Math-Net.Ru

Общероссийский математический портал

А. Н. Шурупов, О функциональной разделимости булевых пороговых функций, *Дискрет. матем.*, 1997, том 9, выпуск 2, 59–73

DOI: <https://doi.org/10.4213/dm476>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.224.187.69

26 апреля 2023 г., 17:43:36

О функциональной разделимости булевых пороговых функций

© 1997 г. А. Н. Шурупов

Получены необходимые и достаточные условия функциональной разделимости булевых пороговых функций. Описаны некоторые классы функционально разделимых и неразделимых функций.

1. Введение

Булева функция $f\{0,1\}^n \rightarrow \{0,1\}$ называется пороговой (б.п.ф.), если существуют линейная форма $L = L(y_1, \dots, y_n) = a_1 y_1 + \dots + a_n y_n$ с действительными коэффициентами и действительное число c такие, что $f(x_1, \dots, x_n) = 0$ для тех и только тех булевых наборов $(x_1, \dots, x_n)$, для которых справедливо неравенство $L(x_1, \dots, x_n) \leq c$.

Число c называется порогом, а пара (L, c) — структурой булевой пороговой функции [1]. У б.п.ф. может быть много структур, называемых эквивалентными. Для любой б.п.ф. всегда существует целочисленная структура, то есть пара (L, c) такая, что коэффициенты линейной формы L и порог c являются целыми числами.

Интерес к пороговым функциям в настоящее время обуславливается их применениями для решения задач распознавания образов [2, 3], в искусственных нейронных сетях [4] и других областях. Кроме того, пороговая функция может быть интерпретирована как процедура принятия решений с помощью взвешенного голосования. В этом случае показано [2, 3], что при статистической независимости ошибок членов коллектива, взвешенное голосование является оптимальным правилом для выбора решения. Подробное изложение многих результатов теории пороговых функций вместе с библиографией (126 наименований) можно найти в [5].

В настоящей работе исследуется возможность представления булевых пороговых функций в виде неповторной суперпозиции над классом пороговых функций. Такие представления изучаются, например, при синтезе устройств из пороговых элементов [6].

Во втором параграфе предлагаемой статьи приводятся общие результаты по анализу декомпозиционных структур булевых функций [7]. Практическое применение этих результатов связано с традиционными способами задания булевых функций, имеющими экспоненциальную сложность. Для класса булевых пороговых функций в [5] высказано предположение об экспоненциальной сложности способа задания в виде д.н.ф. По этим причинам безусловный интерес приобретает задача описания декомпозиций булевой пороговой функции с помощью ее структуры, способа

задания, имеющего линейную сложность. В теореме 2 показывается, что при исследовании декомпозиционной структуры булевой пороговой функции достаточно ограничиться формулами над классом пороговых функций. В теореме 3 в форме ограничений на элементы структуры б.п.ф. сформулированы необходимые и достаточные условия для представления пороговой функции в виде суперпозиции пороговых функций.

Третий параграф посвящен способам анализа декомпозиционной структуры булевой пороговой функции, не связанным с непосредственной проверкой условий теоремы 3. Развита подход к описанию классов пороговых функций, обладающих свойством функциональной разделимости или не обладающих этим свойством.

В четвертом параграфе намечено важное для практических приложений направление анализа существенной зависимости б.п.ф. от своих переменных.

2. Основные результаты

Напомним основные понятия, необходимые для дальнейшего изложения.

Говорят, что булева функция f допускает простую декомпозицию над классом K булевых функций (конечным или бесконечным), если найдутся булевы функции φ и ψ , реализуемые формулами над K , такие, что справедливо представление

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

для некоторых k и перестановки $(i_1, \dots, i_n)$ индексов переменных.

Простая декомпозиция называется нетривиальной, если $1 < k < n$. Функции, допускающие нетривиальные простые декомпозиции, называются функционально разделимыми над соответствующим классом булевых функций. Интерес к изучению простых декомпозиций обусловлен тем фактом, что описание всех неповторных декомпозиций булевой функции, то есть таких декомпозиций $F(\Phi_1, \dots, \Phi_t)$ булевой функции, в которой функции Φ_i зависят от попарно непересекающихся множеств переменных, сводится к нахождению всех ее простых декомпозиций [7]. При изучении вопросов функциональной разделимости булевых функций условно можно выделить два направления. Первое направление исследований рассматривает свойство функциональной разделимости над классом всех булевых функций [7] (в такой постановке говорят просто о функциональной разделимости) и связано в большей степени с задачей реализации заданной булевой функции с помощью функций от меньшего числа переменных. Второе направление имеет дело с задачей описания множества булевых функций, представимых в виде простой декомпозиции над некоторым собственным подклассом K булевых функций, и возникает при реализации булевых функций на заданной элементной базе. Ниже (следствие 2) показывается, что для пороговой функции функциональная разделимость эквивалентна функциональной разделимости над классом Π всех булевых пороговых функций. В частности, отсюда следует, что если булева пороговая функция не допускает простой декомпозиции над Π , то не существует простой декомпозиции и над любым более широким классом булевых функций.

Изложим общие утверждения о простой декомпозиции булевых функций. Матрица разбиения [7] $T^{(k)}$ булевой функции $f(x_1, \dots, x_n)$ определяется как матрица, состоящая из 2^k строк и 2^{n-k} столбцов с элементами

$$t_{u,v} = f(\bar{u}, \bar{v}) = f(u_1, \dots, u_k, v_1, \dots, v_{n-k}),$$

где $\bar{u}, \bar{v}$ — двоичные разложения целых чисел $u, 0 \leq u \leq 2^k - 1$, и $v, 0 \leq v \leq 2^{n-k} - 1$. В дальнейшем там, где это не будет вызывать недоразумений, будем использовать одно и то же обозначение как для числа, так и для его двоичного разложения. В [7] сформулирован и доказан следующий критерий функциональной разделимости булевой функции над множеством всех булевых функций.

