В то же время для $s \leqslant 2$ и слагаемых степени три и выше при ограничениях на число существенных переменных по модулю $\mathcal{U}_s$ уже можно показать однозначность для разложения, имеющего максимальное число слагаемых.

Теорема 1. Если при $s \geqslant 2$ функция $f = f(x_1, \ldots, x_n)$ имеет тривиальную группу инерции $(\mathbf{H}_n)_f^{(s-1)}$ и линейно разложима в бесповторную сумму по модулю $\mathcal{U}_s$, то для этой функции найдётся линейное разложение по модулю $\mathcal{U}_s$ в бесповторную сумму линейно неразложимых (в бесповторную сумму) слагаемых, однозначно определённое в том смысле, что любое другое такое разложение соответствует тому же самому разложению пространства в прямую сумму подпространств, а соответствующие функции линейно эквивалентны по модулю $\mathcal{U}_s$.

Метод доказательства аналогичен тому, который применён в работе [3]. В качестве следствия получаем описание группы инерции таких функций в полной аффинной группе.

Следствие 1. Если в условиях теоремы 1 функция f представлена в виде суммы линейно неразложимых в бесповторную сумму по модулю $\mathcal{U}_s$ функций

$$f \equiv f_1 \oplus \cdots \oplus f_m \pmod{\mathcal{U}_s},$$

причём множество функций $\{f_1, \ldots, f_m\}$ разбивается на t классов аффинной эквивалентности по модулю $\mathcal{U}_s$: $\{f_{\mu_1}, \ldots, f_{\mu_p}\} \subseteq \mathcal{F}_{n_1}$, $\ldots$, $\{f_{\nu_1}, \ldots, f_{\nu_q}\} \subseteq \mathcal{F}_{n_t}$, то для группы инерции бесповторной суммы этих функций справедлив изоморфизм

$$\mathbf{AGL}\,(n,2)^{(s)}_{f_1\oplus\cdots\oplus f_m} \cong [\mathbf{AGL}\,(n_1,2)^{(s)}_{f_{\mu_1}}]\mathbf{S}_p \times \cdots \times [\mathbf{AGL}\,(n_t,2)^{(s)}_{f_{\nu_1}}]\mathbf{S}_q.$$

Здесь через $G_f^{(s)}$ обозначена группа инерции функции f по модулю $\mathcal{U}_s$ в группе G, а $[G]\mathbf{S}_p$ — операция экспоненцирования группы G с помощью симметрической группы S_p степени p. Аналогичное описание справедливо для полной линейной группы $\mathbf{GL}\,(n,2)$.

ЛИТЕРАТУРА

1. *Черемушкин А. В.* Однозначность разложения двоичной функции в бесповторное произведение нелинейных неприводимых сомножителей // Вестник Московского государственного университета леса «Лесной вестник». 2004. № 4(35). С. 86–90.
2. *Черемушкин А. В.* Методы аффинной и линейной классификации двоичных функций // Труды по дискретной математике. М.: Физматлит, 2001. Т. 4. С. 273–314.
3. *Черемушкин А. В.* К вопросу о линейной декомпозиции двоичных функций // Прикладная дискретная математика. 2016. № 1(31). С. 46–56.

УДК 512.55 DOI 10.17223/2226308X/10/24

ОПИСАНИЕ НЕКОТОРЫХ ДЕКОМПОЗИЦИЙ ДЛЯ КВАДРАТИЧНЫХ БУЛЕВЫХ ПОРОГОВЫХ ФУНКЦИЙ

А. Н. Шурупов

Приводятся необходимые и достаточные условия функциональной разделимости квадратичных булевых пороговых функций, задаваемых распавшейся на два константных блока квадратичной формой.

Ключевые слова: *функциональная разделимость, квадратичные булевы пороговые функции.*

Полиномиальная булева пороговая функция $f(x_1,\ldots,x_n)$ определяется следующим образом [1]:

$$f(x_1,\ldots,x_n)=0 \Leftrightarrow g(x_1,\ldots,x_n)\leqslant 0, \tag{1}$$

где g — действительный полином. Если $\deg g=2$, то говорят о квадратичных булевых пороговых функциях (к.б.п.ф.). В последнем случае неравенство из (1) может быть преобразовано в эквивалентное $w(x_1,\ldots,x_n)\leqslant t$, где w — квадратичная форма; t — свободный член многочлена g, взятый с противоположным знаком и называемый порогом. Пару (w,t) часто называют структурой квадратичной пороговой функции f. Если для некоторых m из $\{1,\ldots,n-1\}$ и квадратичных форм u и v справедливо представление $w(x_1,\ldots,x_n)=u(x_1,\ldots,x_m)+v(x_{m+1},\ldots,x_n)$, то этот факт для краткости будем обозначать $w=u+v$.

