

УДК 512.55

**КРИТЕРИИ ФУНКЦИОНАЛЬНОЙ РАЗДЕЛИМОСТИ
КВАДРАТИЧНЫХ БУЛЕВЫХ ПОРОГОВЫХ ФУНКЦИЙ**

А. Н. Шурупов

*Московский государственный технический университет радиотехники, электроники
и автоматики (МИРЭА), г. Москва, Россия*

Работа продолжает исследование функциональной структуры булевых функций, задаваемых действительными линейными неравенствами. Рассматриваются булевы функции, определяемые одним нелинейным неравенством второй степени. Многочлены второй степени среди всех нелинейных многочленов обладают наименьшим размером задания, т. е. свойством, существенным в ряде прикладных задач. Доказаны три критерия функциональной разделимости для булевых квадратичных пороговых функций. Второй критерий не требует анализа табличного задания функции и формулируется в терминах пороговой структуры.

Ключевые слова: функциональная разделимость, декомпозиция, булевы пороговые функции, квадратичные неравенства.

DOI 10.17223/20710410/28/4

**FUNCTIONAL DECOMPOSABILITY CRITERIA FOR QUADRATIC
THRESHOLD BOOLEAN FUNCTIONS**

A. N. Shurupov

*Moscow State Institute of Radio Engineering, Electronics and Automation, Moscow, Russia***E-mail:** ashurupov@mail.ru

Threshold functions provide a simple but fundamental model for many questions investigated in image recognition, artificial neural networks and many other areas. In this paper, the results in Boolean threshold function decomposition are advanced to Boolean functions represented by one quadratic inequality. Quadratic polynomials are the most compact non-linear polynomials and this property sometimes is quite important. We prove three criteria for non-trivial decomposition of quadratic Boolean threshold functions. One of them can be applied without analysis of truth table and only uses the threshold structure parameters.

Keywords: Boolean functions, threshold functions, decomposition, quadratic inequalities.

1. Основные понятия

Проблема описания функционально разделимых булевых функций, то есть функций, допускающих неповторную декомпозицию, исследуется много лет. Прекрасный обзор и ряд глубоких результатов по декомпозиции k -значных функций содержится в [1]. В настоящей работе рассматривается функциональная разделимость булевых функций из одного специфического класса — булевых пороговых функций, задаваемых квадратичными неравенствами. Интерес к пороговым функциям в настоящее

время обуславливается их применениями для решения задач распознавания образов, в искусственных нейронных сетях и других областях [2]. Вопросы функциональной разделимости для булевых (линейных) пороговых функций рассмотрены в [3].

В дальнейшем потребуются следующие понятия (см. [1, 4–6]).

Пусть $F_2(n) = \{f : \{0, 1\}^n \rightarrow \{0, 1\}\}$ — множество всех булевых функций от n переменных.

Определение 1. Пусть K — некоторый непустой класс булевых функций. Если для функции $f \in F_2(n)$ существует представление

$$f(x_1, \dots, x_n) = \varphi(\psi(x_{i_1}, \dots, x_{i_m}), x_{i_{m+1}}, \dots, x_{i_n})$$

для некоторых m , перестановки индексов переменных $(i_1, \dots, i_n)$ и функций $\varphi, \psi \in K$, то говорят, что f допускает *простую неповторную декомпозицию* в классе K . При этом переменные $x_{i_1}, \dots, x_{i_m}$ называются *связанными*, а $x_{i_{m+1}}, \dots, x_{i_n}$ — *свободными*. Везде далее в силу рассмотрения только неповторных декомпозиций будем опускать термин «неповторная». Простая декомпозиция называется *нетривиальной*, если $1 < m < n$. Функции, допускающие нетривиальные простые декомпозиции, называются *функционально разделимыми* над соответствующим классом функций.

Заметим, что определение 1 является более общим по отношению к определению 2.15 работы [6], так как рассматривает декомпозицию в произвольном классе булевых функций. Кроме того, в смысле определения 2.15 указанной работы функционально неразделимой будет булева функция $f(x_1, \dots, x_4) = (x_1x_2 \oplus x_1x_3 \oplus x_2x_3)x_4$, в то время как она является очевидно разложимой (и разделимой в смысле определения 1).