Теорема 1. *Булева функция f допускает простую декомпозицию*

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

в том и только том случае, когда выполняется любое из следующих условий:

- (а) *в матрице $T^{(k)}$ существует не более двух типов различных строк;*
- (б) *в матрице $T^{(k)}$ найдется такой столбец, что все остальные столбцы либо совпадают с ним, либо получаются из него инвертированием всех его элементов, либо состоят из одних нулей, либо из одних единиц.*

Под последовательностью $L^* = (L_0^*, L_1^*, \dots, L_{2^n-1}^*)$ будем понимать неубывающую последовательность значений линейной формы L , вычисленных для всех наборов переменных из множества $\{0, 1\}^n$. Иначе говоря, пусть G — любая подстановка из симметрической группы S_{2^n} подстановок степени 2^n такая, что, если $0 \leq w' \leq w'' \leq 2^n - 1$, то $L(G(w')) \leq L(G(w''))$, где $L(G(w))$ — значение линейной формы $L = L(y_1, \dots, y_n)$ при подстановке вектора двоичного разложения числа $G(w)$ вместо переменных $(y_1, \dots, y_n)$. Тогда $L_w^* = L(G(w))$, $w = 1, \dots, 2^n - 1$. Далее, всякую линейную форму L можно разбить на сумму двух линейных форм

$$L(y_1, \dots, y_n) = U(y_1, \dots, y_k) + V(y_{k+1}, \dots, y_n),$$

где

$$\begin{aligned} U(y_1, \dots, y_k) &= a_1 y_1 + \dots + a_k y_k, \\ V(y_1, \dots, y_{n-k}) &= a_{k+1} y_1 + \dots + a_n y_{n-k}. \end{aligned}$$

Такое представление линейной формы будем называть k -разбиением и обозначать $L = U \dot{+} V$. Задание пороговой функции с помощью структуры является наиболее компактным и естественными в сравнении с другими способами задания булевых функций. Поэтому было бы естественно попытаться получить необходимые и достаточные условия функциональной разделимости пороговых функций в виде соотношений между элементами структуры. Одно затруднение на этом пути заключается в неоднозначности задания функций с помощью структуры. Преодоление отмеченной трудности видится в использовании инвариантов задания пороговых функций с помощью структуры.

Определим понятия нижнего $[a]_L$ и верхнего $\lceil a \rceil_L$ приближений действительного числа a в множестве значений линейной формы L следующим образом:

$$\begin{aligned} [a]_L &= \max \{L(w) \mid w \in \{0, 1\}^n, L(w) \leq a\}, \\ \lceil a \rceil_L &= \min \{L(w) \mid w \in \{0, 1\}^n, L(w) > a\}. \end{aligned}$$

Заметим, что нижнее и верхнее приближения a существуют в том и только том случае, когда $a \geq L_0^*$ и $a < L_{2^n-1}^*$ соответственно, где n — число переменных

формы L . В дальнейшем для удобства максимальный элемент последовательности L^* будем обозначать через $L_{\max}^*$. Кроме того, будем полагать $[a]_L = -\infty$, если $a < L_0^*$, и $[a]_L = \infty$, если $a \geq L_{\max}^*$.

Нетрудно убедиться, что нижнее приближение порога является инвариантом для множества эквивалентных структур с одинаковой линейной формой. Действительно, для любых двух эквивалентных структур (L, c') и (L, c'') выполняются равенства $[c']_L = [c'']_L$, $[c']_L = [c'']_L$. Под задачей Д будем понимать задачу проверки существования нетривиальной простой декомпозиции вида (1) для заданных k и булевой пороговой функции со структурой (L, c) . Воспользуемся теоремой 1 для решения задачи Д. Прежде, чем формулировать соответствующий алгоритм, заметим, что строка матрицы $T^{(k)}$ с номером a , $0 \leq a \leq 2^k - 1$, является таблицей подфункции $f(a, x_{k+1}, \dots, x_n)$ со структурой $(V, c - U(a))$, где $L = U \dot{+} V$ — k -разбиение.

Алгоритм 1.

- (1) Подсчитаем число r различных строк в матрице $T^{(k)}$, $1 < k < n - 1$.
- (2) Если r не более 2, то б.п.ф. f допускает нетривиальную простую декомпозицию вида (1). В противном случае для данного k нетривиальной простой декомпозиции вида (1) не существует.

Обозначим через N_n сложность решения задачи нахождения нижнего приближения произвольного действительного числа в множестве значений линейной формы от n неизвестных. Тогда сложность алгоритма 1 не будет превосходить $O(2^k N_{n-k})$ шагов, где на каждом шаге производится арифметическая операция или операция сравнения над действительными числами. Это следует из того факта, что проверка равенства строк с номерами a' и a'' в матрице $T^{(k)}$ равносильна проверке равенства нижних приближений чисел $c - U(a')$ и $c - U(a'')$ в множестве значений V .

Заметим, что приведенная оценка сложности является оценкой в наихудшем случае и достигается только для функционально разделимых пороговых функций в смысле (1). В ряде исследований ([8, 9]) получены алгоритмы для поиска всех простых декомпозиций произвольной булевой функции. Для этих алгоритмов рассчитаны оценки в среднем, являющиеся лучшими по сравнению с алгоритмом 1, однако, в наихудшем случае, то есть для функционально разделимых функций оценка алгоритма 1 не улучшена.

