УДК 512.54

Невырожденная нормальная форма булевых функций

О.А. Логачев, А.А. Сальников, В.В. Ященко [1]

Проблема аффинной классификации булевых функций впервые была поставлена в конце XIX века. Наиболее известные результаты в этой области — «Гарвардский каталог» типов булевых функций четырех переменных (50-ые годы XX века) и таблица аффинных классов булевых функций пяти переменных (И. Э. Страдзинь, 1975 год). С историей проблемы, полученными результатами и их связями с другими комбинаторно-алгебраическими задачами можно познакомиться в докторской диссертации И. Э. Страдзиня [1].

Булеву функцию $f(x) = f(x_1, \ldots, x_n)$ будем считать заданной на V_n — векторном пространстве размерности n над полем $F_2 = \{0, 1\}$ из двух элементов. Задавать функцию f можно или вектором длины 2^n из нулей и единиц — так называемой таблицей истинности, или многочленом Жегалкина. В последнем случае степень многочлена называется степенью нелинейности булевой функции и обозначается $\deg f$. В теории кодирования с помощью всех булевых функций, удовлетворяющих условию $\deg f \leqslant r$, строятся коды Рида-Маллера $\mathrm{RM}(r, n)$. Булевы функции, в многочлен Жегалкина которых входят только члены одинаковой степени, называют однородными формами. На V_n действует $\mathrm{GA}(n)$ — полная аффинная группа преобразований, состоящая из аффинных преобразований:

$$x \mapsto Ax \oplus b,$$

где A — двоичная обратимая матрица размера $n \times n$, а b — произвольный вектор из V_n. Это действие естественным образом переносится на булевы функции, при этом все множество булевых функций разбивается на орбиты, которые называются аффинными классами; параметры булевых функций, постоянные на аффинных классах, называются аффинными инвариантами. Простейшими аффинными инвариантами являются вес булевой функции (число единиц в ее таблице истинности) и степень нелинейности $\deg f$ булевой функции.

Производной булевой функции $f(x)$ по направлению $\sigma \in V_n$ называют

[1]Работа поддержана Российским фондом фундаментальных исследований (номера проектов 99-01-00929 и 99-01-00941)

булеву функцию $\frac{d\,f}{d\,\sigma}$, определенную равенством

$$\frac{d\,f}{d\,\sigma}\,(x) = f\,(x \oplus \sigma) \oplus f\,(x)\,,$$

здесь $\oplus$ — знак покоординатного суммирования по модулю 2 векторов одинаковой длины. При взятии производной размерность «множества существенных направлений» булевой функции и ее степень нелинейности уменьшаются по крайней мере на единицу (т.к. $\frac{d\,f}{d\,\sigma}(x) = \frac{d\,f}{d\,\sigma}(x \oplus \sigma)$ и старшие однородные формы функций $f(x \oplus \sigma)$ и $f(x)$ равны). Если известны все 2^n производных функции f, то функция восстанавливается с точностью до константы с помощью следующего равенства:

$$f(\sigma) = \frac{d\,f}{d\,\sigma}(0) \oplus f(0).$$

Степень нелинейности функции f равна r тогда и только тогда, когда степень нелинейности всех ее производных не превышает $r-1$ и существует направление, по которому производная имеет степень нелинейности $r-1$. Указанные и другие свойства производной оказались полезными при решении некоторых задач теории кодирования и криптографии ([2, 3, 4, 6]).

Группу r-нелинейности L_f^r функции f для $r \leqslant \deg f - 1$ определим равенством

$$L_f^r = \left\{\sigma \in V_n :\ \deg \frac{d\,f}{d\,\sigma} \leqslant r\right\}.$$

Все L_f^r для любой фиксированной функции f являются линейными подпространствами V_n, причем

$$L_f^0 \leqslant L_f^1 \leqslant \ldots \leqslant L_f^{\deg f - 1} = V_n.$$

Очевидно, что $L_f^{r-1} = V_n$ тогда и только тогда, когда $\deg f \leqslant r$. Раньше изучалось только подпространство L_f^0 (оно называлось группой линейности функции f) и его подпространство $L_f^- = \{\sigma \in V_n :\ f(x \oplus \sigma) = f(x)\}$, которое называлось группой инерции функции f в группе сдвигов, а направления $\sigma \in L_f^-$ назывались несущественными.