Далее без особых оговорок будем в случаях, ясных по контексту изложения, использовать для неотрицательных целых чисел и векторов — их двоичных представлений — одни и те же обозначения. *Таблица разбиения* $T^{(m)}$ *булевой функции* $f(x_1, \dots, x_n)$ *с параметром (разбиения) m* определяется как матрица, состоящая из 2^m строк и 2^{n-m} столбцов с элементами $t_{u,v} = f(u, v) = f(u_1, \dots, u_m, v_1, \dots, v_{n-m})$. Известен [4] критерий функциональной разделимости, приводимый здесь для удобства в формулировке [3].

Теорема 1. Булева функция f допускает простую декомпозицию вида

$$f(x_1, \dots, x_n) = \varphi(\psi(x_1, \dots, x_m), x_{m+1}, \dots, x_n) \quad (1)$$

в том и только в том случае, когда в $T^{(m)}$ существует не более двух типов различных строк.

Введём определение булевых функций, задаваемых квадратичными неравенствами, функциональные свойства которых изучаются в этой работе. Более общее определение полиномиально-задаваемой (или полиномиальной, как в [7]) пороговой функции можно найти вместе с богатой библиографией и обзором результатов по пороговым функциям в [8]. Эти понятия приводятся также в [7], как и следующее определение.

Определение 2. Булева функция $f \in F_2(n)$ называется *квадратичной пороговой* (*к.п.б.ф.*), если существует многочлен $q \in \mathbb{R}[x_1, \dots, x_n]$, такой, что

$$\deg q(x_1, \dots, x_n) = 2; \quad (2)$$

$$f(x_1, \dots, x_n) = 0 \Leftrightarrow q(x_1, \dots, x_n) \leq 0. \quad (3)$$

Традиционные пороговые функции в смысле определения 2 могут быть названы линейными пороговыми функциями. Отметим, что хотя в [7] булева функция в смысле определения 2 называется знаковой функцией многочлена q , а сам многочлен q — пороговым элементом, мы будем использовать также терминологию определения 2 для сохранения преемственности с теорией булевых линейных пороговых функций.

Многочлен q из определения 2 может быть представлен в виде $q(x_1, \dots, x_n) = l(x_1, \dots, x_n) + q_2(x_1, \dots, x_n)$, где l — линейная часть многочлена, а q_2 — квадратичная часть. Так как для булевых переменных справедливо равенство $x = x^2$, многочлен $l = a_1x_1 + \dots + a_nx_n + a_0$ совпадает с $q_1 = a_1x_1^2 + \dots + a_nx_n^2 + a_0$ на булевых значениях переменных. Поэтому в качестве порогового элемента можно взять многочлен $q = q_1 + q_2$, и, без ограничения общности, далее будем рассматривать только такие многочлены для задания квадратичных пороговых функций. Очевидно, что многочлен $q - a_0$ является квадратичной формой. Заметим, что в силу вышеизложенного линейные пороговые булевы функции являются частным случаем квадратичных пороговых функций.

Изменим в целях удобства оперирования квадратичными формами соотношение (3) на равносильное путём переноса свободного члена порогового элемента q в правую часть:

$$f(x_1, \dots, x_n) = 0 \Leftrightarrow g(x_1, \dots, x_n) \leq t,$$

где $g = q - a_0$; $t = -a_0$.

Укажем способы задания квадратичных пороговых функций. Пусть $G = (g_{ij})$ — матрица коэффициентов квадратичной формы g при фиксированном способе их упорядочивания. Пара (G, t) называется *структурой* квадратичной пороговой функции f (и обозначается $f \sim (G, t)$), элементы матрицы G — весами, а t — порогом. Далее в случаях, допускающих однозначное понимание, для простоты вместо (G, t) будем использовать (g, t) . Известно, что структура является неоднозначным способом задания к.п.б.ф. Вместо матрицы коэффициентов многочлена в структуре можно указывать матрицу квадратичной формы. Пусть $g(x_1, \dots, x_n) = \sum_{1 \leq i < j \leq n} g_{ij}x_i x_j + \sum_{i=1}^n g_i x_i^2$ — каноническая форма многочлена квадратичной формы. Тогда элементы матрицы $W_g = (w_{ij})_{i,j=1,\dots,n}$ квадратичной формы $g(x_1, \dots, x_n) = xW_g x^T$ над полем действительных чисел от переменных $x = (x_1, \dots, x_n)$ определяются как

