УДК 512.55 DOI 10.17223/2226308X/12/58

О ПРОБЛЕМЕ РАСПОЗНАВАНИЯ АЛГЕБРАИЧЕСКИХ ПОРОГОВЫХ ФУНКЦИЙ

С. В. Женевский, С. Л. Мельников, А. Н. Шурупов

Доказано существование переборного алгоритма распознавания алгебраических булевых пороговых функций путём нахождения верхних оценок абсолютных значений модуля и коэффициентов линейной формы. Оценка для модуля имеет вид $(n+3)^{(n+5)/2}/2^{n+2}$, а сложность алгоритма — $\mathrm{O}((n/2)^{n^2})$.

Ключевые слова: *алгебраическая булева пороговая функция, проблема распознавания.*

Интерес к алгебраическим булевым пороговым функциям обуславливается простотой их задания, а также тем, что класс алгебраических пороговых функций содержит как собственно пороговые (или линейные пороговые) булевы функции, так и линейные булевы функции. Впервые понятие и свойства алгебраических пороговых функций (булевых и многозначных) введено в [1]. Несмотря на то, что понятие алгебраической булевой пороговой функции близко к понятию булевой пороговой функции, проблема распознавания для алгебраических булевых пороговых функций пока не имеет таких ясных способов решения, которые известны для булевых пороговых функций [2]. В работе доказано существование переборного алгоритма путём нахождения верхних оценок абсолютных значений модуля и коэффициентов линейной формы.

Будем использовать следующие обозначения: $\Omega_k = \{0, 1, \ldots, k-1\}$; $r_m(a)$ — функция взятия остатка при делении целого числа a на m; $F_k(n)$ — множество всех k-значных функций от n переменных; $T_k(n)$ — класс всех k-значных пороговых функций от n переменных; $AT_k(n)$ — класс всех k-значных алгебраических пороговых функций от n переменных; $L_k(n)$ — множество всех линейных функций k-значной логики от n переменных вида $c_0 + c_1x_1 + c_2x_2 + \ldots + c_nx_n \pmod k$.

Определение 1. Функцию $f : \Omega_2^n \longrightarrow \Omega_2$ назовем алгебраической булевой пороговой (а.б.п.ф.), если существуют $\omega = (\omega_0, \omega_1, \ldots, \omega_n) \in \mathbb{Z}^{n+1}$, $\theta \in \mathbb{Z}$, $m \in \mathbb{N} \setminus \{1\}$, такие, что

$$f(x_1, \ldots, x_n) = 0 \quad \Leftrightarrow \quad r_m(\omega_0 + \omega_1x_1 + \omega_2x_2 + \ldots + \omega_nx_n) < \theta,$$
$$f(x_1, \ldots, x_n) = 1 \quad \Leftrightarrow \quad r_m(\omega_0 + \omega_1x_1 + \omega_2x_2 + \ldots + \omega_nx_n) \geqslant \theta,$$

где вычисление линейной формы $\omega_0 + \omega_1x_1 + \omega_2x_2 + \ldots + \omega_nx_n$ происходит в кольце $\mathbb{Z}$, а операции сравнения производятся над полем действительных чисел $\mathbb{R}$.

Рассмотрим понятие *расшифровки* булевой функции из заданного класса $F' \subset F_k(n)$, допускающего некоторый специфичный способ задания [2]. Пусть функция $f \in F'$ задана оракулом, позволяющим по произвольной точке $x \in \Omega_2^n$ определить значение функции $f(x)$. Расшифровкой неизвестной нам функции $f \in F'$ называется процедура однозначного определения специфичного способа задания этой функции по её значениям $f(x^{(1)}), \ldots, f(x^{(t)})$ в точках $x^{(1)}, \ldots, x^{(t)}$.

В [3] вводится понятие *характеризации* пороговой функции. Под характеризацией пороговой функции понимается процедура нахождения вектора весов ω и вектора порогов θ, задающих функцию. Понятие характеризации распространяется на случай алгебраических пороговых функций (а.п.ф.) — в поиск добавляется модуль.

Более общим является понятие *распознавания* пороговой функции (алгебраической пороговой). Его можно встретить в [4] как *recognition*. Распознавание пороговой функции есть процедура определения принадлежности данной функции к классу пороговых и, при положительном ответе, нахождения вектора весов и вектора порогов. Аналогично это понятие распространяется на а.п.ф.

