УДК 681.322

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

ВЗАИМОСВЯЗЬ МЕЖДУ ВСЕМИ ТИПАМИ И МАКСИМАЛЬНЫМИ ТИПАМИ МОНОТОНННЫХ БУЛЕВЫХ ФУНКЦИЙ

ВЗАЄМОЗВ'ЯЗОК МІЖ УСІМА ТИПАМИ ТА МАКСИМАЛЬНИМИ ТИПАМИ МОНОТОНННИХ БУЛЕВИХ ФУНКЦІЙ

INTERRELATION BETWEEN ALL TYPES AND MAXIMAL TYPES OF MONOTONOUS BOOLEAN FUNCTIONS

Аннотация. Установление взаимосвязи между всеми типами и максимальными типами монотонных булевых функций (МБФ) позволяет ускорить этап синтеза цифровых схем на основе МБФ, а также совершенствовать теорию булевых функций. Введены понятия левого и правого дополнения типа МБФ. Выведены рекуррентные формулы для перечисления всех типов произвольного ранга (теорема 1). Доказаны выражения в матричном виде для нахождения матриц распределения всех типов МБФ. Взаимно однозначное соответствие между всеми типами ранга *n* и максимальными типами ранга *n*+1 доказано в теореме 2.

Анотація. Установлення взаємозв'язку між усіма типами і максимальними типами монотонних булевих функцій (МБФ) дозволяє прискорювати етап синтезу цифрових схем на основі МБФ, а також удосконалювати теорію булевих функцій. Уведені поняття лівого та правого доповнення типу МБФ. Виведені рекурентні формули для перелічування усіх типів довільного рангу (теорема 1). Доказані вирази у матричному вигляді для знаходження матриць розподілення усіх типів МБФ. Взаємно однозначне співвідношення між усіма типами рангу *n* та максимальними типами рангу *n*+1 доведено у теоремі 2.

Summary. The interrelation establishment between all types and maximal types of monotonous Boolean functions (MBF) allows to accelerate a stage of synthesis of digital schemes on the MBF basis, and also to improve the Boolean functions theory. Concepts of the left and right adjunction of MBF type are introduced. Recurrent formulas for enumeration of any rank of all types are deduced (the theorem 1). Expressions in a matrix form for finding of matrixes of distribution of all MBF types are proved. One-to-one correspondence between all types of an *n* rank and the maximal types of an *n*+1 rank is proved in the theorem 2.

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.

Важным этапом синтеза цифровых схем на основе специальных классов булевых функций является [2] комбинаторный перебор функций заданного класса. Сложность этого этапа зависит от сложности формул или алгоритмов перечисления функций этого класса и количества функций, которые необходимо перебрать. В [3] предложена классификация МБФ по типам, основанная на способах описания МБФ [1] и напрямую связанная со структурой функциональных схем МБФ, которая позволяет сократить количество перебираемых функций при синтезе МБФ. На основе этой классификации в [4] предложен метод синтеза МБФ путем перечисления типов МБФ, а затем перебора функций, имеющих заданный тип.

Однако в настоящее время известен эффективный способ перечисления [4], основанный на однозначном разложении типа ранга n на 2 типа ранга n–1, лишь для максимальных типов.

Целью работы является нахождение эффективного способа перечисления и нахождения всех типов МБФ произвольного ранга на основе доказательства взаимосвязи максимальных типов ранга $n + 1$ и всех типов ранга n.

В [3] введено понятие типа МБФ, использующее понятие семейств подмножеств Шпернера. Определение типа можно дать и, не используя указанное понятие. Назовем вектор $T = (a_0, a_1,\ldots,a_i,\ldots,a_n)$ из $n + 1$ компоненты, которые нумеруются слева направо от 0 до n, типом

МБФ, если существует МБФ, записанная в минимальной дизъюнктивной форме, такая, что для каждого i $(0 \le i \le n)$ в этой МБФ существует a_i конъюнкций, содержащих по i переменных. Назовем тип Т максимальным, если при увеличении любой его компоненты на 1, полученный вектор не является типом МБФ. В [3-5] определены также различные термины, связанные с типами МБФ. Однако для расширения области действия этих терминов, а также упрощения ряда доказательств целесообразно сначала определить эти термины для множества L всех векторов из целых неотрицательных чисел. Так как множество T всех типов МБФ по определению является подмножеством множества L, то определенные таким образом термины будут определены и для типов МБФ. Пусть $V = (a_0, a_1,\ldots,a_i,\ldots,a_n)$ произвольный вектор из целых неотрицательных чисел. Число n назовем рангом вектора V, число v ненулевых компонент – весом вектора V, номер i первой слева ненулевой компоненты – левой границей вектора V, номер j первой справа ненулевой компоненты – правой границей вектора V, сумму m всех компонент вектора V – мощностью вектора V. Для векторов $V_1 = (a_0, a_1,\ldots,a_i,\ldots,a_{n-1})$ и $V_2 = (b_0, b_1,\ldots,b_i,\ldots,b_{n-1})$ таких, что правая граница вектора V_1 меньше левой границы вектора V_2 (такие пары векторов назовем допустимыми), введем операцию $\oplus$ сдвиг-суммы. Сдвиг-суммой векторов V_1 и V_2 называется вектор $V_3=V_1 \oplus V_2=$ $(b_0,a_0+b_1,\ldots,a_i+b_{i+1},\ldots,a_{n-2}+b_{n-1}, a_{n-1}) = (c_0, c_1,\ldots,c_i,\ldots,c_n)$. Правой частью V_2 вектора V_3, у которого компонента n равна нулю, называется вектор ранга n–1, у которого компоненты с $i+1$ по $n-1$ вектора V_2 совпадают с соответствующими компонентами вектора V_3, а i компонента вектора V_2 больше нуля и меньше или равна i-й компоненты вектора V (здесь i является левой границей вектора V_2). Левой частью V_1 вектора V_3, у которого компонента a_0 равна нулю, называется вектор ранга n – 1, у которого компоненты с нулевой по $j-1$ вектора V_1 совпадают с компонентами с первой по j вектора V_3, а j компонента вектора V_1 больше нуля и меньше или равна $j+1$ компоненты вектора V (при этом j будет правой границей вектора V_1). Очевидно, что если $V_3=V_1 \oplus V_2$, то V_1 левая часть вектора V_3, а V_2 его правая часть. Любой вектор ранга n с компонентами 0 и n равными нулю имеет левую и правую часть. Три вектора (0,0,...,0), (1,0,...,0), (0,0,....,1) ранга n назовем нулевым, левой и правой единицей соответственно. Для этих векторов ранга n определим (0,0,...,0) = (0,0,...,0)$\oplus$(0,0,...,0), (1,0,...,0) = = (0,0,...,0) $\oplus$(1,0,...,0) и (0,0,...,1) = =(0,0,...,1) $\oplus$(0,0,...,0) (здесь все слагаемые в сдвиг-суммах являются векторами ранга n–1). Будем считать, что $V_1 \ge V_2$, если $a_i \ge b_i$ для всех компонент векторов $V_1 \ge V_2$. Строгое неравенство $V_1>V_2$ выполняется, если $V_1 \ge V_2$ и $a_i>b_i$ хотя бы для одной компоненты.