$$w_{ij} = \frac{g_{ij}}{2}, \quad i < j,$$

$$w_{ij} = w_{ji}, \quad i > j,$$

$$w_{ii} = g_i.$$

Очевидно, что $g_{ij} = w_{ij} + w_{ji}$, $i \neq j$. Квадратичная форма называется канонической (или имеет канонический вид), если её матрица диагональная. Известно, что любая ненулевая квадратичная форма над $\mathbb{R}$ эквивалентна некоторой канонической, т. е. существует такая ортогональная матрица C над $\mathbb{R}$, что замена переменных $x = yC$ переводит матрицу W квадратичной формы в каноническую $K_W = \text{diag}(\lambda_1, \dots, \lambda_n)$, где λ_i — собственные значения матрицы W . Отметим, что при такой замене переменные $y = xC^{-1}$ уже не являются, вообще говоря, булевыми при булевых наборах x , и поэтому эквивалентные квадратичные формы задают в общем случае разные к.п.б.ф. Исключением здесь является случай, в котором булевы наборы переменных x и y связаны невырожденной матрицей перехода над $\mathbb{R}$, тогда эта матрица должна быть подстановочной и соответствующие булевы функции отличаются перестановкой переменных.

Для неподстановочных матриц перехода исходная и новая к.п.б.ф. могут быть не связаны друг с другом линейным преобразованием координат. Аналогично, рассматривая линейное преобразование координат над $\text{GF}(2)$, получаем, что новая функция задается неравенством, возможно, более чем второй степени, в отличие от исходной к.п.б.ф.

Пусть $u = \sum_{i,j=1}^m u_{ij}x_i x_j$ — квадратичная форма от m первых переменных, а $v = \sum_{i,j=m+1}^n v_{ij}x_i x_j$ — квадратичная форма от $n - m$ остальных переменных. Тогда через $w = u + v$ обозначим естественным образом составленную из этих форм квадратичную форму от n переменных, для которой также будем использовать обозначение через набор весов $w = (u|v)$. Квадратичная форма такого вида называется *распавшейся*.

Лемма 1. Квадратичная форма w является распавшейся тогда и только тогда, когда существует каноническая форма K_w , такая, что матрица перехода C — распавшаяся, т. е. $C = \text{diag}(C_u, C_v)$.

Доказательство. Необходимость следует из того, что матрица W квадратичной формы — распавшаяся, и поэтому каждую клетку можно независимо от другой привести к диагональной с помощью своей матрицы перехода. Достаточность следует из равенства

$$W = \begin{pmatrix} C_u^{-1} K_u C_u & 0 \\ 0 & C_v^{-1} K_v C_v \end{pmatrix}.$$

Лемма доказана. ■

Пусть $A_w = \{w(x) : x \in \{0, 1\}^n\}$ — мультимножество значений квадратичной формы $w(x)$. Через $\{A_w\}$ обозначим множество значений $w(x)$. Под набором $w^* = (w_0^*, w_1^*, \dots, w_{2^n-1}^*)$ понимается упорядоченный по неубыванию набор элементов мультимножества A_w .

Определим, как в работе [3], понятия нижнего $\lfloor a \rfloor_w$ и верхнего $\lceil a \rceil_w$ приближений действительного числа a в множестве значений $w(x)$ следующим образом:

$$\lfloor a \rfloor_w = \max\{z \in \{A_w\} : z \leq a\}; \quad (4)$$

$$\lceil a \rceil_w = \min\{z \in \{A_w\} : z > a\}. \quad (5)$$

Заметим, что нижнее и верхнее приближения a существуют, если и только если $a \geq w_0^*$ и $a < w_{2^n-1}^*$ соответственно, где n — ранг w . В дальнейшем для удобства максимальный элемент последовательности w^* обозначим через $w_{\max}^*$. Кроме того, положим $\lfloor a \rfloor_w = -\infty$, если $a < w_0^*$, и $\lceil a \rceil_w = \infty$, если $a \geq w_{\max}^*$, и в этом случае будем говорить о бесконечных приближениях.

