УДК 681.322

Ткаченко В.Г.
Ткаченко В.Г.
Tkachenco V.G.

МЕТОД ПОСТРОЕНИЯ БЛОКОВ МОНОТОННЫХ БУЛЕВЫХ ФУНКЦИЙ

МЕТОД ПОБУДОВИ БЛОКІВ МОНОТОННИХ БУЛЬОВИХ ФУНКЦІЙ

THE METHOD FOR CONSTRUCTING BLOCKS OF MONOTONOUS BOOLEAN FUNCTIONS

Аннотация. Разработан метод построения блоков монотонных булевых функций (МБФ) для классификации и анализа этих функций. Этот метод является составной частью метода синтеза надежных цифровых схем на базе МБФ. Проведено сравнение этого метода с методом классификации МБФ на типы. Рассмотрено применение метода построения блоков на примере классификации и анализа МБФ от малого числа переменных. Доказано, что матрица распределения типов МБФ R_n и матрица распределения максимальных типов МБФ M_n произвольного ранга n находятся из матрицы (1) размерности 1×1.

Анотація. Розроблено метод побудови блоків монотонних бульових функцій (МБФ) для класифікації та аналізу цих функцій, на прикладі функцій з малою кількістю змінних. Цей метод є складовою частиною методу синтезу надійних цифрових схем на базі МБФ. Проведено порівняння цього методу з методом класифікації МБФ на типи. Розглянуто застосування методу побудови блоків на прикладі класифікації та аналізу МБФ від малого числа змінних. Доведено, що матриця розподілення типів МБФ R_n і матриця розподілення максимальних типів МБФ M_n довільного рангу n знаходяться з матриці (1) розмірності 1×1.

Summary. The method for constructing blocks of monotonous Boolean functions (MBF) for classification and analysis of these functions is developed. This method is part of the method of synthesis of reliable digital circuits based on MBF. A comparison of this method with the method of classification of MBF by types has been done. Application of the method of constructing blocks on the example of classification and analysis of MBF on a small number of variables is considered. The matrix of MBF types distribution R_n and the matrix of maximal MBF types distribution M_n for arbitrary rank n are found from matrix (1) of dimension 1×1 is proved.

В настоящее время значительно расширилась сфера применения цифровых схем. В области телекоммуникаций эти схемы широко используются при сжатии и кодировании передаваемой информации, при цифровой коммутации, в маршрутизаторах и шлюзах. В связи с этим возникает проблема синтеза надежных цифровых схем. В частности это могут быть цифровые схемы, построенные на основе монотонных булевых функций (МБФ). Такие схемы являются более надежными [1], чем схемы, построенные на основе всех булевых функций.

В [2,3] разработана классификация МБФ на типы и перечисление максимальных типов МБФ. Здесь же показано, что для синтеза цифровых схем на основе МБФ необходимо сначала перебрать типы, а затем выполнить полный перебор всех МБФ, принадлежащих определенному типу. В [4] доказано выражение для перечисления типов МБФ в виде произведения матриц.

Однако в литературе не рассмотрен метод анализа и классификации МБФ на основе построения блоков МБФ (множеств МБФ, связанных рассмотренными далее тремя операциями), который в ряде случаев позволяет сократить перебор МБФ даже по сравнению с методом классификации МБФ на типы.

Целью статьи является разработка метода анализа и классификации МБФ на основе построения блоков МБФ.

Напомним основные понятия, связанные с МБФ. Вектор $P = (a_n,\ldots, a_i,\ldots, a_1, a_0)$, компоненты которого принимают значения из множества $\{0,1\}$, называется [3] входным набором булевой функции от n переменных. Множество всех таких входных наборов образует булев куб ранга n. Сами входные наборы P являются вершинами булева куба. Любая булева функция определяется множеством вершин булева куба, на которых эта функция равна единице. Любое множество несравнимых вершин булева куба называется антицепью. Для задания МБФ [3] достаточно указать некоторую антицепь в булевом кубе. Каждая вершина антицепи (кроме вершин соответствующих входным наборам (0,...,0) и (1,...,1)) определяет конъюнкцию в минимальной дизъюнктивной форме МБФ, соответствующей данной антицепи.