Максимальной правой (левой) частью вектора V ранга n называется его правая (левая) часть, являющаяся типом ранга n – 1 наибольшей возможной мощности. Из определения максимальной правой (левой) части для любого вектора следует, что она либо не определена (если не определена правая (левая) часть), либо единственна. Если для вектора n ранга нулевая и n-я компонента равны нулю, то из него по определению можно выделить как максимальную правую M_2, так и максимальную левую M_1 части. Для таких векторов существуют дополнения (вектора ранга n – 1) D_1 и D_2 соответственно, такие, что $V = D_1 \oplus M_2$ и $V = M_1 \oplus D_2$. Сокращённо будем называть разложение вектора, получающееся после выделения из него максимальной правой (левой) части правым (левым) разложением. Если вектор не является нулевым типом, правой или левой единицей, то мощность его максимальной правой (левой) части больше нуля.

Тип T называется максимальным [3], если при увеличении любой компоненты соответствующего ему вектора на 1, полученный вектор не является типом. В [5] доказано, что любой тип ранга n имеет однозначное правое (левое) разложение на два типа ранга n – 1.

Рассмотрим правое разложение $T =D_1 \oplus M_2$ произвольного типа $T = (a_0, a_1,\ldots,a_i,\ldots,a_n)$ ранга n. Максимальная правая часть M_2 может быть любым типом ранга n – 1. Однако дополнение к фиксированной правой части не может быть любым типом, так как в типе T_2, полученном по формуле $T_2 =T_1 \oplus M_2$ правая часть M_2 может уже не быть максимальной.

Пример 1. Выберем как M_2 тип (0,0,0,4,1,0) ранга 5. Для типов ранга 6 T_1= (0,0,0,4,1,0,0) = = (0,0,0,0,0,0) $\oplus$(0,0,0,4,1,0) и T_2 = (0,0,3,4,1,0,0) = (0,3,0,0,0,0)$\oplus$(0,0,0,4,1,0) тип M_2 будет максимальной правой частью. Типы T_3 = (0,0,3,5,1,0,0) = (0,3,1,0,0,0) $\oplus$ (0,0,0,4,1,0), T_4 = = (0,0,2,7,1,0,0) = (0,2,3,0,0,0)$\oplus$(0,0,0,4,1,0) и T_5 = (0,0,3,6,1,0,0) = (0,3,2,0,0,0) $\oplus$(0,0,0,4,1,0) также имеют M_2 в качестве правой части. Однако во всех трех случаях M_2 не является максимальной правой частью. Для типа T_5 дополнение (0,3,2,0,0,0) даже не является типом. Тип T_3 имеет правое разложение (0,0,3,5,1,0,0) = (0,3,0,0,0,0) $\oplus$ (0,0,0,5,1,0), а значит его максимальная правая часть равна (0,0,0,5,1,0). Типы T_4 и T_5 имеют правые разложения (0,0,2,7,1,0,0) = (0,2,1,0,0,0) $\oplus$ (0,0,0,6,1,0) и (0,0,3,6,1,0,0) = = (0,3,0,0,0,0) $\oplus$ (0,0,0,6,1,0) соответственно, а значит их максимальная правая часть равна (0,0,0,6,1,0). Из этого примера следует, что если тип T ранга 6 имеет правое разложение $T = D_1 \oplus M_2$, то тип D_1 не может быть равен типам (0,3,1,0,0,0) и (0,2,3,0,0,0).

В [4] выведена рекуррентная формула для перечисления максимальных типов ранга n с левой границей i и правой границей j:

$$K(n, i, j) = \sum_{q=i}^{j} K(n-1, i-1, q-1)\left(\sum_{t=q}^{j} K(n-1, t, j)\right). \qquad (1)$$

Из примера 1 ясно, что вывод аналогичной формулы для перечисления всех типов ранга n сложнее, так как при этом нужно учитывать не только количество всех типов меньшего ранга, но и количество допустимых дополнений при правом (левом) разложении типов ранга n. Назовем такие дополнения левыми (правыми) дополнениями. В дальнейшем будем рассматривать правое разложение $T = D_1 \oplus M_2$, максимальную правую часть M_2 и левое дополнение D_1. Для левого разложения выводы будут симметричны ввиду симметричности типов. Количество левых дополнений может быть различно для различных правых максимальных частей даже с одинаковыми границами.

