УДК 519.716

ДЕКОМПОЗИЦИЯ ЧАСТИЧНО СИММЕТРИЧЕСКИХ БУЛЕВЫХ ФУНКЦИЙ НА ОСНОВЕ ПОЛИНОМИАЛЬНОГО РАЗЛОЖЕНИЯ

Л.Б. АВГУЛЬ[1], О.К. ТРУХАН[2]

[1]*Научно - технический центр "ДЭЛС"*
Ф. Скорины, 117, Минск, 220023, Беларусь;

[2]*Военная академия Республики Беларусь*
ВА РБ, Минск, 220057, Беларусь

Поступила в редакцию 8 июня 2004

Предлагается оригинальный метод выполнения полиномиальной декомпозиции частично симметрических булевых функций (ч.с.б.ф.), задаваемых своими локальными кодами. Метод позволяет по таблице локальных кодов производных ч.с.б.ф. получить одновременно локальные коды всех "остаточных" функций при разложении по любому кортежу переменных с произвольной поляризацией.

Ключевые слова: частично симметрическая булева функция, полиномиальное разложение, полином Рида–Мюллера, локальный код.

Введение

Полиномиальные представления булевых функций позволяют во многих случаях получить более простые аналитические выражения по сравнению с базисом И, ИЛИ, НЕ [1]. Эффективность полиномиальной реализации булевых функций подтверждается многочисленными примерами логического синтеза цифровых устройств и поддерживается разработкой соответствующих библиотек вентильного уровня [2, 3].

Высокая сложность процедуры полиномиального разложения, имеющая экспоненциальную зависимость относительно числа переменных, сильно ограничивает размерность решаемой задачи и затрудняет поиск минимальных форм булевых функций даже при использовании современных высокопроизводительных вычислительных средств.

Вместе с тем есть ряд представляющих большой практический интерес для задач логического синтеза инвариантных подклассов булевых функций, задаваемых своими локальными кодами, длина которых существенно меньше длины таблицы истинности. В первую очередь к таким функциям относятся симметрические булевы функции и частично симметрические булевы функции (ч.с.б.ф.), системами которых описывается работа многих цифровых устройств (многооперандных арифметических устройств, преобразователей кодов и т.д.).

Рассматривается оригинальный метод полиномиального разложения представленных локальными кодами ч.с.б.ф. n переменных по $k \le n$ переменным с произвольной поляризацией. Метод основан на отождествлении локальных кодов "остаточных" функций (коэффициентов полиномов Рида–Мюллера) с соответствующими элементами локальных кодов производных ч.с.б.ф.

Локальное кодирование частично симметрических булевых функций

Нетривиальная частичная симметрия индуцирует разбиение вектора переменных $X = (x_1, x_2, ..., x_n)$ ч.с.б.ф. $f = f(X)$ на N кортежей $X_1, X_2, ..., X_N$, $1 < N < n$. При этом f симметрична относительно любой пары переменных, принадлежащих одному и тому же кортежу $1 \le i \le N$.

Пусть $X_i = (x_1^i, x_2^i, ..., x_{n_i}^i)$, $1 \le n_i < n$, $\sum_{i=1}^{N} n_i = n$, $1 \le i \le N$.

Для определенности полагаем, что $X = (X_1, X_2, ..., X_N)$. Тогда число классов эквивалентности ч.с.б.ф. f определяется выражением

$$p = \prod_{i=1}^{N} (n_i + 1).$$

Каждый класс эквивалентности характеризуется вектором

$A = (a_1, a_2, ..., a_N)$, $a_i \in \{0,1,...,n_i\}$, $1 \le i \le N$.

Локальный код $C(f)$ ч.с.б.ф. f есть двоичный вектор длины p, каждая компонента которого равна значению f на соответствующем классе эквивалентности наборов значений ее аргументов.

Упорядочивая векторы A, представим $C(f)$ в виде:

$$C(f) = \left(„^{00...0}, „^{00...1}, ..., „^{00...n_N}, ..., „^{0n_2...0}, „^{0n_2...1}, ..., „^{0n_2...n_N}, ..., „^{1n_2...0}, „^{1n_2...1}, ..., „^{1n_2...n_N}, ..., „^{n_1n_2...0}, „^{n_1n_2...1}, ..., „^{n_1n_2...n_N} \right),$$

где компонента $C^{a_1a_2...a_N}$ равна значению f на наборах переменных из X_i, удовлетворяющих условию $\sum_{l=1}^{n_i} x_l^i = a_i$.

Это означает, что

$$C^{a_1a_2...a_N} = f\left(G_{a_1}^1, G_{n_1-a_1}^0, ..., G_{a_N}^1, G_{n_N-a_N}^0\right),$$

где $G_s^h = (h, h, ..., h)$ — некоторый кортеж длины s, содержащий только элементы $h \in \{0,1\}$, и $G_0^h \equiv \varnothing$.