Введём бинарное отношение $\sim$ на множестве целочисленных матриц одного размера. Будем полагать, что $A\sim B$, если

$$\forall i_1,i_2,j_1,j_2\ (a_{i_1,j_1}<a_{i_2,j_2}\Leftrightarrow b_{i_1,j_1}<b_{i_2,j_2}\ \ \&\ \ a_{i_1,j_1}=a_{i_2,j_2}\Leftrightarrow b_{i_1,j_1}=b_{i_2,j_2}).$$

Очевидно, что отношение $\sim$ является отношением эквивалентности, и множество всех матриц одного размера разбивается на классы эквивалентных матриц по введённому отношению.

Пример 1. Построим класс матриц, эквивалентных единичной матрице E_3: это любые целочисленные матрицы вида

$$\begin{pmatrix} a & b & b\\ b & a & b\\ b & b & a\end{pmatrix},$$

где $a>b$.

Пусть $A_w=\big\{\big\{w(x)\ :\ x\in\{0,1\}^n\big\}\big\}$ — мультимножество значений квадратичной формы $w(x)$. Через $\{A_w\}$ обозначим множество значений $w(x)$; $w^*=\big(w_0^*,w_1^*,\ldots,w_{2^n-1}^*\big)$ — упорядоченный по неубыванию набор элементов множества A_w. В [1] введены понятия нижнего $\lfloor a\rfloor_w$ и верхнего $\lceil a\rceil_w$ приближений действительного числа a в множестве значений $w(x)$:

$$\lfloor a\rfloor_w=\max\{z\in\{A_w\}:z\leqslant a\},\quad \lceil a\rceil_w=\min\{z\in\{A_w\}:z>a\}.$$

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

По аналогии с таблицей $S_f^{(m)}=\|s_{ij}\|$, $i=0,\ldots,2^m-1$, $j=0,\ldots,2^{n-m}-1$, введённой в [1] для к.п.б.ф. f со структурой $(u+v,t)$, элементы которой определяются следующим образом:

$$s_{ij}=0\Leftrightarrow u_i^*+v_j^*\leqslant t,\quad s_{ij}=1\Leftrightarrow u_i^*+v_j^*>t,$$

введём таблицу $Q_w^{(m)}=\|q_{ij}\|$, $i=0,\ldots,2^m-1$, $j=0,\ldots,2^{n-m}-1$, для распавшейся квадратичной формы $w=u+v$, элементы которой определяются следующим образом: $q_{ij}=u_i^*+v_j^*$. Для таблицы $Q_w^{(m)}$, как и для $S_f^{(m)}$, справедливо *свойство монотонности*: если $p\geqslant i$, $q\geqslant j$, то $q_{pq}\geqslant q_{ij}$.

Свойство функциональной разделимости [1, определение 1] булевых функций с данным отношением связывает

Утверждение 1. Пусть w, z — квадратичные формы от n переменных и к.б.п.ф. f со структурой (w,t) допускает простую декомпозицию с параметром m. Если $Q_w^{(m)} \sim Q_z^{(m)}$, то существует такое d, что к.б.п.ф. со структурой (z,d) также допускает простую декомпозицию с параметром m. (Как и в [1], для простоты полагаем, что перестановка переменных в простой декомпозиции для f тождественная.)

Доказательство. Достаточно заметить, что в качестве d можно взять элемент q_{ij}^z, такой, что $q_{ij}^w = \lfloor t \rfloor_w$. Тогда по свойству монотонности и из эквивалентности матриц $Q_w^{(m)}$ и $Q_z^{(m)}$ следует, что $S_f^{(m)} = S_g^{(m)}$, где g — к.б.п.ф. со структурой (z,d). Действительно, $s_{rs}^f = 1 \Leftrightarrow q_{rs}^w > t \geqslant \lfloor t \rfloor_w = q_{ij}^w \Leftrightarrow q_{rs}^z > q_{ij}^z = d \Leftrightarrow s_{rs}^g = 1$. ■

Следствие 1. К.п.б.ф. f со структурой (w,t) и g со структурой (z,d) из утверждения 1 эквивалентны относительно группы перестановок переменных.

Замечание 1. Пусть $w(x) = x_1^2 + \ldots + x_n^2$. Тогда к.п.б.ф. f со структурой (w,t) является функционально неразделимой для невырожденных значений порогов, так как f является линейной п.б.ф. со структурой (ℓ,t), где $\ell = x_1 + \ldots + x_n$, и, следовательно, функционально неразделимой для невырожденных значений порогов [2].