Для изложения дальнейших результатов понадобится ввести в рассмотрение матрицу

$$S^{(k)} = \|s_{ij}\|, \quad i = 0, 1, \dots, 2^k - 1, \quad j = 0, 1, \dots, 2^{n-k} - 1,$$

для б.п.ф. f со структурой (L, c) . Если $L = U \dot{+} V$ — k -разбиение, то определим $S^{(k)}$ следующим образом:

$$s_{ij} = \begin{cases} 0, & \text{если } U_i^* + V_j^* \leq c, \\ 1, & \text{если } U_i^* + V_j^* > c. \end{cases}$$

Легко установить непосредственную связь матрицы $S^{(k)}$ с матрицей $T^{(k)}$. Пусть $G_1 \in S_{2^k}$, $G_2 \in S_{2^{n-k}}$ такие, что

$$U_i^* = U(G_1(i)), \quad V_j^* = V(G_2(j)), \quad i = 0, 1, \dots, 2^k - 1, \quad j = 0, 1, \dots, 2^{n-k} - 1.$$

Тогда, если $p = G_1(i)$, $q = G_2(j)$, то $t_{pq} = s_{ij}$. Для матрицы $S^{(k)}$ справедливо свойство монотонности: если $p \geq i$, $q \geq j$, то $s_{pq} \geq s_{ij}$.

Используя введенные обозначения, нетрудно получить в качестве следствия теоремы 1 следующий критерий функциональной разделимости булевой пороговой функции.

Следствие 1. *Булева пороговая функция f допускает простую декомпозицию вида (1) в том и только том случае, когда выполняется любое из следующих условий:*

- (а) *в матрице $S^{(k)}$ существует не более двух типов различных строк;*
- (б) *в матрице $S^{(k)}$ найдется такой столбец, что все остальные столбцы либо совпадают с ним, либо состоят из одних нулей, либо из одних единиц.*

Легко видеть, что непосредственно на базе теоремы 1 можно построить алгоритм, имеющий на выходе искомую декомпозицию (в случае ее существования) в виде одного из способов задания булевой функции, то есть таблицы, СДНФ, СКНФ, многочлена Жегалкина и так далее. Так как для пороговой функции структура есть наиболее компактный способ задания, возникает задача представления пороговой функции в виде нетривиальной простой декомпозиции над классом Π всех пороговых функций. В следующей теореме для пороговой функции устанавливается эквивалентность функциональной разделимости над множеством всех булевых функций и функциональной разделимости над Π .

Теорема 2. *Булева пороговая функция f со структурой (L, c) допускает простую декомпозицию вида (1) в том и только том случае, когда справедливо представление*

$$f(x_1, \dots, x_n) = g(x_1, \dots, x_k)h_1(x_{k+1}, \dots, x_n) \vee h_2(x_{k+1}, \dots, x_n), \quad (2)$$

где g, h_1, h_2 — булевы пороговые функции.

Доказательство. Докажем необходимость. Пусть f — б.п.ф. со структурой (L, c) . По следствию из теоремы 1 в матрице $S^{(k)}$ существует не более двух типов различных строк. В случае, если все строки совпадают, то функция f зависит несущественно от первых k переменных и, полагая

$$g(x_1, \dots, x_k) = 0, \quad h_1(x_{k+1}, \dots, x_n) = h_2(x_{k+1}, \dots, x_n) = f(0, \dots, 0, x_{k+1}, \dots, x_n),$$

получаем искомое представление (2). Рассмотрим случай, когда в $S^{(k)}$ существуют ровно два типа различных строк. Тогда по свойству монотонности индексы строк одного типа в $S^{(k)}$ образуют последовательность подряд идущих чисел. Пусть строки с индексами $0, 1, \dots, w-1$ совпадают и более таких строк в $S^{(k)}$ нет. Определим матрицы M_1 и M_2 размера $2^k \times 2^{n-k}$ следующим образом. Пусть M_1 имеет нулевыми w первых строк, а остальные совпадают со строкой $\bar{s}_w$, а M_2 состоит из одинаковых строк, совпадающих с $\bar{s}_0$ — первой строкой матрицы $S^{(k)}$. Тогда по свойству монотонности для $S^{(k)}$

$$S^{(k)} = M_1 \vee M_2,$$

где $\vee$ — операция поэлементной дизъюнкции. Для M_1 справедливо представление

$$M_1 = M_1^{(1)} \bar{\wedge} M_1^{(2)},$$

где $\bar{\wedge}$ — операция поэлементной конъюнкции; $M_1^{(1)}$ — матрица размера $2^k \times 2^{n-k}$, состоящая из первых w нулевых и $(2^k - w)$ единичных строк; $M_1^{(2)}$ — матрица размера $2^k \times 2^{n-k}$, состоящая из одинаковых строк, совпадающих с $\bar{s}_w$. Итак,

$$S^{(k)} = M_1^{(1)} \bar{\wedge} M_1^{(2)} \vee M_2.$$

Для завершения доказательства достаточно показать, что матрицы $M_1^{(1)}$, $M_1^{(2)}$, M_2 определяют табличное задание искомым булевым пороговым функций g , h_1 , h_2 в (2).

Пусть $L = U \dot{+} V$ — k -разбиение и подстановки G_1 и G_2 задают связь матрицы $S^{(k)}$ и $T^{(k)}$:

$$t_{G_1(i), G_2(j)} = s_{ij}, \quad i = 0, 1, \dots, 2^{k-1}, \quad j = 0, 1, \dots, 2^{n-k}.$$