Рассмотрим все МБФ рангов от 0 до 3. Имеется всего две МБФ ранга 0. Это $f_0(0)$ тождественно равная 0 и $f_1(0)$ тождественно равная 1. Имеется три МБФ ранга 1. Это $f_0(1)$ тождественно равная 0, $f_1(1)$ тождественно равная 1 и $f_2(1) = x_1$. Имеется шесть МБФ ранга 2. Это $f_0(2)$ тождественно равная 0, $f_1(2)$ тождественно равная 1, $f_2(2) = x_1$, $f_3(2) = x_2$, $f_4(2) = x_1x_2$ и $f_5(2) = x_1 \vee x_2$ ($\vee$ – операций дизъюнкции). Имеется двадцать МБФ ранга 3. Это $f_0(3)$ тождественно равная 0; $f_1(3)$ тождественно равная 1; $f_2(3) = x_1$; $f_3(3) = x_2$; $f_4(3) = x_3$; $f_5(3) = x_1x_2$; $f_6(3) = x_1x_3$; $f_7(3) = x_2x_3$; $f_8(3) = x_1 \vee x_2$; $f_9(3) = x_1 \vee x_3$; $f_{10}(3) = x_2 \vee x_3$; $f_{11}(3) = x_1x_2 \vee x_1x_3$; $f_{12}(3) = x_1x_2 \vee x_2x_3$; $f_{13}(3) = x_1x_3 \vee x_2x_3$; $f_{14}(3) = x_1 \vee x_2 \vee x_3$; $f_{15}(3) = x_1x_2 \vee x_1x_3 \vee x_2x_3$; $f_{16}(3) = x_1x_2x_3$, $f_{17}(3) = x_1 \vee x_2x_3$; $f_{18}(3) = x_2 \vee x_1x_3$ и $f_{19}(3) = x_3 \vee x_1x_2$.

Относительно операций дизъюнкции и конъюнкции все МБФ одного ранга образуют дистрибутивную решетку. Такие решетки R_0, R_1, R_2 и R_3 для рангов МБФ от 0 до 3 изображены на рис. 1. Решетки R_1, R_2 и R_3 отличаются от свободных дистрибутивных решеток такого же ранга добавлением самой верхней и самой нижней вершин.

