УДК 519.713

І. А. Мич (Ужгородський нац. ун-т)

МЕТОД ПОБУДОВИ УЗАГАЛЬНЕНИХ КАНОНІЧНИХ ПОЛІНОМІВ ФУНКЦІЙ ДВОЗНАЧНОЇ ЛОГІКИ

The paper deals with finding coefficients of generated canonical polynomials for the given boolean function that is based on the use of properties of generated conjunctive transformations.

Розглядається алгоритм знаходження коефіцієнтів узагальнених канонічних поліномів для заданої бульової функції, що базується на використанні властивостей узагальнених кон'юнктивних перетворень.

Задання бульових функцій за допомогою канонічних поліномів (поліномів Жегалкіна) є досить зручним аналітичним способом задання цих функцій з урахуванням однозначності їх представлення такими поліномами. Однак більш загальним є представлення бульових функцій за допомогою канонічних поліномів, у які кожна змінна може входити лише в прямому вигляді або лише із запереченням (в інверсному вигляді) [1, 2]. Використання узагальнених кон'юнктивних перетворень для побудови вказаних канонічних поліномів з урахуванням можливості застосування швидких перетворень дає можливість обійтися без побудови матриці відповідного перетворення і зменшити кількість необхідних при цьому арифметичних операцій [3].

Означення 1. *$\tilde{\alpha}$-канонічним поліномом, побудованим із змінних X_1, X_2, X_3, …, X_n, називається вираз вигляду*

$$\sum_{\beta=0}^{2^n-1}{}^{\oplus} a_\beta \otimes R_{\tilde{\alpha}}^{\tilde{\beta}}, \tag{1}$$

де $\beta \in \{0, 1, \ldots, 2^n-1\}$ — номер набору $\tilde{\beta} = (\beta_1, \beta_2, \ldots, \beta_n)$, $(a_0, a_1, \ldots, a_{2^n-1}) \in \in \mathbb{Z}_2^{2^n}$ — вектор коефіцієнтів полінома, $R_{\tilde{\alpha}}^{\tilde{\beta}}$ — елементарна кон'юнкція, побудована із змінних X_1, X_2, …, X_n і породжена наборами $\tilde{\alpha}$ і $\tilde{\beta}$, $\oplus$ і $\otimes$ — відповідно символи операцій додавання і множення по $\bmod 2$.

Очевидно, що кожний поліном (1) однозначно визначається вектором $\tilde{a} = = (a_0, a_1, \ldots, a_{2^n-1}) \in \mathbb{Z}_2^{2^n}$ своїх коефіцієнтів, тобто різних поліномів є стільки, скільки існує різних між собою бульових векторів довжини 2^n, тобто 2^{2^n}. Очевидно також, що різні $\tilde{\alpha}$-канонічні поліноми задають різні бульові функції. А отже, задача побудови $\tilde{\alpha}$-канонічного полінома функції $f(X_1, X_2, \ldots, X_n)$ розв'язується однозначно. Нехай тепер (1) $\tilde{\alpha}$-канонічний поліном бульової функції $f(X_1, X_2, \ldots, X_n)$ заданої вектором $f = (f_0, f_1, \ldots, f_{2^n-1})^T$, тобто

$$f = a_0 \otimes R_{\tilde{\alpha}}^{(0,0,\ldots,0)} \oplus a_1 \otimes R_{\tilde{\alpha}}^{(0,0,\ldots,1)} \oplus \cdots \oplus a_{2^n-1} \otimes R_{\tilde{\alpha}}^{(1,1,\ldots,1)}. \tag{2}$$

З урахуванням властивості 4 матриці узагальненого кон'юнктивного перетворення $K_{\tilde{\alpha}}$ [3] рівність (2) можна переписати у матричному вигляді:

$$f = K_{\tilde{\alpha}} \otimes a, \tag{3}$$

де $\otimes$ — символ операції множення по $\bmod 2$, $a = (a_0, a_1, \ldots, a_{2^n-1})^T$ — вектор коефіцієнтів полінома.

Оскільки над полем $GF(2)$ матриця $K_{\tilde{\alpha}}$ обернена сама собі, то

$$a = K_{\tilde{\alpha}} \otimes K_{\tilde{\alpha}} \otimes a.$$

Звідки, з урахуванням (3), отримаємо

$$a = K_{\tilde{\alpha}} \otimes f. \tag{4}$$

Рівність (4) є основою алгоритму побудови $\tilde{\alpha}$-канонічного полінома заданої бульової функції [3].

Запропонований алгоритм можна модифікувати, якщо ввести в розгляд модифіковане узагальнене кон'юнктивне перетворення, яке визначається матрицею

$$K'_{\tilde{\alpha}} = K'_{(\alpha_1,\alpha_2,\ldots,\alpha_n)} = K'_{\alpha_1} \times K'_{\alpha_2} \times \cdots \times K'_{\alpha_n},$$

де

$$K'_0 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \qquad K'_1 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = K_1.$$

Наприклад, для $n = 3$, $\tilde{\alpha} = (1, 0, 1)$ матриця $K'_{(1,0,1)}$ буде мати вигляд:

$$K'_{(1,0,1)} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

Над полем $GF(2)$

$$(K'_0)^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Тоді на основі властивостей кронекерівського добутку матриць над цим полем

$$(K'_{\tilde{\alpha}})^{-1} = \left(K'_{\alpha_1}\right)^{-1} \times \left(K'_{\alpha_2}\right)^{-1} \times \cdots \times \left(K'_{\alpha_n}\right)^{-1}.$$

