекса, то индекс считается равным 0.

Функцию назовем вырожденной, если $d^{\tau}_{x} f(x) = 0$, где $\tau_i = 0$ при x_i существенной переменной и $\tau_i = 1$ при x_i фиктивной, а невырожденной в противном случае. Функция называется существенной, если все ее переменные существенны.

ТЕОРЕМА 1. *Для любого однородного оператора* t *существует разложение вида:*

$$f(x,z) = \sum_{\tau} \sum_{\sigma} \beta_{\tau\sigma} t^{\tau}_{x} g(x, f^{\gamma}(\sigma,z)) \tag{1}$$

тогда и только тогда, когда $g(x,v)$ *- существенная невырожденная функция, где* $\gamma = d_x g(x,1)$, $\beta_{\tau\sigma} = d_v b^{\bar{\sigma}}_{x} t^{\bar{\tau}}_{x} g(x,v)$.

ДОКАЗАТЕЛЬСТВО. Предварительно покажем, что имеет место следующее равенство: $[\beta_{\tau\sigma}]\cdot[\alpha_{\sigma\tau}] = \mathbf{E}$, где $\mathbf{E}$ - единичная матрица. Рассмотрим элемент произведения этих матриц:

$$\varepsilon_{\delta\tau} = \sum_{\sigma}\beta_{\delta\sigma}\alpha_{\sigma\tau} = \sum_{\sigma} d_v b_x^{\bar{\sigma}} t_x^{\bar{\delta}} g(x,v)\cdot d_v b_x^{\bar{\sigma}} t_x^{\bar{\tau}} g(x,v) =$$

$$= d_x^0\left[d_v t_x^{\bar{\delta}} g(\bar{x},v)\cdot d_v t_x^{\bar{\tau}} g(x,v)\right]. \qquad (2)$$

Пусть $\delta = \tau$ и $x_1,\dots,x_k$ - общие аргументы функций $d_v t_x^{\bar{\tau}} g(\bar{x},v)$ и $d_v t_x^{\tau} g(x,v)$. Тогда (2) можно записать в виде:

$$\varepsilon_{\tau\tau} = d_x\left[\omega(\bar{x}_1^{\bar{\tau}_1},\dots,\bar{x}_k^{\bar{\tau}_k})\,\omega_1(x_1^{\tau_1},\dots,x_k^{\tau_k})\right],$$

где

$$\omega(\bar{x}_1^{\bar{\tau}_1},\dots,\bar{x}_k^{\bar{\tau}_k}) = p_{x'}^{\bar{\tau}'}\left[d_v t_{x''}^0 g(\bar{x}',\bar{x}'',v)\right],$$

$$\omega_1(x_1^{\tau_1},\dots,x_k^{\tau_k}) = p_{x'}^{\tau'}\left[d_v t_{x''}^0 g(x',x'',v)\right],$$

$$x'=(x_1,\dots,x_k),\ x''=(x_{k+1},\dots,x_n),\ \tau'=(\tau_1,\dots,\tau_k).$$

Ввиду равенств $\bar{x}_1^{\bar{\tau}_1} = x_1^{\tau_1}$ и $d_x^0 h(x,y) = d_x^0 h(x,y)$ получаем: $\omega(\bar{x}_1^{\bar{\tau}_1},\dots,\bar{x}_k^{\bar{\tau}_k})\ \omega_1(x_1^{\tau_1},\dots,x_k^{\tau_k}) =$

$= \omega(x_1^{\tau_1},\dots,x_k^{\tau_k})$, откуда следует, что $\varepsilon_{\tau\tau} = 1$ тогда и только тогда, когда функция $g(x,v)$ невырожденная.

Пусть $\delta \neq \tau$. Если имеется хотя бы одна фиктивная переменная, то $\varepsilon_{\delta\tau} = 0$. При отсутствии фиктивных пере -

менных пусть $x_1, \dots, x_k$ - переменные, входящие в запись обеих функций $d_V t_X^{\bar\delta} g(\bar x, v)$ и $d_V t_X^{\tau} g(x, v)$. Поскольку остальные переменные разделены, производные по этим переменным берутся по сомножителям отдельно. Представляя производные в сомножителях в виде сумм и взяв производные по соответствующим переменным, преобразуем (2) к виду:

$$\varepsilon_{\delta\tau} = d_{x_1 \dots x_k}\left\{\left[\Sigma\, d_V g(x_1^{\bar\tau_1}, \dots, x_k^{\bar\tau_k}, \sigma_{k+1}, \dots, \sigma_n, v)\right] \times \right.$$

$$\left. \times \left[\Sigma\, d_V g(x_1^{\tau_1}, \dots, x_k^{\tau_k}, \sigma_{k+1}, \dots, \sigma_n, v)\right]\right\},$$

