Серия «Математика»
2009. Т. 2, № 2, С. 72—81

Онлайн-доступ к журналу:
http://isu.ru/izvestia

ИЗВЕСТИЯ
Иркутского
государственного
университета

УДК 519.71

Оценки сложности шаблонов минимизации полиномиальных форм булевых функций *

К. Д. Кириченко
Восточно-Сибирская государственная академия образования

Аннотация. В статье вводится понятие шаблона минимизации полиномиальных форм булевых функций, приводится классификация шаблонов и доказываются некоторые оценки сложности.

Ключевые слова: булевы функции; полиномиальные нормальные формы; функция Шеннона.

1. Шаблоны минимизации полиномиальных форм

Одной из актуальных задач дискретной математики является задача нахождения и минимизации представлений конечнозначных, и в частности булевых функций. Здесь рассматривается вопрос о представлении булевых функций многочленами. В теории булевых функций такие представления носят название полиномиальных нормальных форм (ПНФ). Некоторые верхние оценки сложности ПНФ можно найти в работах [3, 2, 5, 4].

Сформулируем некоторые определения.

Определение 1. Полиномиальной нормальной формой булевой функции $f(z_1, \ldots, z_n)$ будем называть представление вида

$$f(z_1, \ldots, z_n) = \sum_{i=1}^{s} \prod_{j=1}^{n} (y_j^i z_j \oplus x_j^i \bar{z}_j)$$

Здесь x_j^i и y_j^i это коэффициенты из поля $\{0, 1\}$, при подстановке которых каждая скобка обращается либо в z_i, либо в $\bar{z}_i$, либо в 1. От-

* Работа выполнена при финансовой поддержке РФФИ, грант 09–01–00476а.

метим, что при $x_j^i = y_j^i = 0$, скобка обращается в ноль, однако такая подстановка с точки зрения минимизации бессмысленна.

Определение 2. Сложностью ПНФ $\sum\limits_{i=1}^{s}\prod\limits_{j=1}^{n}(y_j^i z_j \oplus x_j^i \bar{z}_j)$ будем называть число слагаемых s.

Определение 3. Сложностью булевой функции L(f) в классе ПНФ будем называть минимум из сложностей ПНФ, представляющих данную функцию.

Определение 4. Функцией Шеннона $L(n)$ сложности булевых функций в классе ПНФ будем называть максимум из сложностей по всем функциям n переменных.

Для $L(n)$ лучшей по порядку доказанной нижней оценкой является $\frac{2^n}{n\log_2 3}$ [4], а верхней $\frac{2(\log_2 n+1)2^n}{n}$ [3]. В связи с тем что эти оценки на сегодняшний день различаются, интересным и актуальным является вопрос их уточнения.

Для нахождения ПНФ для данной булевой функции f, требуемой сложности s можно воспользоваться методом неопределенных коэффициентов, подставив значения аргументов и значение функции в ПНФ с неопределенными коэффициентами, что позволит получить следующую систему из 2^n уравнений.

$$R = \begin{cases} y_1^1 y_2^1 \cdots y_n^1 \oplus y_1^2 y_2^2 \cdots y_n^2 \oplus \ldots \oplus y_1^s y_2^s \cdots y_n^s = f(1,1,\ldots,1) \\ x_1^1 y_2^1 \cdots y_n^1 \oplus x_1^2 y_2^2 \cdots y_n^2 \oplus \ldots \oplus x_1^s y_2^s \cdots y_n^s = f(0,1,\ldots,1) \\ y_1^1 x_2^1 \cdots y_n^1 \oplus y_1^2 x_2^2 \cdots y_n^2 \oplus \ldots \oplus y_1^s x_2^s \cdots y_n^s = f(1,0,\ldots,1) \\ x_1^1 x_2^1 \cdots y_n^1 \oplus x_1^2 x_2^2 \cdots y_n^2 \oplus \ldots \oplus x_1^s x_2^s \cdots y_n^s = f(0,0,\ldots,1) \\ \ldots \quad\quad \ldots \quad\quad \ldots \quad \ldots \quad\quad \ldots \\ x_1^1 x_2^1 \cdots x_n^1 \oplus x_1^2 x_2^2 \cdots x_n^2 \oplus \ldots \oplus x_1^s x_2^s \cdots x_n^s = f(0,0,\ldots,0) \end{cases}$$

