Един клас от базиси за двоичните функции

Димитър Скордев

Софийски университет "Св. Климент Охридски"
Факултет по математика и информатика

Научна сесия на ФМИ, 29 март 2008 г.

Съдържание

Пълни множества от двоични функции

Разглеждаме двоични функции само с ненулев брой аргументи.

Дефиниция

Нека C е едно множество от двоични функции. Дефинираме множества $D_0^C, D_1^C, D_2^C, \ldots$ по следния начин:

- D_0^C *е множеството на функциите* $\varphi(x_1, \ldots, x_n) = x_i$, *където* $1 \leq i \leq n$.
- D_{r+1}^C *е множеството на функциите от* D_r^C *и функциите* $\varphi(x_1, \ldots, x_n) = \theta(\varphi_1(x_1, \ldots, x_n), \ldots, \varphi_m(x_1, \ldots, x_n))$, *където* $\theta \in C$, $\varphi_1, \ldots, \varphi_m \in D_r$.

Множеството C се нарича пълно, ако всяка двоична функция принадлежи на $D_0^C \cup D_1^C \cup D_2^C \cup \ldots$

Примитивни базиси

Дефиниция

Ако θ е m-местна двоична функция, ще наричаме нейни подфункции функциите $\varphi(x_1, \ldots, x_n) = \theta(x_{i_1}, \ldots, x_{i_m})$, където $\{i_1, \ldots, i_m\} = \{1, \ldots, n\}$. Очевидно при тях имаме $n \leq m$. Онези, за които $n < m$, ще наричаме същински подфункции на θ, а за останалите ще казваме, че са конгруентни на θ.

Дефиниция

Базис се нарича такова пълно множество, на което никое същинско подмножество не е пълно. Един базис ще наричаме примитивен, ако замяната на коя да е функция от него с една или повече нейни същински подфункции също нарушава пълнотата.

Примитивни базиси от едноместни и двуместни функции

Дефиниция

За всяка двоична функция θ ще означаваме с θ^d нейната двойнствена. С $+$ ще означаваме двоично събиране. Полагаме:

$$
\begin{array}{lll}
f_0(x) = 0 & g_0(x,y) = x + y & g_2(x,y) = xy + 1 \\
f_1(x) = x + 1 & g_1(x,y) = xy & g_3(x,y) = xy + y + 1
\end{array}
$$

Лема (а)

Следните 12 множества са примитивни базиси:

$$
\begin{array}{llllll}
\{g_2\} & \{g_2^d\} & \{f_1, g_1\} & \{f_1, g_1^d\} & \{f_0^d, g_0, g_1\} & \{f_0, g_0^d, g_1^d\} \\
\{f_0, g_3\} & \{f_0^d, g_3^d\} & \{f_1, g_3\} & \{f_1, g_3^d\} & \{f_0^d, g_0, g_1^d\} & \{f_0, g_0^d, g_1\}
\end{array}
$$

Примитивни базиси от едноместна и триместна функция

Дефиниция

$$h_1(x,y,z) = xy + xz + yz + 1$$
$$h_2(x,y,z) = xy + xz + yz + x + 1$$
$$h_3(x,y,z) = xy + xz + yz + x + y + 1$$
$$h_4(x,y,z) = xy + xz + yz + x + y + z + 1$$

Лема (b)

Следните 12 множества са примитивни базиси:

$$\begin{array}{cccccc} \{f_0, h_1\} & \{f_0^d, h_1\} & \{f_0, h_3\} & \{f_0^d, h_3\} & \{f_1, h_2\} & \{f_1, h_2^d\} \\ \{f_0, h_2\} & \{f_0^d, h_2^d\} & \{f_0, h_4\} & \{f_0^d, h_4^d\} & \{f_1, h_4\} & \{f_1, h_4^d\} \end{array}$$

Още двадесет примитивни базиса

Дефиниция

$$h_0(x,y,z) = x + y + z$$

$$h_5(x,y,z) = xy + x + z \qquad h_9(x,y,z) = xy + xz + yz + x + y$$

$$h_6(x,y,z) = xz + yz + y \qquad h_{10}(x,y,z) = xyz + x + y$$

$$h_7(x,y,z) = xy + xz + x \qquad h_{11}(x,y,z) = xyz + xz + x$$

$$h_8(x,y,z) = xy + xz + yz \qquad h_{12}(x,y,z) = xyz + xy + x + y + z$$

Лема (с)