Очевидны следующие свойства конечных приближений:

- 1) $\lfloor w_i^* \rfloor_w = w_i^*$, а также $\lfloor w_i^* \rfloor_w = w_j^*$ для всех j , таких, что $w_j^* = w_i^*$;
- 2) $\lfloor a \rfloor_w \leq a$;
- 3) если $w(x) \leq a$, то $w(x) \leq \lfloor a \rfloor_w$;
- 4) $\lceil w_i^* \rceil_w = w_{i+1}^*$, если $w_i^* \neq w_{i+1}^*$;
- 5) $\lceil a \rceil_w > a$.

Введём в рассмотрение таблицу $S^{(m)} = \|s_{ij}\|$, $i = 0, \dots, 2^m - 1$, $j = 0, \dots, 2^{n-m} - 1$, для к.п.б.ф. f со структурой $(u|v, t)$, $\text{rang } u = m$, элементы которой определяются

следующим образом:

$$\begin{aligned} s_{ij} &= 0 \Leftrightarrow u_i^* + v_j^* \leq t, \\ s_{ij} &= 1 \Leftrightarrow u_i^* + v_j^* > t. \end{aligned}$$

Для таблицы $S^{(m)}$ справедливо *свойство монотонности*: если $p \geq i$, $q \geq j$, то $s_{pq} \geq s_{ij}$. Легко установить связь таблиц $S^{(m)}$ и $T^{(m)}$. Пусть g_1, g_2 — подстановки степеней 2^m и 2^{n-m} , такие, что $u_i^* = u(g_1(i))$, $v_j^* = v(g_2(j))$, где $i \in \{0, \dots, 2^m - 1\}$, $j \in \{0, \dots, 2^{n-m} - 1\}$. Тогда $t_{g_1(i), g_2(j)} = s_{i,j}$.

Неочевидной является связь между функциональной разделимостью с параметром m и диагональным видом матрицы весов к.п.б.ф. Действительно, для $m = 1$ любая, в том числе к.п.б.ф., допускает тривиальную декомпозицию, однако при этом матрица квадратичной формы не обязательно является распавшейся с блоком размера 1. Поэтому в дальнейшем при исследовании функциональной разделимости к.п.б.ф. с параметром m будем рассматривать упрощающее предположение, заключающееся в том, что квадратичная форма — распавшаяся.

2. Критерии функциональной разделимости

Следующая теорема является прямым обобщением теоремы 2 работы [3] и утверждает, что для к.п.б.ф. с распавшейся квадратичной формой при решении вопроса о функциональной разделимости достаточно ограничиться классом квадратичных пороговых булевых функций. Для простоты далее везде будем считать, что перестановка переменных в (1) тождественная.

Теорема 2. К.п.б.ф. f со структурой $(u|v, t)$ допускает простую декомпозицию вида (1) над $F_2(n)$ в том и только в том случае, когда справедливо представление

$$f(x_1, \dots, x_n) = g(x_1, \dots, x_m)h_1(x_{m+1}, \dots, x_n) \vee h_2(x_{m+1}, \dots, x_n), \quad (6)$$

где g, h_1, h_2 — к.п.б.ф.