Таким образом, каждый многочлен в левой части уравнения соответствует некоторому двоичному набору. Поэтому мы будем обозначать его $R_{\tilde{\tau}}$, а уравнение записывать в виде $R_{\tilde{\tau}} = f(\tilde{\tau})$

Данная система уже может рассматриваться как система уравнений над полем Z_2. Любому решению такой системы однозначно сопоставляется некоторая ПНФ, представляющая заданную булеву функцию. Если решение системы не существует, то ПНФ длины s отсутствует.

В настоящее время разработано несколько методов решения нелинейных уравнений над полем Z_2, однако ни один из этих методов не позволяет быстро находить решения в общем случае. Так, для примера, наиболее известный в настоящее время метод линеаризации не будет являться достаточно эффективным по причине слишком большой нелинейности в данной системе. Обзор методов решения нелинейных уравнений над конечными полями можно найти в обзоре[1].

Для исследования вопросов сложности ПНФ нами был разработан метод шаблонов.

Пусть определена некоторая подстановка σ, заменяющая некоторые из переменных на термы. Тогда обоначим $R_{\tilde{\tau}}(\sigma)$ многочлен $R_{\tilde{\tau}}$ после подстановки σ

Определение 5. Шаблоном $\langle s(n), \sigma\rangle$ будем называть такую константу $s(n)$, зависящую от числа переменных булевой функции n, и такую подстановку σ, заменяющую некоторые из переменных системы R на некоторые термы (в том числе константы), после применения которой система $R(\sigma)$ может быть разделена на подсистемы $R^0(\sigma), \dots R^k(\sigma)$, такие что каждый многочлен $R^i_{\tilde{\tau}}(\sigma)$ представляется в виде $R^i_{\tilde{\tau}}(\sigma) = L^i_{\tilde{\tau}} + P^i_{\tilde{\tau}}$, причем $L^i_{\tilde{\tau}}$ это многочлен первой степени, и все переменные входящие в L^i (линейные части подсистемы $R^i(\sigma)$) не встречаются в $R^0(\sigma), \dots, R^{i-1}(\sigma)$.

Определение 6. Шаблон будем называть универсальным, если для всех L^i верно что $rang(L^i) = |L_i|$, то есть все многочлены входящие в L^i являются линейно независимыми.

Теорема 1. *Теорема. Пусть $\langle s(n), \sigma\rangle$ некоторый универсальный шаблон. Тогда $L(n) \leq s(n)$*

Доказательство. Определим значения всех переменных, входящих в P^0 как 0. Из определения шаблона следует, что не изменит подсистему L^0 Тогда, из линейной независимости всех многочленов, следует, что все уравнения входящие в подсистему из L^0 могут быть решены. Выберем одно произвольное решение и поставим значения во все уравнения. Далее аналогично придадим оставшимся переменным P^1 значения 0, что вновь не изменит часть L^1. Для нее вновь найдется решение и так далее. □

Определение 7. Мерой универсальности шаблона будем называть сумму рангов его линейных частей. $U(\langle s(n), \sigma\rangle) = \sum\limits_{i=1}^{k} rang(L^i)$

Теорема 2. *Пусть $\langle s(n), \sigma\rangle$ некоторый шаблон. Тогда выполняется следующее неравенство*

$$L(n) \leq s(n) + 2^n - U(\langle s(n), \sigma\rangle)$$

Доказательство. Покажем, что при увеличении $s(n)$ на единицу мера универсальности шаблона также может быть увеличена как минимум на один.

Пусть один из многочленов $L_{\tilde{\tau}}$ является линейно зависимым и этот многочлен входит в уравнение $L_{\tilde{\tau}} + P_{\tilde{\tau}} = f(\tilde{\tau})$. Тогда преобразуем шаблон, увеличив в исходном шаблоне $s(n)$ на единицу.