Следните 20 множества са примитивни базиси: $\{f_0, f_0^d, \theta\}$, *където* $\theta \in \{h_5, h_6, h_7, h_7^d, h_9, h_{10}, h_{10}^d, h_{11}, h_{11}^d, h_{12}, h_{12}^d\}$; $\{\theta, f_1, \tau\}$, *където* $\theta \in \{f_0, f_0^d\}$, $\tau \in \{h_8, h_9\}$; $\{f_0^d, g_0, h_8\}$ *и* $\{f_0, g_0^d, h_8\}$; $\{f_0, f_0^d, h_0, \theta\}$, *където* $\theta \in \{g_1, g_1^d, h_8\}$.

Основната теорема I

Дефиниция

*Две множества от двоични функции ще наричаме **конгруентни**, ако между елементите им може да се установи такова взаимно еднозначно съответствие, че взаимно съответстващите си функции да бъдат конгруентни.*

Теорема (за примитивните базиси)

Едно множество от двоични функции е примитивен базис тогава и само тогава, когато е конгруентно на някой от 44-те примитивни базиса, посочени в леми (a), (b) и (c).

Доказателство. Частта „тогава“ е ясна. За частта „само тогава“, да предположим, че C е произволно пълно множество

Основната теорема II

от двоични функции. Да означим с $[C]$ множеството на всички двоични функции, които са подфункции на функции от C. По критерия на Пост за пълнота множеството C не се съдържа в никой от петте класа T_0, T_1, S, M, L. По една теорема от статията [Zverovich 2005] това позволява да заключим, че всяко от следните пет множества има общ елемент с $[C]$:

$$\{f_0^d, f_1\},\ \{f_0, f_1\},\ \{f_0, f_0^d, g_1, g_1^d, g_2, g_2^d\},$$
$$\{f_1, g_0, g_0^d, g_3, g_3^d, h_0, h_5, h_6, h_7, h_7^d, h_9, h_{10}, h_{10}^d, h_{11}, h_{11}^d, h_{12}, h_{12}^d\},$$
$$\{g_1, g_1^d, g_2, g_2^d, g_3, g_3^d, h_8, h_1, h_2, h_2^d, h_9, h_3, h_4, h_4^d\}.$$

Оттук с допускане на противното и съждителна резолюция се получава, че някой от споменатите 44 базиса се съдържа в $[C]$. Показва се, че множеството C е конгруентно на този базис, когато то самото е примитивен базис. $\square$

Максимална дълбочина на двоична функция

Дефиниция

Когато C е пълно множество от двоични функции и φ е дадена двоична функция, дълбочина на φ относно C наричаме най-малкото естествено число r, за което $\varphi \in D_r^C$.

Лема

Дълбочината на n-местна двоична функция относно пълно множество от двоични функции винаги е по-малка от 2^{2^n}.

Дефиниция

Ако φ е дадена двоична функция, максимална дълбочина на φ наричаме най-голямата от дълбочините на φ относно всевъзможните пълни множества от двоични функции.

Пресмятане на максимални дълбочини

В статията [Skordev 2004] е описан един алгоритъм за пресмятане на максималните дълбочини, който обаче е много неудобен за използване. Ще посочим по-удобен.

Теорема (за максималната дълбочина)

Максималната дълбочина на коя да е двоична функция е равна на най-голямата от дълбочините ѝ относно 44-те примитивни базиса, посочени в леми (a), (b) и (c).

Доказателство. От доказателството на теоремата за примитивните базиси знаем, че за всяко пълно множество C от двоични функции съществува примитивен базис P измежду споменатите 44, състоящ се от подфункции на функции от C. Дълбочината на коя да е двоична функция относно C не надминава дълбочината ѝ относно P. □

Литература

- Skordev, D. Maximal depths of Boolean functions. Год. на Соф. унив., ФМИ, **96** (2004), 89–99.
- Zverovich, I. E. Characterizations of closed classes of Boolean functions in terms of forbidden subfunctions and Post classes. Discrete Applied Mathematics, **149** (2005), 200–218.