Пример 2. Для максимальной правой части M_2 = (0,0,0,6,1,0) левым дополнением может быть любой тип D_1 ранга 5, образующий с M_2 допустимую пару векторов. Это справедливо для любого максимального типа M_2. В то же время для максимальной правой части M_2 = (0,0,0,4,1,0) из примера 1 в качестве левого дополнения D_1 не могут быть взяты типы (0,3,1,0,0,0) и (0,2,3,0,0,0). Кроме того, D_1 не может быть равно типам (0,2,1,0,0,0) (0,2,2,0,0,0), (0,1,n,0,0,0) с $1 \le n \le 6$ и (0,0,n,0,0,0) с $1 \le n \le 10$. Левыми дополнениями для M_2 = =(0,0,0,4,1,0) могут быть только типы (0,0,0,0,0,0), (1,0,0,0,0,0) и (0,n,0,0,0,0) с $1 \le n \le 5$. Таким образом, из 27 типов, образующих с M_2 допустимую пару векторов, левыми дополнениями являются только 7. Левыми дополнениями для M_2 = (0,0,0,n,1,0) с $1 \le n \le 3$ могут быть только типы (0,0,0,0,0,0) и (1,0,0,0,0,0). Левым дополнением для M_2=(0,0,0,0,1,0) также может быть только тип (0,0,0,0,0,0). В последнем случае допустимую пару векторов с M_2 образуют 70 типов.

Из примера 2 видно, что даже максимальные правые части с одинаковыми границами могут иметь различное количество левых дополнений. Однако для левых дополнений выполняется следующая лемма.

Лемма 1. Любые два типа с одинаковыми правыми границами являются левыми дополнениями для одних и тех же максимальных правых частей.

Доказательство. Пусть T_1 произвольный тип ранга $n-1$ с правой границей j. Допустимую пару с ним составляет любой тип T_2 ранга $n-1$ с левой границей большей, чем j. Из них максимальной правой частью не могут быть те и только те типы T_4, которые меньше или равны некоторому типу T_3. В качестве T_3 может быть взят любой тип, который получается из некоторого максимального типа ранга $n-1$ с левой границей j+1 путем уменьшения его компоненты a_{j+1} на 1. Для всех остальных типов T_2 имеем $T_1 \oplus T_2 = T_5$, где T_5 тип ранга n, T_2 его максимальная правая часть, а T_1 левое дополнение. Лемма доказана.

Обозначим через $V(n, i, j)$ количество всех типов ранга n с левой границей i и правой границей j, а через $K(n, i, j)$ количество максимальных типов такого же ранга и с такими же границами.

Пример 3. Найдем возможные максимальные правые части с правой границей 5 для левого дополнения D_1 = (0,1,1,0,0,0,0). Тип D_1 имеет ранг 6 и правую границу 2. Количество допустимых пар с правой границей 5 для этого типа равно $V(6,3,5) + V(6,4,5) + V(6,5,5)$ = =43+20+6 = 69. Количество максимальных типов с границами 3 и 5 $K(6,3,5)$ = 10. Выпишем эти типы, уменьшив компоненту 3 на 1. Это будет множество из 10 типов F = {(0,0,0,0,0,3,0), (0,0,0,0,3,2,0), (0,0,0,0,7,1,0), (0,0,0,1,1,2,0), (0,0,0,1,5,1,0), (0,0,0,3,0,2,0), (0,0,0,3,4,1,0), (0,0,0,4,2,1,0), (0,0,0,6,1,1,0), (0,0,0,9,0,1,0)}. Имеется 43 типа, которые меньше или равны одному из типов множества F. Большинство из этих типов отличается от одного из типов множества F только самой левой ненулевой компонентой, но типы (0,0,0,1,3,1,0) и (0,0,0,3,3,1,0) отличаются второй ненулевой компонентой, а тип (0,0,0,2,3,1,0) отличается от любого из типов множества F по меньшей мере двумя компонентами. Все эти 43 типа не могут быть максимальными правыми частями для левого дополнения D_1. Таким образом, D_1

является левым дополнением для 69–43=26 максимальных правых частей. Из них K(6,3,5)+K(6,4,5)+ K(6,5,5)=10+4+1=15 являются максимальными типами, а 26 – 15 = 11 не являются. Выпишем эти 11 типов: (0,0,0,0,0,4,0), (0,0,0,0,0,5,0), (0,0,0,0,8,1,0), (0,0,0,0,9,1,0), (0,0,0,0,4,2,0), (0,0,0,0,5,2,0), (0,0,0,0,1,3,0), (0,0,0,0,2,3,0), (0,0,0,1,6,1,0), (0,0,0,1,2,2,0) и (0,0,0,4,3,1,0). Эти же 26 максимальных правых частей могут иметь, являясь для них левыми дополнениями, также типы (0,0,n,0,0,0,0) с $1\le n\le 15$, (0,1,n,0,0,0) с $2\le n\le 10$, (0,2,n,0,0,0) с $1\le n\le 6$, (0,3,n,0,0,0) с $1\le n\le 3$ и (0,4,1,0,0,0). Всего имеется 35 левых дополнений с правой границей 2. (35 = 15 + 20 = V(6,1,2) + V(6,2,2)).

Из леммы 1 и примера 3 следует, что для перечисления всех типов достаточно найти для левого дополнения с заданной правой границей количество типов, составляющих с ним допустимую пару типов, но не являющихся максимальными правыми частями.

Лемма 2. Для левого дополнения ранга $n-1$ с правой границей $q-1$ имеется $V(n–1, q, j)$ типов с правой границей j, составляющих с ним допустимую пару типов, но не являющихся максимальными правыми частями.