Легко показать, что для а.п.ф. (в частности, для а.б.п.ф.) структура является неоднозначным способом задания. Приведём доказательство существования у любой а.б.п.ф. $f \in AT_2(n)$ структуры, элементы которой ограничены по абсолютной величине константой, зависящей только от количества переменных n. Этот факт доказывает алгоритмическую разрешимость задачи характеризации а.б.п.ф.

Утверждение 1. Для любой а.б.п.ф. $f \neq \text{const}$ со структурой (ω, θ, m) верно, что $0 < \theta < m$ и всегда найдётся структура (ω', θ, m), такая, что $0 \leqslant \omega_i' < m$, $i = 0, \ldots, n$.

Доказательство. Пусть $f \neq \text{const}$. Заметим, что для любой структуры верно $0 \leqslant r_m(\omega_0 + \omega_1 x_1 + \ldots + \omega_n x_n) < m$. Если $\theta \geqslant m$, то $f \equiv 0$, так как для всех $x \in \Omega_2^n$ верно $r_m(\omega_0 + \omega_1 x_1 + \ldots + \omega_n x_n) < \theta$. Аналогично, при $\theta \leqslant 0$ может быть задана только функция $f \equiv 1$. Таким образом, имеем $0 < \theta < m$. Рассмотрим произвольную функцию $f \in AT_2(n)$. Из свойств колец вычетов следует, что

$$r_m(\omega_0 + \omega_1 x_1 + \ldots + \omega_n x_n) = r_m(r_m(\omega_0) + r_m(\omega_1)x_1 + \ldots + r_m(\omega_n)x_n).$$

То есть вектор весов $\omega' = (r_m(\omega_0), r_m(\omega_1), \ldots, r_m(\omega_n))$, порог θ и модуль m образуют структуру функции f. ■

Далее будем рассматривать функции из множества $AT_2(n) \setminus \{\mathbf{0}, \mathbf{1}\}$ и соответствующие им структуры с весами из множества $\mathbb{Z}_m^{n+1}$ и порогами из множества $(0, m) \subset \mathbb{R}$. Заметим, что для таких функций множества $T(f)$ и $F(f)$ непусты. Из утверждения 1 следует, что для алгоритмической разрешимости задачи распознавания а.б.п.ф. достаточно доказать существование структуры с модулем, не превосходящим некоторую константу, зависящую только от числа переменных n. Обозначим $\dot{x} = (1, x)$. Тогда линейная комбинация $\omega_0 + \omega_1 x_1 + \omega_2 x_2 + \ldots + \omega_n x_n$ может быть записана как скалярное произведение $(\omega, \dot{x})$ векторов $\dot{x}$ и ω.

Для любой функции f из класса $AT_2(n) \setminus \{\mathbf{0}, \mathbf{1}\}$ справедливо следующее: существует набор $\{t_x\}_{x \in \Omega_2^n}$ целых чисел, таких, что выполняется система линейных неравенств (СЛН)

$$\begin{cases} m > (\omega, \dot{x}) + m t_x \geqslant \theta, \ x \in T(f), \\ 0 \leqslant (\omega, \dot{x}) + m t_x < \theta, \ x \in F(f). \end{cases} \tag{1}$$

Утверждение 2. Для всех $x \in \Omega_2^n$ верно $-n - 1 < t_x \leqslant 0$.

Доказательство. Неравенство $t_x \leqslant 0$ следует из первого неравенства в (1) и того, что $\omega_i \geqslant 0$. Докажем неравенство $-n < t_x$. Предположим противное. Пусть $\exists x' \in \Omega_2^n \, (t_{x'} \leqslant -n - 1)$. Заметим, что $\forall \omega \in \mathbb{Z}_m^{n+1} \ \forall x \in \Omega_2^n \ (0 \leqslant (\omega, \dot{x}) < m(n+1))$, так как $0 \leqslant \omega_i < m$ и $0 \leqslant x_i \leqslant 1$. Тогда $(\omega, \dot{x}') + m t_{x'} \leqslant (\omega, \dot{x}') - m(n+1) < 0$. Противоречие.

