RM-эквивалентность и гладкость булевых функций

Мотивацией для вводимых ниже понятий являются задачи из теории кодов Рида-Маллера и теории булевых функций, в которых возникают смежные классы по коду Рида-Маллера фиксированного порядка.

Будем говорить, что две булевых функции RM_r-эквивалентны, если они могут быть получены друг из друга с помощью аффинных замен переменных и прибавления функций степени нелинейности не выше r. Классы RM_r-эквивалентности будем называть RM_r-классами. Ясно, что каждый RM_r-класс состоит из нескольких аффинных классов или из нескольких смежных классов по коду RM_r. Параметры булевых функций постоянные на RM_r-классах, будем называть RM_r-инвариантами.

В другой терминологии, мы будем изучать булевы функции с точностью до действия группы G_r, порожденной группой аффинных замен переменных и группой сдвигов на элементы RM_r. Дадим формальные определения. Рассмотрим конечный алфавит, состоящий из всех булевых функций от n переменных: $\Omega = \mathcal{F}_n = \{f(x)\}$. В симметрической группе подстановок $\Sigma(\Omega)$ на алфавите Ω определим две подгруппы:

$$Aff = \{f(x) \overset{\alpha_{A,b}}{\longmapsto} f(Ax \oplus b) |\ b \in V_n,\ A \text{ — обратимая матрица } n \times n\}$$

— группа аффинных замен переменных и

$$R_r = \{f(x) \overset{\rho_g}{\longmapsto} f(x) \oplus g(x) |\ \deg g \leq r\}$$

— группа сдвигов на элементы RM_r.

Теорема 1. *Группа G_r, порождаемая объединением подгрупп Aff и R_r: $G_r = \langle Aff \bigcup R_r \rangle$ является их полупрямым произведением:*

$$G_r = Aff \bowtie R_r.$$

Доказательство. Для доказательства теоремы достаточно проверить следующие три условия:

1) любой элемент группы G_r может быть представлен в виде произведения элемента группы Aff и элемента группы R_r: $G_r = Aff \cdot R_r$;

2) группа R_r является нормальным делителем в группе G_r: $R_r \lhd G_r$;

3) группы Aff и R_r пересекаются только по единице: $Aff \bigcap R_r = \{\mathbf{e}\}$.

Первые два свойства следуют из следующей цепочки равенств, выполненой для любой булевой функции f:

$$f^{\rho_g\alpha_{A,b}}(x) = (f(x) \oplus g(x))^{\alpha_{A,b}} = f(Ax \oplus b) \oplus g(Ax \oplus b) = f^{\alpha_{A,b}\rho_{g^{\alpha_{A,b}}}}(x),$$

т.е.

$$\rho_g\alpha_{A,b} = \alpha_{A,b}\rho_{g^{\alpha_{A,b}}}.$$

Третье свойство легко доказать от противного. Пусть $\alpha_{A,b} = \rho_g$, т.е. $f(Ax \oplus b) = f(x) + g(x)$. Если $\deg g > 0$, то для функции f с условием $\deg f < \deg g$ получаем противоречивое неравенство $\deg f(Ax \oplus b) < \deg(f(x) \oplus g(x))$. Если же $\deg g = 0$, то противоречие получается с тем, что заведомо существует функция с тривиальной группой инерции в группе сдвигов Σ_n. ■

Следствие 2. *Порядок группы G_r равен произведению порядков групп Aff и R_r: $|G_r| = |Aff| \cdot |R_r|$.*

При изучении смежных классов по RM_r-кодам удобно воспользоваться аппаратом булевых производных. Производной (первой) булевой функции $f(x)$ по направлению $\sigma \in V_n$ будем называть булеву функцию $\frac{df}{d\sigma}(x)$, определённую равенством

$$\frac{df}{d\sigma}(x) = f(x) + f(x + \sigma).$$

При взятии производной число существенных переменных булевой функции и её степень нелинейности уменьшаются по крайней мере на единицу. Степень нелинейности функции f равна k тогда и только тогда, когда степень нелинейности всех её производных не превышает $k-1$ и существует направление, по которому производная имеет степень нелинейности $k-1$.