Доказательство. Пусть E множество из $K(n-1, q, j)$ максимальных типов ранга $n-1$ с левой границей q и правой границей j, а F множество этих же типов, у каждого из которых компонента с номером q уменьшена на 1. Рассмотрим множество G всех типов, меньших или равных одному из типов множества F. Согласно лемме 1, множество F содержит все типы, составляющие с левым дополнением ранга n с правой границей q допустимую пару типов, но не являющиеся максимальными правыми частями. Образуем множество типов H, увеличивая компоненту с номером q каждого типа из множества G на 1. Докажем, что множество H, а значит и множество G содержит $V(n-1, q, j)$ типов. Действительно любой тип из множества H имеет ранг $n-1$, левую границу q и правую границу j. С другой стороны любой тип с такими свойствами меньше одного из максимальных типов множества E и, следовательно, принадлежит множеству H. Лемма доказана.

Лемма 2 дает удобный алгоритм нахождения всех типов с заданными границами, используя типы меньшего ранга. Выведем теперь рекуррентную формулу для перечисления типов с заданными границами.

Теорема 1. Для заданных левой i и правой j границ типа, количество всех типов ранга n вычисляется по формуле:

$$V(n, i, j) = V(n–1, i, j) +V(n–1,i–1,j–1)\ \sum_{q=i}^{j-1} V\ (n–1, i–1, q–1)(\sum_{t=q+1}^{j} V\ (n–1, t, j)). \qquad (2)$$

Доказательство. При выводе формулы перечисления всех типов ранга n будем подсчитывать их правые разложения на типы ранга n–1, которые единственны для каждого типа ранга n. Первое слагаемое в (2) соответствует правым разложениям, в которых левое дополнение является нулевым типом, а максимальная правая часть любым типом ранга n–1 с границами i и j. Второе слагаемое в (2) соответствует правым разложениям, в которых левое дополнение является любым типом ранга n–1 с границами i–1 и j–1, а максимальная правая часть единственным максимальным типом ранга n–1 с одинаковыми левой и правой границами j (с единственной ненулевой компонентой j). Будем теперь менять правую границу левого дополнения q–1 от i–1 до j–2. Когда эта граница равна q–1, то допустимую пару типов с каждым левым дополнением составляют $\sum_{t=q}^{j} V\ (n–1,\ t,\ j)$ типов, т.е. все типы ранга n–1 с левыми границами от q до j и правой границей j. Однако, согласно лемме 2, $V(n–1, q, j)$ из этих типов не являются максимальными правыми частями. Отсюда каждое левое дополнение ранга n–1 с левой границей i–1 и правой границей q–1 может образовывать правое разложение с $\sum_{t=q+1}^{j} V\ (n–1, t, j)$ максимальными правыми частями. Теорема доказана.

Лемма 3. В случае использования левого разложения для заданных левой i и правой j границ типа, количество всех типов ранга n с границами i и j вычисляется по формуле:

$$V(n, i, j) = V(n–1, i–1, j–1)+V(n–1, i, j)+ \sum_{t=i+1}^{j} V\ (n–1, t, j)(\sum_{q=i}^{t-1} V\ (n–1, i–1, q–1)). \qquad (3)$$

Доказательство. По аналогии с леммой 1 несложно установить, что любые два типа с одинаковыми левыми границами являются правыми дополнениями для одних и тех же максимальных левых частей. По аналогии с леммой 2 для правого дополнения ранга n с левой границей t имеется $V(n-1, i-1, t-1)$ типов с левой границей $i-1$, составляющих с ним допустимую пару типов, но не являющихся максимальными левыми частями. При выводе формулы (3) будем подсчитывать правые разложения всех типов ранга n на типы ранга n – 1, которые единственны для каждого типа ранга n. Первое слагаемое в (3) соответствует левым разложениям, в которых правое дополнение является нулевым типом, а максимальная левая часть любым типом ранга n – 1 с границами i – 1 и j – 1. Второе слагаемое в (3) соответствует левым разложениям, в которых правое дополнение является любым типом ранга n – 1 с границами i и j, а максимальная левая часть единственным максимальным типом ранга n – 1 с одинаковыми левой и правой границами i – 1 (с единственной ненулевой компонентой i – 1). В третьем слагаемом по аналогии с теоремой 1 левая граница t правого дополнения меняется от i + 1 до j. Когда эта граница равна t, то допустимую пару типов с каждым правым дополнением составляют $\sum_{q=i}^{t} V(n-1,\ i-1,\ q-1)$ типов, т.е. все типы ранга n – 1 с правыми границами от i – 1 до t – 1 и левой границей i – 1. Однако $V(n-1, i-1, t-1)$ из этих типов не являются максимальными правыми частями. Отсюда каждое правое дополнение ранга n – 1 с левой границей t и правой границей j может образовывать правое разложение с $\sum_{q=i}^{t-1} V(n-1,\ i-1,\ q-1)$ максимальными правыми частями. Как видим, формулы (2) и (3) отличаются только порядком первого и второго слагаемого и порядком суммирования в третьем слагаемом. Лемма доказана.

В [3] определены матрицы распределения максимальных типов ранга n как матрицы, имеющие n + 1 строку и n + 1 столбец с номерами от 0 до n, причем на пересечении i строки и j столбца находится число $K(n, i, j)$ максимальных типов ранга n с границами i и j. Аналогично определяются матрицы распределения всех типов ранга n как матрицы, имеющие n+1 строку и n+1 столбец с номерами от 0 до n, причем на пересечении i строки и j столбца находится число $V(n, i,j)$ всех типов ранга n с границами i и j. На примере покажем, как числа матрицы ранга n получаются из чисел матрицы ранга n – 1 по формуле (2).

Пример 4. На рис. 1 изображены матрицы распределения всех типов рангов 6 и 7. Обозначим их R_6 и R_7. Вычислим элемент $V(7,2,5)$ матрицы R_7. Имеем $V(7,2,5) = V(6,2,5) + V(6,1,4) + V(6,1,1)(V(6,3,5) + V(6,4,5) + V(6,5,5)) + V(6,1,2)(V(6,4,5) + V(6,5,5)) + V(6,1,3)V(6,5,5) = 25 + 25 + 6(43 + 20 + 6) + 20(20 + 6) + 43 \times 6 = 50 + 6 \times 69 + 20 \times 26 + 258 = 308 + 414 + 520 = 1242$, т.е. всего есть 1242 типа с границами 2 и 5. По формуле (2) можно найти любой ненулевой элемент матрицы R_7 кроме $V(7,0,0)$ и $V(7,7,7)$, которые равны 1.