Невырожденной назовем булеву функцию f, для которой $L_f^{\deg f - 2} = \{0\}$. Другими словами, невырожденными называются такие булевы функции, для которых взятие производной по любому ненулевому направлению уменьшает степень нелинейности ровно на единицу. Обоснованность использования в этом случае термина «невырожденная» будет понятна из дальнейших результатов.

Свойство невырожденности булевой функции можно выразить в терминах линейной алгебры, что существенно облегчает изучение невырожденных булевых функций. Если $\deg f = r$, то через $[f]_r$ обозначим однородную форму степени r функции f, а через $\left[\frac{d\,f}{d\,\sigma}\right]_{r-1}$ — однородную форму степени

$r-1$ функции $\frac{d\,f}{d\,\sigma}$. Известно, что

$$\begin{aligned}\frac{d\,f}{d\,(\sigma\oplus\omega)}(x) &= \frac{d\,f}{d\,\sigma}(x)\oplus\frac{d\,f}{d\,\omega}(x\oplus\sigma) = \\ &= \frac{d\,f}{d\,\sigma}(x)\oplus\frac{d\,f}{d\,\omega}(x)\oplus\frac{d^2\,f}{d\,\sigma\,d\,\omega}(x),\end{aligned} \tag{1}$$

откуда

$$\left[\frac{d\,f}{d\,(\sigma\oplus\omega)}\right]_{r-1}(x) = \left[\frac{d\,f}{d\,\sigma}\right]_{r-1}(x)\oplus\left[\frac{d\,f}{d\,\omega}\right]_{r-1}(x).$$

Из последнего равенства следует

Теорема 1. *Отображение*

$$D:(f,\sigma)\longrightarrow\left[\frac{d\,f}{d\,\sigma}\right]_{r-1}$$

для $\sigma\in V_n$ *и* $\deg f=r$ *является билинейным.*

Невырожденность булевых функций связана с отображением D следующим образом: подпространство $L_f^{\deg f-2}$ — это в точности ядро линейного отображения D при фиксированном f:

$$L_f^{\deg f-2}=\left\{\sigma\in V_n:\ \left[\frac{d\,f}{d\,\sigma}\right]_{r-1}=D(f,\sigma)=0\right\}.$$

Невырожденными являются те и только те булевы функции f, для которых $D(f,\sigma)\neq 0$ при всех ненулевых $\sigma\in V_n$, т.е. линейное отображение D при фиксированной f является невырожденным. Полезно отметить следующее легко проверяемое свойство отображения D.

Лемма 1.

$$D(f\oplus\varphi,\sigma)=D(f,\sigma)$$

для любой функции φ *при условии* $\deg\varphi\leqslant\deg f-1$ *и любого направления* $\sigma\in V_n$.

Из леммы 1, в частности, следует, что вместе с функцией f невырожденной является любая функция $f\oplus\varphi$, если $\deg\varphi\leqslant\deg f-1$. Таким образом, невырожденность булевой функции — это свойство, которое определяется только старшей однородной формой функции. Более того, легко видеть, что если $\deg f=r$, то

$$L_f^{r-2}=L_{[f]_r}^{r-2}.$$

С помощью элементарных рассуждений легко проверить, что

$$\frac{d\,[f]_r}{d\,\mathbf{e}_i}(x)=\sum_{\substack{\beta\in V_n\\|\beta|=r-1}}d_\beta^{(i)}x^\beta,$$

где $\mathbf{e}_i = (0,\dots,0,\underset{i}{1},0,\dots,0)$; $x^\beta = x_{j_1}\dots x_{j_{r-1}}$, если в векторе β единицы стоят на местах $j_1,\dots,j_{r-1}$, т.е. $\beta = (0,\dots,0,\underset{j_1}{1},0,\dots,0,\underset{j_{r-1}}{1},0,\dots,0)$;

$$d_\beta^{(i)} = \begin{cases} 0, & \text{если } \beta \geqslant \mathbf{e}_i \text{ (т.е. в векторе } \beta \\ & \text{на } i\text{-ом месте стоит единица);} \\ c_{\beta\oplus\mathbf{e}_i}, & \text{в противном случае,} \end{cases}$$

$f(x) = \sum_{\alpha\in V_n} c_\alpha x^\alpha$.