Приведем подробное изложение доказательства для матрицы M_2 . Для матриц $M_1^{(1)}$, $M_1^{(2)}$ рассуждения практически полностью аналогичны. По построению матрица $M_2 = \|m_{ij}^{(2)}\|$ состоит из одинаковых строк, совпадающих с $\bar{s}_0$, следовательно, матрица $T_2 = \|t_{ij}^{(2)}\|$, $t_{G_1(i), G_2(j)} = m_{ij}^{(2)}$, является таблицей булевой функции, зависящей от переменных $x_{k+1}, \dots, x_n$. Обозначим эту булеву функцию через h_2 . Покажем, что h_2 пороговая. Действительно,

$$\begin{aligned} h_2(v) = h_2(v_1, \dots, v_{n-k}) = 0 &\iff \forall p = 0, \dots, 2^k \quad t_{pv}^{(2)} = 0 \\ &\iff \forall p = 0, \dots, 2^k \quad m_{G_1^{-1}(p), G_2^{-1}(v)} = 0 \iff s_{0,q} = 0, q = G_2^{-1}(v) \\ &\iff U_0^* + V_q^* \leq c \iff U_0^* + V(G_2(q)) \leq c \iff V(v) \leq c - U_0^*. \end{aligned}$$

Таким образом, h_2 — б.п.ф. со структурой $(V, c - U_0^*)$. Аналогично, матрицы $M_1^{(1)}$, $M_1^{(2)}$ задают б.п.ф. g , h_1 со структурами (U, U_{w-1}^*) и $(V, c - U_w^*)$.

Достаточность очевидна.

Следствие 2. Булева пороговая функция разделима тогда и только тогда, когда она функционально разделима над Π .

Для доказательства следствия достаточно заметить, что дизъюнкция и конъюнкция являются пороговыми функциями и, следовательно, представление (2) есть формула над Π .

Теорема 3. Булева пороговая функция f со структурой (L, c) допускает простую декомпозицию вида (1) в том и только том случае, когда найдутся такие числа c_1, c_2 , что выполняются неравенства

$$\max([c_1]_U + [d]_V, [c_2]_V + U_{\max}^*) \leq c < [c_1]_U + [c_2]_V, \quad (3)$$

где $L = U \dot{+} V$ — k -разбиение, $d = c - U_0^*$.

Доказательство. Докажем необходимость. По теореме 2 справедливо представление (2). Тогда система (3) выполняется для приближений порогов $c_1, c_2, c_3 = d$ функций g, h_1, h_2 , участвующих в представлении (2), так как неравенство

$$\lfloor c_1 \rfloor_U + \lfloor c_3 \rfloor_V \leq c$$

является следствием совпадения строк матрицы $S^{(k)}$ с номерами из множества $\{0, 1, \dots, w-1\}$, а выполнение неравенства

$$\lfloor c_2 \rfloor_V + U_{\max}^* \leq c < \lceil c_1 \rceil_U + \lceil c_2 \rceil_V$$

равносильно совпадению остальных строк матрицы $S^{(k)}$.

Докажем теперь достаточность. Пусть для заданного k -разбиения $L = U \dot{+} V$ и числа c система (3) имеет решение c_1, c_2 . Покажем, что функция f имеет вид (2), причем g, h_1, h_2 — б.п.ф. со структурами $(U, c_1), (V, c_2), (V, d)$, соответственно. Правая часть (2) принимает значение ноль в том и только том случае, когда для некоторых $u \in \{0, 1\}^k, v \in \{0, 1\}^{n-k}$ выполняются соотношения

$$\begin{aligned} g(u)h_1(v) &= 0, \\ h_2(v) &= 0, \end{aligned}$$

или

$$\begin{aligned} g(u) &= 0, \\ h_2(v) &= 0, \\ h_1(v) &= 0, \\ h_2(v) &= 0. \end{aligned}$$

Заметим, что случай $c_2 \geq d$ определяет б.п.ф. $f = h_2$. Поэтому положим $c_2 < d$. Тогда, продолжая равносильные преобразования, получим, что

$$\begin{aligned} U(u) &\leq \lfloor c_1 \rfloor_U, \\ V(v) &\leq \lfloor d \rfloor_V, \\ V(v) &\leq \lfloor c_2 \rfloor_V, \end{aligned}$$

что означает справедливость неравенств $U(u) + V(v) \leq \lfloor c_1 \rfloor_U + \lfloor d \rfloor_V \leq c$ или $L(u, v) \leq c$. Итак, доказано включение

$$\begin{aligned} A^0 &= \{(u, v) \in \{0, 1\}^k \times \{0, 1\}^{n-k} \mid g(u)h_1(v) \vee h_2(v) = 0\} \\ &\subseteq A_L^0 = \{w \in \{0, 1\}^n \mid L(w) \leq c\}. \end{aligned} \quad (4)$$

В случае, если правая часть (2) принимает значение единица, то путем аналогичных рассуждений получим, что $L(u, v) > c$, что доказывает включение

$$\begin{aligned} A^1 &= \{(u, v) \in \{0, 1\}^k \times \{0, 1\}^{n-k} \mid g(u)h_1(v) \vee h_2(v) = 1\} \\ &\subseteq A_L^1 = \{w \in \{0, 1\}^n \mid L(w) > c\}. \end{aligned} \quad (5)$$

Объединяя (4) и (5), получим $A^0 = A_L^0$, то есть f имеет вид (2).

Теорема доказана.

Теорема 3, так же, как и теорема 1, позволяет решить задачу Д. Сформулируем соответствующий алгоритм.

Алгоритм 2.