	0	1	2	3	4	5	6
0	1	0	0	0	0	0	0
1	0	6	20	43	25	1	0
2	0	0	15	84	143	25	0
3	0	0	0	20	84	43	0
4	0	0	0	0	15	20	0
5	0	0	0	0	0	6	0
6	0	0	0	0	0	0	1

	0	1	2	3	4	5	6	7
0	1	0	0	0	0	0	0	0
1	0	7	35	147	267	95	1	0
2	0	0	21	224	1080	1242	95	0
3	0	0	0	35	393	1080	267	0
4	0	0	0	0	35	224	147	0
5	0	0	0	0	0	21	35	0
6	0	0	0	0	0	0	7	0
7	0	0	0	0	0	0	0	1

Рисунок 1 – Матрицы распределения всех типов рангов 6 (R_6) и 7 (R_7)

Выражения (2) и (3) позволяют найти один элемент матрицы R_n, однако, используя бинарные операции сложения и умножения матриц можно вычислить всю матрицу R_n. Введем для этого три унарные операции над матрицами и специальную матрицу J_n. Определим, что 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. Матрица A^{**} получается из матрицы A отражением относительно побочной диагонали. Специальная матрица J_n – это квадратная матрица, строки и столбцы которой нумеруются от 0 до n. Элементы матрицы J_n, которые находятся выше главной диагонали в строках с номерами больше 0, равны 1, а все остальные элементы равны 0. Обозначим через $S_{n\text{-}1}$ верхнюю треугольную матрицу размерности $n\times n$ из единиц с обнуленной главной диагональю, тогда $J_n = {}^{+}S_{n\text{-}1}$, а $J_n^{**} = S_{n\text{-}1}{}^{+}$.

Лемма 4. Матрица R_n получается матрицы $R_{\text{n-1}}$ следующим выражением:

$$R_n = (R_{n\text{-}1})^{+} + {}^{+}(R_{n\text{-}1}) + {}^{+}(R_{n\text{-}1}) \times (\,J_{n\text{-}1} \times R_{n\text{-}1})^{+}\,, \tag{4}$$

где операция × – обычное перемножение матриц.

Доказательство. Первые два слагаемых соответствуют всем возможным первым двум слагаемым формулы (2), причем дополнение нулевыми строками и столбцами производится для согласования с размерностью матрицы R_n. Третье слагаемое дает все возможные значения третьего слагаемого формулы (2). Лемма доказана.

Следствие. Используя верхнюю треугольную матрицу из единиц $S_{n\text{-}2}$ размерности $(n–1) \times (n–1)$, из выражения (4) можно получить:

$$R_n = (R_{n\text{-}1})^{+} + {}^{+}(R_{n\text{-}1}) + {}^{+}(R_{n\text{-}1}) \times ({}^{+}S_{n\text{-}2} \times R_{n\text{-}1})^{+}. \tag{5}$$

Лемма 5. Матрица R_n получается матрицы $R_{n\text{-}1}$ следующим выражением:

$$R_n = {}^{+}(R_{n\text{-}1}) + (R_{n\text{-}1})^{+} + {}^{+}(R_{n\text{-}1} \times J_{n\text{-}1}{}^{**}) \times (R_{n\text{-}1})^{+}. \tag{6}$$

Доказательство. Первые два слагаемых соответствуют всем возможным первым двум слагаемым формулы (3). Третье слагаемое дает все возможные значения третьего слагаемого формулы (3). Элементы матрицы $J_{n\text{-}1}{}^{**}$ выше главной диагонали и с номерами столбцов меньше n равны 1, а все остальные элементы равны 0. Лемма доказана.

Следствие. Используя верхнюю треугольную матрицу из единиц $S_{n\text{-}2}$ размерности $(n–1) \times (n–1)$, из выражения (6) можно получить:

$$R_n = {}^{+}(R_{n\text{-}1}) + (R_{n\text{-}1})^{+} + {}^{+}(R_{n\text{-}1} \times S_{n\text{-}2}{}^{+}) \times (R_{n\text{-}1})^{+}. \tag{7}$$

Формулы (5) и (7) внешне похожи на формулы, выведенные в [6] для максимальных типов МБФ, однако не эквивалентны им, так как используют другие операции и треугольные матрицы*.

Покажем, как R_7 получается из R_6 по формуле (4).

Пример 5. Заменим в (4) $R_{n\text{-}1}$ на R_6 и $J_{n\text{-}1}$ на J_6. Найдем сумму $(R_6)^{+} + {}^{+}(R_6)$:

$$\begin{pmatrix} 1&0&0&0&0&0&0&0\\ 0&6&20&43&25&1&0&0\\ 0&0&15&84&143&25&0&0\\ 0&0&0&20&84&43&0&0\\ 0&0&0&0&15&20&0&0\\ 0&0&0&0&0&6&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&0 \end{pmatrix} + \begin{pmatrix} 0&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&6&20&43&25&1&0\\ 0&0&0&15&84&143&25&0\\ 0&0&0&0&20&84&43&0\\ 0&0&0&0&0&15&20&0\\ 0&0&0&0&0&0&6&0\\ 0&0&0&0&0&0&0&1 \end{pmatrix} = \begin{pmatrix} 1&0&0&0&0&0&0&0\\ 0&7&20&43&25&1&0&0\\ 0&0&21&104&186&50&1&0\\ 0&0&0&35&168&186&25&0\\ 0&0&0&0&35&104&43&0\\ 0&0&0&0&0&21&20&0\\ 0&0&0&0&0&0&7&0\\ 0&0&0&0&0&0&0&1 \end{pmatrix}$$