где оба суммирования ведутся по всем наборам $(\sigma_1, \dots, \sigma_k)$. Взяв производные по $x_1, \dots, x_k$, получаем:

$$\varepsilon_{\delta\tau} = \Sigma \left\{\left[\Sigma\, d_V g(\sigma_1^{\bar\tau_1}, \dots, \sigma_k^{\bar\tau_k}, \sigma_{k+1}, \dots, \sigma_n, v)\right] \times \right.$$

$$\left. \times \left[\Sigma\, d_V g(\sigma_1^{\tau_1}, \dots, \sigma_k^{\tau_k}, \sigma_{k+1}, \dots, \sigma_n, v)\right]\right\},$$

внешняя сумма берется по всем наборам $(\sigma_1, \dots, \sigma_k)$. Очевидно, что во внешней сумме на наборах $(\sigma_1, \dots, \sigma_k)$ и $(\bar\sigma_1, \dots, \bar\sigma_k)$ слагаемые совпадают. Таким образом, при $\delta \neq \tau$ получаем $\varepsilon_{\delta\tau} = 0$.

Для доказательства равенства (1) будем преобразовывать его правую часть:

$$\sum_\tau \sum_\sigma \beta_{\tau\sigma} t_X^{\tau} g(x, f^{\gamma}(\sigma, z)) =$$

$$= \sum_\sigma \sum_\tau \beta_{\tau\sigma}\left[f^{\gamma}(\sigma, z) d_V t_X^{\tau} g(x, v) + t_X^{\tau} g(x, 0)\right] =$$

$$= \sum_{\sigma} \left[\sum_{\tau} \beta_{\tau\sigma} d_v t_x^{\tau} g(x\ v) \right] f^{\gamma}(\sigma, z) \oplus$$

$$\oplus \sum_{\sigma} \sum_{\tau} \beta_{\tau\sigma} t_x^{\tau} g(x, 0). \qquad (3)$$

Рассмотрим сумму

$$\sum_{\sigma} \beta_{\tau\sigma} = \sum_{\sigma} d_v b_x^{\bar\sigma} t_x^{\bar\tau} g(x, v) = d_x \left[d_v t_x^{\bar\tau} g(\bar x, v) \right].$$

Эта сумма отлична от нуля тогда и только тогда, когда набор τ содержит нули на местах, соответствующих оператору дифференцирования в заданном операторе. Для упрощения изложения пусть эти места соответствуют $x_1, \ldots, x_k$. Тогда имеем равенства:

$$\sum_{\sigma} \sum_{\tau} \beta_{\tau\sigma} t_x^{\tau} g(x, 0) =$$

$$= \sum_{\tau_{k+1}, \ldots, \tau_n} d_{x_1 \ldots x_k} \left[p_{x_{k+1}, \ldots, x_n}^{\tau_{k+1}, \ldots, \tau_n} g(x, 0) \right] =$$

$$= \sum_{\tau_{k+1}, \ldots, \tau_n} \sum_{\tau_1, \ldots, \tau_k} g(\tau_1, \ldots, \tau_k, x_{k+}^{\tau_{k+1}}, \ldots, x_n^{\tau_n}, 0).$$

Поскольку суммирование ведется по всем наборам $\tau_{k+1}, \ldots$ $\ldots, \tau_n$ для каждой функции $g(\tau_1, \ldots, \tau_k\ x_{k+1}^{\tau_{k+1}}, \ldots$ $\ldots, x_n^{\tau_n}, 0)$, то сумма не зависит от $x_{k+1}, \ldots, x_n$:

$$\sum_{\tau_{k+1}, \ldots, \tau_n} g(\tau_1, \ldots, \tau_k, x_{k+1}^{\tau_{k+1}}, \ldots, x_n^{\tau_n}, 0) =$$

$$= \sum_{\tau_{k+1}, \ldots, \tau_n} g(\tau_1, \ldots, \tau_k, \tau_{k+1}, \ldots, \tau_n, 0).$$