Доказательство. Необходимость. Пусть f — к.п.б.ф. со структурой $(u|v, t)$. По теореме 1 в $S^{(m)}$ существует не более двух типов различных строк. Если все строки совпадают, то функция f зависит несущественно от первых m переменных и, полагая $h_1(x_{m+1}, \dots, x_n) = h_2(x_{m+1}, \dots, x_n) = f(0, \dots, 0, x_{m+1}, \dots, x_n)$, $g(x_1, \dots, x_m) \equiv 0$, получаем искомое представление (1). Рассмотрим случай, когда в $S^{(m)}$ существуют ровно два типа различных строк. Тогда по свойству монотонности индексы строк одного типа в $S^{(m)}$ образуют последовательность подряд идущих чисел. Пусть строки с индексами $0, 1, \dots, r-1$ совпадают и более таких строк в $S^{(m)}$ нет. Определим таблицы M_1 и M_2 размера $2^m \times 2^{n-m}$ следующим образом. M_1 имеет нулевыми r первых строк, а остальные совпадают со строкой $\mathbf{s}_r$. M_2 состоит из одинаковых строк, совпадающих со строкой $\mathbf{s}_0$ — первой строкой таблицы $S^{(m)}$. Тогда по свойству монотонности имеем $S^{(m)} = M_1 \vee M_2$, где дизъюнкция (а также ниже используемая операция булева умножения) применяется к таблицам поэлементно. Для M_1 справедливо представление $M_1 = M_1^{(1)} \cdot M_1^{(2)}$, где $M_1^{(1)}$ — таблица размера $2^m \times 2^{n-m}$, состоящая из первых r нулевых и $(2^m - r)$ 1-константных остальных строк; $M_1^{(2)}$ — таблица размера $2^m \times 2^{n-m}$, состоящая из одинаковых строк, совпадающих с $\mathbf{s}_r$. Итак, имеем $S^{(m)} = M_1^{(1)} \cdot M_1^{(2)} \vee M_2$. Напомним, что булевы умножение и дизъюнкция являются линейно-пороговыми функциями, а значит — к.п.б.ф. Поэтому для завершения доказательства достаточно показать, что $M_1^{(1)}, M_1^{(2)}, M_2$ определяют табличное задание

искомых к.п.б.ф. g, h_1, h_2 в (6). Пусть $w = (u|v)$ и подстановки g_1 и g_2 задают связь таблиц $S^{(m)}$ и $T^{(m)}$. Приведём подробное изложение доказательства для таблицы M_2 . Для $M_1^{(1)}$ и $M_1^{(2)}$ рассуждения практически полностью аналогичны. По построению таблица $M_2 = (m_{ij}^{(2)})$ состоит из одинаковых строк, совпадающих с s_0 , следовательно, $T_2 = (t_{ij}^{(2)})$, $t_{g_1(i), g_2(j)}^{(2)} = m_{i,j}^{(2)}$, является таблицей булевой функции, зависящей от переменных $x_{m+1}, \dots, x_n$. Обозначим эту булеву функцию через h_2 . Покажем, что h_2 — к.п.б.ф. Действительно, справедлива следующая цепочка равносильных утверждений:

$$\begin{aligned} h_2(y) = h_2(y_1, \dots, y_{n-m}) = 0 &\Leftrightarrow \forall p \in \{0, \dots, 2^m - 1\} (t_{p,y}^{(2)} = m_{g_1^{-1}(p), g_2^{-1}(y)}^{(2)} = 0) \Leftrightarrow \\ &\Leftrightarrow s_{0,q} = 0, \quad q = g_2^{-1}(y) \Leftrightarrow u_0^* + v_q^* \leq t \Leftrightarrow u_0^* + v(g_2(q)) \leq t \Leftrightarrow v(y) \leq t - u_0^*. \end{aligned}$$

Таким образом, h_2 — к.п.б.ф. со структурой $(v, t - u_0^*)$. Аналогично, таблицы $M_1^{(1)}$ и $M_1^{(2)}$ задают к.п.б.ф. g и h_1 со структурами (u, u_{r-1}^*) и $(u, t - u_r^*)$ соответственно. Достаточность очевидна. Действительно, искомая декомпозиция имеет вид

$$\varphi(x_1, \dots, x_m) = g, \psi(\varphi, x_{m+1}, \dots, x_n) = \varphi h_1(x_{m+1}, \dots, x_n) \vee h_2(x_{m+1}, \dots, x_n).$$

Теорема доказана. ■

Следующие результаты обобщают теорему 3 работы [3] и сводят исследование функциональной разделимости к.п.б.ф. к анализу её структуры.