В результате к каждому уравнению будет добавлено некоторое произведение n из $2n$ новых переменных, причем все эти произведения являются различными. При этом к многочлену $L_{\tilde{\tau}}$ будет добавлено некоторое произведение $t_1 t_2 \cdots t_n$, где каждая t_i или $x_i^{s(n)+1}$ или $y_i^{s(n)+1}$. Тогда добавим к исходному шаблону новую подстановку в которой t_2, t_3, $\ldots t_n$ будут заменены на 1, а все остальные добавленные переменные на ноль. В результате к $L_{\tilde{\tau}}$ будет добавлена новая переменная t_1, что сделает многочлен линейно независимым и увеличит ранг на единицу. При этом все остальные добавленные произведения обратятся в ноль, то есть все остальные уравнения не изменятся. □

Теорема 3. *Для любого n существует универсальный шаблон длины $L(n)$.*

Доказательство. Из определения функции Шеннона $L(n)$ следует, что для любой булевой функции можно построить ПНФ длины $L(n)$. Это означает, что система уравнений R для $s(n) = L(n)$ будет иметь решение при любых значениях коэффициентов в правой части. Обозначим $\tilde{\gamma}$ вектор коэффициентов в правой части. Фактически $\tilde{\gamma}$ есть векторное представление некоторой булевой функции n переменных. Обозначим за $x_j^i(\tilde{\gamma})$ значение переменной x_j^i в решении системы с вектором коэффициентов $\tilde{\gamma}$. Обозначим за $fx_j^i(t_1, \ldots, t_{2^n})$ булеву функцию, заданную вектором значений $x_j^i(\tilde{\gamma})$ для всех векторов $\tilde{\gamma}$. Аналогично определим функцию fy_j^i. В качестве подстановки для переменных x_j^i и y_j^i возьмем полиномы Жегалкина для функций fx_j^i и fy_j^i соответственно. Очевидно, что такая подстановка обратит многочлен в уравнении с номером k в одну переменную t_k. Очевидно, что такая подстановка удовлетворяет данному определению шаблона. □

Несмотря на то, что универсальный шаблон существует, его построение фактически эквивалентно построению формулы, минимизирующей полиномиальные представления булевых функций. Поэтому в настоящем исследовании напротив построение универсальных шаблонов будет использоваться для нахождения верхних оценок сложности фукции Шеннона ПНФ булевых функций.

2. Шаблоны первого рода

Введем определение шаблона первого рода. Для этого выберем произвольный набор $\tilde{\alpha}^1, \ldots, \tilde{\alpha}^s$ из s булевых векторов длины n. Будем называть его векторным представлением шаблона первого рода. Сам шаблон будет определяться следующим образом. Если $\alpha_j^i = 1$, то заменяем y_j^i на 1, x_j^i оставляем без изменения. Если $\alpha_j^i = 0$, то заменяем y_j^i на 0, а x_j^i на 1.

Напомним, что обозначение $[P]$, где P — некоторый предикат, означает функцию, равную 1, если предикат истинен, и ноль в противном случае. За $||\tilde{\alpha}||$ обозначается вес набора $\tilde{\alpha}$ — количество единиц в наборе.

Теорема 4. *Пусть $\tilde{\alpha}^1, \ldots, \tilde{\alpha}^s$ — векторное представление шаблона первого рода $\langle s(n), \sigma \rangle$. Тогда*

$$U(\langle s(n), \sigma \rangle) = \sum_{\tilde{\tau} \in \{0,1\}^n} \left[\sum_{j=1}^{s} [\tilde{\alpha}^j > \tilde{\tau}][||\tilde{\alpha}^j|| = ||\tilde{\tau}|| + 1] > 0 \right]$$

Словесно эту формулу можно выразить так: мера универсальности шаблона первого рода равна количеству двоичных векторов длины n, таких что заменой некоторого нуля на единицу можно получить один из векторов векторного представления шаблона.