В некоторых случаях матрица $Q_w^{(m)}$ может быть разбита на группы смежных строк и столбцов так, что подматрицы, лежащие на пересечении строк из какой-либо группы строк и столбцов из какой-либо группы столбцов, состоят из одинаковых элементов a. Такие подматрицы будем называть блоками и обозначать через $[a]_{r\times s}$ или $a_{r\times s}$, где $r \times s$ — размер блока. В очевидных случаях указание на размер блока может опускаться. Например, для квадратичной формы $w(x) = x_1^2 + \ldots + x_n^2$ матрица $Q_w^{(m)}$ распадается на $m+1$ групп строк и $n-m+1$ групп столбцов и приобретает блочный вид

$$\begin{pmatrix} 0 & 1 & \ldots & n-m \\ 1 & 2 & \ldots & n-m+1 \\ \vdots & \vdots & \ddots & \vdots \\ m & m+1 & \ldots & n \end{pmatrix}, \tag{2}$$

где блок $[i+j]$ имеет размер $\binom{m}{i} \times \binom{n-m}{j}$. Блочную матрицу (2) будем обозначать $[Q_w^{(m)}]$.

Очевидным является

Утверждение 2. Если матрицы $Q_w^{(m)}$ и $Q_z^{(m)}$ для квадратичных форм w и z эквивалентны, т. е. $Q_w^{(m)} \sim Q_z^{(m)}$, то $[Q_w^{(m)}] \sim [Q_z^{(m)}]$.

Обратное, вообще говоря, неверно, однако в утверждении 1 можно перейти к более общей формулировке.

Утверждение 3. Пусть w, z — квадратичные формы от необязательно одного и того же числа переменных и к.б.п.ф. f со структурой (w,t) допускает простую декомпозицию с параметром m. Если для некоторого натурального r выполняется $[Q_w^{(m)}] \sim [Q_z^{(r)}]$, то существует такое число d, что к.б.п.ф. со структурой (z,d) также допускает простую декомпозицию с параметром m.

Утверждение 3 представляет собой переформулировку утверждения 1 из [3], которое основано на отношении частичного порядка на множестве квадратичных форм. Дальнейшее обобщение утверждения 3 может быть связано с рассмотрением полиномиальных пороговых функций, что показывает следующий пример.

Пример 2. Пусть $\ell(x) = x_1 + \ldots + x_n$ и $w(x) = (x_1 + \ldots + x_n)^k$. Тогда $[Q_\ell^{(m)}] \sim \sim [Q_w^{(m)}]$.

Следующая теорема даёт полное описание нетривиальных простых декомпозиций для к.б.п.ф. с распавшейся на два константных блока квадратичной формой. Доказательство проводится путём непосредственного применения критерия функциональной разделимости для квадратичных булевых пороговых функций [1, теорема 4].

Теорема 1. Пусть квадратичная форма e_m задана матрицей 1_m, квадратичная форма $w = e_m + ae_{n-m}$, $a \in \mathbb{N}$, — распавшаяся, к.б.п.ф. f, заданная структурой (w, t), существенно зависит от всех своих переменных. Тогда f допускает нетривиальную простую декомпозицию с параметром m тогда и только тогда, когда выполняется любое из условий:

1) $t < m^2$ и существует $j \in \{1, \ldots, n-m\}$, что $\lfloor t \rfloor_e + a(j-1)^2 \leqslant t < \lceil t \rceil_e$;
2) $t > m^2$ и существуют $i \in \{1, \ldots, m\}$, $j \in \{1, \ldots, n-m\}$, такие, что

$$\max\{(i-1)^2 + a(n-m)^2, m^2 + a(j-1)^2\} \leqslant t < i^2 + aj^2;$$

3) $t > m^2$ и существуют $i \in \{1, \ldots, m\}$, $j, l \in \{1, \ldots, n-m\}$, такие, что $j < l$ и

$$\max\{(i-1)^2 + a(l-1)^2, m^2 + a(j-1)^2\} \leqslant t < \min\{al^2, i^2 + aj^2\}.$$

ЛИТЕРАТУРА

1. *Шурупов А. Н.* Критерии функциональной разделимости квадратичных булевых пороговых функций // Прикладная дискретная математика. 2015. № 2(28). С. 37–45.
2. *Шурупов А. Н.* О функциональной разделимости булевых пороговых функций // Дискретная математика. 1997. Т. 9. Вып. 2. С. 59–73.
3. *Шурупов А. Н.* Некоторые структурные свойства квадратичных булевых пороговых функций // Прикладная дискретная математика. Приложение. 2015. № 8. С. 48–51.