Теорема 3. К.п.б.ф. f со структурой $(u|v, t)$ допускает простую декомпозицию вида (1) над $F_2(n)$ в том и только в том случае, когда найдутся такие числа c_1 и c_2 , что выполняются неравенства

$$\max([c_1]_u + [t - u_0^*]_v, u_{\max}^* + [c_2]_v) \leq t < [c_1]_u + [c_2]_v. \quad (7)$$

Доказательство. Необходимость. По теореме 2 справедливо представление (6). Тогда неравенства (7) выполняются для соответствующих приближений порогов $c_1 = u_{r-1}^*$, $c_2 = t - u_r^*$, $c_3 = t - u_0^*$ функций g, h_1, h_2 , участвующих в представлении (6). Действительно, неравенство $[c_1]_u + [c_3]_v \leq t$ является следствием совпадения строк таблицы $S^{(m)}$ с номерами из множества $\{0, 1, \dots, r-1\}$, а выполнение неравенства $u_{\max}^* + [c_2]_v \leq t < [c_1]_u + [c_2]_v$ равносильно совпадению остальных строк $S^{(m)}$.

Достаточность. Если все строки таблицы $S^{(m)}$ для функции f одинаковы, имеем тривиальную декомпозицию для функции f , т. е. то, что и требовалось доказать. Поэтому будем считать, что имеем не менее двух типов различных строк в таблице $S^{(m)}$.

Пусть для заданного m -разбиения $(u|v, t)$ и числа t система (7) имеет решение c_1, c_2 . Покажем, что функция f имеет вид (6), причём g, h_1, h_2 — к.п.б.ф. со структурами (u, c_1) , (v, c_2) , (v, c_3) соответственно, где $c_3 = t - u_0^*$. Правая часть (6) определяет некоторую функцию $p(x_1, \dots, x_n) = gh_1 \vee h_2$. Докажем, что функции $p(x_1, \dots, x_n)$ и $f(x_1, \dots, x_n)$ равны.

Рассмотрим случай $c_2 \geq t - u_0^*$. Пусть α — такой индекс столбца, что выполняется $v_\alpha^* \leq c_2 < v_{\alpha+1}^*$ (ниже рассмотрим остальные варианты для α). Тогда из (7) имеем $u_{\max}^* + [c_2]_v = u_{\max}^* + v_\alpha^* \leq t$, и по свойству монотонности $S^{(m)}$ элементы $s_{i,j} = 0$ для всех i и $j \leq \alpha$. С другой стороны, $t \leq u_0^* + c_2 < u_0^* + v_{\alpha+1}^*$, что означает $s_{i,j} = 1$ для всех i и $j > \alpha$. Таким образом, в таблице $S^{(m)}$ все строки одинаковые, что противоречит нашим предположениям. Если же $\alpha + 1 = 0$, то $s_{0,0} = 1$ и $f \equiv 1$, что также приводит к противоречию. К аналогичному результату, а именно $f \equiv 0$, приводит предположение $v_\alpha^* = v_{\max}^*$.

Пусть $c_2 < t - u_0^* = c_3$. Функция $p(x_1, \dots, x_n) = 0$ в том и только в том случае, если для некоторых $y \in \{0, 1\}^m$, $z \in \{0, 1\}^{n-m}$, $x = (y, z)$ выполняется система

$$\begin{cases} g(y)h_1(z) = 0, \\ h_2(z) = 0, \end{cases} \Leftrightarrow \left(\begin{cases} g(y) = 0, \\ h_2(z) = 0, \end{cases} \text{ или } \begin{cases} h_1(z) = 0, \\ h_2(z) = 0 \end{cases} \right).$$

Тогда, продолжая равносильные преобразования, получим

$$\begin{cases} u(y) \leq \lfloor c_1 \rfloor_u, \\ v(z) \leq \lfloor c_3 \rfloor_v, \end{cases} \text{ или } \begin{cases} v(z) \leq \lfloor c_2 \rfloor_v, \end{cases}$$

что означает с учётом (7) выполнение в первом случае неравенства

$$w(y, z) = u(y) + v(z) \leq \lfloor c_1 \rfloor_u + \lfloor c_3 \rfloor_v \leq t,$$

а во втором — $w(y, z) = u(y) + v(z) \leq u_{\max}^* + v(z) \leq u_{\max}^* + \lfloor c_2 \rfloor_v \leq t$.