Доказательство. Обозначим за $T^i_{\tilde{\tau}}$ слагаемое многочлена $R_{\tilde{\tau}}$, составленное из переменных x^i_j и y^i_j. Из определения шаблона $T^i_{\tilde{\alpha}_i}(\sigma) = 1$. Если некоторый набор $\tilde{\tau}$ меньше набора $\tilde{\alpha}_i$ и $j1, \ldots, jk$ — множество номеров меньших компонент, то $T^i_{\tilde{\tau}}(\sigma) = x^i_{j1} x^i_{j2} \ldots x^i_{jk}$. Для всех других наборов $T^i_{\tilde{\tau}}(\sigma) = 0$.

Таким образом, система уравнений $R_{\tilde{\tau}}(\sigma) = f(\tilde{\tau})$ разбивается на подсистемы $R^0, ..., R^n$ по следующему правилу: уравнение $R_{\tilde{\tau}}(\sigma) = f(\tilde{\tau})$ попадает в подсистему R^i, если $||\tilde{\tau}|| = n - i$. При этом все слагаемые первой степени попадут в $L_{\tilde{\tau}}$, прочие слагаемые в $P_{\tilde{\tau}}$. Легко заметить, что каждая переменная входит только в один многочлен $L_{\tilde{\tau}}$, поэтому все непустые многочлены линейно независимы. Из этого и следует формула из формулировки теоремы. □

Для понимания характеристик шаблона рассмотрим меру универсальности случайного шаблона первого рода.

Определение 8. Будем говорить, что шаблон первого рода является случайным с характеристикой p, если для построения используется следующий принцип: последовательно тестируем все возможные двоичные вектора длины n и с вероятностью p, независимо друг от друга, включаем их в шаблон.

Теорема 5. *Математическое ожидание меры универсальности случайного шаблона с характеристикой p выражается следующей формулой.*

$$M(U(\langle s(n), \sigma \rangle)) = 2^n - (2 - p)^n$$

Доказательство. Найдем вероятность того, что из случайно выбранный вектор $\tilde{\tau}$ заменой одной единички на ноль можно получить один из векторов шаблона. Эта вероятность зависит от количества единиц в выбранном наборе, поэтому необходимо использовать формулу сложной

вероятности. Для нахождения искомой вероятности найдем обратную вероятность: вероятность того, что ни один из векторов полученных заменой единицы на ноль не принадлежит шаблону. Это приводит нас к следующей формуле

$$P = 1 - \sum_{i=0}^{n} \frac{1}{2^n} \left(\begin{array}{c} i \\ n \end{array} \right) (1-p)^i = 1 - \frac{(1+1-p)^n}{2^n}$$

Таким образом, метематическое ожидание количества нужных векторов определяется по формуле $2^n - (2-p)^n$. □

Следствие 1. *Существует универсальный шаблон первого рода сложности* $2^n \frac{2\ln n+1}{n}$

Доказательство. В качестве p выберем $\frac{2\ln n}{n}$. Тогда математическое ожидание меры универсальности шаблона примет вид

$$M(U(\langle s(n), \sigma \rangle)) = 2^n - (2 - \frac{2\ln n}{n})^n = 2^n - 2^n(1 - \frac{1}{\ln n})^n >$$

$$> 2^n - 2^n e^{-\ln n} = 2^n \frac{n-1}{n}$$

При этом математическое ожидание мощности шаблона примет вид $s(n) = 2^n \frac{2\ln n}{n}$. Отсюда, с использованием теоремы 2 получаем формулу из формулировки следствия. □

Данная оценка несколько улучшает оценку, найденную автором ранее [3].

3. Шаблоны второго рода

Введем определение шаблона второго рода. Для этого выберем произвольный набор $\tilde{\alpha}^1, \ldots, \tilde{\alpha}^{s/2}$ из $s/2$ булевых векторов длины n. Будем называть его векторным представлением шаблона второго рода. Сам шаблон будет определяться следующим образом. Если $\alpha_j^i = 1$, то заменяем y_j^{2i-1} на 1, x_j^{2i-1} на t_j^i, y_j^{2i} на 1, x_j^{2i} на $t_j^i \oplus 1$. Если $\alpha_j^i = 0$, то заменяем y_j^{2i-1} и y_j^{2i} на 0, а x_j^{2i-1} и x_j^{2i} на 1.