- (1) Представим L в виде k -разбиения $L = U \dot{+} V$, $1 < k < n - 1$.
- (2) В зависимости от значения порога c выясним вид искомой декомпозиции:
  - (а) если $c \geq \max(U_{\max}^*, V_{\max}^*)$, то искомая декомпозиция имеет вид $f = gh$, где g, h — б.п.ф. со структурами $(U, c_1), (V, c_2)$ соответственно и $\lfloor d \rfloor_V = V_{\max}^*$;
  - (б) если $U_{\max}^* \leq c < V_{\max}^*$, то искомая декомпозиция имеет вид $f = gh_1 \vee h_2$, где g, h_1, h_2 — б.п.ф. со структурами $(U, c_1), (V, c_2), (V, c - U_0^*)$ соответственно;
  - (в) если $c < \min(U_{\max}^*, V_{\max}^*)$, то в случае $\lfloor c - V_0^* \rfloor_U + \lfloor c - U_0^* \rfloor_V \leq c$ искомая декомпозиция имеет вид $f = g \vee h$, где g, h — б.п.ф. со структурами $(U, c - V_0^*), (V, c - U_0^*)$. Конец работы алгоритма. В противном случае переходим на п.6;
  - (г) если $V_{\max}^* \leq c < U_{\max}^*$, то в случае $\lfloor c - V_0^* \rfloor_U + V_{\max}^* \leq c$ функция f зависит несущественно от переменных $x_{k+1}, \dots, x_n$ и искомая декомпозиция $f = g$, где g — б.п.ф. со структурой $(U, c - V_0^*)$. Конец работы алгоритма. В случае $\lfloor c - V_0^* \rfloor_U + V_{\max}^* > c$ переходим на п.6.
- (3) Составим систему неравенств

$$\max(x_1 + \lfloor d \rfloor_U, x_2 + U_{\max}^*) \leq c < x_3 + x_4$$

относительно целых неизвестных x_1, x_2, x_3, x_4 .

- (4) Найдем первое решение системы неравенств, удовлетворяющее ограничениям

$$\begin{aligned} \lfloor x_1 \rfloor_U &= x_1, & \lfloor x_3 \rfloor_U &= x_3, & \lfloor x_1 \rfloor_U &= x_3, \\ \lfloor x_2 \rfloor_V &= x_4, & \lfloor x_2 \rfloor_V &= x_2, & \lfloor x_4 \rfloor_V &= x_4. \end{aligned}$$

Если таких решений нет, то переходим на п.6.

- (5) Полагая $c_\varepsilon = x_\varepsilon$, $\varepsilon \in \{1, 2\}$, получим структуры функций в представлении f вида (2). Конец работы алгоритма.
- (6) Представления вида (2) для б.п.ф. со структурой (L, c) не существует, следовательно, по теореме 3 искомая декомпозиция не существует. Конец работы алгоритма.

Алгоритм 2 (в отличие от алгоритма 1) в случае существования нетривиальной простой декомпозиции вида (1) на выходе имеет искомую декомпозицию. Остановимся на вопросе оценки сложности алгоритма 2, которая в значительной мере определяется трудоемкостью п.4 и зависит от способа решения системы неравенств, представленной в п.3. Хотя указанная система и является линейной относительно целых неизвестных x_1, x_2, x_3, x_4 , ограничения в п.4 носят существенно нелинейный характер. Так как в данном случае нас интересует только возможность оценки

трудоемкости п.4, в качестве одного из вариантов реализации п.4 предложим следующий переборный метод решения.

Сформируем последовательности U^* и V^* . Дополним их значениями ∞ и $-\infty$. Пусть m_1, m_2 — количества различных элементов в U^* и V^* . Будем перебирать каждую пару вида (U_i^*, V_j^*) в качестве значений пары переменных (x_1, x_2) . Для переменных (x_3, x_4) используем значения (U_{i+1}^*, V_{j+1}^*) . Тогда система ограничений выполняется, и остается только проверить выполнение системы неравенств. Процедуру перебора значений (x_1, x_2) будем выполнять до первого выполнения системы неравенств. Оценка сложности такого метода имеет вид $O(2^k + 2^{n-k} + m_1 m_2)$. Как правило, практический интерес представляют пороговые функции со структурой (L, c) , для которой $m < 2^n$, где m — количество различных элементов в L^* , n — число переменных функции. Для пороговых функций, удовлетворяющих неравенству $m \geq 2^n$, легко показать существование простой декомпозиции вида (1) при любом значении k . В случае полиномиальных оценок для m_1 и m_2 порядок оценки метода будет определяться первыми двумя слагаемыми в общем выражении.

Для оценки N_n заметим, что задача вычисления верхнего приближения относится к задачам дискретной оптимизации и является частным случаем задачи целочисленного линейного программирования [10]. Для фиксированного числа переменных n существует полиномиальный алгоритм решения задач целочисленного линейного программирования [11]. В частности, для задачи минимизации линейной формы от n переменных на конечном множестве $W \in \mathbf{Z}^n$ существует алгоритм, решающий ее не более, чем за $7n^3 \log_2 |W|$ шагов [12], где каждый шаг состоит в вычислении знака некоторой функции вида

$$\sum_{i=1}^n a_i x_i + a_0.$$

При нахождении верхнего приближения в множестве значений линейной формы от n переменных выполняется неравенство $|W| \leq 2^n$ и, следовательно, сложность этой процедуры не превосходит $7n^4$ шагов.

Пример 1. Пусть f — б.п.ф. со структурой $(x_1 + 2x_2 + 2x_3 + 3x_4 + 3x_5 + 3x_6, 8)$. Выясним существование простой декомпозиции для f при $k = 3$, используя приведенный выше алгоритм. На шаге 2 алгоритма 2 выполняются условия п.(б), поэтому существуют все нижние и верхние приближения. Заметим, что линейная форма $U = x_1 + 2x_2 + 2x_3$ принимает все значения из промежутка $[0, 5]$, то есть $\lceil c_1 \rceil_U = \lfloor c_1 \rfloor_U + 1$. Аналогичные рассуждения дают $\lceil c_2 \rceil_V = \lfloor c_2 \rfloor_V + 3$. Тогда система (3) выглядит так:

$$\begin{aligned} \lfloor c_1 \rfloor_U + 6 &\leq 8, \\ \lfloor c_2 \rfloor_V + 5 &\leq 8 < \lfloor c_1 \rfloor_U + \lfloor c_2 \rfloor_V + 4. \end{aligned}$$