Итак, доказано включение

$$A_p^0 = \{x \in \{0, 1\}^n : p(x) = 0\} \subseteq A_f^0 = \{x \in \{0, 1\}^n : f(x) = 0\}. \quad (8)$$

В случае, если $p(y, z) = 1$, имеем

$$\begin{aligned} (g(y)h_1(z) = 1 \text{ или } h_2(z) = 1) &\Leftrightarrow \left(\begin{cases} g(y) = 1, \\ h_1(z) = 1, \end{cases} \text{ или } h_2(z) = 1 \right) \Leftrightarrow \\ &\Leftrightarrow \left(\begin{cases} u(y) \geq \lceil c_1 \rceil_u, \\ v(z) \geq \lceil c_2 \rceil_v, \end{cases} \text{ или } v(z) > c_3 \right). \end{aligned}$$

Проанализируем последнюю систему. Если выполняется $g(y)h_1(z) = 1$, то по условию получаем

$$w(y, z) = u(y) + v(z) \geq \lceil c_1 \rceil_u + \lceil c_2 \rceil_v > t.$$

В случае $v(z) > c_3$ имеем следующую цепочку неравенств:

$$w(y, z) = u(y) + v(z) > u(y) + c_3 = u(y) - u_0^* + t \geq t.$$

Итак, из $p(y, z) = 1$ получаем $w(y, z) > t$, что доказывает включение

$$A_p^1 \subseteq A_f^1. \quad (9)$$

Объединяя (8) и (9), учитывая, что $|A_p^0 \cup A_p^1| = |A_f^0 \cup A_f^1| = 2^n$, $A_p^0 \cap A_p^1 = A_w^0 \cap A_w^1 = \emptyset$, получим $A_p^0 = A_f^0$ и $A_p^1 = A_f^1$, то есть f имеет вид (6), что и требовалось доказать. Теорема доказана. ■

Замечание 1. Легко видеть, что теоремы 2 и 3 по существу используют только факт декомпозиции полинома $w(x) = w(y, z) = u(y) + v(z)$. По этой причине эти результаты можно обобщить на произвольный функциональный класс, содержащий дизъюнкцию и конъюнкцию.

Пример 1. Построим с использованием теоремы 3 недекомпозируемую квадратичную пороговую булеву функцию от 10 переменных, задаваемую распавшейся матрицей квадратичной формы. Пусть $\mathbf{1}_n$ — целочисленная квадратная матрица размера n , состоящая из одних единиц. Рассмотрим к.п.б.ф. $f(x_1, \dots, x_{10})$, задаваемую структурой $(\mathbf{1}_5 | \mathbf{1}_5, 30)$. Тогда конечное приближение $\lfloor c \rfloor_{\mathbf{1}_5} = a^2$ для некоторого $a \in \{0, \dots, 5\}$, $\lceil c \rceil_{\mathbf{1}_5} = (a+1)^2$ и система (7), принимающая вид

$$\begin{cases} a^2 \leq 5, \\ b^2 \leq 5, \\ (a+1)^2 + (b+1)^2 > 30, \end{cases}$$

очевидно, не имеет решений относительно a и b .