Как и в шаблоне первого рода, система уравнений $R_{\tilde{\tau}}(\sigma) = f(\tilde{\tau})$ разбивается на подсистемы $R^0, ..., R^n$ по правилу: уравнение $R_{\tilde{\tau}}(\sigma) = f(\tilde{\tau})$ попадает в подсистему R^i, если $||\tilde{\tau}|| = n-i$. При этом все слагаемые первой степени попадут в $L_{\tilde{\tau}}$, прочие слагаемые в $P_{\tilde{\tau}}$.

Из определения шаблона следует что если некоторый вектор $\tilde{\alpha}_i$ принадлежит векторному представлению шаблона второго рода и $||\tilde{\alpha}_i|| = m$, то для некоторого набора $\tilde{\tau}$, такого что $||\tilde{\alpha}_i|| = ||\tilde{\tau}|| + 1$, и $\tilde{\tau} > \tilde{\alpha}_i$ то

в уравнение для $f(\tilde{\tau})$ будут входить слагаемые $t^i_j \oplus t^i_j \oplus 1 = 1$. Если же $||\tilde{\alpha}_i|| = ||\tilde{\tau}||+2$, то в уравнение попадут слагаемые $t^i_j t^i_k \oplus (t^i_j \oplus 1)(t^i_k \oplus 1) = t^i_j \oplus t^i_k \oplus 1$.

Определение 9. Будем говорить что переменная шаблона второго рода t^i_j соответствует набору $\tilde{\beta}$, если набор $\tilde{\beta}$ получен из набора $\tilde{\alpha}$ заменой единицы, стоящей в j-той позиции на ноль. Из определения шаблона второго рода следует, что в наборе $\tilde{\alpha}_i$ на j-том месте обязательно находится единица.

Отметим, что переменная t^i_j, соответствующая набору $\tilde{\beta}$ входит только в такие многочлены $R_{\tilde{\tau}}$ для которых $\tilde{\tau} < \tilde{\beta}$. Таким образом, если две переменные соответствуют одному набору, то множества уравнений в которые входят эти переменные совпадают.

Для исследования свойств шаблонов второго рода рассмотрим класс матриц специального вида, которые будут определены далее.

Обозначим за E_{nk} квадратную матрицу размера $\begin{pmatrix} n \\ k \end{pmatrix}$ у которой на побочной диагонали находятся единицы, а остальные элементы нули.

Определение 10. Матрицей биномиальных квадратов B_{nk} будем называть матрицу с коэффициентами из поля Z_2, состоящую из $\begin{pmatrix} n \\ k+1 \end{pmatrix}$ столбцов и $\begin{pmatrix} n \\ k \end{pmatrix}$ строк, которая определяется следующими соотношениями: для $k \geq n$ и $k < 0$ матрица пуста (содержит ноль строк и столбцов). Для остальных значений k матрица имеет вид

$$B_{nk} = \begin{pmatrix} E_{n-1,k} & B_{n-1,k} \\ B_{n-1,k-1} & 0 \end{pmatrix}$$

Приведем пример матриц $B_{4,2}$ и $B_{4,1}$

$$B_{4,2} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} \quad B_{4,1} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Лемма 1. $rang(B_{nk}) = \begin{pmatrix} n-1 \\ k \end{pmatrix}$

Доказательство. Каждому столбцу и каждой строке матрицы сопоставим двоичный наборы длины n. по следующим правилам. Столбцу с номером i будет сопоставлен набор $(1, \tau_2, \ldots, \tau_n)$, если $i \leq \begin{pmatrix} n-1 \\ k \end{pmatrix}$ и