Полиномиальное представление частично симметрических булевых функций

Введем обозначения:

$$Y_i = (x_1^i, x_2^i, ..., x_{k_i}^i), \quad Z_i = (x_{k_i+1}^i, x_{k_i+2}^i, ..., x_{n_i}^i),$$
$$Z = (Z_1, Z_2, ..., Z_N), \quad 1 \le k_i \le n_i, \quad 1 \le i \le N.$$

Полагаем, что полиномиальное разложение выполняется по k_i переменным из Y_i, из которых $0 \le m_i \le k_i$ переменные отрицательно поляризованы (входят в коэффициенты полиномиального разложения или слагаемые полинома Рида–Мюллера только с отрицанием), $1 \le i \le N$.

Пусть $E_{r_i l_i}^{k_i m_i}(Y_i)$ — сумма по модулю два всевозможных попарно различных элементарных конъюнкций ранга r_i, составленных из переменных $\{\bar{x}_1^i, \bar{x}_2^i, ..., \bar{x}_{m_i}^i, x_{m_i+1}^i, x_{m_i+2}^i, ..., x_{k_i}^i\}$ и в которых число переменных без отрицания равно $0 \le l_i \le r_i,\ 0 \le r_i \le k_i$.

Группируя коэффициенты разложения при тождественных "остаточных" функциях, получим общий вид полиномиального разложения ч.с.б.ф. f по $k = \sum_{l=1}^{N} k_i$ переменным, из которых $m = \sum_{l=1}^{N} m_i$ переменные отрицательно поляризованы:

$$P_{k_1 k_2 .. k_N}^{m_1 m_2 ... m_N}(f) = \sum_{r_1=0}^{k_1} \oplus \sum_{l_1=a_1}^{b_1} \oplus E_{r_1 l_1}^{k_1 m_1}(Y_1) \cdot \left(\sum_{r_2=0}^{k_2} \oplus \sum_{l_2=a_2}^{b_2} \oplus E_{r_2 l_2}^{k_2 m_2}(Y_2) \cdot ... \cdot \left(\sum_{r_N=0}^{k_N} \oplus \sum_{l_N=a_N}^{b_N} \oplus E_{r_N l_N}^{k_N m_N}(Y_N) \cdot \Psi_{r_1 r_2 .. r_N}^{l_1 l_2 ... l_N}(Z) \right) ... \right),$$

где $a_i = (r_i - m_i) \cdot \mathrm{sign}(r_i - m_i)$; $b_i = \min(r_i, k_i - m_i)$; $E_{00}^{k_i m_i} \equiv 1$; $\Psi_{r_1 r_2 .. r_N}^{l_1 l_2 ... l_N}(Z)$ — "остаточные" функции.

Функции $\Psi_{r_1 r_2 .. r_N}^{l_1 l_2 ... l_N}(Z)$ могут быть вычислены через производные ч.с.б.ф. f согласно выражению:

$$\Psi_{r_1 r_2 .. r_N}^{l_1 l_2 ... l_N}(Z) = \frac{d^r f\left(Y_1^1, G_{s_1}^1, G_{v_1}^0, Z_1, ..., Y_N^1, G_{s_N}^1, G_{v_N}^0, Z_N\right)}{dY_1^1, dY_2^1, ..., dY_N^1},$$

где $s_i = m_i - r_i + l_i$, $v_i = k_i - m_i - l_i$, $Y_i^1 = (x_1^i, x_2^i, ..., x_{r_i}^i)$, $1 \le i \le N$.

Локальные коды функций $\Psi_{r_1 r_2 .. r_N}^{l_1 l_2 ... l_N}(Z)$ совпадают с локальными кодами "остаточных" функций в дизъюнктивном разложении производных $f^{r_1 r_2 ... r_N} = \frac{d^r f(X)}{dY_1^1, dY_2^1, ..., dY_N^1}$, $r = \sum_{l=1}^{N} r_i$, и находятся по таблице $T(C(f))$ локальных кодов $C(f^{r_1 r_2 ... r_N})$.