Теорема 4. К.п.б.ф. f со структурой $(u|v, t)$ допускает представление вида (1) над $F_2(n)$ тогда и только тогда, когда

$$\left| \{ \lfloor t - b \rfloor_u : b \in \{A_v\}, u_0^* \leq t - b < u_{\max}^* \} \right| \leq 1. \quad (10)$$

Доказательство. Пусть число переменных функции равно n , а параметр разбиения m . Воспользуемся табличным представлением функции f в виде $S^{(m)}$. В силу условия монотонности индексы одинаковых строк таблицы $S^{(m)}$ образуют последовательность подряд идущих целых чисел. По теореме 1 достаточно доказать, что выполнение неравенства (10) означает существование в $S^{(m)}$ не более двух различных типов строк, и наоборот. Строки с индексами i и $i+1$ различны в том и только в том случае, если найдётся такой $j \in \{0, \dots, 2^{n-m} - 1\}$, что $s_{i,j} < s_{i+1,j}$. Это означает $u_i^* + v_j^* \leq t < u_{i+1}^* + v_j^*$, что равносильно существованию $b \in \{A_v\}$, такому, что $u_i^* \leq t - b < u_{i+1}^*$. При этом $u_i^* = \lfloor t - b \rfloor_u$. Таким образом, знакоперемена $(0, 1)$ в b -м столбце однозначно определяется величиной $\lfloor t - b \rfloor_u < u_{\max}^*$. Следовательно, различные конечные нижние приближения $\lfloor t - b \rfloor_u < u_{\max}^*$ соответствуют различным строкам (при этом первая строка не входит в подсчёт, так как не образует знакоперемены). Таким образом, число таких конечных нижних приближений равно числу блоков одинаковых строк таблицы $S^{(m)}$ минус единица. ■

ЛИТЕРАТУРА

1. Черемушкин А. В. Бесповторная декомпозиция сильно зависимых функций // Дискретная математика. 2004. Т. 16. Вып. 3. С. 3–42.
2. Ежов А. А., Шумский С. А. Нейрокомпьютинг и его применения в экономике и бизнесе. М.: МИФИ, 1998. 222 с.
3. Шурупов А. Н. О функциональной разделимости булевых пороговых функций // Дискретная математика. 1997. Т. 9. Вып. 2. С. 59–73.
4. Ashenurst R. L. The decomposition of switching functions // Ann. Comput. Laborat. Harv. Univ. 1959. V. 29. P. 74–116.
5. Дертоузос М. Пороговая логика. М.: Мир, 1967. 343 с.
6. Логачев О. А., Сальников А. А., Яценко В. В. Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004. 470 с.
7. Подольский В. В. Оценки весов персептронов (полиномиальных пороговых булевых функций): автореф. дис. ... канд. физ.-мат. наук. М.: МГУ им. М. В. Ломоносова, 2009.
8. Crama Y. and Hammer P. Boolean Functions. Theory, Algorithms and Applications. Cambridge University Press, 2011.

REFERENCES

1. *Cheremushkin A. V.* Iteration-free decomposition of strongly dependent functions. *Discr. Math. Appl.*, 2004, vol. 14, iss. 5, pp. 439–478.
2. *Ezhov A. A., Shumskiy S. A.* Neyrokomп'yuting i ego primeneniya v ekonomike i biznese [Neurocomputing and its Applications in Economics and Business]. Moscow, MEPhI Publ., 1998. 222 p. (in Russian)
3. *Shurupov A. N.* On the functional decomposability of Boolean threshold functions. *Discr. Math. Appl.*, 1997, vol. 7, iss. 3, pp. 257–272.
4. *Ashenhurst R. L.* The decomposition of switching functions. *Ann. Comput. Laborat. Harv. Univ.*, 1959, vol. 29, pp. 74–116.
5. *Dertouzos M.* Threshold Logic: A Synthesis Approach. Cambridge, MA, The M.I.T. Press, 1965.
6. *Logachev O. A., Sal'nikov A. A., Yashchenko V. V.* Bulevy funktsii v teorii kodirovaniya i kriptologii [Boolean Functions in Coding Theory and Cryptology]. Moscow, MCCME Publ., 2004. 470 p. (in Russian)
7. *Podol'skiy V. V.* Otsenki vesov perseptronov (polynomial'nykh porogovykh bulevykh funktsiy) [Ratings Scales Perceptrons (Polynomial Threshold Boolean Functions)]. Abstract of PhD in Physics and Mathematics thesis. Moscow, MSU Publ., 2009. (in Russian)
8. *Crama Y. and Hammer P.* Boolean Functions. Theory, Algorithms and Applications. Cambridge University Press, 2011.