Найдем произведение матриц $J_6 \times R_6$:

---

* В [6] выведены рекуррентные формулы $M_n = {}^{*}M_{n\text{-}1}\times({}^{*}T_{n\text{-}2}\times M_{n\text{-}1})^{*}$ и $M_n = {}^{*}(M_{n\text{-}1}\times T_{n\text{-}2}{}^{*})\times M_{n\text{-}1}{}^{*}$. Здесь M_n и $M_{n\text{-}1}$ – матрицы распределения максимальных типов рангов n и n-1 соответственно. Матрица $T_{n\text{-}2}$ это верхняя треугольная матрица из единиц размерности $(n - 1)\times(n - 1)$, в которой в отличие от матрицы $S_{n\text{-}2}$ на главной диагонали расположены единицы. 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.

$$\begin{pmatrix} 0&0&0&0&0&0&0\\ 0&0&1&1&1&1&1\\ 0&0&0&1&1&1&1\\ 0&0&0&0&1&1&1\\ 0&0&0&0&0&1&1\\ 0&0&0&0&0&0&1\\ 0&0&0&0&0&0&0 \end{pmatrix} \times \begin{pmatrix} 1&0&0&0&0&0&0\\ 0&6&20&43&25&1&0\\ 0&0&15&84&143&25&0\\ 0&0&0&20&84&43&0\\ 0&0&0&0&15&20&0\\ 0&0&0&0&0&6&0\\ 0&0&0&0&0&0&1 \end{pmatrix} = \begin{pmatrix} 0&0&0&0&0&0&0\\ 0&0&15&104&242&94&1\\ 0&0&0&20&99&69&1\\ 0&0&0&0&15&26&1\\ 0&0&0&0&0&6&1\\ 0&0&0&0&0&0&1\\ 0&0&0&0&0&0&0 \end{pmatrix}$$

Найдем произведение матриц ${}^{+}(R_6) \times (J_6 \times R_6)^{+}$:

$$\begin{pmatrix} 0&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&6&20&43&25&1&0\\ 0&0&0&15&84&143&25&0\\ 0&0&0&0&20&84&43&0\\ 0&0&0&0&0&15&20&0\\ 0&0&0&0&0&0&6&0\\ 0&0&0&0&0&0&0&1 \end{pmatrix} \times \begin{pmatrix} 0&0&0&0&0&0&0&0\\ 0&0&15&104&242&94&1&0\\ 0&0&0&20&99&69&1&0\\ 0&0&0&0&15&26&1&0\\ 0&0&0&0&0&6&1&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0 \end{pmatrix} = \begin{pmatrix} 0&0&0&0&0&0&0&0\\ 0&0&15&104&242&94&1&0\\ 0&0&0&120&894&1192&94&0\\ 0&0&0&0&225&894&242&0\\ 0&0&0&0&0&120&104&0\\ 0&0&0&0&0&0&15&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0 \end{pmatrix}$$

Суммируя полученную матрицу с матрицей $(R_6)^{+} + {}^{+}(R_6)$, получаем R_7.

Найдем теперь количество $V(n)$ всех типов ранга n.

Лемма 6. Количество всех типов ранга n равно:

$$V(n) = 1 + \sum_{i=0}^{n}\sum_{j=i}^{n} V(n,i,j) = 2^n + 1 + \sum_{i=1}^{n-1}\sum_{j=i+1}^{n-1} V(n,i,j)\,. \tag{8}$$

Доказательство. Количество всех типов ранга n равно сумме всех элементов матрицы распределения плюс единица для нулевого типа, т.к. нулевой тип не имеет границ и не представлен в матрице распределения. Так как все ненулевые элементы в матрице распределения расположены на главной диагонали матрицы распределения и выше нее, то при суммировании достаточно брать номер столбца не меньше номера строки. Элемент матрицы распределения на пересечении i строки и i столбца матрицы распределения всех типов ранга n равен C_n^i [4], поэтому сумма всех элементов на главной диагонали равна по формуле бинома Ньютона 2^n. При суммировании элементов выше главной диагонали можно отбросить строку 0 и столбец n, так как ненулевые элементы на них есть только на главной диагонали. Лемма доказана.

В [4] предложена гипотеза о равенстве количества максимальных типов ранга n + 1 и количества всех типов ранга n. На рис. 2 показаны эти значения при изменении n от 0 до 12. Т.к. длинные числа не помещаются в клетке приведенной таблицы, то каждое число в столбце таблицы занимает от 1 до 3 строк. Если десятичные разряды числа нумеровать справа налево, начиная с 0, то в нижней строке располагаются разряды 5-0, в средней – 11-6, а в верхней – 17-12 числа $K(n + 1) = V(n)$.

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$K(n+1)$ $= V(n)$	2	3	5	10	26	96	553	5461	100709	3 718354	289 725509	49513 793526	19 089032 278261

Рисунок 2 – Количества типов различных рангов

Находя матрицы распределения типов по формулам (1) и (2), можно заметить, что совпадают не только общие количества типов, но и значения в отдельных клетках таблиц распределения.

Пример 6. Найдем (рис. 3) по формуле (1) матрицы распределения максимальных типов ранга 7 (M_7) и ранга 8 (M_8).