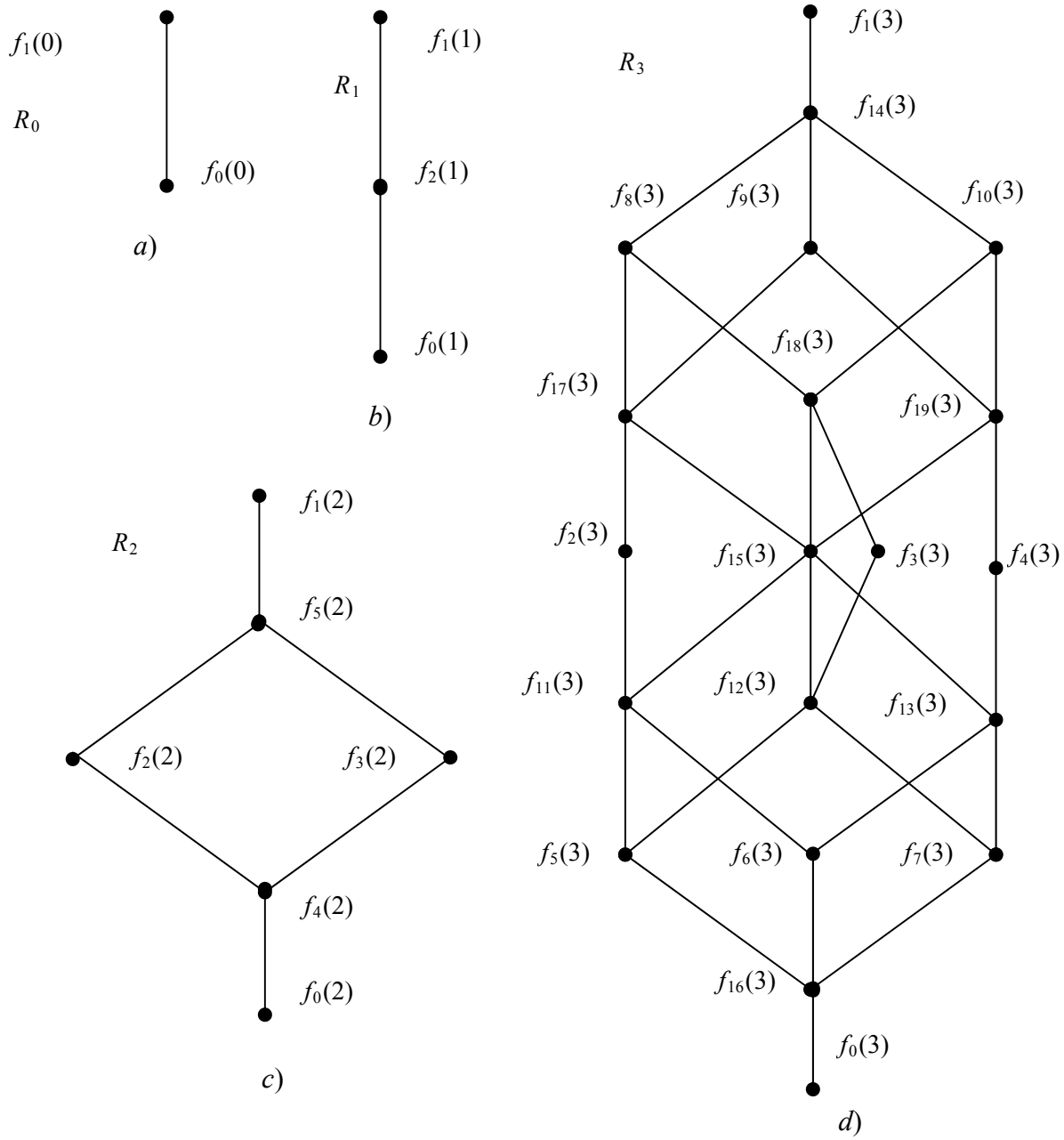

Рисунок 1 – Решетки МБФ *a*)R_0, *b*)R_1, *c*)R_2 и *d*)R_3

В [4] на множестве МБФ любого ранга определены три унарные операции: двойственность, дизъюнктивное дополнение и конъюнктивное дополнение. Для получения дизъюнктивного

дополнения $\overline{f_i}(n)$ от i-й МБФ $f_i(n)$ нужно заменить в минимальной дизъюнктивной форме каждую конъюнкцию из m переменных на конъюнкцию из всех $n - m$ переменных, не входящих в первоначальную конъюнкцию. Для получения конъюнктивного дополнения $\underline{f_i}(n)$ от i-й МБФ $f_i(n)$ нужно заменить в минимальной конъюнктивной форме каждую дизъюнкцию из m переменных на дизъюнкцию из всех $n - m$ переменных, не входящих в первоначальную дизъюнкцию. Для получения двойственной МБФ $f_i^{-1}(n)$ от i-й МБФ $f_i(n)$ нужно заменить в минимальной дизъюнктивной форме все операции конъюнкции на операции дизъюнкции и одновременно заменить все операции дизъюнкции операциями конъюнкции. При этом двойственная МБФ $f_i^{-1}(n)$ получается в минимальной конъюнктивной форме. Для получения двойственной МБФ $f_i^{-1}(n)$ в минимальной дизъюнктивной форме нужно в полученной минимальной конъюнктивной форме раскрыть скобки и привести подобные члены.

Относительно рассмотренных трех операций МБФ рангов 0 и 1 группируются в один блок, состоящий и двух и из трех МБФ соответственно. МБФ ранга 2 можно представить в виде двух блоков, один из которых состоит из четырех МБФ, а другой – из двух МБФ. Все эти блоки показаны на рис. 2. Здесь операция двойственности изображается сплошной линией, операция дизъюнктивного дополнения – штриховой линией и операция конъюнктивного дополнения – штрихпунктирной линией. Например, в блоке, состоящем из МБФ $f_0(2)$, $f_1(2)$, $f_4(2)$ и $f_5(2)$ имеем: $f_1(2) = f_0^{-1}(2)$, $f_5(2) = \underline{f_0}(2)$ и $f_4(2) = \overline{f_1}(2)$.