набор $(\tau_2, \ldots, \tau_n)$ сопоставлен столбцу с номером i в матрице $B_{n-1,k-1}$, и столбцу с номером i будет сопоставлен набор $(0, \tau_2, \ldots, \tau_n)$, в том случае если $i > \left(\begin{array}{c} n-1 \\ k \end{array} \right)$ и набор $(\tau_2, \ldots, \tau_n)$ сопоставлен столбцу с номером $i - \left(\begin{array}{c} n-1 \\ k \end{array} \right)$ в матрице $B_{n-1,k}$. При этом единственному столбцу матрицы $B_{n,n-1}$ сопоставляется единичный набор, а i-тому столбцу матрицы $B_{n,0}$ набор, в котором в i-той позиции находится единица, остальные нули.

Легко показать, что при таком построении все наборы будут содержать ровно $k+1$ единицу, все наборы будут различными и будут упорядочены в порядке лексикографического убывания.

Строке с номером i сопоставим набор $(0, \tau_2, \ldots, \tau_n)$, если $i \leq \left(\begin{array}{c} n-1 \\ k \end{array} \right)$ и набор $(\tau_2, \ldots, \tau_n)$ сопоставлен строке с номером i в матрице $B_{n-1,k}$. Строке с номером i сопоставим набор $(1, \tau_2, \ldots, \tau_n)$, если $i > \left(\begin{array}{c} n-1 \\ k \end{array} \right)$ и набор $(\tau_2, \ldots, \tau_n)$ сопоставлен строке с номером $i - \left(\begin{array}{c} n-1 \\ k \end{array} \right)$ в матрице $B_{n-1,k-1}$.

Аналогично, такое построение гарантирует, что все наборы будут различными, будут содержать ровно k единиц, и будут упорядочены в порядке лексикографического возрастания. Заметим, что количество строк в матрице совпадает с количеством двоичных наборов веса k, а количество столбцов с количеством наборов веса $k+1$. Таким образом, каждый двоичный набор веса k или $k+1$ соответствует одной из строк или столбцов.

Таким образом, если набор $(0, \tau_2, \ldots, \tau_n)$ соответствует строке с номером i, то набор $(1, \tau_2, \ldots, \tau_n)$ соответствует столбцу с номером $\left(\begin{array}{c} n-1 \\ k \end{array} \right) + 1 - i$. Отсюда легко показать что элемент b_{ij} матрицы B_{nk} равен единице тогда и только тогда, когда набор соответствующий строке i строго меньше набора соответствующего столбцу j.

Далее докажем следующее вспомогательное утверждение. Пусть $\tilde{\beta}$ некоторый набор веса $k+2$ и $\tilde{\alpha}^1, \ldots, \tilde{\alpha^{k+2}}$ все наборы веса $k+1$ строго меньшие набора $\tilde{\beta}$. Тогда сумма столбцов матрицы B_{nk}, соответствующих наборам $\tilde{\alpha}^1, \ldots, \tilde{\alpha^{k+2}}$ равна нулю. Действительно, если некоторый набор $\tilde{\gamma}$ веса k меньше набора $\tilde{\beta}$, то найдется ровно два набора из множества $\tilde{\alpha}^1, \ldots, \tilde{\alpha^{k+2}}$, которые будут больше набора $\tilde{\gamma}$. Таким образом, в выбранных столбцах матрицы, в каждой строке либо ни одной, либо ровно две единицы, поэтому сумма таких столбцов равна нулю.

Рассмотрим столбец который соответствует некоторому набору вида $(0, \tau_2, \ldots, \tau_n)$. Этот набор меньше набора $(1, \tau_2, \ldots, \tau_n)$, для которого

из всех $k+2$ меньших его наборов, только один набор $(0, \tau_2, \ldots, \tau_n)$ начинается с нуля, прочие с единицы. Поэтому, из доказанного выше утверждения, столбец соответствующий набору $(0, \tau_2, \ldots, \tau_n)$ является линейной комбинацией некоторых столбцов, соответствующих наборам, которые начинаются с единицы. В силу этого $rang(B_{nk}) \leq \left(\begin{array}{c} n-1 \\ k \end{array} \right)$. Вместе с тем, очевидно, что первые $\left(\begin{array}{c} n-1 \\ k \end{array} \right)$ столбцов являются линейно независимыми, что доказывает лемму. □

Теорема 6. *Для любого шаблона второго рода выполняется неравенство* $U(< s(n), \sigma >) \leq 2^{n-1} - 1$

Доказательство. Очевидно, что ранги линейных частей системы уравнений могут только увеличиться при добавлении переменных. Поэтому, максимальную меру универсальности будет иметь шаблон второго рода, векторное представление которого содержит все двоичные наборы.