	0	1	2	3	4	5	6	7
0	1	0	0	0	0	0	0	0
1	0	1	5	20	43	25	1	0
2	0	0	1	14	84	143	25	0
3	0	0	0	1	19	84	43	0
4	0	0	0	0	1	14	20	0
5	0	0	0	0	0	1	5	0
6	0	0	0	0	0	0	1	0
7	0	0	0	0	0	0	0	1

	0	1	2	3	4	5	6	7	8
0	1	0	0	0	0	0	0	0	0
1	0	1	6	35	147	267	95	1	0
2	0	0	1	20	224	1080	1242	95	0
3	0	0	0	1	34	393	1080	267	0
4	0	0	0	0	1	34	224	167	0
5	0	0	0	0	0	1	20	35	0
6	0	0	0	0	0	0	1	6	0
7	0	0	0	0	0	0	0	1	0
8	0	0	0	0	0	0	0	0	1

Рисунок 3 – Матрицы распределения максимальных типов рангов 7 (M_7) и 8 (M_8)

Сравнивая рис.1 и 3, можно заметить, что все значения в клетках матрицы R_6, не лежащие на главной диагонали, имеются в клетках матрицы M_7. Аналогично, все значения в клетках матрицы R_7, не лежащие на главной диагонали, имеются в клетках матрицы M_8. Можно предположить уточненную гипотезу: $V(n, i, j) = K(n + 1, i, j + 1)$. Предварительно докажем лемму.

Лемма 7. Для максимальных типов ранга n+1 с границами i и i+1 и для всех типов ранга n с правой и левой границами равными i выполняется равенство:

$$V(n, i, i) = K(n + 1, i, i + 1) + 1. \qquad (9)$$

Доказательство. Типы с одинаковой левой границей имеют вес 1, т.е. единственную ненулевую компоненту. Эта компонента может принимать значение от 1 до некоторого максимального значения. В [4] показано, что это максимальное значение равно C_n^i, т.е. $V(n, i, i) = C_n^i$. Там же показано, что количество максимальных типов ранга n и веса 2, у которых правая граница отличается от левой на 1, равно ранга $C_{n-1}^i - 1$. Отсюда $K(n + 1, i, i + 1) = C_n^i - 1$. Лемма доказана.

Докажем теперь уточненную гипотезу.

Теорема 2. Для максимальных типов ранга n+1 с границами i и j+1 и для всех типов ранга n с границами i и j при условии $i < j$ выполняется равенство $V(n, i, j)= K(n + 1, i, j + 1)$.

Доказательство. В доказательстве используем метод математической индукции. Доказываемое равенство выполняется для начальных значений n. Это составляет базу индукции. Предположим, что для некоторого значения n –1 при $i < j$ выполняется равенство:

$$V(n - 1, i, j) = K(n, i, j + 1) \qquad (10)$$

Используя это предположение, докажем утверждение теоремы. Подставляя в (2) выражения (9) и (10), получим:

$$V(n, i, j) = K(n, i, j{+}1) + K(n, i{-}1, j) + 1 + \sum_{t=i+1}^{j} K(n, t, j{+}1) + \sum_{q=i+1}^{j} K(n, i{-}1, q{-}1)\left(1 + \sum_{t=q}^{j} K(n, t, j{+}1)\right). \qquad (11)$$

Согласно [4] имеем $K(n,i–1,i–1) = K(n, j+1,j+1) = 1$, поэтому:

$$V(n ,i, j) = K(n, i–1, j) + \sum_{t=i}^{j+1} K(n, t, j+1) + \sum_{q=i+1}^{j} K(n, i–1, q–1)(\sum_{t=q}^{j+1} K(n, t, j+1)) =$$

$$=K(n, i–1, j)+\sum_{q=i}^{j} K(n, i–1,q–1)(\sum_{t=q}^{j+1} K(n, t, j+1)) =$$

$$= \sum_{q=i}^{j+1} K(n, i–1, q–1)(\sum_{t=q}^{j+1} K(n, t, j+1)) \qquad (12)$$

Согласно (1) последнее выражение равно $K(n+1,i,j+1)$. Таким образом, формула

$$V(n, i, j)= K(n+1, i, j+1) \qquad (13)$$

доказана для всех значений n. Теорема доказана.

Теперь несложно доказать гипотезу [4] о равенстве количества максимальных типов ранга $n+1$ и количества всех типов ранга n.

Лемма 8. Количество $K(n+1)$ максимальных типов ранга $n+1$ равно количеству $V(n)$ всех типов ранга n.

Доказательство. В [4] показано, что $K(n+1) = \sum_{i=0}^{n+1}\sum_{j=i}^{n+1} K(n+1, i.j)$ и элементы $K(n+1, i, i)$ на главной диагонали матрицы распределения максимальных типов ранга $n+1$ равны 1. Всего на этой диагонали $n+2$ единиц.. В лемме 7 показано, что элементы $K(n+1,i,i+1)$ на диагонали соседней с главной равно $C_n^i – 1$. На этой диагонали n таких элементов. Отсюда сумма всех элементов на главной диагонали и соседней с ней равна по формуле бинома Ньютона 2^n+1. Сумма остальных элементов матрицы распределения максимальных типов ранга $n+1$ равна согласно теореме 2 сумме элементов матрицы распределения всех типов ранга n, расположенных не на главной диагонали. Согласно лемме 6, сумма $\sum_{i=0}^{n} V(n, i, i)$ элементов на главной диагонали матрицы распределения всех типов ранга n равна 2^n. Отсюда $\sum_{i=0}^{n+1}\sum_{j=i}^{n+1} K(n+1, i, j) = \sum_{i=0}^{n}\sum_{j=i}^{n} V(n, i, j)$ + 1. Согласно лемме 6, правая часть последнего равенства равна $V(n)$. Отсюда имеем:

$$K(n + 1) = V(n) \qquad (14)$$

и лемма доказана.

Следствие. Между максимальными типами ранга $n + 1$ и всеми типами ранга n существует взаимно однозначное соответствие.

Одним из способов установления взаимно однозначного соответствия является нахождение множества всех типов ранга n, затем множества максимальных типов ранга $n + 1$ и линейное упорядочивание обоих множеств с помощью лексикографического (позиционного покомпонентного) порядка. Тогда взаимно соответствовать друг другу будут каждые два типа, имеющие в этих двух множествах одинаковый номер. В то же время простого алгоритма перехода от произвольного типа ранга n к максимальному типу ранга $n + 1$ пока не найдено.