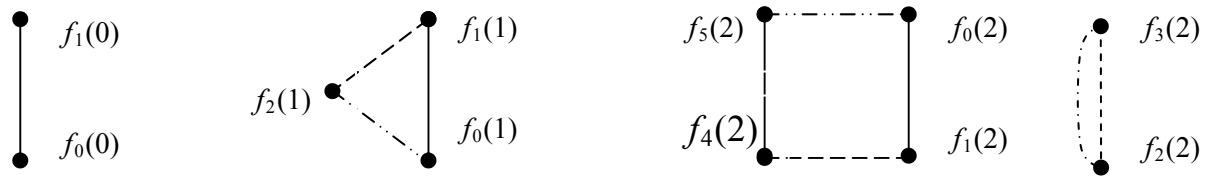

Рисунок 2 – Блоки МБФ рангов от 0 до 2

Все МБФ ранга 3 распадаются на 4 блока по 5 элементов. На рис. 3 показаны эти блоки. МБФ $f_2(3)$, $f_3(3)$, $f_4(3)$ и $f_{15}(3)$ являются самодвойственными.

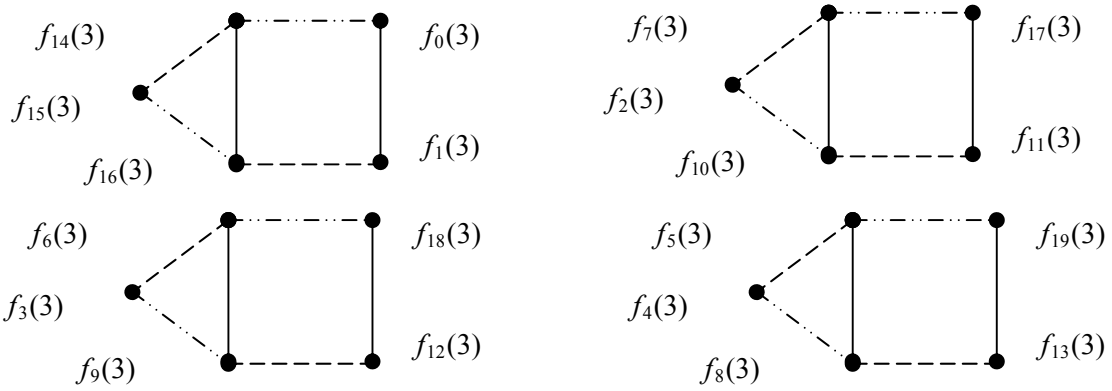

Рисунок 3 – Блоки МБФ ранга 3

Все МБФ любого из блоков на рис. 3 можно получить из одной МБФ, применяя к ней по очереди сначала операцию дизъюнктивного дополнения, а затем операцию двойственности. Так, например, второй блок в верхнем ряду порождается из МБФ $f_2(3) = x_1$ путем получения цепочки МБФ: $f_2(3)$, $f_7(3)$, $f_{10}(3)$, $f_{11}(3)$, $f_{17}(3)$. Аналогично можно получить цепочку $f_3(3)$, $f_6(3)$, $f_9(3)$, $f_{12}(3)$, $f_{18}(3)$, цепочку $f_4(3)$, $f_5(3)$, $f_8(3)$, $f_{13}(3)$, $f_{19}(3)$ и цепочку $f_{15}(3)$, $f_{14}(3)$, $f_{16}(3)$, $f_1(3)$, $f_0(3)$ из МБФ $f_3(3) = x_2$, МБФ $f_4(3) = x_3$ и МБФ $f_{15}(3) = x_1x_2 \vee x_1x_3 \vee x_2x_3$ соответственно. Такие блоки, как на рис. 3, т.е. с одинаковым числом МБФ и одинаковой формы назовем подобными.

Рассмотрим некоторые понятия, связанные с методом классификации МБФ на типы [2]. Будем говорить, что две МБФ от n переменных принадлежат одному типу, если соответствующие

этим МБФ антицепи для любого i от 0 до n содержат одинаковое число наборов с i единицами. В этом случае для каждого i в минимальных дизъюнктивных формах [1] этих МБФ содержится одинаковое число конъюнкций, в которые входят i переменных. В [2] определен тип МБФ, как вектор $T = (a_0, a_1,\ldots,a_i,\ldots,a_n)$ из $n + 1$-й компоненты, которые нумеруются слева направо от 0 до n, причем i-я компонента вектора a_i равна числу входных наборов данной МБФ, содержащих по i единиц. Число n называется рангом типа T; число v ненулевых компонент – весом типа T; номер i первой слева ненулевой компоненты – левой границей типа T; номер j первой справа ненулевой компоненты – правой границей типа T; сумма m всех компонент типа T – мощностью типа T. Тип T называется максимальным, если при увеличении любой компоненты соответствующего ему вектора на 1, полученный вектор не соответствует никакому типу.