Следующая система равносильна системе (1) — двойные неравенства представляются двумя одинарными:

$$\begin{cases} -(\omega, \dot{x}) - m(t_x - 1) > 0, \ x \in T(f), \\ (\omega, \dot{x}) + m t_x - \theta \geqslant 0, \ x \in T(f), \\ -(\omega, \dot{x}) - m t_x + \theta > 0, \ x \in F(f), \\ (\omega, \dot{x}) + m t_x \geqslant 0, \ x \in F(f). \end{cases} \tag{2}$$

Положим $\omega' = (\omega, -\theta, m)$, а также определим две функции $t(x)$ и $q(x)$ из Ω_2^{n+1} в $\mathbb{Z}^{n+3}$ следующим образом:

$$t(x) = \begin{cases} (\dot{x}, 1, t_x), \ x \in T(f), \\ (-\dot{x}, -1, -t_x), \ x \in F(f), \end{cases} \qquad q(x) = \begin{cases} (-\dot{x}, 0, 1 - t_x), \ x \in T(f), \\ (\dot{x}, 0, t_x), \ x \in F(f). \end{cases}$$

Эти функции являются инъективными. Перепишем систему (2), используя обозначения $\omega', x' = t(x), x'' = q(x)$, и получим эквивалентную ей систему из 2^{n+1} неравенств:

$$\begin{cases} (x'', \omega') > 0, \ x \in T(f), \\ (x', \omega') \geqslant 0, \ x \in T(f), \\ (x', \omega') > 0, \ x \in F(f), \\ (x'', \omega') \geqslant 0, \ x \in F(f). \end{cases} \tag{3}$$

Тогда для СЛН

$$\begin{cases} (x'', \omega') \geqslant 1, \ x \in T(f), \\ (x', \omega') \geqslant 0, \ x \in T(f), \\ (x', \omega') \geqslant 1, \ x \in F(f), \\ (x'', \omega') \geqslant 0, \ x \in F(f) \end{cases} \tag{4}$$

система (3) является следствием. ■

Лемма 1. Если система (1) совместна относительно неизвестных (ω, θ, m), то система (4) совместна относительно ω'.

Доказательство. Пусть $(\tilde{\omega}, \tilde{\theta}, \tilde{m})$ — решение системы (1). Это решение является также решением системы (2). Значит, выполняется система

$$\begin{cases} -(\tilde{\omega}, \dot{x}) - \tilde{m}(t_x - 1) = a_x, \ x \in T(f), \\ (\tilde{\omega}, \dot{x}) + \tilde{m}t_x - \tilde{\theta} = b_x, \ x \in T(f), \\ -(\tilde{\omega}, \dot{x}) - \tilde{m}t_x + \tilde{\theta} = a_x, \ x \in F(f), \\ (\tilde{\omega}, \dot{x}) + \tilde{m}t_x = b_x, \ x \in F(f), \end{cases}$$

где $a_x > 0$, $b_x \geqslant 0$. Пусть $a' = \min\limits_{x \in \Omega_2^n} a_x$. Рассмотрим тройку $(\hat{\omega}, \hat{\theta}, \hat{m}) = \dfrac{1}{a'}(\tilde{\omega}, \tilde{\theta}, \tilde{m})$. Очевидно, что она является решением системы (2). Кроме того, $(\hat{\omega}, \hat{\theta}, \hat{m})$ — решение системы

$$\begin{cases} -(\omega, \dot{x}) - m(t_x - 1) \geqslant 1, \ x \in T(f), \\ (\omega, \dot{x}) + mt_x - \theta \geqslant 0, \ x \in T(f), \\ -(\omega, \dot{x}) - mt_x + \theta \geqslant 1, \ x \in F(f), \\ (\omega, \dot{x}) + mt_x \geqslant 0, \ x \in F(f). \end{cases} \tag{5}$$

Системы (5) и (4) совпадают. ■

Лемма 2. Пусть A — матрица размера $n \times n$ с элементами $a_{ij} \in \{0, 1\}$. Тогда $|\det(A)| \leqslant (n+1)^{(n+1)/2}/2^n$.

Доказательство. Рассмотрим матрицу $\widehat{A} = \begin{pmatrix} 1 & (-\mathbf{1})^T \\ \mathbf{1} & 2A - J \end{pmatrix}_{(n+1)\times(n+1)}$, где J — матрица, полностью состоящая из единиц. Прибавив первый столбец этой матрицы ко всем остальным, получим

$$\det(\widehat{A}) = 2^n \det(A). \tag{6}$$

Из неравенства Адамара известно, что $\det(\widehat{A})^2 \leqslant \prod\limits_{i=1}^{n+1}(\sum\limits_{j=1}^{n+1}\widehat{a}_{ij}^2) \leqslant (n+1)^{n+1}$. Подставив (6) в неравенство Адамара, получим требуемое. ■