В [3] и [4] описан метод синтеза цифровых схем на базе МБФ, одним из этапов которого является нахождение множества всех типов ранга n с левой границей i и правой границей j. В [4] показано, что способ нахождения всех типов ранга n, основанный на сравнении этих типов со всеми максимальными типами ранга n, неэффективен, так как с ростом n количество $K(n)$ этих типов очень быстро растет. Используя лемму 2 и теорему 1, можно найти все типы ранга n с заданными границами i и j путем сдвиг-суммы пар типов ранга $n – 1$ и сравнения второго типа каждой пары с максимальными типами ранга $n – 1$. Из рис. 2 видно, что максимальных типов ранга $n – 1$ значительно меньше, чем ранга n. В связи с этим указанный этап синтеза требует меньше затрат времени и памяти, а значит является более эффективным, чем в [4]. Покажем этот этап синтеза на примере.

Пример 7. Допустим, что на базе МБФ от 5 переменных нужно разработать цифровую схему, содержащую элементы И с 2 и 3 входами. Согласно [3] одним из этапов синтеза будет нахождение типов ранга 5 с левой границей 2 и правой границей 3. У этих типов левые дополнения, которые являются типами 4 ранга, могут быть трех видов. Левые дополнения первого вида имеют одинаковые левую и правую границы, равные 1. Таких типов 4: (0,1,0,0.0), (0,2,0,0.0), (0,3,0,0.0) и (0,4,0,0.0). Из леммы 2 найдем типы, которые не могут быть максимальными правыми частями для таких левых дополнений. Максимальными типами ранга 4 с границами 2 и 3 являются 2 типа: (0,0,1,2,0) и (0,0,3,1,0). Уменьшая левую компоненту этих типов на 1, получаем типы: (0,0,0,2,0) и (0,0,2,1,0). Правая максимальная часть для левых дополнений первого вида не может принимать значения: (0,0,0,2,0), (0,0,0,1,0), (0,0,2,1,0) и (0,0,1,1,0). Следовательно, она может принимать 4 значения: (0,0,1,2,0), (0,0,3,1,0), (0,0,0,3,0), и (0,0,0,4,0). Левые дополнения второго вида имеют левую границу 1 и правую границу 2. Таких типов тоже 4: (0,1,1,0.0), (0,1,2,0.0), (0,1,3,0.0) и (0,2,1,0.0). Максимальным типом ранга 4 с одинаковыми левой и правой границами, равными 3, является только тип (0,0,0,4,0). Этот тип и является единственной максимальной правой частью для левых дополнений второго вида. Левые дополнения третьего вида состоят из одного нулевого типа (0,0,0,0,0), который не имеет ни левой, ни правой границы. Максимальной правой частью для него может быть любой тип 4 ранга с левой границей 2 и правой границей 3. Таких типов 4: (0,0,1,1,0), (0,0,1,2,0), (0,0,2,1,0) и (0,0,3,1,0). С помощью операции сдвиг-суммы левые дополнения трех видов с соответствующими им максимальными правыми частями образуют 24 типа 5 ранга с границами 2 и 3: $4\times4+4\times1+1\times4=24$. Выпишем их в лексикографическом порядке: (0,0,1,1,0,0), (0,0,1,2,0,0), (0,0,1,3,0,0), (0,0,1,4,0,0), (0,0,1,5,0,0), (0,0,1,6,0,0), (0,0,1,7,0,0), (0,0,2,1,0,0), (0,0,2,2,0,0), (0,0,2,3,0,0), (0,0,2,4,0,0), (0,0,2,5,0,0), (0,0,3,1,0,0), (0,0,3,2,0,0), (0,0,3,3,0,0), (0,0,3,4,0,0), (0,0,4,1,0,0), (0,0,4,2,0,0), (0,0,4,3,0,0), (0,0,4,4,0,0), (0,0,5,1,0,0), (0,0,5,2,0,0), (0,0,6,1,0,0) и (0,0,7,1,0,0). Каждый из этих типов определяет некоторый класс цифровых схем на основе МБФ [3]. Например, класс (0,0,4,3,0,0) соответствует схемам, содержащим 4 элемента И с 2 входами и 3 элемента И с 3 входами, причем на вход схемы приходят 5 двоичных входных переменных. Следующими этапами рассматриваемого метода синтеза являются поиск класса схем, позволяющего реализовать заданную функцию, и выбор подходящей схемы внутри найденного класса.

На основе доказанных теорем разработана программа, в которой найдены таблицы распределения всех типов и максимальных типов до 15 ранга включительно (в [4] таблица распределения всех типов находилась путем сравнения каждого типа со всеми максимальными типами, что позволило за несколько часов найти такую таблицу только 10 ранга). Эта программа позволяет находить сами типы с заданными границами. Разработка эффективного способа нахождения всех типов МБФ произвольного ранга n с заданными границами i и j позволило исключить операции сравнения каждого типа со всеми максимальными типами, а значит значительно повысить эффективность алгоритма нахождения этих типов.

В заключение отметим следующее. Разработан эффективный способ нахождения всех типов МБФ произвольного ранга n с заданными границами, что позволяет во время синтеза заданной МБФ рассмотреть все возможные классы цифровых схем. Доказаны теоремы, устанавливающие взаимно однозначное соответствие между максимальными типами ранга $n + 1$ и всеми типами ранга n, а также позволяющие рекуррентно находить таблицу распределения всех типов 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. *Самофалов А.Г.* Комбинаторный подход к синтезу специальных классов булевых функций / А.Г. Самофалов, А.П. Марковский // Электронное моделирование. – 2004. – Т.26, №3. – С. 27– 40.
3. *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.
4. *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.
5. *Ткаченко В.Г.* Деревья типов монотонных булевых функций и криптосистемы с блоками переменной длины / В.Г. Ткаченко, О.В. Синявский // Наукові праці ОНАЗ ім. О.С. Попова. – 2009. – №2. – С. 32 – 42.
6. *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.