Для ранга 0 МБФ $f_0(0)$ имеет тип (0), а МБФ $f_1(0)$ имеет тип (1). Максимальным является только тип (1).

Для ранга 1 $f_0(1)$ имеет тип (0,0), $f_1(1)$ – тип (1,0), а $f_1(1)$ – тип (0,1). Максимальными являются типы (1,0) и (0,1).

Для ранга 2 $f_0(2)$ имеет тип (0,0,0), $f_1(2)$ – тип (1,0,0), $f_2(2)$ – тип (0,1,0), $f_3(2)$ – тип (0,1,0), $f_4(2)$ – тип (0,0,1), а $f_5(2)$ – тип (0,2,0). Тип (0,1,0) имеют 2 МБФ. Максимальными являются типы (1,0,0), (0,0,1) и (0,2,0).

Для ранга 3 МБФ $f_0(3)$, $f_1(3)$, $f_{14}(3)$, $f_{15}(3)$ и $f_{16}(3)$ имеют типы (0,0,0,0), (1,0,0,0), (0,3,0,0), (0,0,3,0), и (0,0,0,1) соответственно. Тип (0,1,0,0) имеют МБФ $f_2(3)$, $f_3(3)$ и $f_4(3)$. Тип (0,0,1,0) имеют МБФ $f_5(3)$, $f_6(3)$ и $f_7(3)$. Тип (0,2,0,0) имеют МБФ $f_8(3)$, $f_9(3)$ и $f_{10}(3)$. Тип (0,0,2,0) имеют МБФ $f_{11}(3)$, $f_{12}(3)$ и $f_{13}(3)$. Тип (0,1,1,0) имеют МБФ $f_{17}(3)$, $f_{18}(3)$ и $f_{19}(3)$. Максимальными являются типы (1,0,0,0), (0,0,0,1), (0,3,0,0), (0,0,3,0), и (0,1,1,0).

Для типов и МБФ можно ввести матрицы распределения, в которых строка соответствует левой границе, а столбец правой границе. Обозначим через M_n и R_n матрицы распределения для максимальных типов и всех типов, а через G_n и F_n – матрицы распределения МБФ максимальных типов и всех МБФ ранга n. Для ранга 0 все четыре матрицы M_0, R_0, G_0 и F_0 одинаковы и имеют вид (1), т.е. состоят из одной строки и одного столбца. Для ранга 1 также все четыре матрицы M_1, R_1, G_1 и F_1 одинаковы и имеют вид

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Для ранга 2 матрицы M_2 и G_2 имеют вид $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $R_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ и $F_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Для ранга 3 имеем

$$M_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, G_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 3 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, R_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 1 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \text{ и } F_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 7 & 3 & 0 \\ 0 & 0 & 7 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

В матрицах R_n и F_n не учитывается тип из всех нулей и соответствующая ему МБФ $f_0(n)$, так как в данном случае левая и правая границы не определены. В [3] показано, что типы ранга $n + 1$ можно получать из типов ранга n с помощью операции сдвиг-суммы. В [5] доказано рекуррентное выражение, позволяющее по матрице M_{n-1} находить матрицу M_n:

$$M_n = {}^*M_{n-1} \times ({}^*T_{n-2} \times M_{n-1})^*. \quad (1)$$

В [6] доказано рекуррентное выражение позволяющее по матрице R_{n-1} находить матрицу R_n:

$$R_n = {}^+(R_{n-1}) + (R_{n-1})^+ + {}^+(R_{n-1} \times S_{n-2}{}^+) \times (R_{n-1})^+. \quad (2)$$

В (1) и (2) T_{n-2} и S_{n-2} это верхние треугольные матрицы размерности $(n–1)\times(n–1)$, причем у матрицы T_{n-2} на главной диагонали расположены единицы, а у матрицы S_{n-2} нули. Матрица ${}^*A$ получается из матрицы A добавлением сверху строки и слева столбца, состоящих из нулей, а на пересечении этих строки и столбца добавляется единица. Матрица A^* получается из матрицы A добавлением снизу строки и справа столбца, состоящих из нулей, а на пересечении этих строки и столбца добавляется единица. Матрица ${}^+A$ получается из матрицы A добавлением сверху строки, а слева – столбца, состоящих из нулей. Матрица A^+ получается из матрицы A добавлением снизу строки, а справа – столбца, состоящих из нулей. Таким образом, $M_3 = {}^*M_2 \times ({}^*T_1 \times M_2)^*$, а $R_3 = {}^+(R_2) + (R_2)^+ + {}^+(R_2 \times S_1{}^+)$