Из введенных обозначений очевидно, что при фиксированной функции f образ V_n при отображении D совпадает с линейной оболочкой, натянутой на n однородных форм степени $r-1$, заданных векторами $d_\beta^{(1)},\dots,d_\beta^{(n)}$. Из известного результата линейной алгебры о связи размерностей ядра и образа линейного отображения следует

Теорема 2.

$$\dim L_f^{r-2} = n - \operatorname{rang}\left(d_\beta^{(1)},\dots,d_\beta^{(n)}\right).$$

Для однородных форм выполняется следующее важное свойство.

Лемма 2. *Пусть $\psi(x_1,\dots,x_n)$ — однородная форма степени r. Тогда либо x_i несущественная переменная, либо*

$$\deg\frac{d\,\psi}{d\,\mathbf{e}_i} = r-1.$$

Невырожденную однородную форму степени r от n переменных будем называть для краткости невырожденной (n,r)-формой или, если параметры n и r не нужны, невырожденной формой. С помощью теоремы 2 можно из каждой булевой функции выделить невырожденную форму:

Теорема 3. *Пусть $\deg f = r$, $\dim L_f^{r-2} = n-k$, $V_n = U\dot{+}W$, $L_f^{r-2} = U$. Тогда $k \geqslant r$ и при любом выборе базисов в U и W функция $f(u,w)$ может быть представлена в виде*

$$f(u,w) = \varphi(u,w)\oplus\psi(w),$$

где $\psi(w)$ — невырожденная (k,r)-форма, $\deg\varphi \leqslant r-1$, причем $L_f^m = L_\varphi^m$ для всех $m \leqslant r-2$.

Будем говорить, что две булевых функции одинаковой степени нелинейности RM-эквивалентны [5], если они могут быть получены одна из другой с помощью аффинной замены переменных и прибавления функции степени нелинейности, не превышающей $\deg f - 1$. Из теоремы 3 очевидным образом вытекает

Следствие 1. *Любая булева функция RM-эквивалентна некоторой невырожденной форме.*

Сделаем при необходимости аффинную замену переменных и исключим несущественные для f направления, т.е. в дальнейшем будем считать, что $L_f^- = \{0\}$. Рассмотрим теперь для данной функции f все ее группы r-нелинейности и выберем из них все различные, т.е. найдем цепочку различных подпространств

$$L_f^{r_1} < L_f^{r_2} < \ldots < L_f^{r_s}, \quad L_f^{r_s+1} = V_n$$

так, что

$$L_f^{r_i} = L_f^{r_i+1} = \ldots = L_f^{r_{i+1}-1},\ L_f^{r_{i+1}-1} \neq L_f^{r_{i+1}}.$$

Положим $n - k_i = \dim L_f^{r_i}$, тогда $k_1 > k_2 > \ldots > k_s$, $r_1 < r_2 < \ldots < r_s$, $k_s \geqslant r_s + 2$. Очевидно, что так определенный набор чисел (k_1, r_1), $(k_2, r_2), \ldots, (k_s, r_s)$ является аффинным инвариантом булевой функции. Назовем этот инвариант структурой вырождения булевой функции.

Выясним, к какому виду можно привести булеву функцию с помощью аффинных замен переменных, если известна ее структура вырождения. Заметим вначале, что к функции f можно добавлять любую функцию степени нелинейности не превышающей r_1, при этом структура вырождения f не изменится.Поэтому в дальнейшем, не ограничивая общности, будем считать, что в многочлене Жегалкина функции f нет членов степени нелинейности не превышающей r_1 и, кроме того, $L_f^- = \{0\}$.

Сделав некоторую аффинную замену переменных, можно считать, что

$$L_f^{r_i} = \{(x_1, \ldots, x_{n-k_i}, 0, \ldots, 0), \quad \forall x_j \in F_2\}.$$

Теперь можно несколько раз применить теорему 3 к функциям уменьшающихся степеней нелинейности $r_s + 2$, $r_{s-1} + 2, \ldots, r_1 + 2$ и в результате получить следующее утверждение.