Пример полиномиального разложения частично симметрической булевой функции

Рассмотрим пример выполнения полиномиального разложения ч.с.б.ф. $f = f(X)$, $X = (x_1, x_2, ..., x_7)$, $N = 3$, $n_1 = 3$, $n_2 = n_3 = 2$, которая задана своим локальным кодом:

$$C(f) = \left(„^{000}, „^{001}, „^{002}, ..., „^{310}, „^{311}, „^{312}, „^{320}, „^{321}, „^{322}\right) =$$
$$= (01011010100110011100001101111101110).$$

При $k_1 = 2$, $k_2 = k_3 = 1$, $m_1 = m_2 = 1$, $m_3 = 0$ имеем:

$$P_{211}^{110}(f) = \Psi_{000}^{000}(Z) \oplus E_{11}^{10}(Y_3)\Psi_{001}^{001}(Z) \oplus E_{10}^{11}(Y_2)\left(\Psi_{010}^{000}(Z) \oplus E_{11}^{10}(Y_3)\Psi_{011}^{001}(Z)\right) \oplus$$
$$\oplus E_{10}^{21}(Y_1)\left(\Psi_{100}^{000}(Z) \oplus E_{11}^{10}(Y_3)\Psi_{101}^{001}(Z) \oplus E_{10}^{11}(Y_2)\left(\Psi_{110}^{000}(Z) \oplus E_{11}^{10}(Y_3)\Psi_{111}^{001}(Z)\right)\right) \oplus$$
$$\oplus E_{11}^{21}(Y_1)\left(\Psi_{100}^{100}(Z) \oplus E_{11}^{10}(Y_3)\Psi_{101}^{101}(Z) \oplus E_{10}^{11}(Y_2)\left(\Psi_{110}^{100}(Z) \oplus E_{11}^{10}(Y_3)\Psi_{111}^{101}(Z)\right)\right) \oplus$$
$$\oplus E_{21}^{21}(Y_1)\left(\Psi_{200}^{100}(Z) \oplus E_{11}^{10}(Y_3)\Psi_{201}^{101}(Z) \oplus E_{10}^{11}(Y_2)\left(\Psi_{210}^{100}(Z) \oplus E_{11}^{10}(Y_3)\Psi_{211}^{101}(Z)\right)\right),$$

где

$Y_1 = (x_1, x_2)$; $Y_2 = x_4$; $Y_3 = x_6$; $Z_1 = x_3$; $Z_2 = x_5$; $Z_3 = x_7$;

$Z = (Z_1, Z_2, Z_3) = (x_3, x_5, x_7)$; $E_{10}^{21}(Y_1) = \bar{x}_1$; $E_{11}^{21}(Y_1) = x_2$;

$E_{21}^{21}(Y_1) = \bar{x}_1 x_2$; $E_{10}^{11}(Y_2) = \bar{x}_4$; $E_{11}^{10}(Y_3) = x_6$.

Построим таблицу $T(C(f))$ локальных кодов производных ч.с.б.ф. $f = f(X)$ и по ней определим локальные коды "остаточных" функций:

$C\left(\Psi_{000}^{000}(Z)\right) = (10110110)$; $C\left(\Psi_{001}^{001}(Z)\right) = (10001011)$;

$C\left(\Psi_{010}^{000}(Z)\right) = (10010111)$; $C\left(\Psi_{011}^{001}(Z)\right) = (11101001)$;

$C\left(\Psi_{100}^{000}(Z)\right) = (01011101)$; $C\left(\Psi_{101}^{001}(Z)\right) = (11110011)$;

$C\left(\Psi_{110}^{000}(Z)\right) = (00001110)$; $C\left(\Psi_{111}^{001}(Z)\right) = (01000111)$;

$C\left(\Psi_{100}^{100}(Z)\right) = (11011101)$; $C\left(\Psi_{101}^{101}(Z)\right) = (00110110)$;

$C\left(\Psi_{110}^{100}(Z)\right) = (11100010)$; $C\left(\Psi_{111}^{101}(Z)\right) = (01110111)$;

$C\left(\Psi_{200}^{100}(Z)\right) = (10000000)$; $C\left(\Psi_{201}^{101}(Z)\right) = (11000101)$;

$C\left(\Psi_{210}^{100}(Z)\right) = (11101100)$; $C\left(\Psi_{211}^{101}(Z)\right) = (00110000)$.

Таблица $T(C(f))$ **локальных кодов производных ч.с.б.ф. для рассматриваемого примера**

Производная $f^{r_1r_2r_3}$	Локальный код $C(f^{r_1r_2r_3})$	Производная $f^{r_1r_2r_3}$	Локальный код $C(f^{r_1r_2r_3})$
f^{000}	0101101010011001110000111011111101110	f^{200}	010101000110001001
f^{001}	110111011000001011001101	f^{201}	111100010101
f^{002}	010110010001	f^{202}	000111
f^{010}	100011101011011110010011	f^{210}	111101111000
f^{011}	1010111010011110	f^{211}	00110000
f^{012}	11011101	f^{212}	0000
f^{020}	111110101001	f^{220}	010111
f^{021}	00011101	f^{221}	1100
f^{022}	0101	f^{222}	00
f^{100}	011010010001111010111110011	f^{300}	100100001
f^{101}	101111010011000110	f^{301}	101001
f^{102}	100100011	f^{302}	111
f^{110}	001000110101001101	f^{310}	000101
f^{111}	010001110111	f^{311}	0011
f^{112}	101010	f^{312}	00
f^{120}	001011100	f^{320}	101
f^{121}	011010	f^{321}	11
f^{122}	111	f^{322}	0

Заметим, что в данном случае локальные коды совпадают с таблицами истинности "остаточных" функций, поскольку кортежи Z_1, Z_2 и Z_3 содержат по одной переменной.