Отсюда получаем единственное решение $\lfloor c_1 \rfloor_U = 2$, $\lfloor c_2 \rfloor_V = 3$. Итак, f допускает разложение

$$f(x_1, x_2, x_3, x_4, x_5, x_6) = g(x_1, x_2, x_3)h(x_4, x_5, x_6) \vee h_2(x_4, x_5, x_6),$$

где g — б.п.ф. со структурой $(x_1 + 2x_2 + 2x_3, 2)$, h_1 — б.п.ф. со структурой $(3x_1 + 3x_2 + 3x_3, 3)$, h_2 — б.п.ф. со структурой $(3x_1 + 3x_2 + 3x_3, 8)$. Представляя каждую

функцию в виде многочлена Жегалкина, находим, что

$$f = (x_1x_2 \oplus x_1x_3 \oplus x_2x_3)(x_4x_5 \oplus x_4x_6 \oplus x_5x_6) \vee x_4x_5x_6.$$

3. Описание некоторых классов функционально разделимых пороговых функций

В силу отмеченных в предыдущем разделе сложностных проблем самостоятельный интерес приобретает задача описания множества булевых пороговых функций, одновременно либо функционально разделимых, либо функционально неразделимых. В этом случае исследование функциональной разделимости функций из таких множеств сводится к возможности выбора какого-либо представителя, допускающего эффективное применение теоремы 3. Ниже будут рассмотрены такие булевы пороговые функции, для которых удастся получить эффективно проверяемые необходимые и достаточные условия функциональной разделимости.

Введем следующее отношение порядка на множестве линейных форм. Если последовательность Q^* является подпоследовательностью R^* для линейных форм Q и R (возможно от разного числа переменных), то будем обозначать этот факт $Q \prec R$.

Предложение 1. *Имеют место следующие свойства:*

(а) *если*

$$L = a_1y_1 + \dots + a_ny_n, \quad d = \text{НОД}(\{a_i \mid i = 1, \dots, n\}), \quad m = \frac{1}{d} \sum_{i=1}^n a_i,$$

то

$$L \prec d \sum_{i=1}^m y_i;$$

(б) *если б.п.ф. со структурой (P, c) допускает декомпозицию вида (1) и*

$$P = P_1 \dot{+} P_2, \quad Q_1 \prec P_1, \quad Q_2 \prec P_2$$

для некоторых линейных форм Q_1, Q_2 , то б.п.ф. со структурой $(Q_1 \dot{+} Q_2, c)$ также допускает декомпозицию вида (1).

Доказательство. Для доказательства пункта (а) его достаточно доказать для $d = 1$. В этом случае множество значений линейной формы L принадлежит множеству значений линейной формы $y_1 + \dots + y_m$. Осталось убедиться, что

$$|\{w \in \{0, 1\}^n \mid L(w) = b\}| \leq \binom{m}{b}$$

для любых $b = 0, 1, \dots, m$. Для этого зададим инъективное соответствие между $\{0, 1\}^n$ и $\{0, 1\}^m$ следующим образом. Каждому $w \in \{0, 1\}^n$ такому, что $L(w) = b$, поставим в соответствие $v \in \{0, 1\}^m$ такой, что если $w_i = 1, i \in \{1, \dots, n\}$, то

$$v_{a_1+\dots+a_{i-1}+1} = \dots = v_{a_1+\dots+a_i} = 1.$$

Докажем пункт (b). Пусть k — число переменных линейной формы P_1 , а m — число переменных линейной формы Q_1 . Так как матрица $S_1^{(k)}$ для б.п.ф. со структурой (P, c) полностью определяется последовательностями $(P_1)^*$, $(P_2)^*$, и матрица $S_2^{(m)}$ для б.п.ф. со структурой $(Q_1 + Q_2, c)$ является подматрицей $S_1^{(k)}$, то $S_2^{(m)}$ имеет не большее число типов различных строк, чем $S_1^{(k)}$, что и требовалось доказать.

Предложение 1 позволяет указать способ построения классов функционально разделимых (или функционально неразделимых) пороговых функций, равно как и подход к анализу функциональной разделимости заданной пороговой функции. Пусть $\{U_i\}$ и $\{V_i\}$ — множества линейных форм от m_i и n_i переменных, $m_i, n_i > 1$, имеющие верхние грани U и V . Тогда по п.(б) предложения 1, если пороговая функция со структурой $(U + V, c)$ функционально разделима, то и любая пороговая функция со структурой $(U_i + V_j, c)$ также будет функционально разделимой. Аналогичным образом нетрудно получить двойственное утверждение для свойства функциональной неразделимости.

Замечание 1. Пусть T_n — группа переименований переменных (группа Джевонса), E_n — множество булевых функций, составляющих класс эквивалентности относительно T_n [13]. Тогда свойство функциональной разделимости является инвариантом множества E_n . Точнее, если для какой-нибудь функции из E_n существует декомпозиция вида $F(\Phi_1, \dots, \Phi_m)$, то и любая другая функция из E_n допускает декомпозицию вида $F(\Phi'_1, \dots, \Phi'_m)$, где Φ'_j зависит от такого же количества переменных, что и Φ_j , $j = 1, \dots, m$. Кроме того, множество пороговых функций замкнуто относительно преобразований переменных из T_n . Поэтому при изучении свойства функциональной разделимости пороговых функций достаточно описать простые нетривиальные декомпозиции функций с натуральнозначными структурами вида (1).

По замечанию 1 и пункту (а) предложения 1 в качестве верхней грани линейной формы, задающей произвольную булеву пороговую функцию, всегда можно выбрать линейную форму вида $d(y_1 + \dots + y_m)$. Ниже полностью решается задача анализа функциональной разделимости пороговых функций, задаваемых с помощью линейных форм такого вида. Кроме того, далее рассматриваются и другие достаточно представительные с точки зрения предложенного подхода классы булевых пороговых функций.