Теорема 4. *Пусть $(k_1, r_1), \ldots, (k_s, r_s)$ — структура вырождения булевой функции f, причем*

$$\begin{aligned} V_n &= U_1 \dot{+} U_2 \dot{+} \ldots \dot{+} U_s \dot{+} W, \\ L_f^{r_i} &= U_1 \dot{+} U_2 \dot{+} \ldots \dot{+} U_i, \\ \deg f &= r_s + 2. \end{aligned}$$

Тогда при любом выборе базисов в U_i, W функция $f(u_1, u_2, \ldots, u_s, w)$ может быть представлена в виде

$$\begin{aligned} f(u_1, u_2, \ldots, u_s, w) = \varphi(u_1, u_2, \ldots, u_s, w) \oplus \psi_1(u_2, \ldots, u_s, w) \oplus \\ \psi_2(u_3, \ldots, u_s, w) \oplus \ldots \oplus \psi_{s-1}(u_s, w) \oplus \psi_s(w), \end{aligned}$$

где $\psi_i(u_{i+1}, \ldots, u_s, w)$ — невырожденная $(k_i, r_i + 2)$-форма, $\varphi(u_1, u_2, \ldots, u_s, w)$ — невырожденная $(n, r_1 + 1)$-форма.

Очевидно также и обратное утверждение.

Теорема 5. *Пусть* $V_n = U_1 \dot{+} U_2 \dot{+} \ldots \dot{+} U_s \dot{+} W$, $\dim U_1 \dot{+} U_2 \dot{+} \ldots \dot{+} U_i = n - k_i$, $i = 1, \ldots, s$, $k_1 > k_2 > \ldots > k_s$, $r_1 < r_2 < \ldots < r_s$, $k_s \geqslant r_s + 2$, $\psi_i(u_{i+1}, \ldots, u_s, w)$ — *невырожденные* $(k_i, r_i + 2)$-*формы*, $\varphi(u_1, u_2, \ldots, u_s, w)$ — *невырожденная* $(n, r_1 + 1)$-*форма. Тогда функция*

$$f(u_1, u_2, \ldots, u_s, w) = \varphi(u_1, u_2, \ldots, u_s, w) \oplus \psi_1(u_2, \ldots, u_s, w) \oplus \psi_2(u_3, \ldots, u_s, w) \oplus \ldots \oplus \psi_{s-1}(u_s, w) \oplus \psi_s(w),$$

степени нелинейности $r_s + 2$ *имеет структуру вырождения* $(k_1, r_1), \ldots, (k_s, r_s)$.

Разложение, полученное в теореме 4, позволяет дать еще одну интерпретацию пар (k, r), входящих в структуру вырождения булевой функции f. Будем рассматривать все базисы пространства V_n и выписывать многочлены Жегалкина функции f в этих базисах. Через f_r^B обозначим сумму одночленов степени большей r, входящих в многочлен Жегалкина функции f в базисе B, а через $k_r^B(f)$ число существенных переменных булевой функции f_r^B. Из предыдущих построений очевидно, что если пара (k, r) входит в структуру вырождения функции f, то

$$k = \min_B k_r^B(f).$$

Теорема 4 представляет самостоятельный интерес, но ее можно рассматривать и как определенный этап на пути решения проблемы аффинной классификации булевых функций. В последнем случае можно считать, что проблема сведена, в первую очередь, к аффинной классификации невырожденных форм.

Пример. Легко проверить, что для квадратичных форм введенное условие невырожденности совпадает с классическим условием невырожденности. Достаточно заметить, что матрица линейного отображения D в этом случае — это симплектическая матрица квадратичной формы. Поэтому из известной классификации квадратичных форм вытекает, что невырожденные $(n, 2)$-формы существуют только при четных n и с помощью аффинной замены переменных любая невырожденная $(2m, 2)$-форма может быть приведена к виду

$$x_1 y_1 \oplus x_2 y_2 \oplus \ldots \oplus x_m y_m.$$

Список литературы

1. *Страдзинь И. Э.* Групповая инвариантность в конечнозначной логике. Докторская диссертация. Рига, 1988.

2. *Логачев О. А., Сальников А. А., Ященко В. В.* // Дискретная математика. 1997. Т.9. № 4. С.3–20.

3. *Ященко В. В.* // Проблемы передачи информации. 1997. Т.33. Вып.1. С.75-86.

4. *Сидельников В. М., Першаков А. С.* // Проблемы передачи информации. 1992. Т.28. Вып.3. С.80–94.

5. *Логачев О. А., Сальников А. А., Ященко В. В.* О RM-эквивалентности булевых функций. Конференция «Дискретная математика и ее приложения». 1998, Московский государственный университет им.М.В.Ломоносова.

6. *Черемушкин А. С.* Кубические формы от восьми переменных. «Проблемы теоретической кибернетики», XII Международная конференция, Нижний Новгород, 17–22 мая 1999 г.