Естественным обобщением понятия первой производной является производная порядка k по направлению подпространства $L < V_n$ размерности k:

$$D^L f(x) = \sum_{z \in x+L} f(z) = \sum_{y \in L} f(x+y).$$

Число существенных переменных и степень нелинейности функции $D^L f(x)$ меньше соответствующих параметров функции f по крайней мере на k. Для фиксированного k мы имеем $\begin{bmatrix} n \\ k \end{bmatrix}_2$ производных порядка k для данной функции f, где $\begin{bmatrix} n \\ k \end{bmatrix}_2$ — коэффициент Гаусса, равный числу подпространств размерности k из пространства V_n. Если каким-нибудь образом перенумеровать все $\begin{bmatrix} n \\ k \end{bmatrix}_2$ подпространств, то мы получим вектор длины $\begin{bmatrix} n \\ k \end{bmatrix}_2$, состоящий из булевых функций $D^L f(x)$.

Лемма 3. *Вектор из булевых производных порядка k однозначно задаёт смежный класс по коду RM_{k-1}.*

Доказательство. Предположим, что

$$D^L f(x) \equiv D^L \varphi(x), \quad \forall L < V_n,\ \dim L = k.$$

Поэтому

$$D^L(f + \varphi) \equiv 0, \quad \forall L < V_n,\ \dim L = k,$$

а это, очевидно возможно тогда и только тогда, когда $\deg(f+\varphi) \le k-1$. Последнее равенство как раз и означает, что функции f и φ лежат в одном смежном классе по коду RM_{k-1}.■

Естественно назвать максимальными производные порядка $\deg f$. Все максимальные производные — это нули или единицы, причём этот вектор длины $\begin{bmatrix} n \\ \deg f \end{bmatrix}_2$ из нулей и единиц однозначно задаёт смежный класс по коду $\mathrm{RM}_{\deg f-1}$.

Обратимся теперь ко второму составляющему понятия RM_r-эквивалентности — аффинным заменам переменных.

Лемма 4. *Пусть две булевых функции лежат в одном аффинном классе. Тогда их векторы из производных порядка k (k — любое) отличаются перестановкой координат и некоторой (одной) аффинной заменой переменных у всех производных.*

Доказательство. Пусть функции f и φ лежат в одном аффинном классе, т.е. для некоторой невырожденной матрицы A и вектора $b \in V_n$ выполнено тождество

$$\varphi(x) = f(Ax+b), \quad \forall x \in V_n.$$

Тогда по определению производной порядка k по направлению подпространства L имеем

$$D^L\varphi(x) = \sum_{y\in L}\varphi(x+y) = \sum_{y\in L} f\left((Ax+b)+Ay\right) =$$

$$== \sum_{z\in A^{-1}L} f\left((Ax+b)+z\right) = \left(D^{A^{-1}L}f\right)(Ax+b).\blacksquare$$

Предположим, что нам известны аффинные классы (все или некоторые). Если $\mathcal{A}$ — аффинный класс, то через $N_f(k,\mathcal{A})$ обозначим число производных порядка k у функции f, которые принадлежат данному аффинному классу $\mathcal{A}$. Очевидно, что для любой функции f выполнено

$$\sum_i N_f(k,\mathcal{A}_i) = \begin{bmatrix} n \\ k \end{bmatrix}_2,$$

где суммирование проводится по всем аффинным классам. Используя Лемму 3 и Лемму 4 легко получить следующее полезное утверждение.

Теорема 5. *Числа $N_f(k,\mathcal{A})$ для любого k и любого аффинного класса $\mathcal{A}$ являются RM_{k-1} -инвариантами.*

Важным частным случаем Теоремы 5 является $k = \deg f$. Обозначим через $\mathcal{A}_1$ аффинный класс, состоящий из одной функции, тождественно равной 1. Тогда $N_f(\deg f, \mathcal{A}_1)$ — это число единиц в векторе из максимальных производных функции f.

Для максимальных производных можно получить простое аналитическое выражение. Введём следующие обозначения. Пусть $f(x)$ — однородная форма степени r, заданная многочленом Жегалкина

$$f(x) = \sum_{\substack{\omega\in V_n \\ |\omega|=r}} c_\omega^f x^\omega.$$

Здесь суммирование ведётся по всем $\binom{n}{r}$ векторам веса r, а $x^\omega = x_{i_1} \cdot \ldots \cdot x_{i_r}$, если $i_1, \ldots, i_r$ — номера всех единиц в векторе ω. Пусть $L < V_n$ — подпространство размерности r, $I_L(x)$ — его характеристическая функция

$$I_L(x) = \begin{cases} 1, & \text{если} \quad x \in L \\ 0, & \text{если} \quad x \notin L. \end{cases}$$