Теорема 1. Для любой а.б.п.ф. $f \in AT_2(n)$ существует структура с таким модулем m, что верно неравенство

$$m \leqslant \frac{(n+3)^{(n+5)/2}}{2^{n+2}}.$$

Доказательство. Используем идеи из [5]. Пусть $f \in AT_2(n)\setminus\{\mathbf{0},\mathbf{1}\}$. Тогда система (1) совместна. Значит, по лемме 1 совместна и система (4). Рассмотрим множество решений системы (4) в пространстве $\mathbb{R}^{n+3}$. Это замкнутое множество, граничные точки которого обращают $n+3$ неравенства из СЛН (2) в равенства. Пусть $\omega^{'}$ — такая точка. Тогда имеем СЛУ $M\omega^{'} = b^{\downarrow}$, где M — матрица размера $(n+3)\times(n+3)$ вида

$$\begin{pmatrix}
-x^{(1)} & 0 & 1-t_1 \\
\vdots & \vdots & \vdots \\
-x^{(l_1)} & 0 & 1-t_{l_1} \\
x^{(l_1+1)} & 1 & t_{l_1+1} \\
\vdots & \vdots & \vdots \\
x^{(l_2)} & 1 & t_{l_2} \\
-x^{(l_2+1)} & -1 & -t_{l_2+1} \\
\vdots & \vdots & \vdots \\
-x^{(l_3)} & -1 & -t_{l_3} \\
x^{(l_3+1)} & 0 & t_{l_3+1} \\
\vdots & \vdots & \vdots \\
x^{(n+2)} & 0 & t_{n+2}
\end{pmatrix},$$

а вектор $b^{\downarrow}$ лежит в Ω_2^{n+3}. По правилу Крамера имеем $\omega_{n+3}^{'} = \det(M_{n+3})/\det(M)$, где M_{n+3} — матрица, полученная из матрицы M заменой $(n+3)$-го столбца на столбец $b^{\downarrow}$. Разложим определитель матрицы M_{n+3} по $(n+3)$-му столбцу:

$$\det(M_{n+3}) = \sum_{j=1}^{n+3}(-1)^{n+3+j}\, b_j\, \det(M_{n+3\,j}).$$

Здесь матрица $M_{n+3\,j}$ — подматрица M_{n+3}, полученная удалением j-й строки и $(n+3)$-го столбца, b_j — j-й элемент вектора $b^{\downarrow}$. Заметим, что при умножении вектора $\omega^{'}$ на любое $\alpha \geqslant 1$ мы получим решение системы (2). Тогда домножением вектора $\omega^{'}$ на $|\det(M)|$ получим целое решение СЛН (2):

$$\omega_{n+3}^{''} = \operatorname{sign}(\det(M)) \sum_{j=1}^{n+3}(-1)^{n+3+j}\, b_j\, \det(M_{n+3\,j}).$$

Оценим элемент $\omega_{n+3}^{''}$. Из леммы (2) известно, что определитель матрицы размера $n\times n$, состоящей из 0 и 1, не превосходит $(n+1)^{(n+1)/2}/2^n$. В нашем случае матрица $M_{n+3\,j}$

состоит из элементов $0, 1, -1$, но любая её строка не может содержать 1 и -1 одновременно. Значит, $\det(M_{n+3\,j}) = (-1)^q |\det(M_{n+3\,j})|$, где q — количество неположительных строк матрицы $M_{n+3\,j}$. Для матриц M_{ij} верно аналогичное. Итак, имеем

$$|\omega''_{n+3}| \leqslant \sum_{j=1}^{n+3} |b_j \det(M_{n+3\,j})| = \sum_{j=1}^{n+3} |\det(M_{n+3\,j})| \leqslant \frac{(n+3)^{(n+5)/2}}{2^{n+2}}.$$

Теорема доказана. ■

Теорема 1 позволяет сформулировать переборный алгоритм 1 распознавания а.б.п.ф. Можно ограничиться рассмотрением случая, когда веса и порог меньше модуля. На каждом шаге алгоритма фиксируется параметр m и перебираются значения остальных параметров от 0 до $m-1$.

Алгоритм 1. Распознавание алгебраических булевых пороговых функций

Вход: функция $f \in F_2(n)$, заданная оракулом.

Выход: структура функции в случае, если $f \in AT_2(n)$, либо ответ, что функция не принадлежит классу $AT_2(n)$.

1: $m := 2$.

2: Для всех векторов $(\omega, \theta) \in \mathbb{Z}_m^{n+2}$ проверяем выполнимость системы неравенств (1). Если какой-либо вектор (ω_1, θ_1) привёл к тому, что все неравенства оказались верными, то функция f является алгебраической пороговой, а тройка (ω_1, θ_1, m) — её структурой.