Для этой же ч.с.б.ф. по таблице $T(C(f))$ определим коэффициенты и построим полином Рида–Мюллера при $m_1 = 2$, $m_2 = 1$, $m_3 = 2$:

$$P^{212}(f) = 1 \oplus \bar{x}_6\bar{x}_7 \oplus \bar{x}_4\left(1 \oplus \bar{x}_6\bar{x}_7\right) \oplus x_5\left(\bar{x}_6 \oplus \bar{x}_7 \oplus \bar{x}_6\bar{x}_7\right) \oplus$$
$$\oplus \bar{x}_4x_5\left(1 \oplus \bar{x}_6 \oplus \bar{x}_7\right) \oplus \left(\bar{x}_1 \oplus \bar{x}_2\right)\left(1 \oplus \bar{x}_4\left(\bar{x}_6 \oplus \bar{x}_7 \oplus \bar{x}_6\bar{x}_7\right) \oplus \right.$$
$$\left. \oplus x_5\left(1 \oplus \bar{x}_6 \oplus \bar{x}_7\right) \oplus \bar{x}_4x_5\left(1 \oplus \bar{x}_6\bar{x}_7\right)\right) \oplus x_3\left(\left(\bar{x}_6 \oplus \bar{x}_7 \oplus \bar{x}_6\bar{x}_7\right) \oplus \right.$$
$$\left. \oplus \bar{x}_4\left(1 \oplus \bar{x}_6 \oplus \bar{x}_7 \oplus \bar{x}_6\bar{x}_7\right) \oplus x_5\left(1 \oplus \bar{x}_6 \oplus \bar{x}_7\right) \oplus \bar{x}_4x_5\bar{x}_6\bar{x}_7\right) \oplus$$
$$\oplus \bar{x}_1\bar{x}_2\left(1 \oplus \bar{x}_6 \oplus \bar{x}_7 \oplus \bar{x}_4 \oplus x_5\left(1 \oplus \bar{x}_6 \oplus \bar{x}_7\right) \oplus \bar{x}_4x_5\left(\bar{x}_6 \oplus \bar{x}_7\right)\right) \oplus$$
$$\oplus \left(\bar{x}_1x_3 \oplus \bar{x}_2x_3\right)\left(\left(1 \oplus \bar{x}_6 \oplus \bar{x}_7 \oplus \bar{x}_6\bar{x}_7\right) \oplus \bar{x}_4 \oplus \bar{x}_4x_5\right) \oplus$$
$$\oplus \bar{x}_1\bar{x}_2x_3\left(\bar{x}_6\bar{x}_7 \oplus x_5\left(1 \oplus \bar{x}_6 \oplus \bar{x}_7\right) \oplus \bar{x}_4x_5\left(1 \oplus \bar{x}_6 \oplus \bar{x}_7\right)\right).$$

Заключение

Эффективность предложенного метода декомпозиции ч.с.б.ф. обусловлена тем, что по построенной один раз таблице локальных кодов ее производных достаточно просто по формальным правилам определяются коэффициенты всех полиномов Рида–Мюллера и локальные коды всех "остаточных" функций в полиномиальном разложении по любому кортежу переменных с произвольной поляризацией. Поскольку при этом для задания ч.с.б.ф. используется локальный код, а не таблица истинности, то ограничений на число переменных практически не существует.

Метод может быть успешно применен при синтезе широкого класса цифровых устройств.

DECOMPOSITION PARTLY SYMMETRICAL BOOLEAN FUNCTIONS ON BASE OF POLYNOMIAL EXPANSIONS

L.B. AVGUL, A.K. TRUCHAN

Abstract

It is offerred the original method of polynomial decomposition partly symmetrical boolean functions (p.s.b.f.), assigned by their local codes. The method allows on table of p.s.b.f. local codes to get simultaneously local codes of all "remaining" functions at decomposition on any tuple variable with free polarization.

Литература

1. *Sasao T.* //Proceedings of the IFIP WG 10.5 Workshop on Application of the Reed-Muller Expansions in Circuit Design. 1995. P. 11–20.
2. *Sasao T., Besslich Ph.W.* // IEEE Transaction on Computers. 1990. Vol. 39. № 2. P. 262–266.
3. *Saul J.* // Proceedings of the European Conference on Design Automation. 1992. P. 109–113.