Окончательно получаем:

$$\sum_{\sigma}\sum_{\tau}\beta_{\tau\sigma}t_x g(x,0) = \sum_{\tau} g(\tau_1,\ldots,\tau_n,0) =$$
$$= d_x g(x,0) = d_x g(x,1)\oplus 1 = \bar{\gamma} .$$

Продолжим преобразования в первой части суммы (3)

$$\sum_{\tau} \beta_{\tau\sigma} d_v t_x^{\tau} g(x,v) = \sum_{\tau} d_v b_x^{\bar\sigma} t_x^{\bar\tau} g(x,v)\; d_v t_x^{\tau} g(x,v) =$$
$$= \sum_{\tau} d_v t_x^{\tau} g(x,v)\cdot d_v b_x^{\bar\sigma} t_x^{\bar\tau} g(x,v) .$$

При $x = \delta$ имеем

$$\sum_{\tau} d_v b_x^{\delta} t_x^{\tau} g(x,v)\cdot d_v b_x^{\bar\sigma} t_x^{\bar\tau} g(x,v) = \sum_{\tau}\alpha_{\delta\tau}\,\beta_{\tau\sigma} .$$

Полученная сумма равна 1 тогда и только тогда, когда $\delta = \sigma$, по определению $\beta_{\sigma\tau}$ и доказанному свойству $[\beta_{\tau\sigma}] = [\alpha_{\sigma\tau}]^{-1}$. Таким образом, имеет место равенство

$$\sum_{\tau}\beta_{\sigma\tau}\, d_v t_x^{\tau} g(x\ v) = x_1^{\sigma_1},\ldots, x_n^{\sigma_n} .$$

Исходя из полученных соотношений, продолжим преобразования правой части равенства (1):

$$\sum_{\sigma}\Big[\sum_{\tau}\beta_{\sigma\tau} d_v t_x^{\tau} g(x,v)\Big] f^{\gamma}(\sigma,z) \oplus \sum_{\sigma}\sum_{\tau}\beta_{\sigma\tau} t_x^{\tau} g(x,0) =$$
$$= \sum_{\sigma} x_1^{\sigma_1}\cdot\ldots\cdot x_n^{\sigma_n} f^{\gamma}(\sigma,z)\oplus\bar{\gamma} =$$
$$= \sum_{\sigma} x_1^{\sigma_1}\cdot\ldots\cdot x_n^{\sigma_n} f^{\gamma}(\sigma,z)\oplus$$

$$\bigoplus_{\sigma} \Sigma\, x_1^{\sigma_1}\cdot\ldots\cdot x_n^{\sigma_n}\bar{\gamma} = \sum_{\sigma} x_1^{\sigma_1}\cdot\ldots\cdot x_n^{\sigma_n}(f^{\gamma}(\sigma,z)\oplus\bar{\gamma}) =$$

$$= \sum_{\sigma} x_1^{\sigma_1}\cdot\ldots\cdot x_n^{\sigma_n}\cdot f(\sigma,z) = f(x,z).$$

Теорема доказана.

Важным частным случаем невырожденных функций являются функции, реализуемые бесповторными формулами. Формула над множеством переменных является бесповторной, если символ каждой переменной входит в ее запись не более одного раза, и полной, если каждая переменная имеет вхождение. Полная бесповторная формула над системой функций $\{\neg, \cdot, \vee, |, \downarrow, \rightarrow, \nrightarrow, \leftarrow, \nleftarrow\}$ определяет существенную невырожденную функцию, поэтому непосредственно получаем следующее

СЛЕДСТВИЕ. *Для любой полной бесповторной формулы* $F(x)$ *существует разложение вида:*

$$f(x,z) = \sum_{\tau}\sum_{\sigma} \beta_{\tau\sigma} t_x^{\tau} F(x) f(\sigma,z),$$

где t *– любой однородный оператор* $\beta_{\tau\sigma} = b_x^{\bar{\sigma}} t_x^{\bar{\tau}} F(x)$.

На основании приведенных разложений получим достаточно большой класс полиномиальных канонических формул булевых функций. С одной стороны, канонические формы могут быть получены по одной невырожденной функции действием различных однородных операторов, с другой стороны, действием одного оператора на различные невырожденные функции. Известные полиномиальная совершенная нормальная форма [4] и поляризованный полином Жегалкина [5,6] являются частными случаями канонических форм над однородными операторами. Отметим, что в [7] рассматривались полиномиальные канонические формы над произвольными системами функций.