3: Если $m < (n+3)^{(n+5)/2}/2^{n+2}$, то $m := m+1$ и перейти на шаг 2, иначе функция не является а.б.п.ф. Выход.

Утверждение 3. Оценка сложности алгоритма распознавания а.б.п.ф. имеет вид $\mathrm{O}((n/2)^{n^2})$.

Доказательство. Параметр m, согласно теореме 1, перебирается от 2 до $(n+3)^{(n+5)/2}/2^{n+2}$. Вектор весов и порог перебираются от 0 до $m-1$. Значит, сложность алгоритма оценивается величиной

$$\sum_{m=2}^{(n+3)^{(n+5)/2}/2^{n+2}} m^{n+2} = \frac{(n+3)^{(n^2+7n+10)/2}}{2^{n^2+4n+4}} = \mathrm{O}\left((n/2)^{n^2}\right).$$

Утверждение доказано. ■

ЛИТЕРАТУРА

1. *Сошин Д. А.* Конструктивный метод синтеза сбалансированных k-значных алгебраических пороговых функций // Computational Nanotechnology. 2015. No. 4. P. 31–36.
2. *Золотых Н. Ю.* Расшифровка пороговых и близких к ним пороговых функций многозначной логики: дис. ... канд. физ.-мат. наук. Нижегородский госуниверситет. Н. Новгород, 1998.
3. *Бурделев А. В., Никонов В. Г.* О построении аналитического задания k-значной пороговой функции // Computational Nanotechnology. 2015. No. 2. P. 5–13.
4. *Crama Y. and Hammer P. L.* Boolean Functions: Theory, Algorithms and Applications. Encyclopedia of Mathematics and its Applications. Cambridge: Cambridge University Press, 2011.

5. *Antony M.* Discrete Mathematics of Neural Networks: Selected Topics. SIAM, Philadelphia, 2001.

УДК 621.391:519.7 DOI 10.17223/2226308X/12/59

MDS-МАТРИЦЫ, ПОСТРОЕННЫЕ С ПОМОЩЬЮ СОПРОВОЖДАЮЩИХ МАТРИЦ МНОГОЧЛЕНОВ И ПОДСТАНОВОЧНЫХ МАТРИЦ

О. Кой Пуэнте

Предлагается новый метод построения MDS-матриц порядка $k = 4, 6$ над полем GF(256), основанный на возведении в степень сопровождающих матриц некоторых многочленов и последующим сложением с подстановочной матрицей. Оценивается число операций сложения по модулю 2, необходимых для вычисления образов векторов при действии соответствующих линейных преобразований. Построенные матрицы представляют интерес для использования в шифрсистемах, ориентированных на низкоресурсную реализацию.

Ключевые слова: *MDS-матрицы, сопровождающие матрицы многочленов, подстановочные матрицы, конечные поля, низкоресурсная криптография, XOR-сложность.*

Введение

Пусть $Q = \mathrm{GF}(2^n) = \mathrm{GF}(2)[x]/g(x)$ — конечное поле из 2^n элементов, где $g(x)$ — неприводимый многочлен степени n над полем GF(2). Множество всех вектор-строк длины k над полем Q обозначим через Q^k, а множество всех матриц размера $k \times k$ над полем Q — через $Q_{k,k}$.

Определение 1 [1]. Показатель рассеивания ρ матрицы $A \in Q_{k,k}$ определяется равенством

$$\rho(A) = \min_{\mathbf{a} \neq \mathbf{0}} \{\mathrm{w}(\mathbf{a}) + \mathrm{w}(\mathbf{a}A)\},$$

где $\mathrm{w}(\mathbf{a})$ — вес Хэмминга вектора $\mathbf{a} \in Q^k$, то есть количество его ненулевых элементов.

Определение 2 [1, 2]. Матрица $A \in Q_{k,k}$ называется MDS-матрицей, если $\rho(A) = k + 1$.

Определение 3 [2]. Пусть $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{k-1} x^{k-1} + x^k \in Q[x]$. Матрица $S_f \in Q_{k,k}$, определённая равенством

$$S_f = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ a_0 & a_1 & a_2 & \cdots & a_{k-1} \end{pmatrix},$$

называется сопровождающей матрицей многочлена $f(x)$.

В [3] предложено оценивать сложность реализации линейного слоя в блочных шифрсистемах подсчётом количества вентилей XOR, необходимых для реализации