$\times (R_2)^+$. Если допустить, что ${}^*T_{-1}= T_{-1}{}^* = (1)$ и ${}^+T_{-1}= T_{-1}{}^+ = (0)$, то все матрицы видов M_n и R_n рекуррентно порождаются выражениями (1) и (2) из матрицы (1) размерности 1×1.

Как видно из рис. 2 и 3 для МБФ ранга n имеется меньше блоков, чем типов. Кроме того, среди блоков имеются подобные, тогда как все типы различны. Все МБФ подобных блоков получаются одинаковым образом с помощью рассмотренных трех операций. В отдельных случаях, как для блоков порожденных МБФ $f_2(3) = x_1$, $f_3(3) = x_2$ и $f_4(3) = x_3$, все МБФ подобных блоков получаются друг из друга заменой переменных. Перебор всех МБФ ранга n можно организовать следующим образом. Берется произвольная МБФ ранга n. С помощью рассмотренных трех операций для нее строится блок. Затем берется произвольная МБФ ранга n, не входящая в этот блок, и для нее тоже строится блок. Подобные действия повторяются, пока существуют МБФ, не входящие в уже построенные блоки. Таким образом, все МБФ ранга n будут разбиты на блоки. Достоинством метода является то, что все МБФ внутри блока связаны между собой 3 операциями и то, что при построении блоков часть подобных блоков можно не строить, сократив перебор. К недостаткам можно отнести то, что о блоках в настоящее время известно меньше, чем о типах. В частности число типов и число максимальных типов можно подсчитать, не делая перебора всех МБФ, с помощью выражений (1) и (2). Для блоков и подобных блоков сделать такое пока нельзя.

В заключение отметим следующее. Разработан метод анализа и классификации МБФ на основе построения блоков МБФ. Показано применение этого метода и метода, основанного на классификации МБФ на типы, к анализу МБФ с малым числом переменных (от 0 до 3). Применение метода построения блоков МБФ упрощается, если заранее известно число блоков и число подобных блоков. Поэтому для упрощения синтеза цифровых схем в дальнейшем следует изучать разбиение на блоки МБФ отдельных рангов, а также искать закономерности разбиения на блоки общие для МБФ всех рангов. Если удастся для матриц F_n найти выражение подобное выражениям (1) или (2), то тем самым будет решена проблема Дедекинда подсчета всех МБФ заданного ранга n.

Литература

1. *Ткаченко В.Г.* Отказы цифровых схем и представления монотонных булевых функций / В.Г. Ткаченко // Наукові праці ОНАЗ ім. О.С. Попова. – 2006. – № 2. – С. 45 – 69.
2. *Ткаченко В.Г.* Классификация монотонных булевых функций при синтезе цифровых схем / В.Г. Ткаченко // Наукові праці ОНАЗ ім. О.С. Попова. – 2008. – № 1. – С. 35 – 43.
3. *Ткаченко В.Г.* Перечисление типов монотонных булевых функций при синтезе цифровых схем / В.Г. Ткаченко // Наукові праці ОНАЗ ім. О.С. Попова. – 2008. – № 2. – С. 54 – 69.
4. *Иваницкий А.М.* Взаимосвязь между матроидами и монотонными булевыми функциями электрических цепей/ А.М.Иваницкий, В.Г. Ткаченко //Наукові праці ОНАЗ ім. О.С. Попова. – 2009. – № 1. – С. 18 – 26.
5. *Ткаченко В.Г.* Построение корректирующего кода для криптосистем на основе типов монотонных булевых функций / В.Г. Ткаченко, О.В. Синявский // Наукові праці ОНАЗ ім. О.С. Попова. – 2010. – № 1. – С. 85 – 92.
6. *Ткаченко В.Г.* Взаимосвязь между всеми типами и максимальными типами монотонных булевых функций/ В.Г. Ткаченко //Наукові праці ОНАЗ ім. О.С. Попова. – 2010. – № 2. – С. 60 – 69.