ТЕОРЕМА 2. *Разложение над образами функции* $g(x)$ *по любому однородному оператору* t *вида:*

$$f(x) = \sum_{\tau} \beta_{\tau} t_x^{\tau} g(x)$$

является канонической формой тогда и только тогда, когда $g(x)$ *- существенная невырожденная функция,*

где $\beta_{\tau} = d_x\left[f(x) t_x^{\bar{\tau}} g(x)\right]$.

ДОКАЗАТЕЛЬСТВО. Из теоремы 1 в случае разложения по всем аргументам функции $g(x)v$ и путем подсчитывания γ и $\beta_{\tau\sigma}$ получим: $\gamma = d_x g(x)\cdot 1 = 1$, $\beta_{\tau\sigma} = d_v b_x^{\bar{\sigma}} t_x^{\bar{\tau}}(g(x)v) =$

$= b_x^{\bar{\sigma}} t_x^{\bar{\tau}} g(x)$,

$$f(x) = \sum_{\tau}\sum_{\sigma} \beta_{\tau\sigma} t_x^{\tau}(g(x) f^{\gamma}(\sigma)) = \sum_{\tau}\sum_{\sigma} \beta_{\tau\sigma} t_x^{\tau} g(x) f(\sigma) =$$

$$= \sum_{\tau}\left[\sum_{\sigma} \beta_{\tau\sigma} f(\sigma)\right]\cdot t_x^{\tau} g(x) =$$

$$= \sum_{\tau}\left[\sum_{\sigma} b_x^{\bar{\sigma}} t_x^{\bar{\tau}} g(x) f(\sigma)\right]\cdot t_x^{\tau} g(x) =$$

$$= \sum_{\tau}\left[\sum_{\sigma} b_x^{\sigma} t_x^{\bar{\tau}} g(\bar{x})\ f(\sigma)\right]\cdot t_x^{\tau} g(x) =$$

$$= \sum_{\tau} d_x\left[t_x^{\bar{\tau}} g(\bar{x}) f(x)\right]\cdot t_x^{\tau} g(x),$$

что и требовалось.

В обратную сторону доказательство очевидно, так как сумма вырожденных функций является вырожденной.

СЛЕДСТВИЕ. *Пусть* $F(x)$ *— полная бесповторная формула,* t *- однородный оператор, тогда разложение*

$$f(x) = \sum_{\tau} \beta_{\tau} t_x^{\tau} F(x),$$

где $\beta_{\tau} = d_x\left[f(x)\ t_x^{\bar{\tau}} F(\bar{x})\right]$, *является канонической формой булевых функций.*

Это следствие получается аналогично следствию к теореме 1.

Литература

1. ВИНОКУРОВ С.Ф., ПЕРЯЗЕВ Н.А. Полиномиальные разложения булевых функций по невырожденным функциям //Алгебра и логика. - 1991. - Т. 30, № 6. - С. 631-637.

2. ВИНОКУРОВ С.Ф., ПЕРЯЗЕВ Н.А.Представление булевых функций полиномиальными формами //Кибернетика и системный анализ. - 1992. - № 2. - С. 210-213.

3. ВИНОКУРОВ С.Ф. Полиномиальные операторные разложения и канонические формы булевых функций. - Иркутск, 1992. - 26 с. (Препринт/Иркутский университет).

4. МАЧИКЕНАС Э.К., СУПРУН В.П. О полиномиальном разложении булевых функций. - Деп. в ВИНИТИ 09.03.88, № 1899-В88. - 31 с.

5. MULLER D.E. Application of Boolean algebra to switching circuit design and error detection //IRE Trans. Electron. Comput. - 1954. - Vol. 3, N 3. - P. 6-12.

6. REED I.S. A class of multiple-error-correcting codes and the decoding scheme //IRE Trans. Inform. Theory. - 1954. - Vol. 4, N 9. - P. 38-49.

7. АВСАРКИСЯН Г.С. Обобщенные полиномиальные формы булевых функций и синтез многовыходных логических схем //Автоматика и телемеханика. - 1983. - № 11. - С. 111-119.

Поступила в ред.-изд.отд.

17 сентября 1992 года