Замечание 2. Для любой линейной формы можно указать промежутки

$$\Delta_1 = [L_0^*, L_1^*), \quad \Delta_2 = [L_{2^n-2}^*, L_{2^n-1}^*)$$

такие, что структура (L, c) , $c \in \Delta_1$, определяет б.п.ф.

$$f = (x_1 \oplus \alpha_1) \vee \dots \vee (x_n \oplus \alpha_n),$$

а структура (L, c) , $c \in \Delta_2$, определяет б.п.ф.

$$f = (x_1 \oplus \beta_1) \dots (x_n \oplus \beta_n)$$

для некоторых α и β из $\{0, 1\}^n$. Более того, если $c < \inf \Delta_1$, то $f \equiv 1$, а если $c \geq \sup \Delta_2$, то $f \equiv 0$.

Значения порога, указанные в замечании 2, будем называть вырожденными.

Опишем все простые декомпозиции некоторых классов б.п.ф., допускающих вложение в смысле п.(b) предложения 1.

Предложение 2. Пусть $L = y_1 + \dots + y_n$. Тогда для невырожденных значений порога c пороговая функция со структурой (L, c) не имеет нетривиальных декомпозиций вида (1).

Доказательство. Достаточно доказать утверждение для простой декомпозиции вида (2) в случае, если $[c]_L = c$. Нетрудно показать, что при невырожденных значениях порога б.п.ф., определенная в условии, зависит существенно от переменных $x_1, \dots, x_n$. В зависимости от возможного значения порога c рассмотрим три случая:

$$(a) \quad c \geq \max(U_{\max}^*, V_{\max}^*);$$

$$(b) \quad U_{\max}^* \leq c < V_{\max}^*;$$

$$(c) \quad c < \min(U_{\max}^*, V_{\max}^*).$$

Тогда, учитывая, что в наших условиях

$$[c]_L = c, \quad U_{\max}^* = k, \quad V_{\max}^* = n - k,$$

и для конечных приближений $[c_\varepsilon]_Q = [c_\varepsilon]_Q + 1$, $\varepsilon = 1, 2$, $Q = U, V$, система (3) будет иметь следующие следствия: случай (a) дает вырожденное значение порога $c = n - 1$; в случае (b) получим $k = 1$, что соответствует возможному наличию только тривиальных декомпозиций; и, наконец, случай (c) дает вырожденное значение порога $c = 0$. Утверждение доказано.

Следствие 3. Если структура (Q, c) пороговой функции f такова, что

$$Q = Q_1 \dot{+} Q_2, \quad y_1 + \dots + y_{n_\varepsilon} < Q_\varepsilon$$

для некоторых $n_1, n_2 > 1$, $0 < c < n_1 + n_2 - 1$, то f не имеет нетривиальных декомпозиций вида (1).

Предложение 3. Пусть

$$L = y_1 + \dots + y_k + a(y_{k+1} + \dots + y_n), \quad a > 1, \quad a \in \mathbb{N}, \quad 1 < k < n.$$

Булева пороговая функция со структурой (L, c) , существенно зависящая от всех своих переменных, допускает простую декомпозицию вида (1) тогда и только тогда, когда выполняется любое из условий:

$$c \geq \max(k, a(n - k), a(n - k) + k - a), \quad (6)$$

при этом $f = g x_{k+1} \dots x_n$, где $g = g(x_1, \dots, x_k)$ — булева пороговая функция со структурой $(U, [c] - a(n - k))$;

$$\max(k, [c]_V + k - a) \leq c < a(n - k), \quad (7)$$

при этом $f = gh_1 \vee h_2$ — представление вида (2), где g, h_1, h_2 — булевы пороговые функции со структурами $(U, [c] - [c]_V), (V, [c]_V - a), (V, [c]_V)$ соответственно;

$$c < \min(a, k), \quad (8)$$

при этом $f = g \vee x_{k+1} \vee \dots \vee x_n$, где $g = g(x_1, \dots, x_n)$ — булева пороговая функция со структурой (U, c) .

Доказательство. Достаточно доказать предложение 3 для представления f вида (2). Для конечных нижних и верхних приближений порогов c_1, c_2 и c_3 функций g, h_1 и h_2 в представлении (2) выполняются соотношения

$$U_{2^k-1}^* = k, \quad V_{2^{n-k}-1}^* = a(n-k), \\ [c_1]_U = [c_1]_U + 1, \quad [c_2]_V = [c_2]_V + a, \quad [c_3]_V = [c]_V,$$

и $[c_2]_V, [c_3]_V, [c]_V$ делятся на a . Как и при доказательстве предложения 2, рассмотрим три случая для проверки совместности системы (3). В первом случае после равносильных преобразований системы (3) получаем, что

$$[c_2]_V = a(n-k-1), \\ [c_1]_U \geq k-a, \\ 0 \leq [c_1]_U \leq k-1, \\ \max([c_1]_U + a(n-k), [c_2]_V + k) \leq c < [c_1]_U + [c_2]_V + a + 1. \quad (9)$$

Так как $[c_1]_U \geq k-a$,

$$\max([c_1]_U + a(n-k), [c_2]_V + k) = [c_1]_U + a + (n-k).$$

Следовательно, $[c] = [c_1]_U + a(n-k)$. Тогда, выражая $[c_1]_U$ через c , систему (9) можно переписать в виде

$$\max(k, a(n-k), a(n-k) + k - a) \leq c \leq a(n-k) + k - 1.$$

С учетом существенной зависимости f от всех переменных это неравенство равносильно (6). При этом приближение $[c_2]_V = a(n-k-1)$ однозначно определяет б.п.ф. $h(y_1, \dots, y_{n-k}) = y_1 \dots y_{n-k}$.