Однією з особливостей матриці $K'_{\tilde{\alpha}}$ є те, що в β-у стовпці цієї матриці поміщені значення елементарної кон'юнкції $R^{\tilde{\beta}}_{\tilde{\alpha}}$ на елементах множини $\mathbb{Z}_2^n$. Тому з урахуванням властивостей матриці $K'_{\tilde{\alpha}}$, аналогічно (4), отримаємо

$$a = (K'_{\tilde{\alpha}})^{-1} \otimes f. \tag{5}$$

При знаходженні матричного добутку (5) також можливе виконання швид-

ких перетворень на основі факторизації матриці $(K'_{\tilde\alpha})^{-1}$ за допомогою матриць

$$F^{(n)}_{(K'_0)^{-1}} = \begin{pmatrix} 0&1&0&0&0&0&\dots&0&0\\ 0&0&0&1&0&0&\dots&0&0\\ \vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\ddots&\vdots&\vdots\\ 0&0&0&0&0&0&\dots&0&1\\ 1&1&0&0&0&0&\dots&0&0\\ 0&0&1&1&0&0&\dots&0&0\\ \vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\ddots&\vdots&\vdots\\ 0&0&0&0&0&0&\dots&1&1 \end{pmatrix},\ F^{(n)}_{(K'_1)^{-1}} = \begin{pmatrix} 1&0&0&0&0&0&\dots&0&0\\ 0&0&1&0&0&0&\dots&0&0\\ \vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\ddots&\vdots&\vdots\\ 0&0&0&0&0&0&\dots&1&0\\ 1&1&0&0&0&0&\dots&0&0\\ 0&0&1&1&0&0&\dots&0&0\\ \vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\ddots&\vdots&\vdots\\ 0&0&0&0&0&0&\dots&1&1 \end{pmatrix}.$$

З вигляду цих матриць легко отримати формули швидких перетворень для обчислення добутку

$$(K'_{\tilde\alpha})^{-1}\otimes f = F^{(n)}_{(K'_{\alpha_1})^{-1}}\otimes\left(F^{(n)}_{(K'_{\alpha_2})^{-1}}\otimes\dots\otimes\left(F^{(n)}_{(K'_{\alpha_n})^{-1}}\otimes f\right)\dots\right). \tag{6}$$

Отримаємо:

$$\left(F^{(n)}_{(K'_0)^{-1}}\otimes f\right)_i = \begin{cases} f_{2i+1}, & \text{якщо } i<\frac{2^n}{2},\\ f_{2i-2^n}\oplus f_{2i-2^n+1}, & \text{якщо } i\ge\frac{2^n}{2}, \end{cases} \tag{7}$$

$$\left(F^{(n)}_{(K'_1)^{-1}}\otimes f\right)_i = \begin{cases} f_{2i}, & \text{якщо } i<\frac{2^n}{2},\\ f_{2i-2^n}\oplus f_{2i-2^n+1}, & \text{якщо } i\ge\frac{2^n}{2}, \end{cases} \tag{8}$$

$i=0,\,1,\,\dots,\,2^n-1$.

Приклад 1. *Для бульової функції* $f=(0,0,1,1,1,0,1,0)^T$ *побудувати* $\tilde\alpha$*-канонічний поліном для* $\tilde\alpha=(1,0,1)$.

Обчисливши добуток $(K'_{\tilde\alpha})^{-1}\otimes f$ на основі формул (7), (8) отримаємо:

$$(K'_{\tilde\alpha})^{-1}\otimes f=(1,0,1,0,0,1,1,0)^T.$$

Згідно (5) маємо $a_0=a_2=a_5=a_6=1$, $a_1=a_3=a_4=a_7=0$. Побудуємо елементарні кон'юнкції $R^{\tilde\beta}_{\tilde\alpha}$ для заданого $\tilde\alpha=(1,0,1)$ та наборів $\tilde\beta$ з номерами $\beta\in\{0,2,5,6\}$, на яких добуток $(K'_{\tilde\alpha})^{-1}\otimes f$ приймає значення рівне 1:

$$R^{(0,0,0)}_{(1,0,1)}=1,\quad R^{(0,1,0)}_{(1,0,1)}=\bar Y,\quad R^{(1,0,1)}_{(1,0,1)}=XZ,\quad R^{(1,1,0)}_{(1,0,1)}=X\bar Y.$$

Будуємо суму по $\bmod 2$ знайдених елементарних кон'юнкцій, отримаємо

$$P_{(1,0,1)}(f)=1\oplus\bar Y\oplus X\bar Y\oplus XZ.$$

1. *Супрун В. П.* Сложность булевых функций в классе канонических поляризованных полиномов // Дискретная математика. – 1993. – **5**, вып. 2. – С. 111–115.
2. *Винокуров С. Ф., Перязев Н. А.* Полиномиальные разложения булевых функций // Кибернетика и систем. анализ. – 1993. – №6. – С. 34–47.
3. *Мич І. А., Трофимлюк О. Т.* Застосування узагальнених кон'юнктивних перетворень в теорії бульових функцій // Вісник держ. ун-ту "Львівська політехніка". Сер. прикл. матем. – 1998. – №337. – С.47–49.

Одержано 08.10.2007