Как известно, степень нелинейности $I_L(x)$ равна $n - r$. Выпишем в форме многочлена Жегалкина старшие члены функции $I_L(x)$, т.е. положим

$$I_L(x) = \sum_{\substack{\alpha \in V_n \\ |\alpha| = n-r}} c_\alpha^L x^\alpha + I'_L(x), \quad \deg I'_L(x) \le n - r.$$

Для коэффициентов c_α^L несложно получить точное аналитическое выражение. Как известно пространство L задаётся однородной системой из $n - r$ линейных уравнений: $H_L x^\downarrow = \mathbf{0}^\downarrow$, или

$$\begin{cases} h_1^1 x_1 \oplus h_1^2 x_2 \oplus \cdots \oplus h_1^n x_n = 0 \\ \cdots \\ h_{n-r}^1 x_1 \oplus h_{n-r}^2 x_2 \oplus \cdots \oplus h_{n-r}^n x_n = 0, \end{cases}$$

где

$$H = \begin{Vmatrix} h_1^1 & h_1^2 & \ldots & h_1^n \\ h_2^1 & h_2^2 & \ldots & h_2^n \\ \vdots & \vdots & \ldots & \vdots \\ h_{n-r}^1 & h_{n-r}^2 & \cdots & h_{n-r}^n \end{Vmatrix}$$

— $(n-r) \times n$-матрица над $\mathbf{GF}(2)$, строки которой линейно-независимы. Используя символ скалярного произведения, систему уравнений можно переписать в виде:

$$\begin{cases} \langle \overrightarrow{h}_1, \overrightarrow{x} \rangle = 0 \\ \cdots \\ \langle \overrightarrow{h}_{n-r}, \overrightarrow{x} \rangle = 0, \end{cases}$$

Тогда характеристическая функция $I_L(\overrightarrow{x})$ может быть записана в виде:

$$I_L(\overrightarrow{x}) = \left(\langle \overrightarrow{h}_1, \overrightarrow{x} \rangle \oplus 1 \right) \left(\langle \overrightarrow{h}_2, \overrightarrow{x} \rangle \oplus 1 \right) \cdot \ldots \cdot \left(\langle \overrightarrow{h}_{n-k}, \overrightarrow{x} \rangle \oplus 1 \right).$$

Отсюда очевидно, что для того, чтобы вычислить коэффициент c_α^L необходимо в матрице H выделить квадратную $(n - r) \times (n - r)$ подматрицу H_α (фактически из матрицы H необходимо взять те столбцы номера, которых совпадают с номерами координат вектора α равных единице) и подсчитать сумму всевозможных произведений её неколлинеарных элементов (напомним, что элементы $h_{j_1}^{i_1}$ и $h_{j_2}^{i_2}$ матрицы H называются неколлинеарными, если $i_1 \ne i_2$ и $j_1 \ne j_2$), т.е. вычислить перманент матрицы: $\operatorname{per} H_\alpha$. Учитывая, что в случае поля из двух элементов $\mathbf{GF}(2)$ понятия перманента и определителя совпадают, окончательно имеем:

$$c_\alpha^L = \det H_\alpha.$$

В этих обозначениях из определения $D^L f$ путём простых преобразований получаем следующее утверждение.

Лемма 6. *Для любой однородной формы f степени r и любого подпространства L размерности r выполнено равенство*

$$D^L f(x) = \sum_{\substack{\omega \in V_n \\ |\omega|=r}} c^f_\omega c^L_{\overline{\omega}}.$$

Все $\begin{bmatrix} n \\ r \end{bmatrix}_2$ подпространств размерности r разбиваются на $2^{\binom{n}{r}}$ классов в зависимости от вектора коэффициентов c^L_α, $\forall \alpha \in L$, $|\alpha| = r$. В соответствии с Леммой 3, если два подпространства попадают в один класс, определяемый вектором a_α, то эти подпространства задают одно и то же значение производной для всех функций

$$D^L f(x) = D^{L'} f(x) = \sum_{\substack{\omega \in V_n \\ |\omega|=r}} c^f_\omega a_{\overline{\omega}} = \left(a, c^f\right).$$

Через P_a, $a \in V_{\binom{n}{r}}$ обозначим число подпространств размерности r, у которых вектор коэффициентов a^L_α совпадает с данным вектором a. RM_{r-1}-инвариант $N_f(\deg f, \mathcal{A})$ выражается через числа P_a следующим образом

$$N_f(\deg f, \mathcal{A}) = \sum_{\substack{a \in V_{\binom{n}{r}} \\ (a, c^f)=1}} P_a.$$