Во втором случае заметим, что из условия существенной зависимости f от всех переменных следует, что $[c_2]_V < [c_3]_V$. Тогда, выписывая систему неравенств (3), после элементарных равносильных преобразований, получаем, что

$$[c_1]_U = [c] - [c]_V, \\ [c_2]_V = [c]_V - a, \\ [c_3]_V = [c]_V, \\ k \leq c < a(n-k) \\ [c]_V + k - a \leq c,$$

что равносильно (7). В третьем случае система неравенств (3) принимает вид

$$c < \min(k, a), \\ [c]_U + [c]_V \leq c. \quad (10)$$

Легко видеть, что для существования простой декомпозиции достаточно выполнения только первого неравенства в (10), что и составляет суть утверждения (8). При этом в представлении (2) $h_1 = 1$, а h_2 имеет вид $y_1 \vee \dots \vee y_{n-k}$. Предложение доказано.

Следствие 4. *Предложение 3 справедливо для любой пороговой функции со структурой (Q, c) такой, что*

$$Q = Q_1 \dot{+} Q_2, \quad Q_1 \prec y_1 + \dots + y_k, \quad Q_2 \prec a(y_1 + \dots + y_{n-k})$$

для некоторых k и n .

Заметим, что условия (6) и (8) относятся к б.п.ф., вес которых удовлетворяет соотношениям $\|f\| = \|g\| \leq 2^k$ и $\|f\| = 2^n - (2^k - \|g\|)$, соответственно.

Пример 2. Рассмотрим ту же функцию, что и в примере 1. Легко видеть, что $x_1 + 2x_2 + 2x_3 \prec x_1 + x_2 + x_3 + x_4 + x_5$. Проверим выполнение условий предложения 3 для б.п.ф. со структурой $(x_1 + x_2 + x_3 + x_4 + x_5 + 3x_6 + 3x_7 + 3x_8, 8)$. Для $k = 5$, $a = 3$, $n = 8$ выполняется (7). Тогда $[c_1]_U = 2$, $[c_2]_V = 3$, $[d]_V = 6$. Осталось заметить, что $(3x_1 + 3x_2 + 3x_3, 6)$ и $(3x_1 + 3x_2 + 3x_3, 8)$ — эквивалентные структуры.

4. О существенных переменных булевых пороговых функций

Так как при поиске нетривиальных декомпозиций б.п.ф. в первую очередь необходимо исключить несущественные переменные, выясним необходимые и достаточные условия существенной зависимости б.п.ф. от своих переменных. Как и в предыдущем разделе, в силу замечаний 1 и 2 будем рассматривать б.п.ф. с натуральнозначными структурами.

Обозначим через $L^{(i)}$ линейную форму от $n - 1$ переменной, получаемую из $L(y_1, \dots, y_n) = a_1y_1 + \dots + a_ny_n$ путем удаления члена с коэффициентом a_i .

Предложение 4. *Переменная x_i , $1 \leq i \leq n$, является существенной для б.п.ф. f со структурой (L, c) в том и только том случае, когда существует такой двоичный набор $w = (w_1, \dots, w_{n-1})$, что $c - a_i < L^{(i)}(w) \leq c$.*

Доказательство. По определению переменная x_i является несущественной для f тогда и только тогда, когда для любых наборов w' и w'' , отличающихся только по i -й координате, выполняется равенство $f(w') = f(w'')$. Последнее означает, что

$$L(w') \leq c,$$

$$L(w'') \leq c,$$

$$L(w') > c,$$

$$L(w'') > c.$$

Полагая $w_j = w'_j$, $j = 1, \dots, i - 1$, $w_j = w'_{j+1}$, $j = 1, \dots, n$, получаем, что $L^{(i)}(w) \leq c - a_i$ или $L^{(i)}(w) > c$, что и доказывает утверждение.

Следствие 5. Если $L^{(i)}$ достигает порога c , то x_i — существенная переменная, $1 \leq i \leq n$.

Список литературы

1. Дертоузос М. *Пороговая логика*. Мир, Москва, 1967.
2. Нильсон Н. *Обучающие машины*. Мир, Москва, 1967.
3. Дуда Р., Харт П. *Распознавание образов и анализ сцен*. Мир, Москва, 1976.
4. Wasserman P. D. *Neural Computation. Theory and Practice*. Van Nostrand Reinhold, New York, 1989.
5. Зуев Ю. А. Пороговые функции и пороговые представления булевых функций. *Матем. вопросы кибернетики* (1994) **5**, 5–61.
6. Бутаков Е. А. *Методы синтеза релейных устройств из пороговых элементов*. Энергия, Москва, 1970.
7. Ashenurst R. L. The decomposition of switching functions. *Ann. Comput. Laborat. Harv. Univ.* (1959) **29**, 74–116.
8. Shen V. Y., McKellar A. C., Weiner P. A fast algorithm for disjunctive decomposition of switching functions. *IEEE Trans. Comput.* (1971) **20**, 304–309.
9. Thase A. A fast algorithm for the proper decomposition of Boolean functions. *Philips Res. Reports* (1972) **27**, 140–150.
10. Схрейвер А. *Теория линейного и целочисленного программирования*. Мир, Москва, 1991.
11. Lenstra H. W. Integer programming with a fixed number of variables. *Math. Operations Research* (1983) **8**, 538–548.
12. Мошков М. Ю. О задаче минимизации линейной формы на конечном множестве. *Комбинаторно-алгебраические методы в прикладной математике*. Изд-во ГГУ, Горький, 1985.
13. Страздинь И. Э. *Таблицы типов булевых функций четырех переменных*. Депон. №1495–74, АН Латв. ССР, Рига, 1974.

Статья поступила 20.09.1994.

Переработанный вариант поступил 19.04.1996.