Каждой переменной при этом соответствует некоторый набор. Очевидно, что при этом всем двоичным наборам кроме единичного, будет соответствовать некоторая переменная. При этом если одному набору соответствует несколько переменных, то все эти переменные входят в одни и те же уравнения, поэтому все такие переменные, кроме одной, могут быть удалены и ранг при этом не уменьшится.

Отметим, что многочлены, входящие в L^0 и L^1 будут пустыми, так как из определения шаблона второго рода следует, что в них не будет ни одной переменной. Для $i \geq 2$ L^i будет содержать $\left(\begin{array}{c} n \\ i \end{array} \right)$ уравнений и $\left(\begin{array}{c} n \\ i+1 \end{array} \right)$ переменных. Каждому многочлену при этом соответствует некоторый набор веса i, а переменной некоторый набор веса $i+1$.

Переменная соответствующая набору $\tilde{\beta}$ будет входить в многочлен $L^i_{\tilde{\tau}}$, только в том случае если $\tilde{\tau} < \tilde{\beta}$. Таким образом, множество многочленов L^i для шаблона второго рода, составленного из всех двоичных векторов задается матрицей $B_{n,n-i}$.

Таким образом, получаем следующее значение для меры универсальности шаблона

$$U(\langle s(n), \sigma \rangle) = \sum_{i=2}^{n} rang(B_{n,n-i}) = \sum_{i=0}^{n-2} rang(B_{n,i}) = \sum_{i=0}^{n-2} \left(\begin{array}{c} n-1 \\ i \end{array} \right) = 2^{n-1} - 1$$

□

Из доказанной теоремы следует что шаблоны второго рода неприменимы для получения более точных оценок $L(n)$, однако некоторые их свойства позволяют сделать предположение о том, что объединение

шаблонов первого и второго рода позволит в дальнейшем получить более эффективные оценки.

Список литературы

1. Агибалов Г. П. Методы решения систем полиномиальных уравнений над конечным полем // Вестник Томского Государственного Университета. — Август 2006. — С. 4-9.
2. Винокуров С. Ф., Казимиров А. С. Верхняя оценка сложности булевых функций в классе ПНФ // Алгебра и теория моделей. Сборник статей. Изд-во НГТУ.— 2003. — С. 160-165.
3. Кириченко К.Д. Верхняя оценка сложности полиномиальных нормальных форм булевых функций // Дискретная математика. Том 17, выпуск 3. — 2005. — С. 81-88.
4. Even S., Kohavi I., Paz A. On minimal modulo 2 sums of products for switching function// IEEE Trans. Elect. Comput. — Oct. 1967. — P. 671–674.
5. Sasao T. FPGA design by generalized functional decomposition// Logical Synthesis and Optimization. — Kluwer Academic Publishers. — 1993. — P. 233-258.

K. D. Kirichenko
Bounds of the minimization patterns' complexity of ESOP

Abstract. In this paper we introduce the concept of minimization pattern for ESOP. We propose the classification of patterns and prove some bounds of their complexity.

Кириченко Константин Дмитриевич, кандидат физико-математических наук, Восточно-Сибирская государственная академия образования, 664011, Иркутск, ул. Нижняя набережная 6,тел.: (3952)241097 (constkir@gmail.com)

Konstantin Kirichenko, East Siberian State Teacher Training University, 6, Nignyya Naberegnaya, Irkutsk, 664011 Phone: (3952)241097 (constkir@gmail.com)